2. *Котельников Г.П.* Повышенная гравитационная нагрузка в системе реабилитационных мероприятий у травматолого-ортопедических больных // VI съезд травматологов-ортопедов России: Тезисы докладов. Н. Новгород, 1997. С. 820.

3. *Котовская А.Р., Шипов А.А., Виль-Вильямс И.Ф.* Медико-биологические аспекты проблем создания искусственной силы тяжести. М.: Слово, 1996. 203 с.

4. *Акулов В.А.* Теоретико-множественный анализ сценариев управления перспективными центрифугами космического назначения. Тр. научно-практической конф. «Инновации в условиях развития информационно-коммуникационных технологий». Инфо 2007. Сочи. 1–10 октября 2007. С. 63–68.

5. *Акулов В.А.* Мехатронные системы генерации искусственной силы тяжести наземного и космического применения / под ред. Г.П. Аншакова. М.: Машиностроение, 2011. 161 с.

6. *Акулов В.А.* Анализ и синтез систем медицинского назначения с управляемой искусственной силой тяжести: дисс. … докт. наук. Самара, 2013. 252 с.

Information – measuring system for gravitational therapy

***Maria Vladimirovna Beloglazova**, four-year student, Samara State Aerospace University (national research university)*

***Vladislav Alekseevich Akulov**, professor, dr.sci.tech., Samara State Technical University,*

The article describes research results of latent mechanism of human blood circulation in artificial and natural gravity conditions. It gives a detailed analysis of development of informational and analytical system consisting of model of the form «human-centrifuge» and remotely controlled measurement system. For the first time in CIS it was modeled the gravity of Mars and the Moon with evaluation of human conditions in low gravity.

Keywords: Medical centrifuge, gravitational therapy, measuring system, radiocontrol, ankle-brachial index.

УДК 004.056.5:002

ПРОЦЕДУРА ПРИМЕНЕНИЯ МЕТОДОЛОГИИ АНАЛИЗА РИСКОВ OCTAVE В СООТВЕТСТВИИ СО СТАНДАРТАМИ СЕРИИ ИСО/МЭК 27000-27005

***Елена Константиновна Баранова**, доцент кафедры информационной безопасности,*
НИУ ВШЭ,
E-mail: ekbaranova@hse.ru,
http://www.hse.ru,
***Александр Степанович Забродоцкий**,*
E-mail: azabro@yandex.ru

Рассматривается процедура анализа рисков информационной безопасности на основе методологии OCTAVE и требования международных стандартов серии ИСО/МЭК 27000-27005, предъявляемые к процессу оценки рисков, а также вопросы соответствия предложенной процедуры требованиям вышеуказанных стандартов.

Ключевые слова: информационная безопасность, менеджмент информационной безопасности, анализ риска, оценка риска, методология OCTAVE.

Анализу информационных рисков в нашей стране традиционно не уделяли должного внимания до принятия Доктрины информационной безопасности в 2000 г., однако, в последние годы эта тема активно изучается и внедряется в практику специалистами в области информационной безопасности (ИБ). При этом особое внимание уделяется

практическому применению существующих методологий анализа рисков и их совершенствованию.


Е.К. Баранова

Также в последние годы ведется работа по разработке и внедрению в систему ИБ организаций международных стандартов серии 27000, определяющих требования к системе менеджмента информационной безопасности (СМИБ).

Большой популярностью в последнее время пользуется методология анализа рисков информационной безопасности OCTAVE, разработанная институтом Software Engineering Institute (SEI) при университете Карнеги Меллона (Carnegie Mellon University).


А.С. Забродоцкий

Метод OCTAVE – это метод оперативной оценки критических угроз, активов и уязвимостей. Методика предполагает создание группы анализа рисков ИБ. Группа анализа включает сотрудников бизнес-подразделений, эксплуатирующих систему, и сотрудников информационного отдела.

При этом данная методика не лишена некоторых недостатков. Так методология не предусматривает интеграции анализа риска в СМИБ организации, имеются проблемы с организацией мониторинга рисков и проведением повторных оценок рисков, не предполагает механизмов управления остаточными рисками, не позволяет исключить риски.

Для анализа рисков в методике OCTAVE предлагается подход из восьми шагов, объединенных в четыре фазы (рисунок 1).

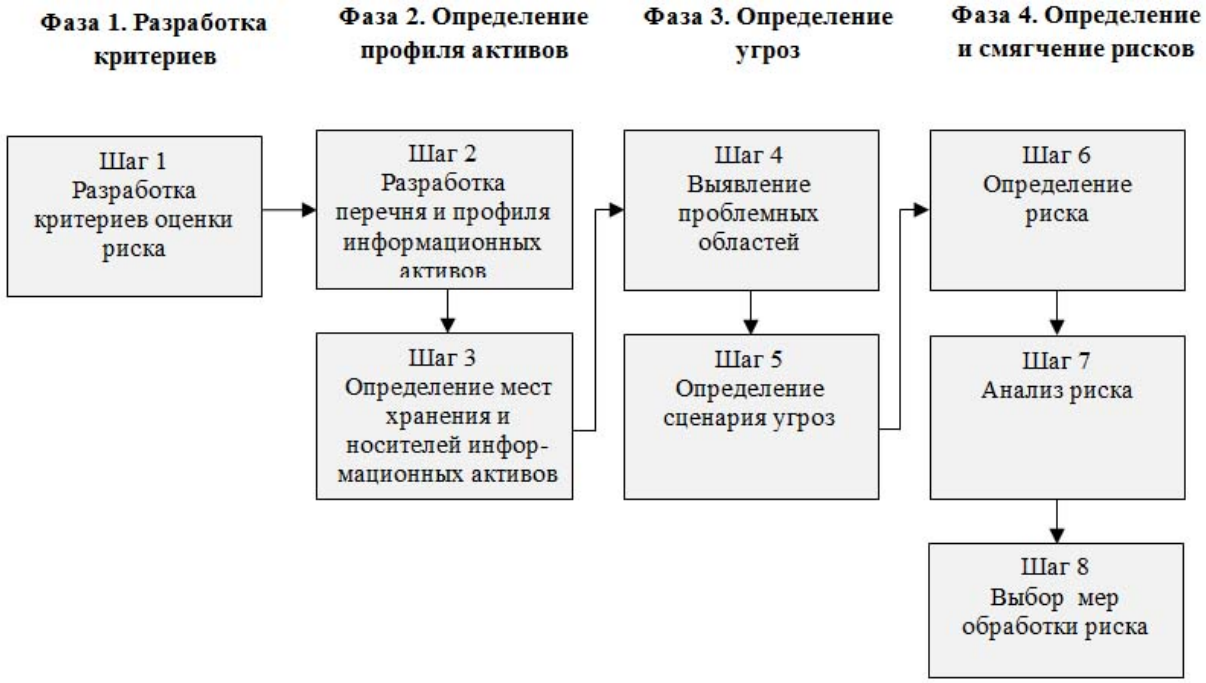

Рисунок 1 – Этапы анализа рисков по методике OCTAVE

Рабочие листы и опросные анкеты, применяемые в процессе анализа рисков, содержатся в англоязычном описании методики «Introducing OCTAVE Allegro: Improving the Information Risk Assessment Process», представленном на сайте www.cert.org.

Рассмотрим общий алгоритм действий группы анализа рисков, основанный на методике OCTAVE, а также рекомендации по внедрению в СМИБ организации оценки рисков на постоянной основе и мониторингу рисков ИБ.

На шаге 1 необходимо определить критерии оценки рисков ИБ, то есть совокупность качественных показателей, которая позволит установить значения оценки риска и последствия реализации риска. Без введения таких критериев невозможно оценить зависимость организации от тех или иных рисков.

В качестве таких критериев могут быть использованы требования безопасности, применяемые на предприятии, уровень инвестиций и затрат на ИБ, стратегическая ценность и критичность затронутых информационных активов и т.п. На первом шаге необходимо установить те воздействия на ИБ, которые наиболее приоритетны и критичны для организации (например, утечка конфиденциальной информации, подрыв авторитета на рынке, дискредитация репутации среди партнеров и клиентов, здоровье и физическая безопасность сотрудников). Критерии оценки рисков должны отражать осознание информационных рисков, существующих в сфере деятельности организации. Критерии устанавливают диапазон последствий реализации риска: низкие, средние и высокие.

Шаг 2 начинается с составления перечня информационных активов и определения их профиля. Профиль – это информация, описывающая актив его уникальными особенностями, качествами, характеристиками, стоимостью. Профилирование позволяет четко определить «границы» актива и требования безопасности к нему. Профиль создается для каждого актива и описывается на отдельном листе. Профиль актива представляет собой входные данные для следующих шагов и основой для выявления угроз и рисков.

Далее выполняется шаг 3. Информационные активы могут храниться не только в самой организации, но и вне ее пределов. Например, организация может допускать к обслуживанию своей инфраструктуры другие организации-поставщики услуг. Если такой поставщик услуг не выполняет требования безопасности активов, к обслуживанию которых он допущен, то это само по себе несет риск. Риск может содержаться в самом факте хранения, передачи или обработке актива в постороннем месте. Это нарушает защиту информационного актива. Еще большую угрозу несет привлечение таким поставщиком услуг субподрядчиков, о которых владелец актива может и не знать.

Таким образом, для получения адекватного профиля актива важно определить все места хранения, передачи и обработки актива – контейнеры, а также находится ли он в зоне прямого управления организацией.

На шаге 3 группа анализа составляет карту актива, где указываются все места его хранения, передачи и обработки, которые могут стать точками уязвимости или, наоборот, точками, которые можно полностью контролировать, гарантируя защищенность актива.

Местом хранения актива может являться техническое средство, программное обеспечение, бумажный носитель или сотрудник организации. Причем, люди здесь особенно важны, так как при получении защищаемой информации они становятся «контейнерами» актива. Такие риски необходимо своевременно выявлять.

На шаге 4 выявляются проблемные области в ИБ организации. Целью шага 4 является не составление полного перечня всех возможных угроз, а оперативное определение тех угроз, которые сразу очевидны для аналитика.

В шаге 5, на основе выявленных проблемных областей, составляются сценарии угроз, которые визуально эффективно представлять в виде дерева, где, с целью более надежного рассмотрения угроз, каждая ветвь рассматривается для каждого информационного актива. Для облегчения определения сценария угроз по каждой ветви необходимо использовать опросные анкеты. Этот шаг также позволяет учесть вероятности реализации угроз, что помогает на более поздних шагах разработать мероприятия по снижению риска. Как правило, в этом случае используется качественная шкала, и вводятся три уровня вероятности реализации угрозы: высокая, средняя и низкая.

На шаге 6 после определения угроз и выявления последствий их реализации, определяют риски ИБ. Необходимо определить, как именно риск будет воздействовать

на организацию или актив, при этом риск определяется для каждого актива, чтобы оценить его критичность для организации или самого актива. Для каждого риска определяется не менее одного последствия, конкретные примеры приведены в таблице 1.

Таблица 1

Примеры определения риска

Сценарий угроз	Следствие
В результате неверной политики доступа к файлам личную информацию о болезни пациента узнал посторонний сотрудник	Раскрыта врачебная тайна в отношении пациента. На медицинскую организацию наложили крупный штраф
Из компании собирается уволиться сотрудник, разрабатывающий новое ПО. Код новой программы, кроме него, никто не знает	Из-за незавершенного проекта компания понесет крупные убытки.
Злоумышленником была исправлена информация в медицинских документах пациента	Резкое ухудшение здоровья или смерть пациента. Уголовное дело против медицинской организации

На шаге 7 определяется количественная мера ущерба, который будет нанесен организации при реализации угрозы. Это относительная оценка, которая позволяет расставить риски по их приоритету. Например, если для компании наиболее важна ее репутация на рынке, то в первую очередь надо смягчать риски именно этой проблемной области.

На заключительном шаге выбираются меры обработки определенных рисков с учетом их приоритета для организации.

Решение о принятии, уменьшении или отложении риска основывается на ряде факторов, основными из которых являются величина воздействия риска и вероятность его реализации. Если риск может серьезно воздействовать на организацию, но при этом маловероятен, то, возможно, его не нужно смягчать. Решение о том, какие риски смягчать, а какие нет, должны принимать аналитики и/или руководство организации.

Выбор стратегии смягчения риска – сложная задача и ее решение может потребовать взаимодействия с другими специалистами организации. Выбранная стратегия должна гарантировать защиту активов в соответствии с критериями безопасности. Необходимо учитывать затраты на смягчение риска, так как они, как минимум, не должны превышать стоимость актива.

Кроме того, не все риски могут быть устранены полностью. Выбранная стратегия может привести к остаточному риску, который необходимо либо принять, либо смягчить.

Оценку рисков ИБ необходимо проводить на постоянной основе, при этом проводить ее рекомендуется не менее чем раз в год. Это связано с быстрым развитием информационных технологий и, как следствие, с возникновением новых рисков ИБ, возможным устареванием и исключением некоторых ранее принятых рисков или потерей эффективности мер, принятых ранее.

Риски ИБ необходимо регулярно отслеживать, для чего необходимо внедрять систему мониторинга рисков. Для этого, помимо ежегодного повторного анализа рисков, необходимы следующие мероприятия.

1 На постоянной основе проводить с работниками разъяснительную работу по угрозам ИБ, которые могут нести те или иные уязвимости, привлекать их к процессу ежегодной оценки рисков, анализировать информацию, полученную от них.

2 Установить единые правила поведения сотрудников на рабочих местах, требовать их выполнения, прививать работникам культуру ИБ. К данному вопросу следует подойти с особым вниманием, чтобы при внедрении таких правил не нарушить права работников.

3 Сравнивать результаты работы, фигурирующие в отчетах и докладах, с текущим положением дел, а также с информацией, поступающей от других источников, проводить дополнительные поверки в случае несоответствия.

4 Обмениваться информацией с регулирующими государственными органами по вопросам соблюдения законодательства и прочим вопросам, которые отражают функционирование процесса управления рисками.

5 Обмениваться информацией с заказчиками и клиентами по вопросам защиты конфиденциальных данных.

6 К процессу оценки рисков привлекать сотрудников организации.

7 При ежегодном анализе рисков частично менять состав группы анализа из числа работников организации, что позволит взглянуть на риски «свежим взглядом», а также усилит культуру ИБ среди сотрудников.

8 Тщательно документировать каждый процесс анализа рисков.

Предлагаемые меры позволят своевременно реагировать на вновь возникающие угрозы, а также отсеивать из рассмотрения те угрозы, которые по тем или иным причинам потеряли свою актуальность.

Далее рассмотрим на сколько предлагаемая процедура анализа рисков соответствует требованиям линейки международных стандартов ИСО/МЭК серии 27000–27005.

Международные стандарты ИСО/МЭК 27000–27005 в общем представляют собой руководство по менеджменту риска ИБ в организации, устанавливая и поддерживая требования к СМИБ.

Согласно ГОСТ Р ИСО/МЭК 27005-2010 процесс менеджмента ИБ состоит из этапов, показанных на рисунке 2.

Согласно ГОСТ Р ИСО/МЭК 27005-2010 процесс оценки риска состоит из анализа риска, включающего идентификацию риска и установление значения риска, и собственно оценки риска.

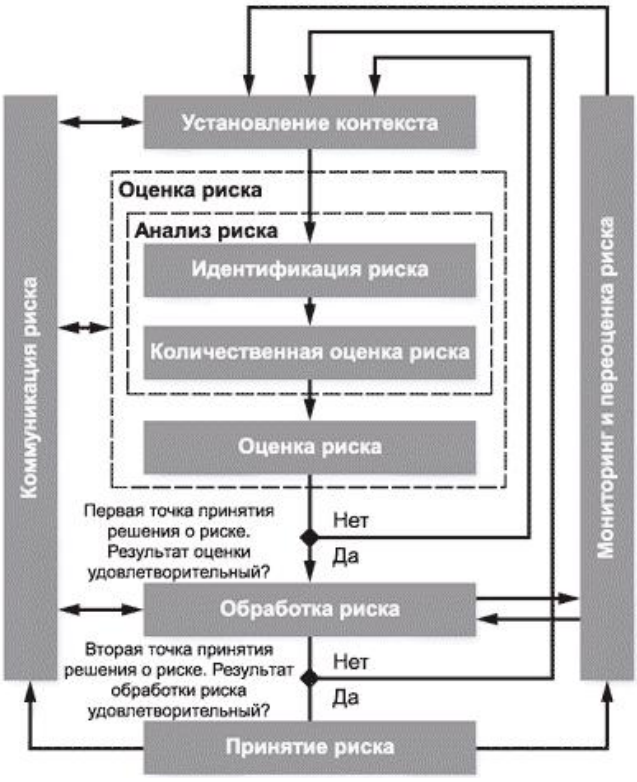

Рисунок 2 – Процесс менеджмента риска информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-2010

Анализ риска включает: идентификацию риска (определение активов, определение угроз, определение существующих мер и средств контроля и управления, выявление уязвимостей, определение последствий) и установление значения риска (оценка последствий, оценка вероятности инцидента, установление значений уровня рисков).

Оценка рисков должна идентифицировать риски, определить количество и приоритеты рисков на основе критериев для принятия риска и целей, значимых для организации.

Следуя рекомендациям ГОСТ Р ИСО/МЭК 27002-2012: оценки рисков следует выполнять периодически, чтобы учитывать изменения в требованиях безопасности и в ситуации, связанной с риском, например, в отношении активов, угроз, уязвимостей, воздействий, оценивания рисков.

Прежде чем рассмотреть обра-

ботку некоего риска, организация должна выбрать критерии определения приемлемости или неприемлемости рисков.

В процессе оценки риска устанавливается ценность информационных активов, выявляются потенциальные угрозы и уязвимости, которые существуют или могут существовать, определяются существующие меры и средства контроля и управления и их воздействие на идентифицированные риски, определяются возможные последствия и, наконец, назначаются приоритеты установленным рискам, а также осуществляется их ранжирование по критериям оценки риска, зафиксированным при установлении контекста.

В результате оценки риска согласно ГОСТ Р ИСО/МЭК 27003-2012 необходимо:

– определить угрозы и их источники;

– определить существующие и планируемые меры и средства контроля и управления;

– определить уязвимости, которые могут в случае угрозы нанести ущерб активам или организации;

– определить последствия потери конфиденциальности, сохранности, доступности, безотказности или нарушения других требований к безопасности для активов;

– оценить влияние на предприятие, которое может возникнуть в результате предполагаемых или фактических инцидентов информационной безопасности;

– оценить вероятность чрезвычайных сценариев;

– оценить уровень риска;

– сравнить уровни риска с критериями оценки и приемлемости рисков.

Применяемая для оценки риска методология должна предусматривать действия, указанные ниже.

1 Определение активов.

2 Определение угроз.

3 Выявление уязвимостей.

4 Определение последствий.

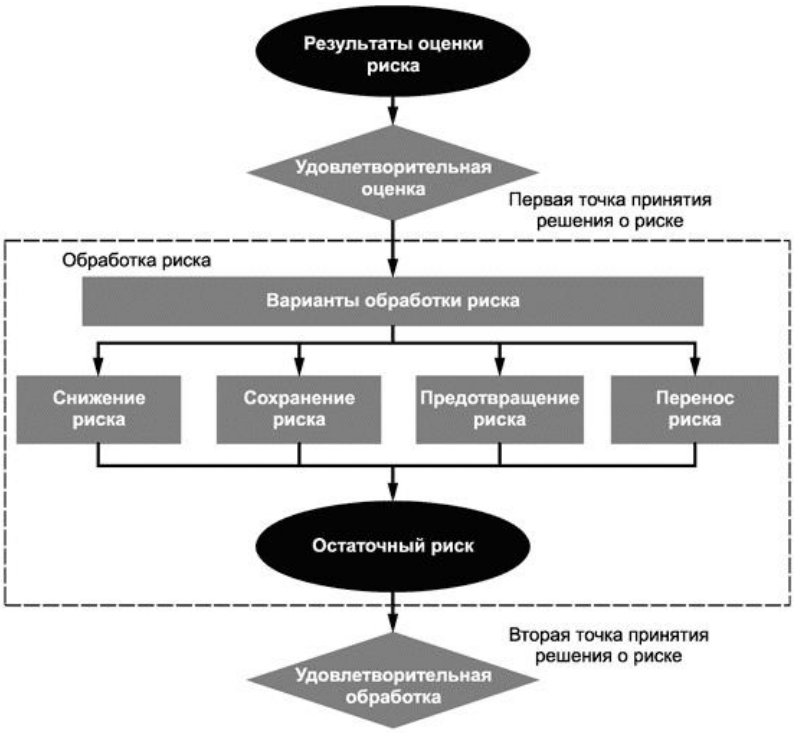

Рисунок 3 − Деятельность по обработке риска в соответствии с ГОСТ Р ИСО/МЭК 27005-2010

5 Оценка вероятности инцидента.

6 Установление значений уровня рисков.

7 Соотнесение рисков с критериями.

8 Определение мер обработки риска.

Схема деятельности по обработке риска показана на рисунке 3.

Помимо указанных действий в организации должен предусматриваться и мониторинг рисков.

Должны подвергаться мониторингу и переоценке риски и их факторы (т.е. ценность активов, влияние, угрозы, уязвимости, вероятность возникновения) с целью определения любых изменений в контексте ор-

ганизации на ранней стадии, и должно поддерживаться общее представление обо всей картине риска. Процесс менеджмента риска ИБ подлежит постоянному мониторингу, анализу и улучшению.

В общем виде соответствие предлагаемой процедуры применения методологии OCTAVE стандартам серии ИСО/МЭК 27000–27005 отображено в таблице 2.

Таблица 2

Соответствие стандартам серии ИСО/МЭК 27000–27005

Требование	**Ссылка на стандарт**		**Соответствие в процедуре**
	стандарт	**пункт**	
Определение критериев приемлемости или неприемлемости рисков	27001	4.2.1	Шаг 1
	27002	4.1	
	27003	8.1	
	27005	7.2	
Определение активов	27001	4.2.1	Шаги 2 и 3
	27005	8.2.1.2	
Определение угроз и их источников	27001	4.2.1	Шаг 4
	27003	8.1	
	27005	8.2.1.3	
Определение уязвимостей	27001	4.2.1	Шаг 5
	27003	8.1	
	27005	8.2.1.5	
Оценка вероятности сценариев	27001	4.2.1	Шаг 5
	27003	8.1	
	27005	8.2.2.3	
Определение последствий	27001	4.2.1	Шаг 5
	27003	8.1	
	27005	8.2.1.6	
Оценка влияния инцидентов ИБ	27001	4.2.1	Шаг 6
	27003	8.1	
Оценка уровня риска	27001	4.2.1	Шаг 7
	27005	8.2.2.5	
Обработка риска	27001	4.2.1	Шаг 8
	27002	4.2	
	27003	8.1	
	27005	8.2.2	
Мониторинг рисков ИБ	27001	4.2.3	Мониторинг
	27005	12	

Стандарты серии ИСО/МЭК 27000-27005 устанавливают четкие требования к оценке рисков как к процессу в целом, так и к его этапам по отдельности. Предложенные процедуры методологии OCTAVE позволяют соблюсти данные требования.

К сожалению, объемы данной публикации не позволяют в полной мере описать алгоритм действия группы анализа рисков, процесс мониторинга рисков и подробно рассмотреть требования стандартов ИСО/МЭК 27000-27005. Однако авторы статьи надеются, что им удалось привлечь интерес читателя к данной теме.

Литература

1. *Баранова Е.К.* Методики анализа и оценки рисков информационной безопасности // Вестник Московского университета им. С.Ю. Витте. Сер. 3: Образовательные ресурсы и технологии. 2015. № 1(9). С. 73–79.

2. *Баранова Е.К., Зубровский Г.Б.* Управление инцидентами информационной безопасности. Проблемы информационной безопасности / Труды I Международной научно-практической конференции «Проблемы информационной безопасности». Гурзуф, Крымский федеральный университет им. В.И. Вернадского, 26–28 февраля 2015 г. С. 27–33.

3. Introducing OCTAVE Allegro: Improving the Information Risk Assessment Process – Software Engineering Institute, 2007. 154 с.

4. Software Engineering Institute Carnegie Mellon University. URL: http://www.cert.org

The procedure of applying the methodology of the OCTAVE risk analysis in accordance with the standards of the series ISO/IEC 27000-27005

Alexander Stepanovich Zabrodotsky

***Elena Konstantinovna Baranova**, Associate professor of the Information Security Department HIGHER SCHOOL OF ECONOMICS NATIONAL RESEARCH UNIVERSITY*

Examines the process of information security risk analysis based on the methodology OCTAVE and the requirements of the international standards of series ISO/IEC 27000-27005 applicable to the risk assessment process, as well as issues of compliance of the proposed procedure to the requirements of the above standards.

***Keywords:** information security, management of information security, risk analysis, risk assessment, methodology OCTAVE.*

УДК 621.3

ИНТЕГРИРОВАННЫЕ МЕТОДЫ ОДНОМЕРНОЙ УПАКОВКИ

***Виктор Михайлович Курейчик**, д-р техн. наук, профессор, зав. кафедрой ДМиМО,*
E-mail: Kur@tgn.sfedu.ru,
***Лилия Владимировна Курейчик**, студентка гр. Ктбо2-7,*
E-mail: Kur@tgn.sfedu.ru,
ИКТиБ Южный федеральный университет,
http:www.sfedu.ru

В настоящее время при решении задач науки и техники важными являются методы искусственного интеллекта, связанные с решением трудных комбинаторно-логических задач упаковки различной размерности. В работе описываются интегрированные методы локального и биоинспирированного поиска решения задач одномерной упаковки большой размерности. Принципиальным отличием работы является то, что предложена новая архитектура обработки информации в виде «матрешки» и модифицированные алгоритмы упаковки на основе «муравьиных», «пчелиных», алгоритмов «полета кукушки» и «поведения волков». Это позволяет создать комбинированные технологии поиска и адаптировать этот процесс к требованиям внешней среды. Проведены экспериментальные исследования. Выполнено сравнение предложенных алгоритмов с современными стандартами, что показало преимущество и эффективность предложенных методов.

Ключевые слова: комбинированный поиск, упаковка, биоинспирированные и эвристические алгоритмы, пчелиные, муравьиные, алгоритмы полета кукушки, «поведение волков».

Работа выполнена при финансовой поддержке гранта РФФИ № 15-07-05523,№ 13-07-12-091 офи_м.

В.М. Курейчик

1. Введение

Главный вызов в науке и технике XXI века – это конвергенция наук и технологий. При этом основная технология сегодня это информационная технология (ИТ) – технология нового междисциплинарного уровня. Как отмечено в [1], она является приоритетной в новом мировом бренде научного развития НБИК (нано-, био-, инфо-, когни-). Особенно важно, что здесь объединяются

Л.В. Курейчик