УДК 377.354; 629.4.047.8 **DOI: 10.14529/iimj170102**

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ СОЗДАНИЯ И ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМ, ОБЕСПЕЧИВАЮЩИХ БЕЗОПАСНОСТЬ КАДРОВ ПРИ РАБОТЕ С НОВЫМИ ИНФОРМАЦИОННЫМИ ТЕХНОЛОГИЯМИ

БОГАТЕНКОВ С.А.
Южно-Уральский государственный университет (НИУ), г. Челябинск

Аннотация. Отсутствие комплексного подхода к учету влияния рисков при создании и оценке эффективности систем, обеспечивающих безопасность кадров при работе с новыми информационными технологиями, приводит к недостаточной эффективности создаваемых систем. В статье на основе учета влияния экономических, информационных, дидактических, психологических и социальных рисков предлагается модель создания и оценки эффективности систем, обеспечивающих безопасность кадров при работе с новыми информационными технологиями. Применение модели показано для дистанционных образовательных технологий, информационно-измерительных систем и систем автоматизированного проектирования.

Ключевые слова: подготовка кадров, безопасность, дистанционные образовательные технологии, информационно-измерительные системы, системы автоматизированного проектирования.

Введение

В современном информационном обществе обостряется проблема, связанная с усилением традиционных и возникновением новых рисков для безопасности профессиональной деятельности. К ним относятся риски экономического, информационного, психологического, социального и дидактического характера [1].

Во-первых, увеличение ущерба от крупномасштабных аварий в крупных энергосистемах мира свидетельствует об обострении проблемы *экономической* безопасности. Например, 14 августа 2003 г. в США произошла авария с каскадным развитием, когда выход одного элемента энергосистемы привел к прекращению ее работы из-за перегрузок и повреждения других ее элементов. В итоге массовыми отключениями электроэнергии были охвачены крупнейшие города в северо-восточной части США и Канады. Общая потеря нагрузки составила 61800 Мвт. В результате этой аварии 50 млн. потребителей не получали электроэнергию в среднем около 4 суток. Ущерб только в США составил около 10 млрд. дол., а в Канаде – более 2 млрд. канадских дол.[2].

В России ущерб от техногенных катастроф, аварий соизмерим с ежегодным ростом ВВП. Проблема обеспечения техногенной энергобезопасности на 70 % связана с человеческим фактором [3].

Во-вторых, появился класс новых *информационных* рисков, связанных с кибертерроризмом. Ущерб от киберпреступности за 2012 год оценивается в $2 миллиарда в России и $110 миллиардов во всем мире [4].

В-третьих, уровень развития информационных технологий стер границы между государствами в информационном пространстве и создал беспрецедентные возможности для подавления противника без использования традиционных средств поражения. Появился класс новых *психологических* рисков, связанных с информационно-сетевой войной. Основой ее является массированное воздействие на морально-психологическое состояние руководства и население страны-противника [5].

Усиление рисков и тесная взаимосвязь проблемы обеспечения безопасности с человеческим фактором актуализируют целесообразность качественной подготовки

кадров к работе с новыми информационными технологиями (ИТ). При этом необходимо дополнительно учитывать угрозы, возникающие в процессе проектирования такой подготовки в условиях электронного практико-ориентированного образования. С одной стороны, возрастает угроза *дидактической* безопасности, связанная с необходимостью планирования эффективных образовательных траекторий для подготовки персонала с различным уровнем компетенций под конкретные требования работодателей. С другой стороны, возрастает угроза *социальной* безопасности, обусловленная недостаточной мотивацией персонала для применения ИТ в профессиональной деятельности. Но в целом, очевидна проблема, состоящая в необходимости формирования готовности участников образовательного процесса к использованию ИТ в аспекте безопасности.

С одной стороны, ведутся исследования по профессиональному обучению с помощью ИТ. Например, V. Vexler обозначил технологии построения информационной модели обучения [6].

С другой стороны, имеются результаты в направлении информационной подготовки конкретных специалистов. Например, В.П. Поляковым разработана методология обучения информационной безопасности студентов вузов в условиях развития информатизации общества [7].

Однако проблема, состоящая в необходимости формирования готовности участников образовательного процесса к использованию средств ИТ в аспекте безопасности, в достаточной степени не решена, поскольку специфическими особенностями решения задачи по созданию системы обеспечения безопасности являются:

- неполнота и неопределенность исходной информации о составе ИТ и характерных угрозах;

- многокритериальность задачи, связанная с необходимостью учета большого числа частных показателей (требований) систем обеспечения безопасности;

- наличие как количественных, так и качественных показателей, которые необходимо учитывать при решении задач разработки и внедрения систем обеспечения безопасности;

- невозможность применения классических методов оптимизации.

Подобные проблемы решаются в результате создания информационно-аналитических систем управления проектами в условиях риска и неопределенности с помощью моделей и методов, представляющих собой соответствующую методологию [8]. Похожие проблемы решены в результате моделирования процессов функционирования стейкхолдеров [9] и благодаря разработке методологии стратегического управления развитием корпоративных систем [10]. Известна методология создания систем защиты, обеспечивающих информационную безопасность информационных технологий [11].

Каждый специалист по-своему решает задачу обеспечения безопасности и применяет свои способы и методы для достижения заданных целей. При этом каждый из них в своем конкретном случае находит свои правильные решения. Однако, как показывает практика, совокупность таких правильных решений не дает в сумме положительного результата – система безопасности в общем и целом работает неэффективно [12].

Разговаривая об одних и тех же вещах, специалисты зачастую не понимают друг друга, поскольку у каждого из них свой подход, своя модель представления системы обеспечения безопасности. Такое положение дел обусловлено отсутствием системного подхода, который определил бы взаимные связи (отношения) между существующими понятиями, определениями, принципами, способами и механизмами обеспечения безопасности кадров при работе с новыми ИТ.

В статье на основе учета влияния экономических, информационных, дидактических, психологических и социальных рисков предлагается модель создания и оценки эффективности систем, обеспечивающих безопасность кадров при работе с новыми информационными технологиями.

1.Модель системы, обеспечивающей безопасность кадров при работе с ИТ

Практическая задача обеспечения безопасности состоит в разработке модели системы процессов профессиональной деятельности, которая на основе научно-методического аппарата, позволяла бы решать задачи создания, использования и оценки безопасности для проектируемых и существующих систем.

Такие модели должны удовлетворять ряду требований [12].

Во-первых, модель должна *использоваться* в качестве руководства по созданию системы безопасности; методики формирования показателей и требований к системе; методики оценки системы; модели системы для проведения исследований.

Во-вторых, модель должна *обладать свойствами* универсальности, комплексности, простоты использования, наглядности и практической направленности.

В-третьих, модель должна быть *самообучаемой* и функционировать в условиях *неопределенности* исходной информации.

В-четвертых, модель должна *позволять*: установить взаимосвязь между показателями; задавать различные уровни защиты; получать количественные оценки; контролировать состояние системы; применять различные методики оценок; оперативно реагировать на изменения условий функционирования; объединить усилия различных специалистов единым замыслом.

Основной задачей модели является научное обеспечение процесса создания системы безопасности персонала при работе с новыми ИТ путем оценки безопасности принимаемых решений и выбора рационального варианта реализации системы обеспечения безопасности персонала.

Модель системы обеспечения безопасности персонала при работе с новыми ИТ представляется целесообразным рассматривать в трехмерном измерении: направления, этапы и основы.

Направления формируются исходя из конкретных особенностей профессиональной деятельности при использовании новых ИТ. В общем случае, предлагается их связать с угрозами экономического, информационного, дидактического, психологического и социального характера.

Этапы (последовательность шагов) создания системы необходимо реализовать для каждого направления.

Основами любой сложной системы, в том числе и системы обеспечения безопасности персонала являются: законодательная, нормативно-правовая и научная база; структура и задачи органов и подразделений, обеспечивающих безопасность; организационно-технические и режимные меры и методы; программно-технические способы и средства. Для каждого направления и этапа определяется элемент основы.

Предложенная модель представления системы безопасности в виде трехмерной матрицы (таблица 1) позволяет не только жестко отслеживать взаимные связи между элементами защиты, но может выступать в роли руководства по созданию системы безопасности.

Таблица 1

Модель представления системы безопасности кадров при работе с ИТ

Направление	Этап	Основа
1.Экономическое	1.1.	1.1.X
	1.2.	1.2.Y
	1.3.	1.3.Z
2.Информационное	2.1.	2.1.X
	2.2.	2.2.Y
	2.3.	2.3.Z
3.Дидактическое	3.1.	3.1.X
	3.2.	3.2.Y
	3.3.	3.3.Z
4.Психологическое	4.1.	4.1.X
	4.2.	4.2.Y
	4.3.	4.3.Z
5.Социальное	5.1.	5.1.X
	5.2.	5.2.Y
	5.3.	5.3.Z

2.Создание системы обеспечения безопасности кадров

Применение модели для создания системы безопасности кадров при работе с дистанционными образовательными технологиями (ДОТ), информационно-измерительными системами ИИС и системами автоматизированного проектирования САПР приведено в таблицах 2-4.

Таблица 2

Система обеспечения безопасности кадров при работе с ДОТ

Направление	Этап	Основа
1.Экономическое	1.1.Необоснованный выбор ДОТ	Выбор ДОТ по экономическому критерию
	1.2.Необоснованный выбор образовательных концепций	Выбор образовательных концепций по экономическому критерию
	1.3.Потеря и искажение данных	Организация процедуры восстановления и коррекции данных
2.Информационное	2.1.Субъективные ошибки преподавателей и студентов	Разработка обучающих программ
	2.2.Несанкционированный доступ к ДОТ	Организация санкционированного доступа к ДОТ

Продолжение таблицы 2

3.Дидактическое	3.1.Недостаточный учет взаимосвязей специальностей	Компетентностно ориенированное управление подготовкой кадров
	3.2.Недостаточный учет базового образования студентов	
	3.3.Недостаточная квалификация преподавателей	Повышение квалификации преподавателей
4.Психологическое	4.1.Отсутствие мотивации персонала к применению ДОТ	Разработка системы морального и материального стимулирования
	4.2.Недостаточно эффективная образовательная среда	Разработка эффективной образовательной среды
5.Социальное	5.1.Потеря работы	Повышение квалификации кадров

Таблица 3

Система обеспечения безопасности кадров при работе с ИИС

Направление	Этап	Основа
1.Экономическое	1.1.Необоснованный выбор ИИС	Выбор ИИС по экономическому критерию
	1.2.Отсутствие унификации баз данных различных ИИС	Разработка программы унификации баз данных различных ИИС
	1.3.Потеря и искажение данных	Организация участка дежурных инженеров
2.Информационное	2.1.Субъективные ошибки персонала	Организация противоаварийных тренировок
	2.2.Недостоверные измерительные каналы	Метод поиска недостоверных измерительных каналов
	2.3.Недопустимые потери энергии	Метод поиска недопустимых потерь энергии
3.Дидактическое	3.1.Неэффективная организация процесса подготовки персонала	Организация эффективной подготовки персонала
	3.2.Недостаточный учет требований работодателей	Компетентностно ориенированное управление подготовкой кадров
	3.3.Недостаточная квалификация преподавателей	Повышение квалификации преподавателей
4.Психологическое	4.1.Отсутствие мотивации персонала к применению ИИС	Разработка системы морального и материального стимулирования
	4.2.Отсутствие эффективной образовательной среды	Разработка эффективной образовательной среды
5.Социальное	5.1.Потеря работы	Повышение квалификации кадров

Таблица 4

Система обеспечения безопасности кадров при работе с САПР

Направление	Этап	Основа
1.Экономическое	1.1.Необоснованный выбор САПР	Выбор САПР по экономическому критерию
	1.2.Неэффективные методы проектирования	Применение эффективных методов проектирования
	1.3.Отсутствие унификации баз данных различных САПР и сложность их адаптации	Применение программ унификации баз данных различных САПР и обеспечение возможности адаптации
2.Информационное	2.1.Субъективные ошибки персонала в связи с многообразием и неоднозначностью информации	Использование графических и текстовых подсказок
3.Дидактическое	3.1.Неэффективная организация процесса подготовки персонала	Организация эффективной подготовки персонала
	3.2.Недостаточный учет требований работодателей	Компетентностно-ориенированное управление подготовкой кадров
4.Психологическое	4.1.Отсутствие мотивации персонала к применению ИИС	Разработка системы морального и материального стимулирования
	4.2.Отсутствие эффективной образовательной среды	Разработка эффективной образовательной среды
5.Социальное	5.1.Потеря работы	Повышение квалификации кадров

Процесс создания системы безопасности кадров состоит в последовательном заполнении элементов модели с учетом особенностей конкретного вида ИТ. Информация в таблицах 2-4 по применению ДОТ, ИИС и САПР сформирована на основе результатов исследований, опубликованных в статьях [13-15].

3.Эффективность системы обеспечения безопасности кадров

Оценить эффективность создаваемой или уже функционирующей системы безопасности можно также на основе трехмерной матрицы. Только теперь по показателям (элементам матрицы) надо выставить соответствующие оценки.

Методика оценки безопасности подготовки кадров к работе с ИКТ основана на определении рисков, т.е. степени влияния на безопасность различных компонентов угроз. Сначала формируется перечень возможных этапов, затем на основе мнений независимых экспертов каждому этапу ставится в соответствие значение степени риска по трехбалльной шкале («1» - влияние незначительное, «2» - среднее, «3» - сильное).

Результаты использования методики на примере подготовки кадров к работе с ДОТ, ИИС и САПР приведены в табл.5-7.

Таблица 5

Оценка системы обеспечения безопасности кадров при работе с ДОТ

Направление	Этап	Степень риска
1.Экономическое	1.1.Необоснованный выбор ДОТ	3
	1.2.Необоснованный выбор образовательных концепций	3
	1.3.Потеря и искажение данных	3
2.Информационное	2.1.Субъективные ошибки преподавателей и студентов	3
	2.2.Несанкционированный доступ к ДОТ	3
3.Дидактическое	3.1.Недостаточный учет взаимосвязей специальностей	2
	3.2.Недостаточный учет базового образования студентов	
	3.3.Недостаточная квалификация преподавателей	2
4.Психологическое	4.1.Отсутствие мотивации персонала к применению ДОТ	2
	4.2.Недостаточно эффективная образовательная среда	2
5.Социальное	5.1.Потеря работы	2

Таблица 6

Оценка системы обеспечения безопасности кадров при работе с ИИС

Направление	Этап	Степень риска
1.Экономическое	1.1.Необоснованный выбор ИИС	3
	1.2.Отсутствие унификации баз данных различных ИИС	3
	1.3.Потеря и искажение данных	3
2.Информационное	2.1.Субъективные ошибки персонала	3
	2.2.Недостоверные измерительные каналы	3
	2.3.Недопустимые потери энергии	3
3.Дидактическое	3.1.Неэффективная организация процесса подготовки персонала	2
	3.2.Недостаточный учет требований работодателей	2
	3.3.Недостаточная квалификация преподавателей	2
4.Психологическое	4.1.Отсутствие мотивации персонала к применению ИИС	2
	4.2.Отсутствие эффективной образовательной среды	2
5.Социальное	5.1.Потеря работы	2

Таблица 7

Оценка системы обеспечения безопасности кадров при работе с САПР

Направление	Этап	Степень риска
1.Экономическое	1.1.Необоснованный выбор САПР	3
	1.2.Неэффективные методы проектирования	3
	1.3.Отсутствие унификации баз данных различных САПР и сложность их адаптации	3
2.Информационное	2.1.Субъективные ошибки персонала в связи с многообразием и неоднозначностью информации	3
3.Дидактическое	3.1.Неэффективная организация процесса подготовки персонала	2
	3.2.Недостаточный учет требований работодателей	2
4.Психологическое	4.1.Отсутствие мотивации персонала к применению ИИС	2
	4.2.Отсутствие эффективной образовательной среды	2
5.Социальное	5.1.Потеря работы	2

После определения угроз и их степеней риска разрабатывается перечень мероприятий по минимизации их влияния на безопасность. При этом сначала исследуются угрозы с максимальной степенью влияния, затем – со средней и, наконец, с незначительной.

Заключение

На основе учета влияния экономических, информационных, дидактических, психологических и социальных рисков предложена модель создания и оценки эффективности систем, обеспечивающих безопасность кадров при работе с новыми информационными технологиями.

Применение модели показано для дистанционных образовательных технологий, информационно-измерительных систем и систем автоматизированного проектирования.

Литература:

1. Гнатышина, Е.А. Информационная подготовка педагогов профессионального обучения в аспекте безопасности: монография / Е.А. Гнатышина, С.А. Богатенков, Е.В. Гнатышина, Н.В. Уварина. – Челябинск: Изд-во Челяб. гос. пед. ун-та , 2015. – 415 с.

2. Логинов, Е.Л. Сетевые информационные атаки на системы управления энергетическими объектами критической инфраструктуры / Е.Л. Логинов, А.Н. Райков. – Теплоэнергетика. 2015. №4. С. 3−9.

3. Толмачев, В.Д. О кадровом обеспечении современной энергетики / В.Д. Толмачев. – Энергобезопасность и энергосбережение. 2011. №1.

4. Norton Cybercrime Report (2012, May 9). 2012 Norton Cybercrime Report. Retrieved November 30, 2014, from http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

5. Богатенков, С.А. Управление качеством информационной подготовки кадров по критерию безопасности: монография. – Челябинск: Челябинский филиал Военно-воздушной академии, 2015. – 186 с.

6. Vexler, V. A., Bazhenov, R. I., & Bazhenova, N. G. (2014). Entity-relationship model of adult education in regional extended education system. Asian Social Science, 10(20), 1-14. http://dx.doi.org/10.5539/ass.v10n20p1

7. Поляков, В.П. Методическая система обучения информационной безопасности студентов вузов: дис…д-ра пед.наук. – Н.Новгород: Волжский гос. инж.-пед.ун-т, 2006. – 538 с.

8. Гельруд, Я.Д. Управление проектами: методы, модели, системы: моногр. /Я.Д. Гельруд, О.В. Логиновский; под ред. докт. техн. наук, проф. А.Л. Шестакова – Челябинск: Издательский центр ЮУрГУ, 2015. – 330 с.

9. Логиновский, О.В. Информационно-аналитическая система управления проектами на базе использования комплекса математических моделей функционирования стейкхолдеров / О.В. Логиновский, Я.Д. Гельруд. – Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника, 2015, Т. 15. № 3. С. 133-141.

10. Логиновский, О.В. О методологии стратегического управления развитием корпоративных информационных систем в условиях неопределенности / О.В. Логиновский, Ю.А. Зеленков. – Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника, 2013, Т. 13. № 3. С. 83-91.

11. Домарев, В.В. Безопасность информационных технологий. Методология создания систем защит / В.В. Домарев. – К.: ООО "ТИД "ДС", 2002 – 688 с.

12. Домарев, В.В. Моделирование процессов создания и оценки эффективности систем защиты информации [Электронный ресурс]. – Режим доступа: http://citforum.ru/security/articles/model_proc/ (дата обращения:29.12.2016).

13. Богатенков, С.А. Методология управления подготовкой кадров к работе с системами автоматизированного проектирования технологических процессов по критерию безопасности / С.А. Богатенков, Н.Д. Юсубов – Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника, 2016, Т. 16. № 4. С. 94-102.

14. Гельруд, Я.Д. Управление безопасностью подготовки кадров к работе с информационными и коммуникационными технологиями в информационном обществе / Я.Д. Гельруд, С.А. Богатенков. – Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника, 2016, Т. 16. № 3. С. 40-51.

15. Богатенков, С.А. Методология управления подготовкой кадров к работе с дистанционными образовательными технологиями по критерию безопасности / С.А. Богатенков – Дистанционное и виртуальное обучение, 2016, 12. С. 33-43.

Богатенков Сергей Александрович – канд. тех. наук, доцент кафедры информационных технологий в экономике, Южно-Уральский государственный университет (НИУ), г. Челябинск; e-mail: ser-bogatenkov@yandex.ru.

Дата поступления 13 марта 2017 г.

DOI: 10.14529/iimj170102

MODELING OF PROCESSES OF CREATION AND EVALUATION OF THE EFFECTIVENESS OF SYSTEMS FOR ENSURING SAFETY OF PERSONNEL WHEN WORKING WITH NEW INFORMATION TECHNOLOGIES

BOGATENKOV S.A.
South Ural State University (National Research University), Chelyabinsk

Abstract. The lack of an integrated approach to risk-based influence in the creation and evaluation of the effectiveness of systems to ensure the safety of

personnel working with the new information technologies, leading to inefficiency created systems. On the basis of taking into account the impact of economic, information, didactic, psychological and social risks, a model creation and evaluation systems to ensure the safety of staff working with new information technologies. The use of the model is shown for distance learning technologies, information-measuring systems and computer-aided design.

Keywords: training, security, distance education technologies, information-measuring systems, computer-aided design.

References

1. Gnatyshina, E.A. Information training of teachers of vocational education in aspect of safety: monograph / E.A. Gnatyshina, S.A. Bogatenkov, E.V. Gnatyshina, N.V. Uvarina. – Chelyabinsk: Publishing house of CSPU, 2015. – 415 p.

2. Loginov, E.L. Network information attacks to control systems of power objects of critical infrastructure / E.L. Loginov, A. N. Raykov. – Power system. 2015. No. 4. Pp 3−9.

3. Tolmachev, V.D. About staffing of modern power / E.L Tolmachev. – Energy security and energy saving. 2011. No. 1.

4. Norton Cybercrime Report (2012, May 9). 2012 Norton Cybercrime Report. Retrieved November 30, 2014, from http://now-static.norton.com/now/en/pu/images/ Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

5. Bogatenkov, S.A. Quality management of information training by criterion of safety: monograph. – Chelyabinsk: Chelyabinsk branch of Military and air academy, 2015. – 186 p.

6. Vexler, V. A., Bazhenov, R. I., & Bazhenova, N. G. (2014). Entity-relationship model of adult education in regional extended education system. Asian Social Science, 10(20), 1-14. http://dx.doi.org/10.5539/ass.v10n20p1

7. Polyakov, V.P. Methodical system of training of information security of students of higher education institutions: thesis of Doctor of pedagogical sciences. – N. Novgorod: Volga State Engineering and Pedagogical University, 2006. – 538 p.

8. Gelrud, Ya.D. Project management: methods, models, systems: monograph. / Ya.D. Gelrud, O.V. Loginovskii; edited by Doctor of Engineering, the prof. A.L. Shestakov – Chelyabinsk: Publishing center SUSU, 2015. – 330p.

9. Loginovskii, O. V. An information and analytical control system of projects on the basis of applying a complex of mathematical models of functioning of stakeholders / O.V. Loginovskii, Ya.D. Gelrud. – Bulletin of South Ural State University. Series: Computer technologies, management, radio electronics, 2015, V. 15. No. 3. Pp. 133-141.

10. Loginovskii, O.V. About the methodology of strategic management of development of corporate information systems in the conditions of uncertainty / O.V. Loginovskii, Yu.A. Zelenkov. – Bulletin of South Ural State University. Series: Computer technologies, management, radio electronics, 2013, V. 13. No. 3. Pp 83-91.

11. Domarev, V.V. Information safety of technologies. Methodology of creating protection systems / V.V. Domarev. – K.: LLC “TID “DS””, 2002 – 688 p.

12. Domarev, V.V. Modeling of processes of creation and assessment of efficiency of systems of information security [An electronic resource]. – Access mode: http://citforum.ru/security/articles/model_proc/ (access date:29.12.2016).

13. Bogatenkov, S.A. Methodology of management of training staff to work with computer-aided engineering systems of technological processes on criterion of safety / S. A. Bogatenkov, N.D. Yusubov the Bulletin of South Ural State University. Series: Computer technologies, management, radio electronics, 2016, V. 16. No. 4. Pp. 94-102.

14. Gelrud, Ya.D. Management of safety of training staff to work with information and communication technologies in information society / Ya.D. Gelrud, S.A. Bogatenkov. – Bulletin of South

Ural State University. Series: Computer technologies, management, radio electronics, 2016, V. 16. No. 3. Pp. 40-51.

15. Bogatenkov, S.A. Methodology of management of training staff to work with remote educational technologies for criterion of safety / S.A. Bogatenkov – Distance and virtual learning, 2016, 12. Pp. 33-43.

Bogatenkov Sergey – Ph.D., assistant professor of information technology in the economy, South Ural State University (National Research University), Chelyabinsk, e-mail: ser-bogatenkov@yandex.ru.

Received 13 March 2017

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Богатенков,С.А. Моделирование процессов создания и оценки эффективности систем, обеспечивающих безопасность кадров при работе с новыми информационными технологиями / С.А. Богатенков // *Журнал управление инвестициями и инновациями.* – 2017. – №1. Стр. 13 – 23. DOI: 10.14529/iimj170102

FOR CITATION

Bogatenkov S.A. Modeling of processes of creation and evaluation of the effectiveness of systems for ensuring safety of personnel when working with new information technologies. *Investment and innovation management journal*. – 2017. – No. 1. Pp. 13 – 23. DOI: 10.14529/iimj170102