Инфокоммуникационные технологии и системы

УДК 65.01 **DOI: 10.14529/ctcr160305**

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ПОДГОТОВКИ КАДРОВ К РАБОТЕ С ИНФОРМАЦИОННЫМИ И КОММУНИКАЦИОННЫМИ ТЕХНОЛОГИЯМИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Я.Д. Гельруд, С.А. Богатенков

Южно-Уральский государственный университет, г. Челябинск

В современном информационном обществе обостряется проблема, связанная с усилением традиционных и возникновением новых угроз безопасности при работе с информационными и коммуникационными технологиями. К ним относятся угрозы экономического, информационного, психологического, социального и дидактического характера. Перспективным направлением для решения проблемы является электронное обучение, сводящее к минимуму перечисленные угрозы.

В статье рассматривается методология управления безопасностью подготовки кадров к работе с информационными и коммуникационными технологиями в условиях усиления угроз. Предлагаемая методология опирается на принципы безопасности, классификацию ИКТ-компетенций, модель условий и факторов управления, шаблоны поведения (паттерны). Среди паттернов выделены методы принятия решений и методика оценки безопасности подготовки кадров на основе анализа опыта работы и применения математических моделей.

Методология управления безопасностью подготовки кадров к работе с информационными и коммуникационными технологиями обеспечивает минимизацию угроз экономического, информационного, психологического, социального и дидактического характера. Результаты использования методологии продемонстрированы на примере подготовки кадров к работе с информационно-измерительными системами на Челябинской ТЭЦ-2.

Ключевые слова: безопасность, информационные и коммуникационные технологии, подготовка кадров, электронное обучение.

Введение

Подготовка кадров к работе с информационными и коммуникационными технологиями (ИКТ) становится предметом изучения специалистов различных областей профессиональной деятельности. Это связано с проникновением и возрастанием деструктивного влияния ИКТ на все сферы жизнедеятельности.

Например, в последние годы в крупных энергосистемах мира участились случаи крупномасштабных аварий. 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 61 800 МВт. В результате этой аварии 50 млн потребителей не получали электроэнергию в среднем около 4 суток. Ущерб только в США составил около 10 млрд долл., а в Канаде – более 2 млрд канадских долл. [1].

Развитие практико-ориентированного подхода в образовании, целесообразность совмещения процессов профессиональной и образовательной деятельности требует применения эффективных способов процессов генерации и передачи знаний. Одним из возможных инструментов, позволяющих решать эту острую проблему современности, является электронное обучение. Оно воз-

никло благодаря развитию Интернета и мультимедиа, его ключевыми моментами являются консалтинг, контент, технологии, сервисы и поддержка [2]. В настоящее время мировая индустрия электронного обучения стремительно развивается, на начало текущего века она составила $48 млрд [3]. По данным консорциума Sloan на 2011 г. в США в онлайн-обучении в высших учебных заведениях было вовлечено шесть миллионов студентов [4].

В современном информационном обществе обостряется проблема, связанная с усилением традиционных и возникновением новых угроз безопасности при работе с информационными и коммуникационными технологиями. В работах [5, 6] выделены угрозы экономического, информационного, психологического, социального и дидактического характера.

Во-первых, Интернет создаёт фантастические возможности для общения и сбора любой информации с граждан, которая может быть использована для влияния на людей в корыстных целях. То есть создался целый класс новых **информационных** угроз. Кроме того, в связи с развитием электронного обучения увеличивается количество электронных публикаций учебного материала, обладающего различной степенью актуальности, новизны и приоритетности, т. е. усиливается угроза его необоснованного выбора.

Во-вторых, появился класс новых **экономических** угроз, связанных с кибертерроризмом. Ущерб от киберпреступности за 2012 г. оценивается в $2 млрд в России и $110 млрд во всем мире [7]. Кроме того, в связи с появлением большого количества автоматизированных средств, отличающихся функциональными и стоимостными характеристиками, усиливается угроза их необоснованного выбора.

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** угроз, связанных с информационно-сетевой войной. Основой ее является массированное воздействие на морально-психологическое состояние руководства и население страны-противника. Кроме того, в связи с уменьшением времени общения преподавателя со студентом при электронном обучении возрастает роль формы представления учебной информации, с точки зрения ее восприятия, усвоения и контроля, т. е. усиливается традиционная угроза для психологической безопасности, определяемая формой представления учебной информации.

Перечисленные угрозы актуализируют целесообразность качественной подготовки кадров к работе с ИКТ в аспекте безопасности. 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 ИКТ в профессиональной деятельности. Но в целом, очевидна **проблема**, состоящая в необходимости формирования готовности участников образовательного процесса к использованию ИКТ в аспекте безопасности.

С одной стороны, ведутся исследования по профессиональному обучению с помощью ИКТ. Например, V. Vexler обозначил технологии построения информационной модели обучения [8].

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 [9].

Однако проблема, состоящая в необходимости формирования готовности участников образовательного процесса к использованию средств ИКТ в аспекте безопасности, в достаточной степени не решена, поскольку существующие работы в этом направлении ориентированы на традиционные формы обучения, требующие значительных трудовых и временных затрат. Кроме того, существует определенная зависимость встраиваемых в учебный процесс ИКТ-компетенций и

ИКТ-модулей от федеральных государственных образовательных стандартов (ФГОС), регламентирующих применение конкретных компетенций, отвечающих за подготовку тех или иных специалистов. Все это создает **угрозы безопасности** для *своевременной* подготовки кадров к использованию средств ИКТ.

Отличительной особенностью практико-ориентированных форм взаимодействия от традиционного обучения является ориентация на требования работодателей к готовности кадров использовать средства ИКТ, а не на ФГОС, что позволяет обеспечить своевременность подготовки кадров в результате сокращения ее сроков.

На основании анализа состояния вопроса выявлено **противоречие** между потребностью практической деятельности к готовности кадров для применения средств ИКТ, с одной стороны, и недостаточной разработанностью теоретико-методологических основ для *своевременной* подготовки кадров к такой готовности в условиях развития информационного общества и усиления угроз безопасности, с другой стороны. Проблема исследования заключается в необходимости решения данного противоречия.

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 [10]. Похожие проблемы решены Я.Д. Гельрудом, О.В. Логиновским в результате моделирования процессов функционирования стейкхолдеров и разработки методологии стратегического управления развитием корпоративных систем [10].

В статье рассматривается методология управления безопасностью подготовки кадров к работе с информационными и коммуникационными технологиями в условиях усиления угроз. Предлагаемая методология опирается на принципы безопасности, классификацию ИКТ-компетенций, модель условий и факторов управления и на шаблоны поведения (паттерны). Среди паттернов выделены методы принятия решений и методика оценки безопасности подготовки кадров на основе анализа опыта работы и применения математических моделей.

1. Методика оценки безопасности подготовки кадров

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 угроз безопасности, затем на основе мнений независимых экспертов каждой угрозе ставится в соответствие значение степени риска по трехбалльной шкале («1» – влияние незначительное, «2» – среднее, «3» – сильное).

Проблемы применения ИИС на энергоемких предприятиях связаны с большим различием их функциональных, технических и стоимостных характеристик. Существуют определенные трудности экономически обоснованного выбора их структуры и состава в связи с увеличением номенклатуры и спектра указанных характеристик. Возникает ряд вопросов. Чем определяется эффективность ИИС? Как учитывать важность измеряемых величин при выборе системы учета? Например, учет расхода коммерческих теплоносителей на Челябинской ТЭЦ-2 выполняется двумя автоматизированными системами, а учет расхода некоммерческих теплоносителей – одной. Правильно ли сделан выбор? В каком направлении и каким образом целесообразно дальше развивать ИИС или следует остановиться на достигнутом? Как рационально использовать оперативный и ремонтный персонал подразделений АСУ и экономически обосновать его численность с учетом текущих и перспективных работ? Где искать резервы для сокращения численности эксплуатационного и управленческого персонала в результате автоматизации вычислительных и информационных работ? В связи с переходом к рыночной экономике эти вопросы стали крайне актуальными, поэтому их решение представляет большой интерес для руководителей предприятий и подразделений [11].

Результаты использования методики на примере подготовки кадров к работе с автоматизированными информационно-измерительными системами (АИИС) на Челябинской ТЭЦ-2 приведены в табл. 1.

Таблица 1

Оценка безопасности подготовки кадров к работе с ИИС на Челябинской ТЭЦ-2

Номер угрозы	Содержание угрозы	Степень риска
Угрозы для экономической безопасности		
1	Необоснованный выбор АИИС	3
2	Отсутствие унификации баз данных различных АИИС	3
3	Потеря и искажение данных	3
Угрозы для информационной безопасности		
4	Субъективные ошибки персонала	3
5	Недостоверные измерительные каналы	3
6	Недопустимые потери энергии	3
Угрозы для дидактической безопасности		
7	Неэффективная организация процесса подготовки персонала	2
8	Недостаточный учет требований работодателей	2
9	Недостаточная квалификация преподавателей	2
Угрозы для социальной и психологической безопасности		
10	Отсутствие мотивации персонала к обучению	2
11	Потеря работы	2

2. Паттерны стратегического поведения

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.

В результате исследования проблемы сформулированы **принципы безопасности** при работе с ИКТ: дидактической, экономической, информационной, психологической, социальной. Приведем их.

Принцип *дидактической* безопасности определяет способ проектирования, основанный на требованиях образовательных стандартов, работодателей и образовательной организации.

Принцип *экономической* безопасности предполагает использовать методы и средства, уменьшающие отношение цены к качеству, в том числе шаблоны рабочих программ, учебно-методических комплексов, пособий, учебников, так как в этом случае уменьшается трудоемкость и, следовательно, цена.

Принцип *информационной* безопасности определяет способ проектирования, обеспечивающий защиту, актуальность информации в результате применения систем реального времени, в том числе интернет-технологий и завершающийся получением авторского свидетельства на соответствие требованиям новизны и приоритетности в результате регистрации электронного ресурса, например, в объединенном фонде электронных ресурсов «Наука и образование».

Принцип *психологической* безопасности предполагает при проектировании использовать мультимедийные технологии, эйдотехнические и мнемонические методы представления учебной информации и контрольно-измерительных материалов. В этом случае возрастает качество усвоения и контроля учебной информации.

Принцип *социальной* безопасности предполагает при проектировании использование технологий формирования мотивации персонала для применения информационно-коммуникационных технологий.

Управление подготовкой кадров, реализующее принципы безопасности, выполняется на основе моделей и методов или с помощью организационно-правовых мероприятий, называются паттернами. Шаблоны поведения, реализующие подготовку кадров, называются паттернами. Паттерны стратегического поведения на примере подготовки кадров к работе с ИИС на Челябинской ТЭЦ-2 приведены в табл. 2.

Таблица 2

Паттерны стратегического поведения при подготовке кадров к работе с ИИС на Челябинской ТЭЦ-2

№ п/п	Содержание угрозы	Содержание паттерна
Управление на основе моделей и методов		
1	Необоснованный выбор АИИС	Выбор АИИС по критерию экономической безопасности
2	Недостоверные измерительные каналы	Поиск недостоверных измерительных каналов
3	Недопустимые потери энергии	Поиск недопустимых потерь энергии
4	Отсутствие унификации баз данных различных АИИС	Унификация баз данных различных АИИС
5	Неэффективная организация процесса подготовки персонала	Проектирование подготовки кадров по критерию дидактической безопасности
Организационно-правовое управление		
6	Потеря и искажение данных	Организация участка дежурных инженеров
7	Субъективные ошибки персонала	Организация противоаварийных тренировок
8	Отсутствие мотивации персонала к обучению	Моральное и материальное стимулирование
9	Недостаточный учет требований работодателей	Внесение изменений в должностные инструкции персонала
10	Недостаточная квалификация преподавателей	Привлечение к обучению специалистов, имеющих большой опыт научной, практической и руководящей работы
11	Потеря работы	Повышение квалификации или перевод на другую работу

3. Выбор АИИС по критерию экономической безопасности

В работах [12−14] рассмотрены примеры выбора автоматизированных средств учета энергоносителей, вибродиагностики оборудования и регистрации аварийных ситуаций на Челябинской ТЭЦ-2.

Аспект экономической безопасности состоит в обоснованном выборе автоматизированного средства. Например, зная стоимость энергоносителя за отчетный период (Z) и относительные погрешности расчета расхода энергоносителя до и после внедрения (Δ_1, Δ_2) автоматизированного рабочего места по учету энергоносителей (АРМ-Э), по формуле (1) можно ориентировочно оценить экономический эффект от внедрения и принять решение о приобретении соответствующего АРМ-Э [16]:

$$E = 0{,}005(\Delta_1 - \Delta_2)Z. \quad (1)$$

На Челябинской ТЭЦ-2 в результате использования ЭВМ и замены планиметра планшетом уменьшилась на 1,5 % погрешность определения суточных расходов природного газа, пара и воды и значительно сократилось время расчета корректированных расходов [12].

4. Поиск недостоверных измерительных каналов и недопустимых потерь энергии

На большинстве энергоемких предприятий России и ближнего зарубежья эксплуатируются коммуникационные и измерительные каналы, имеющие большой срок службы, что приводит к необходимости частой проверки надежности их работы. Кроме того, имеют место случаи несанкционированного подключения к источникам тепловой и электрической энергии.

Приведенные факты свидетельствуют об актуальности задачи обеспечения безопасной работы распределенных систем, в которых отношения местоположений элементов (или групп элементов) играют существенную роль с точки зрения функционирования системы, а, следовательно, и с точки зрения анализа и синтеза системы. Для распределённых систем характерно распределение функций, ресурсов между множеством элементов (узлов) и отсутствие единого управ-

ляющего центра, поэтому выход из строя одного из узлов не приводит к полной остановке всей системы.

Техническая диагностика распределенных систем транспортировки энергоресурсов выполняется в результате анализа величин сетевой инфраструктуры, состоящей из балансов контуров, включающих измерительные каналы источников и потребителей энергоресурсов.

На рис. 1−3 приведены примеры сетевой инфраструктуры транспортировки энергоресурсов Челябинской ТЭЦ-2.

Баланс электроэнергии представляет собой распределенную систему, включающую совокупность взаимосвязанных балансов по секциям 110 кВ, 10 кВ и 6 кВ (рис. 1) [16].

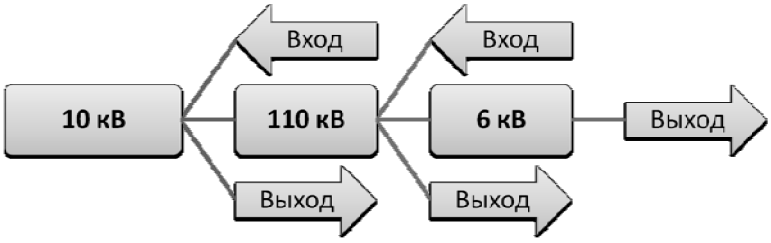

Рис. 1. Баланс электроэнергии

Пароводяной баланс представляет собой распределенную систему, включающую совокупность взаимосвязанных балансов: питательной воды, пара и воды на котлах, свежего пара и пара 13 кгс/см^2 (рис. 2). Баланс потерь пара и воды позволяет анализировать данные потери (рис. 3) [17].

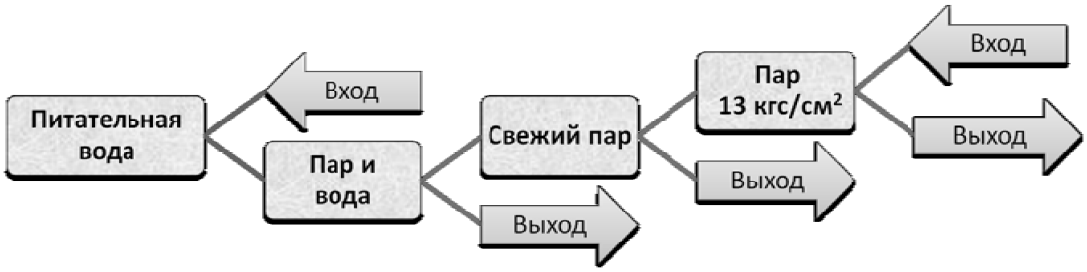

Рис. 2. Пароводяной баланс

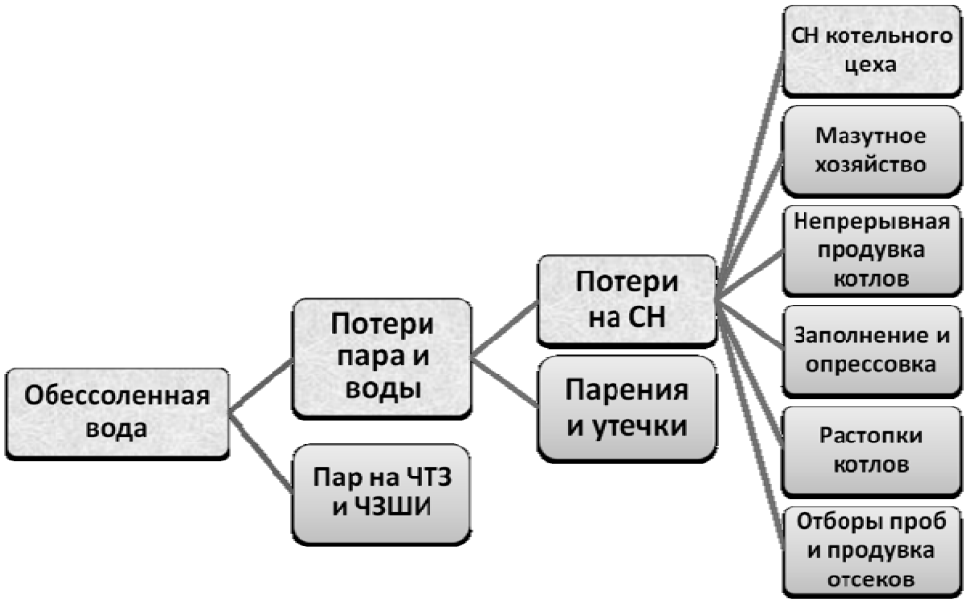

Рис. 3. Баланс потерь пара и воды

Традиционно процессы поиска недопустимых потерь энергии и технической диагностики измерительных каналов выполнятся по утвержденному графику и связаны с длительным пребыванием персонала в зонах возможного поражения от действия электроэнергии или энергоносителей. Поэтому для обеспечения безопасной работы целесообразно минимизировать время нахождения персонала в опасных зонах.

Решение инженерных задач поиска недопустимых потерь энергии и технической диагностики измерительных каналов на современном этапе немыслимо без применения автоматизированных информационно-измерительных систем. Использование методик поиска недопустимых потерь энергии и технической диагностики измерительных каналов с помощью КТС «Энергия» позволяет решать эти задачи, не находясь в опасных зонах [16, 17].

Однако при этом предъявляются повышенные требования к уровню квалификации персонала, так как с одной стороны, он должен знать особенности технологического процесса, с другой стороны, должен быть квалифицированным пользователем КТС «Энергия». Кроме того, процесс решения этих задач отнимает достаточно много времени.

На кафедре «Прикладная математика» Южно-Уральского государственного университета на основе сетевого моделирования созданы алгоритмы и программы, в которых отсутствуют перечисленные недостатки [18, 19].

Методики и программные продукты, реализующие поиск недопустимых потерь энергии и технической диагностики измерительных каналов с помощью АИИС внедрены на Челябинской ТЭЦ-2.

5. Унификация баз данных различных АИИС

Наличие двух информационных систем на ТЭЦ-2 увеличило риск, связанный с необходимостью унификации бизнес-процесса в результате использования различных информационных систем.

Необходимость унификации обусловлена различиями в организации информации:

– по способу кодирования (например, в АРМ используется система кодированных имен AKS, в КТС – нумерация измерительных каналов);

– по структуре файлов данных (в АРМ – формат DBF, в КТС – формат языка Паскаль);

– по временным характеристикам (в АРМ имеется доступ к суточной информации любого месяца года, в КТС – только к информации за последние десять суток).

Из-за этих различий значительно увеличиваются время и трудоемкость эксплуатации программ (например, расчета технико-экономических показателей работы ТЭС), использующих данные обеих систем, что приводит к их недоиспользованию и снижению эффективности. Для получения экономического эффекта в этом направлении необходима комплексная информационно-измерительная система с единой организацией измеряемой информации.

Для совместного использования баз данных АРМ и КТС специалистами отдела АСУ ТЭЦ-2 проведены мероприятия по наладке комплексной информационно-измерительной системы [20].

1. Применение генератора документов КТС позволило преодолеть различия во временных характеристиках измеренных величин. Разработан ежедневный учет электроэнергии. Документы включают показания счетчиков на начало суток, их время работы, выработку или потребление и среднюю мощность активной или реактивной электроэнергии. Суточные выходные документы по учету энергоносителей показывают время работы, расход газа, пара или воды, а также среднесуточные значения давления и температуры. Организован ежедневный вывод документов в текстовые файлы на сетевом диске сервера ЛВС для дальнейшей передачи в общую базу данных.

2. Разработана программа преобразования суточных выходных текстовых документов в соответствующие месячные файлы АРМ формата DBF. Данная программа реализована на основе таблицы соответствий параметров учета КТС кодам системы AKS, используемой в АРМ. Применение программы позволило преодолеть различия в способах кодирования и структурах файлов данных АРМ и КТС.

В результате сгенерирована общая база данных двух систем АРМ и КТС. Это позволило значительно уменьшить объем информации, вводимой с клавиатуры в ряде прикладных программ.

Однако возросший объем базы данных привел к увеличению времени работы программ по следующим причинам:

1. Расчеты по формулам в АРМ проводились перед каждым созданием документа.

2. Работа с нормативно-справочной информацией в АРМ требует знания правил формирования кодов AKS и поэтому очень трудоемка для пользователя.

Для снижения трудоемкости работы выполнены следующие мероприятия:

1. Расчеты по формулам стали выполняться только один раз после ввода исходной информации.

2. Разработана программа автоматизированного синтеза и анализа кодов системы AKS с помощью классификации объектов.

В результате внедрения в производство всех информационных систем специалисты Челябинской ТЭЦ-2 получили возможность анализировать дополнительную информацию. Описанный подход к наладке такой системы, основанный на применении функциональных объектов различных классов, позволяет эффективно использовать прикладное программное обеспечение.

6. Проектирование подготовки кадров по критерию дидактической безопасности

В результате анализа опыта работы в условиях внедрения АИИС на Челябинской ТЭЦ-2 разработана методика проектирования подготовки кадров по критерию безопасности. В основу методики положена классификация ИКТ-компетенций и комплексная модель условий и факторов управления [21−24].

Предлагается следующая уровневая **классификация ИКТ-компетенций**:

1) владение навыками документооборота с помощью АИИС;

2) умение решать задачи профессиональной деятельности с помощью АИИС;

3) умение решать проблемы использования АИИС, связанные с их разработкой, адаптацией, выбором и эксплуатацией.

Основой обеспечения безопасности процесса формирования ИКТ-компетентности является **комплексная модель условий и факторов управления** подготовкой кадров для работы с АИИС (табл. 3). Модель позволяет обоснованно подбирать персонал на соответствующие должности и планировать подготовку кадров для работы с АИИС.

Таблица 3

Комплексная модель условий и факторов управления подготовкой кадров для работы с АИИС

Номер группы	ИКТ-компетентность	Сертификат	Опыт работы в предыдущей группе
1	Владение навыками документооборота с помощью АИИС	Сертификат № 1	Нет
2	Умение решать задачи профессиональной деятельности с помощью АИИС	Сертификат № 2	Да
3	Умение решать проблемы использования АИИС, связанные с их разработкой, адаптацией, выбором и эксплуатацией	Сертификат № 3	Да

Заключение

Предложена методология управления безопасностью подготовки кадров к работе с АИИС, которая обеспечивает минимизацию угроз экономического, информационного, психологического, социального и дидактического характера.

Результаты использования методологии продемонстрированы на примере подготовки кадров к работе с АИИС на Челябинской ТЭЦ-2 и включают следующие паттерны стратегического поведения:

1. Выбор АИИС по критерию экономической безопасности.
2. Поиск недостоверных измерительных каналов.
3. Поиск недопустимых потерь энергии.
4. Унификация баз данных различных АИИС.
5. Проектирование подготовки кадров по критерию дидактической безопасности.

Литература

1. 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.

2. Nagy, A. The impact of e-learning / A. Nagy // E-Content. – 2005. – P. 79–96. – Springer Berlin Heidelberg. – http://dx.doi.org/10.1007/3-540-26387-X_4. DOI: 10.1007/3-540-26387-X_4

3. EC. Communication from the Commission: E-Learning – Designing «Tejas at Niit» tomorrow's education. – Brussels: European Commission, 2000.

4. Allen, E. Going the distance: Online education in the United States / E. Allen, J. Seaman. – Babson Park, MA: Babson Survey Research Group, 2011.

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

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

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

8. Vexler, V.A. Entity-relationship model of adult education in regional extended education system / V.A. Vexler, R.I. Bazhenov, N.G. Bazhenova // Asian Social Science. – 2014. – Vol. 10, no. 20. – P. 1–14. – http://dx.doi.org/10.5539/ass.v10n20p1. DOI: 10.5539/ass.v10n20p1

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

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

11. Богатенков, С.А. Модели, методы и средства информационной поддержки принятия решений в системе информационной подготовки кадров / С.А. Богатенков // Информатизация инженерного образования: материалы Междунар. науч.-метод. конф., Москва, 15–16 апреля 2014 г. // Национ. исследоват. ун-т МЭИ, 2014. – С. 29–35.

12. Богатенков, С.А. Опыт внедрения и эксплуатации автоматизированного рабочего места инженера производственно-технического отдела и комплекса технических средств «Энергия» на ТЭЦ-2 Челябинска / С.А. Богатенков, Э.С. Варыпаев // Промышленная энергетика. – 1996. – № 11. – С. 7−8.

13. Богатенков, С.А. Опыт внедрения и перспективы развития автоматизированной системы вибродиагностики оборудования на Челябинской ТЭЦ-2 / С.А. Богатенков, А.В. Павлов // Электробезопасность. – 1997. – № 1. – С. 50−56.

14. Богатенков, С.А. Опыт внедрения и перспективы развития автоматизированной системы регистрации аварийных событий на Челябинской ТЭЦ-2 / С.А. Богатенков, И.М. Тарасов // Электробезопасность. – 1996. – № 3−4. – С. 53−56.

15. Варыпаев, Э.С. Автоматизированный учет расхода природного газа / Э.С. Варыпаев, С.А. Богатенков, О.В. Байдин // Газовая промышленность. – 1994. – № 3. – С. 32.

16. Богатенков, С.А. Методика технической диагностики измерительных каналов комплекса технических средств «Энергия» / С.А. Богатенков, И.М. Тарасов // Электробезопасность. – 1996. – № 2. – С. 19–22.

17. Богатенков, С.А. Повышение эффективности мероприятий по энергосбережению с помощью автоматизированных средств учета энергии / С.А. Богатенков // Промышленная энергетика. – 1997. – № 12. – С. 2–5.

18. Богатенков, С.А. Автоматизация поиска недопустимых потерь энергии с помощью автоматизированных средств учета энергии / С.А. Богатенков, Е.Н. Трубина, Д.С. Богатенков // Электробезопасность. – 1998. – № 3–4. – С. 39–46.

19. Богатенков, С.А. Автоматизация технической диагностики измерительных каналов с помощью автоматизированных средств учета энергии / С.А. Богатенков, Е.С. Борткевич // Электробезопасность. – 1999. – № 1. – С. 39–44.

20. Богатенков С.А. Опыт наладки комплексной информационно-измерительной системы на ТЭЦ-2 Челябинска / С.А. Богатенков // Промышленная энергетика. – 1997. – № 3. – С. 5−7.

21. Богатенков, С.А. Требования к информационной подготовке кадров в условиях применения информационно-измерительных систем / С.А. Богатенков // Концепт. – 2014. – № 1. – С. 16–20.

22. Богатенков, С.А. Формирование компетентности педагогических кадров для работы с комплексом технических средств «Энергия» в аспекте безопасности / С.А. Богатенков // Мир науки, культуры и образования. – 2014. – № 6. – С. 29–35.

23. Богатенков, С.А. Система формирования информационной и коммуникационной компетентности: учеб. пособие / С.А. Богатенков. – Челябинск: Изд-во Челяб. гос. пед. ун-та, 2014. – 297 с.

24. Богатенков, С.А. Проектирование безопасной информационной подготовки: моногр. / С.А. Богатенков // – Челябинск: Изд-во Челяб. гос. пед. ун-та, 2013. – 276 с.

Гельруд Яков Давидович, д-р техн. наук, профессор кафедры информационно-аналитического обеспечения управления в социальных и экономических системах, Южно-Уральский государственный университет, г. Челябинск; gelrud@mail.ru.

Богатенков Сергей Александрович, канд. техн. наук, доцент кафедры информационных систем, Южно-Уральский государственный университет, г. Челябинск; ser-bogatenkov@yandex.ru.

Поступила в редакцию 25 мая 2016 г.

DOI: 10.14529/ctcr160305

SECURITY MANAGEMENT TRAINING TO WORK WITH INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE INFORMATION SOCIETY

***Ya.D. Gelrud**, gelrud@mail.ru,*
***S.A. Bogatenkov**, ser-bogatenkov@yandex.ru*
South Ural State University, Chelyabinsk, Russian Federation

In today's information society, exacerbated the problem with strengthening traditional and emerging threats to security when working with information and communication technologies. These include threats to economic, informational, psychological, social and didactic nature. A promising direction to solve the problem is e-learning, minimize these threats.

The article discusses the methodology of safety management training to work with information and communication technologies in the face of increasing threats. The proposed methodology relies on the principles of safety, classification of competencies, the model of conditions and management factors and patterns of behavior (patterns). Among the patterns selected decision-making methods and methodology of safety assessment training based on the analysis of experience and application of mathematical models.

The methodology of safety management training to work with information and communication technologies ensure the minimization of threats of economic, informational, psychological, social and didactic nature. The results of using the proposed methodology are demonstrated on the example of training to work with information-measuring systems at Chelyabinsk CHPP-2.

Keywords: security, information and communication technology, training, e-learning.

References

1. Loginov E.L., Raykov A.N. [Network Information Attack on the Control Systems of Critical Infrastructure Energy Facilities]. *Power System*, 2015, no. 4, pp. 3–9. (in Russ.)

2. Nagy A. (2005). The Impact of E-learning. In E-Content (pp. 79–96). Springer Berlin Heidelberg. Available at: http://dx.doi.org/10.1007/3-540-26387-X_4. DOI: 10.1007/3-540-26387-X_4

3. EC (2000). Communication from the Commission: E-Learning – Designing "Tejas at Niit" Tomorrow's Education. Brussels: European Commission.

4. Allen E., & Seaman J. (2011). Going the Distance: Online Education in the United States, 2011. Babson Park, MA: Babson Survey Research Group.

5. Bogatenkov S.A. *Upravlenie kachestvom informatsionnoyi podgotovki kadrov po kriteriyu bezopasnosti: monografiya* [Quality Management of the Information Security Training of Personnel Criterion: Monograph]. Chelyabinsk, Chelyabinsk Branch of the Air Force Academy, 2015. 186 p.

6. Gnatyshina E.A., Bogatenkov S.A., Gnatyshina E.V., Uvarina N.V. *Informatsionnaya podgotovka pedagogov professional'nogo obucheniya v aspekte bezopasnosti: monografiya* [Information Preparation of the Teachers of Vocational Training in the Security Aspect: Monograph]. Chel. State Ped. University Press, 2015. 415 p.

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

8. 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. Available at: http://dx.doi.org/10.5539/ass.v10n20p1. DOI: 10.5539/ass.v10n20p1

9. Polyakov V.P. *Metodicheskaya sistema obucheniya informatsionnoy bezopasnosti studentov vuzov: diss. d-ra ped. nauk* [Methodical Information Security System of Training University Students: Diss. Dr. Teach. Science]. Nizhny Novgorod, Volga State Technical University, 2006. 538 p.

10. Gel'rud Y.D., Loginovskiy O.V. *Upravlenie proektami: metody, modeli, sistemy. Monografiya* [Project Management: Methods, Models, Systems: Monograph]. South Ural St. Univ. Publ. Center, 2015. 330 p.

11. Bogatenkov S.A. [Models, Methods and Tools of the Information Decision Support System Information Training]. *Informatizatsiya ingenernogo obrazovaniya: materialy Mezhdunar.nauch.-metod. konf.* [Informatization Engineering Education: Proc. of Intern. Scientific-Method. Conf.]. Mosocw, April 15–16, 2014, pp. 29–35. (in Russ.)

12. Bogatenkov S.A., Varypaev E.S. [Experience in the Implementation and Operation of the Workstation Engineer of Production and Technical Department and Technical Means to "Energy" on the Chelyabinsk CHPP-2]. *Industrial power*, 1996, no. 11, pp. 7–8. (in Russ.)

13. Bogatenkov S.A. [Experience of Implementation and Prospects of Development of the Automated Systems of Vibration Diagnostics Equipment on the Chelyabinsk CHPP-2]. *Electrical Safety*, 1997, no. 1, pp. 50–56. (in Russ.)

14. Bogatenkov S.A., Tarasov I.M. [Experience of Implementation and Prospects of Development of the Automated Emergency Events Registration System at Chelyabinsk CHP-2]. *Electrical Safety*, 1996, no. 3–4, pp. 53–56. (in Russ.)

15. Varypaev E.S., Bogatenkov S.A., Baidin O.V. [Automated Accounting of Natural Gas]. *Gas Industry*, 1994, no. 3, pp. 32. (in Russ.)

16. Bogatenkov S.A., Tarasov I.M. [Methods of Measuring Channels of Technical Diagnostics of the Technical Means "Energy"]. *Electrical Safety*, 1996, no. 2, pp. 19–22. (in Russ.)

17. Bogatenkov S.A. [Improving of the Efficiency of Energy-Saving Measures with the Help of Automated Energy Accounting]. *Industrial Energy*, 1997, no. 12, pp. 2–5. (in Russ.)

18. Bogatenkov S.A., Trubina E.N., Bogatenkov D.S. [Search Automation of Unacceptable Energy Losses via Automated Energy Accounting]. *Electrical Safety*, 1998, no. 3–4, pp. 39–46. (in Russ.)

19. Bogatenkov S.A., Bortkewich E.S. [Automation of Technical Diagnostics of Measuring Channels with Automated Energy Accounting]. *Electrical Safety*, 1999, no. 1, pp. 39–44. (in Russ.)

20. Bogatenkov S.A. [Experience of Setting up an Integrated Information Measuring Systems at Chelyabinsk CHP-2]. *Industrial power*, 1997, no. 3, pp. 5–7. (in Russ.)

21. Bogatenkov S.A. [Requirements for Informational Training in Terms of Information and Measuring Systems]. *Concept*, 2014, no. 1, pp. 16–20. (in Russ.)

22. Bogatenkov S.A. [Formation of the Competence of Teaching Staff to Work with the Hardware Complex "Energy" in the Aspect of Security]. *World of Science, Culture and Education*, 2014, no. 6, pp. 29–35. (in Russ.)

23. Bogatenkov S.A. *Sistema formirovaniya informatsionnoy i kommunikatsionnoy kompetentnosti: uchebnoe posobie* [System of Formation of Information and Communication Competence: Textbook]. Chel. State. Ped. University Press, 2014. 297 p.

24. Bogatenkov S.A. *Proektirovanie bezopasnoy informatsionnoy podgotovki: monografiya* [Designing Secure Information Training Monograph]. Chel. State Ped. University Press, 2013. 276 p.

Received 25 May 2016

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Гельруд, Я.Д. Управление безопасностью подготовки кадров к работе с информационными и коммуникационными технологиями в информационном обществе / Я.Д. Гельруд, С.А. Богатенков // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2016. – Т. 16, № 3. – С. 40–51. DOI: 10.14529/ctcr160305

FOR CITATION

Gelrud Ya.D., Bogatenkov S.A. Security Management Training to Work with Information and Communication Technologies in the Information Society. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*, 2016, vol. 16, no. 3, pp. 40–51. (in Russ.) DOI: 10.14529/ctcr160305