МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ И И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

Модель системы управления информационной безопасностью в условиях дистанционного обучения

Выпускная квалификационная работа по направлению
44.04.04 Профессиональное обучение (по отраслям)
Направленность (профиль) «Управление информационной безопасностью в профессиональном образовании»
Форма обучения очная

Проверка на объем заимствований:
74,94% авторского текста
Работа рекомендована к защите
«15» 05 2023 г.
Зав. кафедрой АТ,ИТиМОТД
_____Руднев В.В.

Выполнил(а):
Студент(ка) группы ОФ-209-210-2-1
Курчатов Егор Артемович
Научный руководитель:
Белевитин Владимир Анатольевич,
д.т.н., профессор кафедры АТ,ИТ и МОТД

Челябинск
2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность работы. Активное внедрение информационных технологий (ИТ) во все сферы человеческой деятельности предопределяет необходимость использования современных форм подготовки высокопрофессиональных квалифицированных кадров в области профессионального образования. Сегодня в силу вступает новая тенденция образования, основанная на двух направлениях:

– развитие открытого, дистанционного образования, технологической основой которого являются информационные и телекоммуникационные технологии

– универсализация содержания и методик обучения, что решается посредством широкого внедрения и развития электронных форм передачи материала.

Дистанционное обучение позволяет учиться в своем собственном темпе, исходя из своих потребностей в образовании и личностных особенностей. Так же оно позволяет не ограничивать себя в выборе образовательного учреждения, независимо от того, в каком регионе проживает обучающийся. В процессе дистанционного обучения используются современные технологии, что также позволяет освоить навыки, которые в будущем пригодятся в работе и повседневной жизни. Одним из самых главных удобств является возможность самим корректировать и составлять график обучения, расписание занятий, а также список изучаемых предметов. Нельзя не отметить еще одно достоинство – это обучение в максимально комфортной и привычной обстановке, что способствует повышению его продуктивности. Существующие системы дистанционного образования ориентированы на широкий спектр направлений подготовки специалистов и не учитывают особенности подготовки специалистов в сфере информационных технологий.

Помимо этого современные образовательные стандарты предполагают переход от групповой подготовки к индивидуальным программам, с возможность выбора обучающимся предпочтительных дисциплин для изучения.

Актуальность диссертационной работы заключается в необходимости разработки моделей, алгоритмов и программных средств для создания современной адаптивной системы дистанционного обучения в сфере информационных технологий, которая будет соответствовать современным образовательным стандартам и в тоже время поддерживать индивидуализацию учебного процесса для повышения качества его результатов.

Цель работы. разработка структуры и алгоритмического обеспечения модели системы управления информационной безопасностью в условиях дистанционного обучения.

Для достижения поставленной цели в работе решались следующие основные задачи:

1. Анализ существующих методов реализации адаптивного подхода в дистанционном обучении, определение требований к разрабатываемой системе на основании действующих стандартов;
2. Разработка Модели системы управления дистанционного обучения в сфере информационных технологий;
3. Разработка моделей и методов адаптации на уровне планирования учебного процесса;
4. Разработка программного обеспечения, реализующего адаптивную систему дистанционного обучения.

Проблема. Основная проблема исследования заключается в неготовности системы дистанционного образования и незащищенность информации.

Объект исследования – система дистанционного образования

Предмет исследования – структура и алгоритмическое обеспечение модели системы управления информационной безопасностью в условиях дистанционного обучения.

Методы исследования. Теоретическая часть работы построена на исследовании процессов создания, накопления и обработки информации. Научные результаты получены с использованием методов системного анализа и математического моделирования, теории принятия решений, теории оптимизации, теории графов, сетевого планирования и управления.

Научная новизна. В диссертационной работе получены следующие результаты, характеризующиеся научной новизной:

1. Разработана структура модели системы управления, отличающаяся наличием блока коррекции учебного плана, который позволяет на основе модели обучающегося осуществлять динамическое изменение индивидуального учебного плана на любом этапе обучения;

2. Предложены количественные характеристики учебных дисциплин (эффективность, вес, коэффициенты согласованности и рассогласованности интересов обучающегося и требований рынка труда), учитывающие реализуемые ими компетенции и обеспечивающие максимальную адаптацию учебного процесса при проектирования учебного плана

3. Предложен комплекс компонентов оптимизационной модели, включающий ограничения на коэффициенты согласованности, технологические и стратегические ограничения, а также различные варианты целевых функций, особенностью которого является многоальтернативный подход к разработке оптимального учебного плана, адаптированного к обучающемуся;

4. Предложен двухэтапный алгоритм формирования учебного плана, включающего совокупность дисциплин, покрывающих заданный набор компетенций, отличительной особенностью которого является

эвристическая процедура выбора дисциплин, основанная на жадной стратегии;

5. Разработан программный комплекс, реализующий предложенные в работе методы организации учебного процесса, отличающийся особой структурной организацией компонентов, позволяющих в интерактивном режиме изменять модель обучаемого и корректировать учебный план.

Практическая ценность работы. В результате проведенных исследований разработаны теоретические основы создания адаптивной системы дистанционного образования, реализованные в программном комплексе. Полученные результаты в форме моделей и алгоритмов могут быть использованы как элементы для разработки индивидуального учебного плана обучающегося, а также подходов к оптимизации учебного плана на основе согласования требований рынка труда и предпочтений обучающегося. Основные результаты диссертационных исследований внедрены в учебный процесс в негосударственном учебном учреждении «Центр рационального природопользования».

Содержание работы. В первой главе обоснована необходимость свойства адаптации для образовательной системы в области информационных технологий, что обусловлено ее постоянной динамикой. Проведен обзор и сравнительный анализ подходов к построению современных систем дистанционного обучения. Сформированы требования к разрабатываемой адаптивной системе дистанционного обучения в сфере информационных технологий. Во второй главе предложена структура адаптивной системы дистанционного обучения, подробно описаны компоненты данной системы и их взаимосвязь. Разработана математическая модель взаимодействия информационных процессов. В третьей главе проводится алгоритмизация процесса создания индивидуального учебного плана с учетом предпочтений обучающегося. Предложены параметры согласования компетенций и содержания учебного процесса с точки зрения

предпочтений обучающегося и требований рынка труда. В четвертой главе описывается структура программной платформы, позволяющая экспериментально проверить эффективность вышеописанных моделей и алгоритмов. Приводится общее описание разработанного программного комплекса. Рассматривается его графический интерфейс и функциональные возможности.

База исследования. Базой исследования было выбрано бюджетное учреждение профессионального образования Ханты-Мансийского автономного округа - Югры «Советский политехнический колледж»

Сокращенное наименование образовательной организации:

БУ «Советский политехнический колледж»

Учредитель:

Ханты-Мансийский автономный округ - Югра

Органы государственной власти, осуществляющие функции и полномочия учредителя:

Департамент образования и молодежной политики Ханты-Мансийского автономного округа - Югры (Депобразования и молодежи Югры)
Адрес: 628011, Ханты-Мансийский автономный округ - Югра, г.Ханты-Мансийск, ул.Чехова, д.12.
Телефон/факс: Телефон: (3467) 360-161 доб. 2501.
Адрес сайта: depobr-molod.admhmao.ru
E-mail: doimp@admhmao.ru

Департамент по управлению государственным имуществом Ханты-Мансийского автономного округа – Югры (Депимущества Югры)
Адрес: ул. Ленина, 54/1, г. Ханты-Мансийск, Ханты-Мансийский автономный округ – Югра (Тюменская область), 628012
Телефон/факс: Телефон: (3467) 30-32-10, факс (3467) 30-32-77
Адрес сайта: http://www.depgosim.admhmao.ru/
E-mail: dgs@admhmao.ru

Режим, график работы

- колледж работает по пятидневной рабочей неделе;
- обучение проходит в одну смены;
- начало занятий 8.30 ч., заканчивается в 16.00 ч.в соответствии с расписанием занятий ;

Для слушателей колледжа и студентов заочной формы обучения занятия начинаются и заканчиваются согласно срокам, установленным учебным планом, образовательной программой, расписанием занятий, графиком учебного процесса, договором.
Выходной день: суббота, воскресенье.
Места осуществления образовательной деятельности, в том числе не указанных в приложении к лицензии (реестре лицензий) на осуществление образовательной деятельности в соответствии с частью 4 статьи 91 Федерального закона от 29 декабря 2012г. N 273-ФЗ "Об образовании в Российской Федерации": 628240, Ханты-Мансийский автономный округ - Югра, город Советский, улица Макаренко, дом 1; 628240, Ханты-Мансийский автономный округ - Югра, город Советский, улица Макаренко дом 3. 628240, Ханты-Мансийский автономный округ - Югра, город Советский, Восточная промзона, 628240, Ханты-Мансийский автономный округ - Югра, город Советский, улица Кошевого, дом 20, 628240, Ханты-Мансийский автономный округ - Югра, город Советский, улица Гастелло, дом 16

Адрес:
628240, Российская Федерация, Тюменская область,
Ханты-Мансийский автономный округ - Югра,
г. Советский, ул. Макаренко, 1
Контакты
Телефоны:
8 (34675) 3-22-71
Электронная почта:
sovpk@mail.ru

ГЛАВА 1. ПУТИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В данной главе рассмотрено текущее состояние дистанционного образования в России и за рубежом. Выявлены достоинства и недостатки существующих систем дистанционного обучения. Представлены особенности образования, в частности дистанционного, в сфере информационных технологий. Предложены способы повышения качества дистанционного образования в сфере информационных технологий на основе обеспечения его соответствия новым образовательным стандартам.

1.1 Дистанционное обучение, его особенности и существующие системы

Активное внедрение информационных технологий во все сферы человеческой деятельности предопределяет необходимость использования современных форм подготовки высокопрофессиональных квалифицированных кадров в области высшего профессионального образования.

28 февраля 2012 года президентом России подписан Федеральный закон № 11-ФЗ «О внесении изменений в Закон Российской Федерации "Об образовании" в части применения электронного обучения, дистанционных образовательных технологий». Данный закон регламентирует порядок организации электронного и дистанционного образования в России.

Статья 15 пункт 1 данного закона гласит: «При реализации образовательных программ вне зависимости от форм обучения могут применяться электронное обучение, дистанционные обучение в порядке, установленном органом федеральной исполнительной власти, осуществляющим функции государственной политики и нормативному и правовому регулированию в образовательной сфере».

Под электронным обучением понимается организация учебного процесса с применением хранящейся в базе данных и используемой при

подготовке образовательных программ информации и обеспечивающих ее обработку технологий, средств, а также телекоммуникационных сетей, обеспечивающих трансляцию по линиям связи указанной информации, взаимодействие всех участников образовательного процесса.

Под дистанционными образовательными технологиями понимаются технологии, реализуемые в большей степени с применением информационных сетей при дистанционном взаимодействии обучающихся и системы обучения либо педагогов.

«При реализации программ образования с применением преимущественно электронного обучения, дистанционного обучения в образовательных учреждениях должны быть обеспечены условия для функционирования информационной и электронно-образовательной среды, включающей в себя электронные поисковые ресурсы, электронные образовательные ресурсы, совокупность технологий информационного характера, технологий телекоммуникации, соответствующих технических средств и обеспечивающей освоение обучающимися учебных планов в необходимом объеме независимо от мест их нахождения»

В соответствии с указанными изменениями в силу вступает новейшая тенденция образовательного процесса, основанная на следующих направлениях

1. Распространение доступного, дистанционного образования, технологической основой которого служат информационные технологии и средства телекоммуникации;

2. Стандартизация наполнения и методологии обучения, что решается путем повсеместного внедрения и распространения электронных форм представления и передачи материала.

В данных случаях, определенно, весомую роль получают электронные системы обучения, представляющие собой комплекс учебно-методических

материалов, способствующих лучшему усвоению обучающимися учебных компетенций по специальности

Электронные обучающие системы в себя включают:

1. Учебные стандарты дисциплин;
2. Лекционные занятия;
3. Учебный план и указания по выполнению практических и лабораторных заданий, курсовых работ;
4. Методические пособия и руководства для самостоятельной работы обучающихся;
5. Тестовые испытания по дисциплинам;
6. Справочные материалы;
7. Ссылки на электронные библиотеки;

Наиболее оптимальной формой организации процесса обучения с использованием электронных обучающих систем является дистанционное образование. Схема организации дистанционного обучения представлена на рисунке 1.1.1.

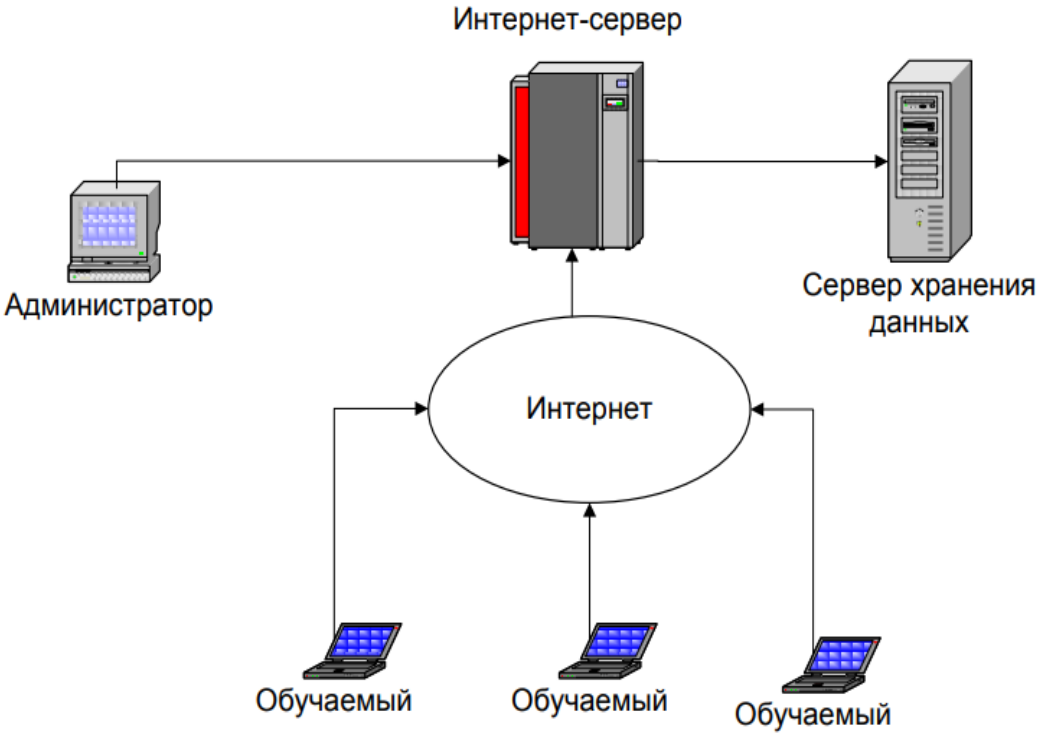

Рисунок 1.1.1 – Схема процесса дистанционного обучения

В Концепции развития и создания дистанционного обучения (ДО) в России приведено такое определение ДО: «Дистанционное образование – комплекс образовательных мер и услуг, предоставляемых большому объему населения в стране и за ее пределами при помощи специализированной информационно-образовательной среды, основанной на средствах обмена учебной информацией дистанционно (спутниковое телевидение, радио, компьютерная связь и т.п.). ДО является одной из основных форм непрерывного образовательного процесса, которое призвано реализовать права человека на получение образовательных услуг».

Выделяют следующие преимущества ДО:

1. Обучение в индивидуальном темпе – скорость познания учебных материалов устанавливается непосредственно обучающимся в зависимости от его личных желаний и обстоятельств.

2. Свобода и гибкость обучения – обучающийся может выбрать любой из предоставляемых на выбор многочисленных курсов обучения, а также абсолютно самостоятельно рассчитывать сроки и продолжительность занятий по дисциплинам.

3. Доступность обучения для любого человека – независимо от вашего географического и иного положения, вы имеете возможность получить образование дистанционно в любом ВУЗе, поддерживающем указанные технологии, что позволяет удовлетворить образовательные потребности каждого человека.

4. Скорость взаимодействия – эффективное осуществление взаимосвязи между преподавателем и обучающимся является неотъемлемым элементом учебного процесса.

5. Технологичность учебного процесса – использование в учебном процессе новейших достижений информационных и телекоммуникационных технологий.

6. Социальное равноправие – подразумевает одинаковые возможности получения дистанционного образования в независимости от места проживания, состояния здоровья, национальной принадлежности и материального состояния обучающегося

7. Творчество – благоприятные условия для личного самовыражения обучающегося в процессе обучения.

Наряду с указанными достоинствами также имеется несколько недостатков:

1. Отсутствует вербальное взаимодействие между обучающимся и преподавателем, т.е. отсутствуют те моменты, связанные с индивидуальным подходом к обучению и воспитательным процессом. Ведь если рядом нет преподавателя, который эмоционально окрашивает материал и способствует восприятию материала, это, несомненно, весомый минус.

2. В процессе домашнего обучения отсутствует часть индивидуально психологических факторов, которая характерна для классического образования. Для получения дистанционного образования необходима строгая самодисциплина, а результат обучения непосредственно зависит от самостоятельности обучающегося.

3. Необходима возможность постоянного доступа к источникам получения учебных материалов (электронных учебников, видеоматериалов и т.д.), а для этого нужна серьезная техническая база, в том числе, высокоскоростной доступ к сети Интернет

4. Отсутствуют такие важные формы занятий, как практические занятия, семинары, которые необходимы для успешного закрепления материала и более качественного его усвоения.

5. Электронные ресурсы обучения не всегда хорошо реализованы и удовлетворяют действующим требованиям и стандартам из-за недостаточной квалификации специалистов, которые их реализовывали.

6. В дистанционном образовании обучение ведется предпочтительно только в письменной форме. Для некоторых обучающихся отсутствие возможности и излагать свои знания и навыки в устной форме может вызвать собой некачественное усвоение материала и множество прочих проблем.

Наиболее широкое развитие ДО получило в настоящее время в тех странах, где исторически для этого сложились необходимые предпосылки, а именно: хорошо развитая телекоммуникационная инфраструктура, наличие большой территории государства (где есть немало удаленных от центра районов) и развитая система традиционного образования. Это, прежде всего такие страны, как США, Канада, Австралия и Великобритания. В этих странах действуют различные учебные заведения и образовательные телекоммуникационные сети, позволяющие всем желающим пройти дистанционное обучение.

На рисунке 1.1.2 приведена тенденция развития дистанционного образования в США в промежуток времени с 2005 по 2012 годы.

Рисунок 1.1.2 – Тенденция развития дистанционного образования

В России дистанционное обучение также используется, и существует ряд систем, некоторые из которых поставляются зарубежными

разработчиками, другие же разработаны в России и учитывают особенности образования нашей страны.

На необходимость развития дистанционного образования указывает новый закон об образовании. Обзор основных систем дистанционного обучения приведен в таблице 1.

Таблица 1.1.1. Обзор существующих систем дистанционного обучения

Название системы	Особенности
IBM Lotus Workplace Collaborative Learning, IBM 2009	Универсальная обучающая система, представляющая собой надежную и масштабируемую систему дистанционного обучения. Достоинства: – возможность составлять учебные программы проведение занятий; – возможность контролировать результаты обучения и тестового контроля; – возможность организовать дискуссии и обмен опытом. Недостатки: – привязка к решениям компании IBM; – сложность русификации и локализации.
Oracle Learning Management, Oracle 2007	Интернет-система для обеспечения процессов обучения и повышения квалификации. Достоинства: – контролирует все этапы процесса обучения: составление учебных курсов, планирование учебного процесса, доставку обучающимся курсов и других необходимых материалов, контроль и анализ знаний; – предоставляет возможность индивидуализации обучения. Недостатки: – требовательная к аппаратным ресурсам, требует СУБД Oracle.

Moodle 2002	Представляет собой бесплатное веб-приложение, предоставляющее возможность создавать порталы для онлайн-обучения. Достоинства: – распространяется бесплатно; – открытый исходный код; – инструментарий для создания обучающих и контролирующих программ; – большой опыт использования; – поддержка в текущее время. Недостатки: – тяжелая масштабируемость.
Naumen Learning, NAUMEN 2007	Комплексная система для организации работы учебных центров, разработки учебных материалов и обеспечения дистанционного обучения. Достоинства: – обучение в любое подходящее время, персонализированные учебные программы; – возможность дистанционно обучать группы обучающихся, находящихся в разных регионах. Недостатки: – отсутствует поддержка стандартов хранения учебного контента.
СДО "ДОЦЕНТ", УНИАР 2011	Автоматизированная система дистанционного обучения которая представляет собой комплекс программно-методических механизмов обучения, доподготовки и тестирования обучающихся, основанный на современных методиках образования

	на базе компьютерных обучающих ресурсов и тестирующих средств. Достоинства: – инструментальные возможности создания обучающих и тестирующих программ; – средства организации централизованной базы данных учебного центра для хранения статистики, ведения разнообразных отчетв. Недостатки: – слабая масштабируемость; – привязка к продуктам компании Microsoft.

Спрос на услуги образования определяется заинтересованностью пользователей в данных услугах, наличием необходимой технической оснащенности и информированностью о такой услуге. Рынок ДО в России пока находится на этапе формирования и, как показали проведенные Центром информационно-аналитического обеспечения дистанционного обучения социологические исследования, масштабы распространенности дистанционных образовательных услуг в основном зависят от предлагаемых технологий обучения:

– технология обучения, основанная на использовании учебной литературы, заинтересует 10% людей, предрасположенных к выбору дистанционного обучения;

– технология обучения, основанная на использовании учебной литературы и аудиозаписей, заинтересует 11,6 % людей, предрасположенных к выбору дистанционного обучения;

– в сочетании с видеозаписями должна привлечь 14,7% людей, расположенных к выбору дистанционной формы обучения.

Помимо систем дистанционного обучения в ВУЗах, существует успешный опыт применения дистанционного обучения в сфере

информационных технологий такими компаниями как Microsoft и CISCO Network. Данные компании предлагают дистанционное обучение для специалистов в области информационных технологий с целью повышения своего профессионального уровня, а так же предоставляют возможность получения международных сертификатов, подтверждающих знаний в любой стране мира.

В зависимости от средств дистанционного обучения и форм коммуникации можно выделить три разновидности технологической организации ДО: единичная, мультимедиа, гипермедиа.

Иерархия технологий, применяемых для организации учебного процесса, приведена на рисунке 1.1.3.

Модель единичной медиа означает использование какого-либо средства приобретения знаний и канала передачи информации, например обучение через чат, учебные радио- или телепередачи. В данном случае основным средством обучения является, печатный текст. Практически отсутствует обоюдная коммуникация, что приближает эту модель ДО к традиционному российскому заочному обучению.

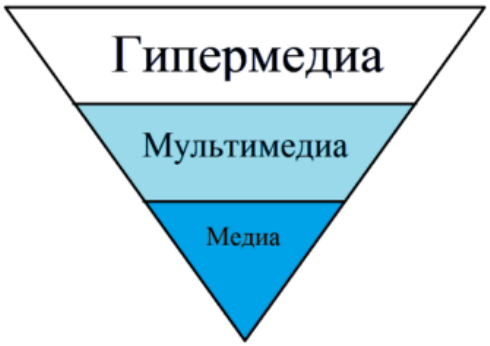

Рисунок 1.1.3 – Технология представления учебного материала

В мультимедийном подходе к ДО используют средства обучения – учебные пособия в печатном виде, компьютерные учебные программы на различных носителях, аудио- и видеозаписи и т. п. Однако преобладает при этом передача учебной информации в «одну сторону». При необходимости

используются части очного обучения – митинги обучающихся и преподавателей, подведение итоговых учебных семинаров или консультаций, очные экзамены и т. п.

Моделью ДО нового поколения является гипермедиа, что предусматривает использование современных информационных технологий при преобладающей роли компьютерных телекоммуникаций. Наиболее простой формой при этом является использование электронной почты и видеосвязи, а также аудиообучение (сочетание телефона и телефакса). При текущем развитии эта модель ДО включает использование таких средств, как видео, телефон и телефакс (для проведения видеоконференций) при одновременном широком использовании дисков, различных средств.

Классические методы разработки онлайн обучающих материалов, зачастую, дороги, требуют много времени и требуют специализированных навыков. Чтобы полностью реализовать онлайновое обучение, компании используют системы управления содержимым обучения – Learning Content Management System (LCMS) – для быстрой организации, развертывания и управления контентом онлайновых курсов.

Learning Content Management System (LCMS) – это программный и аппаратный комплекс, используемый для представления, хранения, сборки и доставки пользователю персонализированного учебного контента в форме «обучающих объектов»).

В 2000 г. инициативная группа ADL (Advanced Distributed Learning) разработала стандарт SCORM (Sharable Content Object Reference Model), созданный для систем дистанционного обучения. Данный стандарт содержит ряд требований к организации учебного контента и всей системы ДО. SCORM основан на стандарте XML и позволяет поддержать совместимость компонентов и возможность их многоразового использования: учебный материал представлен небольшими разделами, которые могут включаться в учебные курсы и использоваться системой ДО независимо от того, кем, где и

с помощью чего были созданы [66]. Структура пакета SCORM приведена на рисунке 1.1.4.

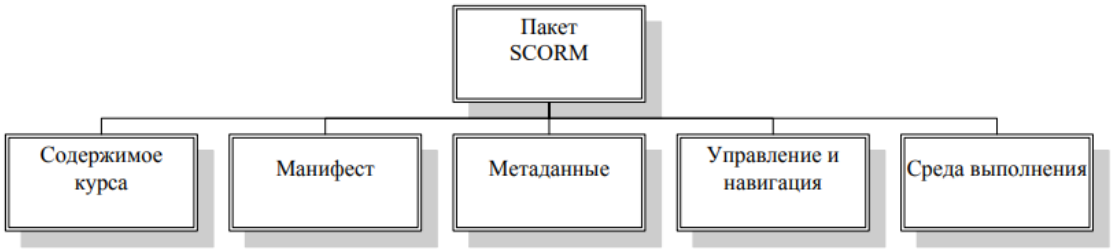

Рисунок – 1.1.4 Структура SCORM – пакета

SCORM – это набор спецификаций и стандартов (рисунке 1.1.5), которые представлены в несколько разделов:

– Модель хранения содержания.

– Среда текущего выполнения.

– Поиск и навигация.

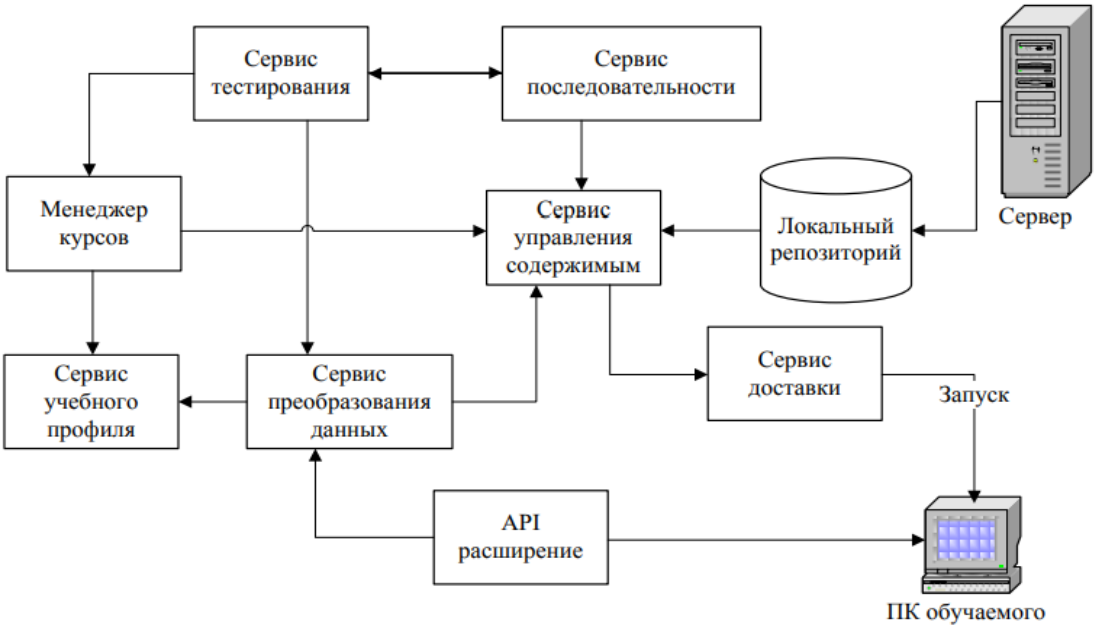

Рисунок 1.1.5 – Схема процесса реализации отображения современного SCORM – пакета

В настоящее время на рынке образовательных услуг отсутствуют системы дистанционного обучения, удовлетворяющие образовательным

стандартам четвертого поколения, а так же использующие адаптивный подход к образовательному процессу.

1.2 Особенности образования в сфере информационных технологий

В настоящее время становится понятным, что роль информационных технологий в нашем обществе занимает важное место. Промышленный рост вернул всеобщую актуальность информационных систем управления предприятиями, все более значимое место занимают СМИ на основе Интернет Технологий, развивается Интернет-индустрия, значимой частью экономики России становится программирование. Движущей силой данных процессов являются специалисты в области ИТ.

Информационные технологии (ИТ) являются одним из основных фокусов развития нашего общества. Несмотря на то, что их широкое внедрение в экономике началось около 25 лет назад, и на достигнутые успехи в различных областях экономики, их развитие продолжается, и современное общество ждут еще серьезные изменения, связанные с более широким и систематичным использованием информационных технологий во всех сферах человеческой деятельности. Поэтому в них достаточно ярко отражаются все особенности текущего развития.

Подготовка высококвалифицированных специалистов в области ИТ обладает рядом особенностей:

1. Информационные технологии развиваются стремительно, достаточно не следить за изменениями и тенденциями в течении 3-5 лет, чтобы полностью потеряться в массе новых терминов и технологических средств. При этом развитие происходит кумулятивно – новые технологии зачастую включают в себя части предшествующих.

2. Источники знаний для информационных технологий, включая программы курсов и знания преподавателей, зачастую развиваются медленнее, чем технологии, поэтому развитие новых технологий становится

все труднее, так же, как и подготовка преподавателей, способных обучить им. Быстрое развитие приводит к необходимости постоянной смены области деятельности, чтобы оставаться в числе ведущих специалистов, и поэтому у таких специалистов меньше все времени остается для передачи накопленного опыта и знаний, участия в воспроизводстве кадров в этой отрасли

3. Все острее становится проблема обучения ИТ-специалистов высшей квалификации, обладающих широким спектром знаний, как в этой области, так и в ряде других, способных адекватно оценивать перспективы новых технологий, проводить исследования в области ИТ-технологий, видеть всю полноту проблем, возможных при решении конкретной прикладной задачи, и их влияние на итоговые характеристики продуктов и услуг.

Все перечисленные факторы характеризуют необходимость пристального внимания к подготовке ИТ-специалистов и принятия ряда мер, которые помогли бы обеспечить соответствие приобретаемых ими знаний и навыков потребностям дальнейшего развития нашего общества.

Задача подготовки конкурентоспособного ИТ-специалиста требует постоянного обновления учебного контента, вследствие высоких темпов развития данной области.

Компетентность это, прежде всего, общая возможность и готовность человека к деятельности, основанные на приобретенных знаниях и опыте, которые приобретены в процессе обучению, ориентированы на самостоятельное участие личности в учебно-познавательном процессе и направлены на успешную интеграцию в общество. Компетенция это способность использовать полученные знания и личностные качества для прикладных задач в определенной области.

Компетентностная модель обучающегося, с одной стороны, охватывает квалификацию, связывающую его будущую деятельность с предметами и объектами труда, с другой стороны, отражает промежуточные требования к результату образования.

На рисунке 1.2.1 приведена модель компетентности магистра прикладной информатики.

Таким образом, при разработке модели системы управления информационной безопасностью необходимо ориентироваться на компетентностную модель и учитывать компетенции, которыми должен обладать обучающийся по завершении обучения. Овладение компетенциями один из основных критериев оценки качества обучения. Компетенции должны быть учтены при формировании учебного плана и подборе учебных курсов, оптимально покрывающих требуемые направления подготовки. Оценка результатов обучения также должна проводиться на основе анализа достижимости тех компетенций, которые предопределены стандартом данной области.

Рис. 1.2.1 Модель компетентности магистра прикладной информатики

1.3 Теоретические предпосылки создания

Существующий компетентностный подход к образовательному процессу предполагает разработку учебного плана основываясь на наборе компетенций, которыми должен обладать обучающийся по окончании

обучения. Однако необходимо учитывать предпочтения данных компетенций с точки зрения текущего состояния рынка труда. В рассмотренных ранее системах дистанционного обучения (Oracle Learning Management, СДО "ДОЦЕНТ") при составлении учебного плана решается оптимизационная задача, описываемая следующей математической моделью:

$$\begin{cases} \sum_{i=1}^{m} O_{чi} \to \min \\ \forall D_j \subset УП\left(\bigcap_{i=1}^{m} C_i = C\right), \\ \sum_{i=1}^{m} O_{ЗЕТi} \le O_{ЗЕТ}^{MAX}, \\ \sum_{i=1}^{m} O_{чi} \le O_{ч}^{MAX}, \end{cases}$$

где $C = \{C_1, ..., C_n\}$ – множество компетенций, которые необходимо «покрыть» включенными в учебный план дисциплинами;

$O_{ч}^{MAX}$ – максимальный объем времени (в часах) отведенного на изучение дисциплин;

$O_{ЗЕТ}^{MAX}$ – максимальный объем учебного плана в зачетных единицах;

Недостатком данной модели является отсутствие параметров, характеризующих востребованность включаемых в учебный план дисциплин с точки зрения рынка труда. Для создания современной модели системы управления информационной безопасностью необходимо дополнить модель данными параметрами.

Так же необходимо разработать эвристическую процедуру составления учебного плана, позволяющую решать поставленную оптимизационную задачу.

На данный момент существует множество алгоритмов из теории сетевого планирования, позволяющих максимально эффективно распределять учебное время и вносить изменения в учебный план, если у обучающегося возникает в этом необходимость. Для внедрения данных

методов в разрабатываемую МСУИБ необходимо наличие блока создания и коррекции учебного плана ее структуре.

1.4 Цели и задачи исследования

Как сказано выше, информационные технологии обладают одним из самых высоких темпов развития среди современных наук. Для создания современной конкурентоспособной адаптивной системы дистанционного обучения необходимо сформулировать ряд требований, который она должна удовлетворять:

1. Реализация дистанционного подхода к образовательному процессу. Дистанционное обучение является современным и развивающимся подходом к организации образовательного процесса. К тому же образование, полученное дистанционно, имеет равнозначный статус с классическим очным. По статистическим данным на конец 2022 года около 81% жителей России имеет доступ к сети Интернет, в том числе 46% обладают доступом со скоростью не менее 5 Мбит/с. Статистические данные также говорят о том, что большой процент граждан имеет технические средства для получения образования или повышения квалификации дистанционно.

2. Образовательная система должна обладать универсальным и простым в реализации средством обновления учебных материалов. Для обеспечения этого требования наиболее подходящим, на наш взгляд, является стандарт для формирования учебного материала SCORM, который позволяет постоянно обновлять и дополнять учебный материал, что важно для сферы информационных технологий, а также предоставляет возможности взаимодействия для систем обучения, если их используется несколько.

3. Еще одним важным требованием к системе является ее адаптивность. Современные образовательные стандарты требуют индивидуального подхода к процессу обучения. Необходимо учитывать индивидуальные особенности и предпочтения обучающегося при

составлении учебного плана, формировании учебных элементов и оценивании результатов обучения. Данный подход позволит максимально оптимизировать процесс обучения, наполнив его учебным материалом, идеально подходящим потребностям и особенностям каждого обучающегося.

4. В основу организации процесса обучения должен быть положен компетентностный подход. Необходимо чтобы процесс обучения был направлен на развитие и совершенствование определенных компетенций, которые формируются текущим состоянием рынка труда и существующими образовательными стандартами. Набор компетенций, характерный для подготовки по выбранному направлению, должен быть учтен на всех этапах обучения, начиная от формирования учебного плана и заканчивая оценкой результатов обучения.

5. Необходимо основываться на достоинствах и недостатках существующих на данный момент систем обучения. Как в России, так и за рубежом уже имеются системы, успешно используемые для подготовки высококвалифицированных специалистов. Опыт использования данных систем, а так же анализ их недостатков позволит создать современную конкурентную систему, соответствующую современным стандартам

6. Ориентация системы на подготовку кадров в сфере информационных технологий. Многие специальности данной области (программирование, архитектура систем) требуют постоянного практического применения полученных навыков для профессионального роста обучающегося. Необходимо наполнить систему функционалом, позволяющим реализовать дистанционные практические и лабораторные работы. А так же разрабатывать практические задания для проверки качества обучения.

Целью диссертационной работы является разработка структуры и алгоритмического обеспечения адаптивной системы дистанционного

обучения в сфере информационных технологий с использованием компетентностного подхода.

Для достижения поставленной цели в работе решаются следующие основные задачи:

1. анализ существующих методов реализации адаптивного подхода в дистанционном обучении, определение требований к разрабатываемой системе на основании действующих стандартов;
2. разработка структуры адаптивной системы дистанционного обучения в сфере информационных технологий
3. разработка моделей и методов адаптации на уровне планирования учебного процесса;
4. разработка программного обеспечения, реализующего адаптивную систему дистанционного обучения.

ГЛАВА 2. РАЗРАБОТКА СТРУКТУРЫ И МОДЕЛИ ВЗАИМОДЕЙСТВИЯ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ

В данной главе представлен системный подход к разработке системы дистанционного образования. Определены основные подсистемы и элементы, представлены структурная и функциональная модель системы.

Современным направление в области систем электронного обучения являются системы обучения с адаптивным подходом. Основной особенностью данных систем является адаптация учебного материала к индивидуальным особенностям обучающегося. Адаптивность – свойство системы, характеризующее ее способность изменяться под текущее состояние внешней среды или входных параметров.

В разрабатываемой системе обучения адаптация происходит на нескольких уровнях:

1. Адаптация на уровне планирования учебного процесса предполагает разработку учебного плана, адаптированного под конкретного обучающегося, что позволяет сформировать индивидуальный учебный план и обучаться в соответствии с индивидуальной образовательной траекторией. Данный этап является наиболее важным в процессе обучения. Именно на данном этапе необходимо предложить обучающемуся такой набор дисциплин, который удовлетворил бы его запросы и цели, учитывал текущие тенденции рынка труда, был бы оптимизирован по времени и основывался на взаимосвязи дисциплин для исключения дублирования информации.

2. Адаптация на уровне содержания учебного материала. Для реализации данного свойства необходимо проделать большую работу по формированию учебного контента по каждой дисциплине с возможностью выбора предпочтительной формы представления информации. Данный подход требует серьезных затрат интеллектуального труда, но в результате позволяет получить совершенно новую, высокоэффективную систему обучения.

3. Адаптация на уровне контроля знаний. Индивидуальные характеристики каждого обучающегося определяются на начальном этапе обучения при помощи специальных тестов и в дальнейшем служат параметрами обучения, коррекцию которых необходимо осуществлять на протяжении всего процесса обучения. Особенность восприятия может меняться в процессе обучения, и своевременный учет данных изменений позволит так же повысить качество обучения

4. Проблемы в структуре информационной безопасности дистанционного обучения

В обучении адаптация предполагает индивидуализацию содержимого учебных курсов и тестовых заданий, предназначенных для контроля знаний, для каждого обучающегося. Адаптация может происходить по различным параметрам, например по объему предлагаемого материала или по форме его представления. Задача адаптивных систем обучения – оптимизация учебного процесса путем предоставления обучающемуся учебного материала в наиболее предпочтительной форме. Результатом такого подхода является повышения качества и эффективности учебного процесса.

2.1 Проблемы информационной безопасности в системе дистанционного образования

Дистанционное обучение далеко не новое явление. Уже много лет широко распространено заочное обучение. Одним из самых новых веяний является обучающее телевидение, но, тем не менее, и оно имеет опыт десятилетий. В настоящее время мы ощущаем на себе "виртуальную лихорадку" (некоторые могли бы назвать это "золотой лихорадкой") дистанционного обучения вследствие появления сети Интернет. В этой статье будет рассмотрено, почему это происходит.

За последние несколько лет возросшая популярность Web-технологий, а также свободный доступ в Интернет посредством модемной связи, значительно повлияли на увеличение числа пользователей сети Интернет.

Благодаря Интернету мы можем наслаждаться прямым доступом к различным ресурсам мультимедиа во всем мире, как если бы мы просматривали страницы, хранящиеся на нашем собственном компьютере в гипертекстовом формате. Потенциал Web-технологий неизбежно влечет преподавателей во всем мире, так как эти технологии позволяют объединять образовательные ресурсы, разбросанные по всему миру, в нечто похожее на "сделанные на заказ" мультимедийные базы данных, созданные для своих собственных образовательных целей.

Интернет, необходимые средства связи и компьютерные технологии позволяют сделать компьютерное обучение более интересным. Появляются все новые и новые проекты и изобретения в этой области использования сети Интернет. Поэтому полезно представить краткий обзор некоторых важных типов образовательных систем, основанных на использовании компьютеров.

Самое первое из всех известных изобретений - "Интернетовские книги". Подготовка электронных версий лекционных записей и книг - наиболее легкий и оперативный путь в Интернет. В этом случае совершенно не требуются какие-то особенные знания по программированию, нет необходимости знать языки Hypertext Markup Language (HTML) или JAVA. Вспомогательные программы позволяют экспортировать все, что нужно, практически из любого текстового редактора в HTML.

Разработчики образовательных программ для детей давным-давно поняли, что компьютерные игры намного интереснее, чем учеба. Обучение детей, совмещенное с веселой игрой, в которой дети проходят несколько уровней сложности, казалось, решало все проблемы. Внимание учащихся сконцентрировано, налицо высокая эффективность обучения, тренировка реакции ...- этот список может быть легко продолжен. Но игровая модель приемлема не во всех областях образования, ее использование ограничено определенной группой пользователей - детьми.

Также в связи с быстрым развитием современных технологий большую популярность приобрели обучающие системы, основанные на Web-технологиях. Так как Интернет доступен всем в мире независимо от времени и местоположения, то использование таких систем не требует дорогостоящего оборудования.

Персональный компьютер с практически любой операционной системой, Web-браузер, модем и телефонная связь позволяют войти в сеть Интернет и, следовательно, обучаться через Интернет. Системы обучения, основанные на Web-технологиях, - асинхронны, поэтому они не требуют одновременного присутствия преподавателя и учеников. Заранее приготовленные лекции передаются по сети.

Внешний интерфейс чаще всего создается на HTML и усовершенствуется на Java, Javascript или Dynamic HTML. Но существуют и некоторые преграды и ловушки, непременно появляющиеся при обучении через Интернет. В то же время часто мы делаем шаг назад из-за просто эмоциональных суждений в средствах массовой информации или же мнений, основанных на плохом знании вопроса. В этой статье описаны тенденции развития дистанционного обучения через Интернет и сделана попытка раскрыть все "за" и "против" дистанционного обучения на сегодняшний день.

Имеются три причины огромного интереса к дистанционному обучению через Интернет.

Первая состоит в том, что существует потребность в простой достоверной информации.

Вторая - в том, что технологии для удовлетворения этих потребностей есть уже сейчас и в дальнейшем будут только совершенствоваться.

И третья причина состоит в том, что все сферы деятельности рассматривают дистанционное обучение как новый важный рынок и, следовательно, возможность деловой деятельности.

Год от года все возрастающее число людей нуждается в обучении определенного типа и вне образовательных учреждений для того, чтобы иметь возможность работать в полную силу. Только в США сегодня тратится свыше 200 миллиардов долларов в год на дополнительное образование и более 50 миллиардов долларов в год на повышение квалификации.

Первоначально Интернет был нацелен на передачу и прием простой текстовой информации. Но "аппетит растет во время еды", и вскоре потребовалось передавать электронные изображения, потом - аудио- и видеоинформацию. Сегодняшние требования к Интернету - это возможность размещения большого программного обеспечения, которое легко бы работало у пользователя.

В настоящее время на развитие дистанционного обучения влияют два основных фактора: доступ в Интернет и его качество связи. Обычно от 20 до 50 миллионов пользователей одновременно пользуются chat, surf, электронной почтой или просто "находятся" в Интернете. Но, чем большее количество человек одновременно работает в Интернете, тем хуже качество связи.

Пределы его возможностей проявляются каждый день: низкое качество связи, длительная загрузка и продолжительное время ответа. Но те слушатели, которые имеют современное качество связи по Интернет, могут работать с Web-сайтами с объемной графикой, хорошим качеством аудиоинформации и даже с небольшим количеством видеоматериалов. Самое лучшее качество обучения будет именно у этих людей. Однако, чтобы материал дошел до каждого конкретного слушателя, он должен быть в основном текстовым, но в некоторых случаях это слишком большое ограничение.

Наконец, существуют такие люди, которые не имеют доступа в Интернет, т.к. либо не имеют его вообще, либо место, откуда можно войти в Интернет, не приспособлено для учебы. Не каждая комната и не в каждом

доме отвечает условиям, необходимым для обучения через Интернет. Это связано с тем, что дистанционное обучение может потребовать несколько часов работы в Интернет, а, так как большинство пользователей Интернет (по крайней мере, для дистанционного обучения) используют телефонные линии, доступ должен производиться оттуда, где телефон будет свободен все это время.

Помимо этого, во многих местах доступ в Интернет с целью дистанционного обучения возможен, но работа в Интернете будет причинять беспокойство окружающим или наоборот - окружающие будут мешать сосредоточиться учащемуся. По мнению студентов дистанционных курсов Стенфордского университета - все эти проблемы далеко не просты.

Еще одна задача, требующая скорейшего решения, заключается в том, что дистанционное обучение должно быть интерактивным. Студенты должны иметь возможность общаться с преподавателями. При анализе работы многих существующих обучающих систем часто оказывается, что взаимодействие ограничивается возможностью перемещения по системе и почтовым общением с лектором и другими студентами.

В настоящее время при возможности осуществления хорошего качества связи этого уже не достаточно. Всем бы очень хотелось, чтобы дистанционное образование представляло собой "виртуальный класс", состоящий из студентов и преподавательского состава, территориально находящихся далеко друг от друга, даже в разных странах.

В будущем курсы дистанционного обучения могли бы обслуживаться целой командой специалистов, например, один преподаватель мог бы планировать и организовывать курс, второй - "читать" лекции, третий - обеспечивать взаимосвязь между учащимися, четвертый - оценивать старания студентов. Микропроцессорные средства могли бы помогать учащимся и их учителям в развитии индивидуальных курсов дистанционного

обучения, состоящих из определенной последовательности маленьких "обучающих модулей".

Преподаватели контролировали бы вход в обучающую программу, учебные материалы, такие, как слайды или мультимедийные презентации, пусковые браузеры на компьютерах студентов, а также то, что преподавателю нужно для процесса обучения, например, доску объявлений, библиотеки и, наконец, самих учеников. Преподаватель читал бы лекции (аудио) прямо через Интернет. Студенты обращали бы на себя внимание преподавателей с помощью электронного "поднятия руки".

Большинство из этих идей, возможно, будет воплощено в жизнь в ближайшем будущем. А пока что можно с уверенностью говорить о том, что дистанционное обучение через Интернет сегодня востребовано и, следовательно, будет быстро развиваться. Ведь для его развития сейчас имеются все возможности, как в техническом плане, так и в интеллектуальном. Ну, а когда перед человеком стоит определенная цель, и для ее достижения необходимы дополнительные знания, то получить их можно не только традиционными способами, но и путем дистанционного обучения через Интернет. И эти знания будут не хуже, а то и лучше тех, которые получат студенты, обучающиеся, например, в каком-либо очном учебном заведении.

Международная комиссия ЮНЕСКО определяет два основных принципа современного образования: "образование для всех" и "обучение в течение всей жизни". Эти принципы, несомненно, верны, но в суровых российских условиях и под влиянием стереотипов возникает несколько проблем проблем.

1) Проблема неравномерной плотности населения на территории России. Подавляющее большинство высших учебных заведений и высококвалифицированных преподавателей концентрируются в Центральном регионе (Московская и Санкт-Петербургская область), а

население рассредоточено по всей необъятной стране, где, бывает, совсем нет ВУЗов. Поступление в ВУЗ в другом городе стоит отнюдь не маленьких денег, поэтому часто недопустимо.

А что говорить о существовании потребности в повышении квалификации и образования рабочих, живущих в отдаленных в регионах? Они, кроме всего прочего, часто имеют семьи, и переезд в другой город для них означает возникновение множества значительных проблем.

2) Проблема времени. Сегодня темп жизни большинства современных людей вынуждает их расписывать свое время по минутам. Учиться необходимо всем, но как? И даже такие формы обучения как вечернее и воскресное эту проблему не решают.

3) Проблема денег. О том, сколько стоит сейчас образование, особенно высшее, и говорить не стоит. А так же существует подготовка к поступлению с множеством репетиторов и куча другие расходов! Конкурс на бюджетные места очень трудно выдержать, но ведь платное обучение мало кто сможет «потянуть».

Дистанционное образование является компромиссом для всех вышеперечисленных проблем. Что же это такое? Исходя из вышесказанного, это отдаленное обучение, т.е. на расстоянии, когда преподаватель (тьютор) и ученик могут находиться на любом расстоянии друг от друга. Учебные материалы предоставляются через Интернет, да и практически все обучение проводят с помощью новых технологий.

Именно они и обеспечивают общедоступность и низкую стоимость дистанционного образования, предоставляя возможности получить образование без переезда в другой город.

Развитие дистанционного образования появилось благодаря современным достижениям в области развития технологий, средств массовой информации и связи и т.д. Оно использует такие достижения как компьютерные и информационные технологии, учебное телевидение,

спутниковые системы связи, распространение компьютерных учебных программам, видеодисков с ними и т.д.

Выделяют три вида дистанционных технологий, применяемых в процессе обучения.

Первый вид - кейс-технология на основе бумажных носителей. Это в первую очередь учебно-методические пособия, называемые рабочими тетрадями, которые сопровождаются тьютором. Тьютор поддерживает со студентами телефонную, почтовую и др. связь, а также может непосредственно встречаться со студентами в консультационных пунктах или учебных центрах.

Вторая технология - телевизионно-спутниковая. Она очень дорогая и пока мало используется. Главный ее недостаток - слабая интерактивность, то есть обратная связь. И, наконец, третья технология - это интернет-обучение, или сетевая технология. Чаще всего в процессе дистанционного обучения используются все вышеназванные технологии в разных пропорциях.

Дистанционное образование берет своё развитие в Европе и США в начале 70-х годов. Причины распространения и возникновение данного вида образования просты: каждый человек, желающий получить образование, вне зависимости от его демографических признаков и места нахождения может учиться и получить диплом любого вуза.

Большинство специалистов в области образования считают, что дистанционное образование подает большие надежды, так как оно подходит многим людям, и стоит значительно дешевле традиционного. Кроме того, можно исключать определенные дисциплины, если вы их уже проходили, т.е. получать "образование по заказу", которое также дает некоторые преимущества в цене. Естественно, у этого вида обучения, как и у других, существуют свои плюсы и минусы в получении и усвоении материала. Если вы склоняетесь к этому варианту образования, то следует помнить следующее:

К плюсам дистанционного образования относится:

Обучение дисциплинам в индивидуальном темпе - скорость изучения материалов устанавливается самим студентом в зависимости от его личных обстоятельств и желаний.

Свобода и гибкость обучения - студент может выбрать любой из предоставляемых на выбор многочисленных курсов обучения, а также абсолютно самостоятельно рассчитывать время и продолжительность своих занятий.

Доступность обучения для любого человека - независимо от вашего географического и временного положения, вы можете получить образование дистанционно в любом ВУЗе, поддерживающем данные технологии, что позволяет удовлетворить образовательные потребности любого человека.

Скорость общения - эффективное осуществление обратной связи между преподавателем и студентом является неотъемлемым элементом процесса обучения.

Технологичность образовательного процесса - использование в процессе обучения новейших достижений и открытий информационных и телекоммуникационных технологий.

Социальное равноправие - подразумевает равные возможности получения дистанционного образования в независимости от места проживания, состояния здоровья, национальности и материального состояния обучаемого.

Творчество - благоприятные условия для творческого самовыражения студента в процессе усвоения знаний. Но существуют и очевидные минусы:

Отсутствие реального, «людского» общения между учениками и преподавателями. То есть отсутствуют все те моменты, связанные с индивидуальным подходом к обучению и воспитанием. А если рядом нет преподавателя, который обычно эмоционально окрашивает знания и способствует восприятию материала, это, конечно, значительный минус.

Целый ряд индивидуально-психологических условий отсутствует при домашнем обучении. Для получения дистанционного образования необходима регулярная жесткая самодисциплина, а результат обучения напрямую зависит от самостоятельности, способностей и самосознательности студента.

·Необходим постоянный доступ к источникам получения образовательных материалов (электронных учебников, видеоматериалов и т.д.). Для этого нужна хорошая техническая оснащенность дома, но не все желающие получить образование имеют компьютер и доступ к Интернету.

Отсутствие практических занятий, необходимых для закрепления теории и более качественного усвоения знаний.

Отсутствует регулярный контроль со стороны над обучающимся, что для русского человека является скорее отрицательным признаком. Мало кому удается самостоятельно перебороть лень. ·Обучающие электронные программы и курсы не всегда хорошо разработаны и удовлетворяют всем международным требованиям из-за недостаточной квалификации специалистов, создающих подобные учебные пособия, так как на сегодняшний день это ещё новое и недостаточно изученное направление.

В дистанционном образовании обучение ведется в основном только в письменной форме. Для некоторых студентов отсутствие возможности и требований излагать свои знания в устной форме может повлечь за собой некачественное усвоение знаний и множество других проблем Специфика дистанционной формы обучения оказывает влияние на отбор и структурирование содержания обучения.

Основной особенностью дистанционного обучения является интерактивность, возможность использования информационно-коммуникационных технологий для организации взаимодействия всех участников учебного процесса.

В дистанционном обучении могут применяться технологии совместной творческой деятельности (метод проектов), проблемные ролевые игры, кейс-метод, разнообразные формы контроля, как автоматизированные, так и открытые виды контроля и др.

Разнообразные виды деятельности, творческие задания, тщательно подобранные ссылки на надёжные источники интернет-ресурсов, а также интерактивные формы общения друг с другом и с преподавателем, способствуют повышению эффективности процесса обучения и защищённости обучаемых от негативной информации сети Интернет.

Мы рассматриваем современные педагогические технологии как средства информационной безопасности слушателей дистанционных курсов и как одно из условий для обеспечения информационной безопасности. К сожалению, многие разработчики курсов дистанционного обучения, сетевые преподаватели не уделяют должного внимания именно педагогическому аспекту. интернет обучение безопасность

Проблема обеспечения информационной безопасности процесса дистанционного обучения является сегодня особенно актуальной. Как было сказано выше, решение данной проблемы зависит от многих факторов: от медиаобразования, от сформированности критического мышления обучаемых, от профессиональной компетентности преподавателя, его мастерства и много другого.

Одним из условий обеспечения информационной безопасности является подготовка педагогических кадров, владеющих современными педагогическими и информационными технологиями организации учебного процесса с учётом особенностей дистанционного обучения.

На обеспечение информационной безопасности курса дистанционного обучения влияют все компоненты курса: цель, задачи, содержание курса, виды деятельности, педагогические технологии, методы, организационные формы, дополнительные источники, интернет-ресурсы, то есть, всё то, что

составляет информационно-образовательноую среду курса дистанционного обучения.

В научных исследованиях имеются различные подходы к определению информационной безопасности. В Доктрине информационной безопасности Российской Федерации даётся следующее определение: Информационная безопасность - это состояние защищённости национальных интересов Российской Федерации в информационной среде, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Понятие информационной безопасности Малых Т.А. понимает как состояние защищенности жизненно важных интересов личности, проявляющееся в умении выявлять и идентифицировать угрозы информационного воздействия и умении скомпенсировать негативные эффекты информационного воздействия ?7?.

Безопасность - это отсутствие угроз, либо состояние защищенности от угроз. Информация - это сведения (сообщения) независимо от формы их представления. Информационная безопасность - это отсутствие угроз со стороны информации.

В настоящее время важно не только создавать условия информационной безопасности учебного процесса, как в очной, так и в дистанционной форме обучения, но и формировать информационную безопасность на любом этапе обучения, начиная с дошкольного возраста.

Сущность сформированности информационной безопасности человека состоит в умении выявлять информационную угрозу; определять степень ее опасности; уметь предвидеть последствия информационной угрозы и противостоять им.

Информационно-образовательные ресурсы - это средства обучения, основанные на сетевых технологиях. К ним относятся:

- ресурсы в виде информационных источников (виртуальные библиотеки, музеи, электронные журналы и газеты, видео и аудиофайлы);
- образовательные программы, курсы дистанционного обучения;
- электронные учебно-методические пособия и др.

Образовательные ресурсы могут использоваться для обучения школьников (студентов) отдельным дисциплинам или комплексу дисциплин в виртуальной школе, виртуальном университете, ресурсном центре, а так же в системе повышения квалификации и подготовки педагогических кадров.

Использование интернет-ресурсов в учебном процессе может осуществляться в нескольких направлениях. Прежде всего, - это их интеграция в учебный процесс очного, очно-заочного или заочного обучения.

В данном случае учитель школы или педагог вуза интегрирует информационные ресурсы интернета или электронные учебно- методические пособия в программы обучения своему предмету, используя их на уроках (занятиях) в очной форме или в процессе подготовки к урокам (занятиям).

Исследуя проблему безопасности электронного обучения В.И.Зуев и Е.П.Чирко (Институт социальных и гуманитарных знаний, Казань) выделяют следующие угрозы нормальному функционированию системы электронного обучения:

- - неавторизованный доступ к цифровому контенту;
- - нарушение целостности и неадекватность учебных ресурсов;
- - нарушение нормального функционирования служб и сервисов;
- - нарушение безопасности процедур тестирования

Наряду с другими учёными, они доказывают, что источниками психолого -педагогических факторов риска являются как информационная среда, её ресурсы, так и сам человек, конкретный индивид. Они выделяют риски, связанные со студентами и риски, связанные с профессорско-преподавательским составом.

Риски, связанные со студентами:

- риск, связанный с неспособностью студента выдерживать заданный преподавателем и электронной системой темп обучения;
- риск, связанный с необходимостью постоянной мотивации студента;
- риск, связанный с неадекватной самооценкой и поведением студента;
- риск, связанный с неспособностью студента наладить контакт с преподавателем;
- технологический риск (высокая компетенция студента в области ИКТ, программного обеспечения и сервисов Web 2.0).

Риски, связанные с профессорско-преподавательским составом:

- риски, связанные с компетентностью ППС;
- риски, связанные с организацией учебного процесса;
- риски, возникающие непосредственно в ходе учебного процесса.

Безопасность электронного обучения, как считают В.И.Зуев и Е.П. Чирко, необходимо обеспечивать в нескольких взаимозависимых областях, которые и влияют на качество электронного обучения. Предложенная ими модель безопасности электронного обучения (см. рис.1) в виде куба, представляет три плоскости, включающие в себя среду, ресурсы и людей:

- среда - всемирная сеть интернет; веб-среда организации или учебного заведения; персональная веб-среда.
- ресурсы - программное обеспечение, информационные ресурсы, учебные ресурсы.
- люди - администрация, преподаватели, студенты

Информационно - коммуникационные технологии выступают как средства обучения для реализации определённых педагогических технологий.

Для обеспечения информационной безопасности курса дистанционного обучения сетевой преподаватель должен хорошо владеть методикой проведения дискуссий, ролевых и деловых игр в сети, мозгового штурма,

лабораторных работ, электронной лекции, телеконференции, видеоконференции, тематического вебсеминара и т.д. Эффективность дистанционного обучения во многом зависит от рационального использования в учебном процессе педагогических и информационных технологий.

Другое направление - это использование Интернет-ресурсов в учебном процессе дистанционного обучения.

В данном случае учебный процесс осуществляется средствами информационных и коммуникационных технологий, образовательной средой является Интернет, а Интернет-ресурсы составляют содержание дистанционного курса.

Однако курс дистанционного обучения можно рассматривать как самостоятельный образовательный ресурс интернета, и в тоже время, в содержание курса включать дополнительные материалы из информационно образовательных ресурсов интернета.

В этой связи, возникает угроза информационного плана, что требует от разработчиков и преподавателей курса тщательного отбора учебного материала и систематической проверки дополнительных источников на их достоверность и актуальность. Таким образом, отбор учебного материала для дистанционного обучения является одним из условий обеспечения информационной безопасности слушателей дистанционного курса.

Пути решения проблемы информационной безопасности подрастающего поколения лежат в педагогической области. Преподаватель, владеющий педагогическим мастерством, а, следовательно, и педагогическими технологиями способен организовать учебный процесс так, чтобы развивать информационную грамотность, навыки критического мышления, готовить сознание учащихся к противодействию угрозам негативной информации.

В этой связи проблема обучения информационной безопасности, как учеников, так и преподавателей, становится всё более актуальной в современном информационном обществе.

Система повышения квалификации и переподготовки педагогических работников, профессиональная подготовка студентов требует включения в содержание обучения материала по информационной безопасности, отвечающего критериям профессиональной направленности.

Обучение преподавателей педагогическим технологиям необходимо сочетать с обучением информационной безопасности.

Профессиональную компетентность преподавателя дистанционного обучения следует рассматривать с учётом обеспечения информационной безопасности учебного процесса.

2.2 Структура МСУИБ в сфере информационных технологий

Построение адаптивной системы обучения необходимо начать с разработки структуры данной системы. В предыдущей главе описаны основные требования к разрабатываемой системе. На основе анализа данных требований разрабатываемая система представима с точки зрения системного подхода с учетом входных и выходных параметров системы, поведения компонентов системы в процессе обучения.

Подсистема формирования модели обучающегося. Данная подсистема предназначена для формирования и коррекции модели обучающегося. Формирование модели происходит при добавлении нового пользователя в систему. Коррекция модели происходит по завершении каждого этапа обучения. Данная подсистема включает следующие элементы:

Модель обучающегося – совокупность характеристик обучающегося, измеряемых во время работы системы с обучающимся, и определяющая степень усвоения им знаний по изучаемому предмету и способы представления учебной информации. Значение данных характеристик

изменяется в процессе работы системы. Модель обучающегося является основным компонентом системы, с помощью которого реализуется адаптация. Более подробно модель обучающегося будет рассмотрена в следующем разделе.

База личностных тестовых заданий – набор тестовых заданий, предназначенных для определения индивидуальных особенностей обучающегося и формирования с их учетом модели обучающегося. Личностные тестовые задания являются элементами психологии. С их помощью можно определить наиболее предпочтительный для конкретного обучающегося способ представления информации (графическая, текстовая, схематическая и т.д.), оптимальный для усвоения за одно занятие дидактический объем учебного материала и т.д. Результаты личностных тестов позволяют определить исходные значения модели обучающегося, используемые при адаптации учебного материала. Данные значения будут корректируются в процессе обучения.

База параметров модели – набор различных характеристик обучающегося, соответствующих модели обучающегося, которые могут использоваться в процессе адаптации учебного материала. Из содержащихся характеристик будут выбраны подходящие для конкретного обучающегося.

Блок тестирования предназначен для определения личностных характеристик обучающегося. Определение личностных характеристик необходимо для дальнейшего создания психологического профиля обучающегося и определения параметров используемых для адаптации учебного материала к индивидуальным особенностям данного обучающегося. В данном блоке используются тестовые задания из описанной выше базы личностных тестов.

В блоке формирования модели происходит создание модели конкретного обучающегося. На основании результатов выполнения обучающимся личностных тестов из базы параметров модели выбираются

подходящие параметры и устанавливаются их значения. На начальных этапах обучения модель является неточной, в дальнейшем параметры модели обучающегося постоянно корректируются, тем самым, достигается высокая точность адаптации учебного материала.

Блок коррекции модели используется для корректировки значений параметров адаптации конкретного обучающегося после прохождения им тестового контроля знаний по завершении обучения. Учебный материал, предлагаемый обучающемуся, адаптируется исходя из параметров модели, сформированной по результатам личностного тестирования. Следует заметить, что личностное тестирование может недостаточно точно определить некоторые параметры адаптации (например предпочтительная форма представления материала). По результатам тестирования полученных в процессе обучения знаний можно уточнить данные параметры и подкорректировать их значение в модели.

Подсистема планирования обучения предназначена для определения целей обучения и формирования учебных элементов. Данный этап является очень важным в процессе обучения, так как для качественного обучения необходимо оптимальным образом сформировать учебный план, удовлетворяющий не только предпочтениям обучающегося, но и текущим требованиям рынка труда, тем самым, повысив дальнейшую конкурентоспособность обучающегося.

База тестовых заданий начального уровня содержит тесты для определения исходного уровня знаний обучающегося. Определение начального уровня знаний является необязательным этапом, так как, зачастую, обучающийся начинает изучение совершенно неизвестной ему области, в которой у него отсутствуют какие-либо знания. Тем не менее, в ряде случаев это необходимый этап, позволяющий исключить из учебного плана уже известный материал и, тем самым, оптимизировать процесс обучения.

Блок формирования целей обучения необходим для определения конечного результата, который должен быть достигнут. Данные выводы делаются на основании знаний, которыми пользователь уже обладает по каждому из разделов учебного курса. На данном этапе знания обучающегося по каждому из разделов могут быть отнесены к некоторым нечетким группам «отличные», «хорошие» и т.д. В зависимости от того, к какой группе отнесены знания по каждому разделу, будут расставлены приоритеты и определены затраты на изучение каждого из них. Например, если по некоторому разделу уровень знаний обучающегося определен как «отличный», то этот раздел потребует минимум времени на изучение и повторение, а раздел, по которому знания отсутствуют вообще, будет рассмотрен максимально подробно.

Блок формирования плана обучения необходим для составления последовательности работы системы в процессе обучения конкретного обучающегося. На основании сформированных ранее целей обучения формируется строгая последовательность предлагаемых пользователю учебных разделов с установленными приоритетами. На следующем этапе формируются учебные элементы, то есть единицы учебного материала, предлагаемые обучающемуся для изучения. Как правило, под учебным элементом понимается некоторая часть учебного контента, которая полностью раскрывает определенную часть учебной дисциплины и, в то же время по дидактическому(смысловому) объему, может быть усвоена за одно занятие. В качестве учебного элемента может рассматриваться тема объемом 15-12 тысяч символов текста. Если в материале присутствуют формулы, диаграммы или таблицы, то этот символьный объем одного учебного элемента уменьшается.

Для формирования учебных элементов используются два ресурса: база знаний учебного материала и модель адаптации. Рассмотрим их более подробно.

База знаний – база данных, разработанная для оперирования знаниями (метаданными). Полноценные базы знаний содержат в себе не только фактическую информацию, но и правила поиска, вывода и обработки информации. Применительно к адаптивной образовательной системе под фактической информацией понимается непосредственно материал учебного курса, а под метаданными понимаются параметры данного материала, используемые для адаптации к индивидуальному обучающемуся и для формирования учебных элементов.

Модель адаптации – математическая модель, описывающая взаимодействие адаптивной системы с базой знаний в процессе обучения с использованием параметров модели обучающегося. В модели адаптации описаны правила выборки учебного материала с учетом параметров адаптации, а также описан процесс внесения изменений в модель обучающегося в процессе обучения. Модель адаптации использует алгоритмы, основанные на способе реализации базы знаний. Так, например, если для представления базы знаний адаптивной системы используются семантические сети, то модель адаптации может быть основана на алгоритмах теории графов.

Блок обучения находится вне выделенных подсистем. В данном блоке обучающемуся предлагается сформированные для изучения учебные элементы.

Подсистема оценки результатов обучения необходима не только для контроля качества знаний, но и для определения соответствия результатов обучения поставленным ранее целям.

После завершении обучения необходимо проверить уровень полученных знаний обучающегося, сделать выводы о достижении целей обучения, скорректировать при необходимости модель обучающегося и определить дальнейшие действия. Для реализации всех вышеперечисленных действий служит подсистема оценки результатов обучения.

Одним из основных ресурсов подсистемы является база тестовых заданий для оценки результатов обучения. Тестовые задания обладают атрибутами, позволяющими адаптировать процесс тестирования обучающегося. Например, если модель содержит информацию о предпочтительной для обучающегося форме представления заданий (открытая, закрытая, задания на соответствие и т.д.), то тестовые задания будут выбраны согласно данному параметру.

В блоке тестирования обучающемуся предлагается выполнить тестовые задания. После тестирования, в блоке коррекции тестовых заданий будет произведено изменения параметра сложности каждого задания. Завершение тестирования является также основой для выполнения блока коррекции модели обучающегося.

В блоке блок оценки достижения целей проверяется, были ли достигнуты цели, поставленные на этапе формирования целей обучения. Если уровень знаний обучающегося по разделу достиг уровня «отлично» или «хорошо», то можно сделать вывод что раздел изучен. В противном случае считается, что цель по данному разделу не достигнута.

Поле оценки достижения целей принимается решение о дальнейшем поведении системы. Если все поставленные цели достигнуты, то обучение можно считать завершенным. В противном случае происходит переход в блок формирования целей, где вновь определяются необходимые для повторного изучения разделы.

Помимо структуры разрабатываемой МСУИБ необходимо так же представить ее функциональную модель, которая позволяет представить последовательность процессов, протекающих в МСУИБ . В рамках стандарта IDEF0 функционального моделирования и графической нотации, предназначенного для формализации и описания процесса функционирования разрабатываемых систем, каждому процессу поставлены в соответствие:

- входные данные;
- выходные данные;
- стандарты и нормативы;
- ресурсы, необходимые для протекания данных процессов.

В качестве стандартов и нормативов в процессе функционирования МСУИБ выступают:

- образовательные стандарты;
- требования рынка труда;
- стандарты функционирования систем дистанционного обучения.

2.3 Разработка модели обучающегося

Важным параметром МСУИБ является качество взаимодействия ее с пользователем. Необходимо учитывать как предопределенные параметры адаптации (предпочтительный стиль обучения, выбранная предметная область), так и динамически изменяющиеся в процессе обучения (уровень подготовки, текущие цели и компетенции). Вся необходимая информация хранится в модели обучающегося. Основой разработки качественной адаптивной системы является разработка модели обучающегося.

Модель обучающегося – совокупность характеристик обучающегося, измеряемых во время работы системы с обучающимся, и определяющей степень усвоения им знаний по изучаемому предмету, а также методы (правила) обработки этой совокупности. В первую очередь, эти правила должны проводить изменения самой модели обучающегося по результатам его работы с системой.

Модель обучающегося должна включать в себя информацию: о цели обучения; о знаниях обучающегося в рамках изучаемого курса (текущее состояние процесса обучения); об особенностях подачи учебных материалов и выбора контрольных заданий и вопросов;

В процессе обучения МСУИБ активно использует модель обучающегося, постоянно корректируя ее параметры, а также на их основе адаптирует процесс обучения, делая его максимально эффективным для каждого обучающегося. Разрабатываемая система предполагает итерационный подход к процессу обучения, то есть в процессе обучения пользователь проходит многочисленные этапы. В начале каждого этапа определяются цели обучения, формируется учебный план. По завершении каждого этапа происходит анализ достижения целей, корректировка параметров модели обучающегося, которые будут учтены в очередном этапе и т.д.

Модель обучающегося содержит параметры, приведенные в таблице 2.1.1.

Таблица 2.1.1 – Параметры модели обучающегося

Тип данных	**Профиль**	**Характеристики**
Неизменяемые данные	Базовый профиль	Персональная информация (ПИ)
		Предыдущее образование (ПО)
		Квалификация (К)
		Первоначальные знания (ПЗ)
		Недостатки (Н)
	Психологический профиль	Стиль обучения (СО)
		Познавательные способности (ПС)
		Профессиональная ориентированность (ПрО)
Изменяемые данные		Цели обучения (ЦО)
		Учебный план (УП)
		Данные предыдущих этапов (ДПЭ)
		Полученные знания (ПоЗ)
		Результаты тестирования (РТ)
		Приобретенные навыки (ПН)

Как видно, в модели (рисунок 2.2.1) присутствуют как постоянные (неизменяемые) данные, так и данные, постоянно корректируемые в процессе обучения (цели обучения, учебный план, полученные знания, результаты тестирования)

Модель обучающегося представим в виде структуры с множеством элементов, как динамически меняющихся, так и неизменных на протяжении всего обучения.

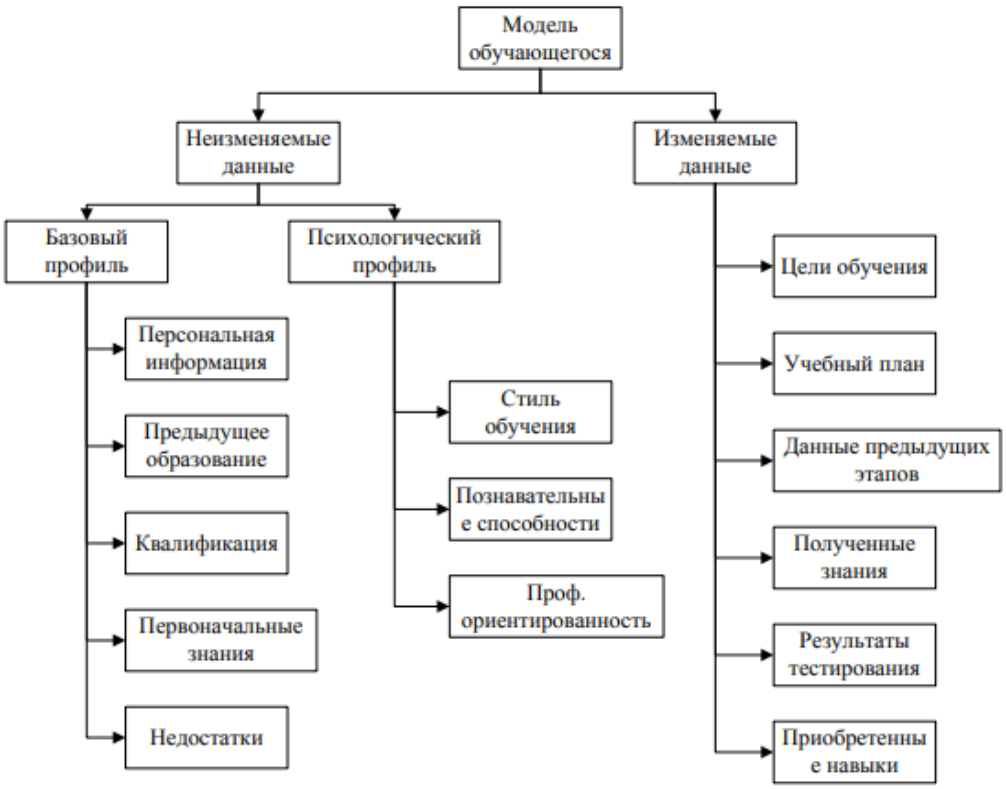

Рисунок 2.2.1 – Структура компонентов модели обучающегося

Преимуществом данной модели является возможность хранить в ней всю необходимую для адаптации и последующего анализа информацию.

2.4 Разработка математической модели взаимодействия информационных процессов МСУИБ

Информационный процесс – совокупность последовательных действий (операций), производимых над информацией (в виде данных, сведений,

фактов, идей, гипотез, теорий и пр.) для получения какого-либо результата (достижения цели).

МСУИБ в сфере информационных технологий представляет собой сложный объект, в состав которого входит множество отдельных подсистем. Каждая из подсистем является отдельным информационным процессом. На каждом этапе обучения происходит сбор, обработка и накопление большого количества информации. Необходимо разработать математическую модель взаимодействия информационных процессов.

Данная модель позволит структурировать используемую в процессе работы системы информацию, а так же прогнозировать состояние системы на любом этапе обучения, изменяя входные данные.

Первым этапом моделирования будет определения характера взаимодействия системы с внешней средой. Для этого необходимо определить входные и выходные параметры системы. Как показано на рисунке 2.3.1, на систему в процессе ее работы оказывается ряд воздействий со стороны внешней среды и со стороны обучающегося.

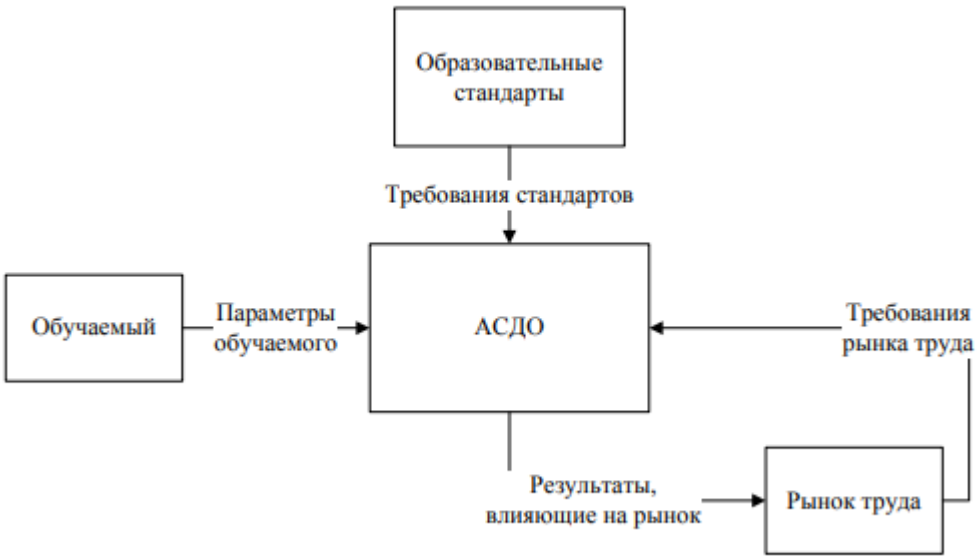

Рисунок 2.3.1 – Входные и выходные параметры системы

Данные воздействия разделены на три группы:

1. Требования образовательных стандартов;
2. Требования рынка труда;
3. Параметры обучающегося.

В рамках взаимодействия каждого обучающегося с системой данные воздействия разделяются на статические и динамические. К статическим относятся требования стандартов и рынка труда, так как данные требования не изменяются в процессе обучения. Параметры обучающегося являются динамическими, так как они изменяются в процессе обучения.

Множество значений входных воздействий, реализуемых за весь период функционирования системы, назовем входным процессом и обозначим через Xt , тогда

$$X_t = \{x(t) : t \in T\}.$$

Множество значений входных воздействий Xt , как сказано выше, необходимо разделить на два подмножества:

X D множество значений динамических воздействий, имеющих различные значения в каждый момент времени t ;

Xs множество значений статических воздействий, неизменных на всем периоде обучения

Таким образом,

$$X_t = \{X_D, X_S\}.$$

Множество значений выходных воздействий, реализуемых за весь период функционирования системы, назовем выходным процессом и обозначим через Yt , тогда

$$Y_t = \{y(t) : t \in T\}.$$

Между входными и выходными параметрами системы существует связь, запишем ее в виде уравнения

$$A(T, X_t, Y_t) = 0.$$

К примеру, из указанных выше входных и выходных параметров видно, что идентификационная информация обучающегося, поступая на вход системы, позволяет получить на выходе содержимое личного профиля обучающегося. Данная зависимость входных и выходных параметров в рамках системы дистанционного обучения хорошо просматривается в технологии реализации клиент-серверных программ «запрос – ответ». Данная технология предусматривает поведение системы, расположенной на сервере, определяемое входными параметрами со стороны обучающегося.

Однако не всегда существуют прямые зависимости между входными и выходными параметрами системы. Зачастую поступающий входной параметр изменяет внутреннее свойство системы, которое будет использовано для дальнейшей ее работы.

Совокупность внутренних свойств системы, определенных на момент времени, обозначим через z( ) и учтем в (1), которое будет иметь следующий вид

$$B(T, z(\xi), X_t, Y_t) = 0.$$

Появление в уравнении z ( ) преследует одну цель – обеспечить однозначную связь между Xt и Yt . По своему смыслу z( ) представляет собой совокупность существующих свойств системы, знание которых в настоящий момент времени позволяет определить ее поведение в будущем.

Перепишем уравнение в следующем виде:

$$Y_t = G(T, z(\xi), X_t),$$

где G – оператор выходов;

Такое представление системы является более удобным, так как позволяет определить выходные параметры системы

Исходя из уравнения следует, что в любой момент времени система находится в некотором состоянии, следовательно, уравнение может быть записано для любого t T и фрагмента выходного процесса Xt .

Таким образом,

$$Y_{t\eta} = G(t\eta, z(\xi), X_{t\eta}),$$

где $t\eta$ – интервал времени $[t,\eta]$.

Рассмотрим не весь выходной процесс Yt или его фрагмент Yt , а выходное воздействие y( ) . Тогда из (3) и (4),учитывая, что ( ) t t y Y Y , получим

$$y(\eta) = G(T, z(\xi), X_t);\ y(\eta) = G(t\eta, z(t), X_{t\eta}).$$

На интервале $t\eta$ можно приравнять правые части уравнения

$$G(t\eta, z(t), X_{t\eta}) = G(T, z(\xi), X_t).$$

где H – оператор, устанавливающий однозначную зависимость zt() от пары (( ),) z X t , которая задана на интервале t и называется оператором перехода

Уравнение называется уравнением состояния. Оно определяет конечное состояние системы zt по заданным начальному состоянию z( ) и фрагменту входного процесса Xt

До сих пор мы предполагали, что на входы и на выходе системы в каждый момент времени t имеется одно входное xt( ) и одно выходное y t( ) воздействия. В реальной ситуации таких воздействий может быть несколько. В таком случае необходимо рассматривать входные и выходные параметры как векторные величины 1 ( ) (( ),..., ( )) N x t x t x t и 1 ( ) (( ),..., ( )) M y t y t y t , компоненты которых ( ) n x t и ( ) m y t представляют собой значения n -го входного и m-го выходного воздействия. Пусть ( ) n n x t X , ( ) m m y t Y для всех t T , X n и Y m будем называть множествами допустимых значений воздействий ( ) n x t и ( ) m y t соответственно. Декартово произведение

$$X^N = X_1 \times ... \times X_N$$

образует пространство входных воздействий такое, что любой набор входных воздействий, реализуемых в момент времени t T , задается точкой (вектором) ( ) n x t X . Аналогично для вектора выходных воздействий y t( ) вводится пространство выходных воздействий 1 ... M Y Y Y M .

Ранее мы отмечали, что состояние системы представляет собой набор ее внутренних свойств. Пространство состояний представим, так же, в виде декартова произведения 1 ... K Z Z Z K .

ГЛАВА 3. РАЗРАБОТКА МОДЕЛИ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Оценка уровней выполнения функций безопасности

Настоящая Методика оценки угроз безопасности информации (далее – Методика) разработана в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

Методика определяет порядок и содержание работ по определению угроз безопасности информации, реализация (возникновение) которых возможна в информационных системах, автоматизированных системах управления, информационно-телекоммуникационных сетях, информационнотелекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах (далее – системы и сети), а также по разработке моделей угроз безопасности информации систем и сетей.

Методика применяется для определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях, отнесенных к государственным и муниципальным информационным системам, информационным системам персональных данных, значимым объектам критической информационной инфраструктуры Российской Федерации, информационным системам управления производством, используемым организациями оборонно-промышленного комплекса, автоматизированным системам управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

В иных случаях решение о применении настоящей Методики принимается обладателями информации или операторами систем и сетей.

В документе не рассматриваются методические подходы по оценке угроз безопасности информации, связанных с нарушением безопасности шифровальных (криптографических) средств защиты информации, а также угроз, связанных с техническими каналами утечки информации.

Методика ориентирована на оценку антропогенных угроз безопасности информации, возникновение которых обусловлено действиями нарушителей.

На основе настоящей Методики могут разрабатываться отраслевые (ведомственные, корпоративные) методики оценки угроз безопасности информации, которые учитывают особенности функционирования систем и сетей в соответствующей области деятельности. Разрабатываемые отраслевые (ведомственные, корпоративные) методики оценки угроз безопасности информации не должны противоречить положениям настоящей Методики.

В Методике используются термины и определения, приведенные в приложении 1 к настоящей Методике, а также термины и определения, установленные законодательством Российской Федерации и национальными стандартами в области защиты информации и обеспечения информационной безопасности

Положения настоящей Методики применяются для оценки угроз безопасности информации в системах и сетях, решение о создании или модернизации (развитии) которых принято после даты ее утверждения, а также в эксплуатируемых системах и сетях.

Модели угроз безопасности информации систем и сетей, разработанные и утвержденные до утверждения настоящей Методики, продолжают действовать и подлежат изменению в соответствии с настоящей Методикой при развитии (модернизации) соответствующих систем и сетей.

В связи с утверждением настоящего методического документа не применяются для оценки угроз безопасности информации

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК России, 2008 г.) и Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (ФСТЭК России, 2007 г.)

3.1.1.Порядок оценки угроз безопасности информации

Оценка угроз безопасности информации проводится в целях определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях с заданной архитектурой и в условиях их функционирования – актуальных угроз безопасности информации.

Основными задачами, решаемыми в ходе оценки угроз безопасности информации, являются:

- определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
- инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;
- определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;
- оценка способов реализации (возникновения) угроз безопасности информации;
- оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;
- оценка сценариев реализации угроз безопасности информации в системах и сетях

Исходными данными для оценки угроз безопасности информации являются:

- общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;
- описания векторов (шаблоны) компьютерных атак, содержащиеся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);
- документация на системы и сети (а именно: техническое задание на создание систем и сетей, частное техническое задание на создание системы защиты, программная (конструкторская) и эксплуатационная (руководства, инструкции) документация, содержащая сведения о назначении и функциях, составе и архитектуре систем и сетей, о группах пользователей и уровне их полномочий и типах доступа, о внешних и внутренних интерфейсах, а также иные документы на системы и сети, разработка которых предусмотрена требованиями по защите информации (обеспечению безопасности) или национальными стандартами);
- договоры, соглашения или иные документы, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (в случае функционирования систем и сетей на базе

информационно - телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры);

- нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и функционируют системы и сети, содержащие в том числе описание назначения, задач (функций) систем и сетей, состав обрабатываемой информации и ее правовой режим;
- технологические, производственные карты или иные документы, содержащие описание управленческих, организационных, производственных и иных основных процессов (бизнес-процессов) в рамках выполнения функций (полномочий) или осуществления видов деятельности обладателя информации, оператора (далее – основные (критические) процессы);
- результаты оценки рисков (ущерба), проведенной обладателем информации и (или) оператором.

Указанные исходные данные могут уточняться или дополняться с учетом особенностей области деятельности, в которой функционируют системы и сети.

Оценка угроз безопасности информации должна носить систематический характер и осуществляться как на этапе создания систем и сетей, так и в ходе их эксплуатации, в том числе при развитии (модернизации) систем и сетей. Систематический подход к оценке угроз безопасности информации позволит поддерживать адекватную и эффективную систему защиты в условиях изменения угроз безопасности информации и информационных ресурсов и компонентов систем и сетей. Учет изменений угроз безопасности информации обеспечит своевременную выработку адекватных и эффективных мер по защите информации (обеспечению безопасности) в системах и сетях.

На этапе создания систем и сетей оценка угроз безопасности информации проводится на основе их предполагаемых архитектуры и

условий функционирования, определенных по результатам изучения и анализа исходных данных на них. В ходе эксплуатации систем и сетей, в том числе при развитии (модернизации) систем и сетей, оценка угроз безопасности информации проводится для реальной архитектуры систем и сетей и условий их функционирования, полученных по результатам анализа исходных данных, инвентаризации информационных ресурсов, анализа уязвимостей и (или) тестирования на проникновение систем и сетей, а также иных методов исследований уровня защищенности систем и сетей и содержащейся в них информации.

По результатам оценки, проведенной в соответствии с настоящей Методикой, должны быть выявлены актуальные угрозы безопасности информации, реализация (возникновение) которых может привести к нарушению безопасности обрабатываемой в системах и сетях информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств ее обработки) и (или) к нарушению, прекращению функционирования систем и сетей.

На этапе создания систем и сетей результаты оценки угроз безопасности информации должны быть направлены на обоснование выбора организационных и технических мер по защите информации (обеспечению безопасности), а также на выбор средств защиты информации и их функциональных возможностей.

На этапе эксплуатации систем и сетей результаты оценки угроз безопасности информации должны быть направлены на оценку эффективности принятых технических мер, в том числе используемых средств защиты информации

Оценка угроз безопасности информации проводится подразделением по защите информации (отдельными специалистами, назначенными ответственными за обеспечение защиты информации (обеспечение

безопасности)) обладателя информации или оператора с участием подразделений или специалистов, ответственных за эксплуатацию систем и сетей (ИТ-специалистов, специалистов автоматизированных систем управления, специалистов связи и др.), основных (профильных) подразделений обладателя информации или оператора. Для оценки угроз безопасности информации по решению обладателя информации или оператора в соответствии с законодательством Российской Федерации могут привлекаться специалисты сторонних организаций.

Для оценки угроз безопасности информации рекомендуется привлекать специалистов, обладающих следующими знаниями и умениями:

- основ оценки рисков, а также основных рисков от нарушения функционирования систем и сетей и нарушения безопасности обрабатываемой информации (далее – информационные риски);
- угроз безопасности информации и способов их реализации (возникновения);
- тактик и техник проведения компьютерных атак (реализации угроз безопасности информации);
- основных типов компьютерных инцидентов и причин их возникновения; основных уязвимостей систем и сетей;
- нормативных правовых актов по созданию и функционированию систем и сетей, защите информации (обеспечению безопасности) в них, основных (критических) процессов (бизнес-процессов) обладателя информации и (или) оператора;
- оценивать информационные риски;
- классифицировать и оценивать угрозы безопасности информации;
- определять сценарии (тактики, техники) реализации угроз безопасности информации;
- определять источники и причины возникновения компьютерных инцидентов;

- проводить инвентаризацию систем и сетей, анализ уязвимостей, тестирование на проникновение систем и сетей с использованием соответствующих автоматизированных средств;
- оценку уровня защищенности (аудит) систем и сетей и содержащейся в них информации.

Оценка угроз безопасности информации проводится с использованием экспертного метода. В интересах снижения субъективных факторов при оценке угроз безопасности информации рекомендуется создавать экспертную группу. Рекомендации по формированию экспертной группы и проведению экспертной оценки угроз безопасности информации приведены в приложении 2 к настоящей Методике.

При оценке угроз безопасности информации могут использоваться программные средства, позволяющие автоматизировать эту деятельность.

Для получения (уточнения) отдельных исходных данных (например, объектов воздействия и их интерфейсов, уязвимостей) в интересах оценки угроз безопасности информации на этапе эксплуатации систем и сетей применяются автоматизированные средства инвентаризации систем и сетей, анализа уязвимостей, тестирования на проникновение систем и сетей, а также иные средства, используемые для исследований уровня защищенности систем и сетей и содержащейся в них информации.

В случае оценки угроз безопасности информации для систем и сетей, функционирующих на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, угрозы безопасности информации определяются как для самих систем и сетей, так и для информационно-телекоммуникационной инфраструктуры, на которой они функционируют

2.11. При размещении систем и сетей на базе информационно телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, принадлежащей поставщику услуг, оценка угроз

безопасности информации проводится оператором во взаимодействии с поставщиком услуг.

В случае размещения систем и сетей на базе информационно телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, для которой поставщик услуг не оценил угрозы безопасности информации или не представил результаты такой оценки, оператор при оценке угроз безопасности информации исходит из предположения, что информационно-телекоммуникационная инфраструктура центра обработки данных или облачная инфраструктура, являющаяся средой функционирования для его систем и сетей, подвержена угрозам безопасности информации (скомпрометирована нарушителем с максимальным уровнем возможностей).

Результаты оценки угроз безопасности информации отражаются в модели угроз, которая представляет собой описание систем и сетей и актуальных угроз безопасности информации. Рекомендуемая структура модели угроз безопасности информации приведена в приложении 3 к настоящей Методике.

По решению обладателя информации или оператора модель угроз безопасности информации разрабатывается как для отдельной системы или сети, так и для совокупности взаимодействующих систем и сетей оператора. При разработке модели угроз безопасности информации для отдельной системы и сети, она должна содержать описание угроз безопасности информации, актуальных для информационно-телекоммуникационной инфраструктуры, на базе которой эта система или сеть функционирует, а также угроз безопасности информации, связанных с интерфейсами взаимодействия со смежными (взаимодействующими) системами и сетями.

Допускается разработка одной модели угроз безопасности информации для нескольких однотипных создаваемых систем и сетей обладателя информации или оператора.

Модель угроз безопасности информации должна поддерживаться в актуальном состоянии в процессе функционирования систем и сетей.

В процессе функционирования систем и сетей. Ведение модели угроз безопасности информации и поддержание ее в актуальном состоянии может осуществляться в электронном виде с учетом приложения 3 к настоящей Методике.

Изменение модели угроз безопасности информации осуществляется в случаях:

- изменения требований нормативных правовых актов Российской Федерации, методических документов ФСТЭК России, регламентирующих вопросы оценки угроз безопасности информации
- изменений архитектуры и условий функционирования систем и сетей, режима обработки информации, правового режима информации, влияющих на угрозы безопасности информации;
- выявления, в том числе по результатам контроля уровня защищенности систем и сетей и содержащейся в них информации (анализа уязвимостей, тестирований на проникновение, аудита), новых угроз безопасности информации или новых сценариев реализации существующих угроз;
- включения в банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru) сведений о новых угрозах безопасности информации, сценариях (тактиках, техниках) их реализации.

Оценка угроз безопасности информации включает следующие этапы:

- определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
- определение возможных объектов воздействия угроз безопасности информации;
- оценку возможности реализации (возникновения) угроз безопасности информации и определение их актуальности.

3.2 Анализ системы дистанционного образования

Затронута проблема информационной безопасности систем дистанционного образования вуза. Проанализирована архитектура и функции типовой системы дистанционного образования. Выявлены наиболее уязвимые и критичные места. Проведен анализ причин и последствий нарушения информационной безопасности системы дистанционного образования. Выделены три основных направления защиты системы дистанционного образования. Показана необходимость периодической оценки защищенности системы. Разработана и математически описана модель оценки защищенности системы дистанционного образования. Разработан программный прототип, автоматизирующий предложенную модель. Проведены экспериментальные исследования модели оценки защищенности системы дистанционного образования. Сделаны выводы о применимости и эффективности модели. The security problem of distance education systems affected by the article. Architecture and functions typical of distance education system are analyzed. The distance education system vulnerabilities are revealed. The causes and consequences of violations of information security in distance education system analysis. The three main areas of protection are marked. The need for periodic evaluation of the security of the system is shown. Developed and formalized assessment model described the security system of distance education. The software prototype that automates the proposed model developed. Experimental studies of security evaluation model of distance education. Conclusions about the applicability and effectiveness of the model are made.

В связи с активным совершенствованием информационных технологий и распространением локальных и глобальных сетей, все большее значение в успешной деятельности практически любого вуза приобретает наличие системы дистанционного образования. И это не только требование современных федеральных образовательных стандартов, в области высшего

образования, но и жизненная необходимость, поскольку «…современное дистанционное образование дает равные возможности всем людям независимо от социального положения (студентам, гражданским и военным, безработными и т. д.) в любых районах страны и за рубежом реализовать права человека на образование и получение информации» [1]. Как показывает практика, системы дистанционного образования (СДО) представляют собой гетерогенные, распределенные приложения, которые строятся на базе информационной системы (ИС) вуза и активно используют web-ресурсы для организации интерактивного взаимодействия обучающихся и преподавателя. В процессе своего функционирования данная система подвергается ряду негативных воздействий случайного и умышленного характера, что в результате может привести к нарушению информационной безопасности не только СДО, но и всей ИС вуза, а также нанести ущерб всем участникам образовательного процесса. Соответственно, для снижения ущерба от подобных воздействий и предотвращения рисков информационной безопасности (ИБ) необходимо применять специализированные средства и механизмы защиты. При этом объем и виды мероприятий принимаемых для защиты информации зависят не только от желания и возможностей вуза, но и определяется рядом обязательных требований регуляторов: ФСТЭК России, ФСБ России, Роскомнадзор и др. А для контроля над эффективностью системы защиты и мероприятий по устранению последствий инцидентов ИБ, а также степенью выполнения требований регуляторов к уровню обеспечения ИБ следует проводить регулярную оценку уровня защищенности СДО и ИС вуза.

В настоящее время существуют множество подходов к оценке защищенности информации в различных системах [2 - 6], однако, большинство из них являются универсальными и требуют адаптации к конкретному виду систем и специфики их использования. В связи с этим, актуальной задачей является разработка новых и модернизация

существующих подходов к оценке защищенности, которые учитывали именно особенности организации и функционирования СДО вуза

Проблемы информационной безопасности СДО

Для выявления ключевых проблем ИБ, причин и источников их возникновения, а также оценки их последствий, необходимо предварительно рассмотреть типовую СДО и выявить в ней наиболее критичные и уязвимые места. Анализ литературных источников [7-9] показывает, что СДО является частью ИС системы вуза, часть функциональных компонентов которой, в виде веб-приложения, вынесена в глобальную сеть (рисунок 3.1.1).

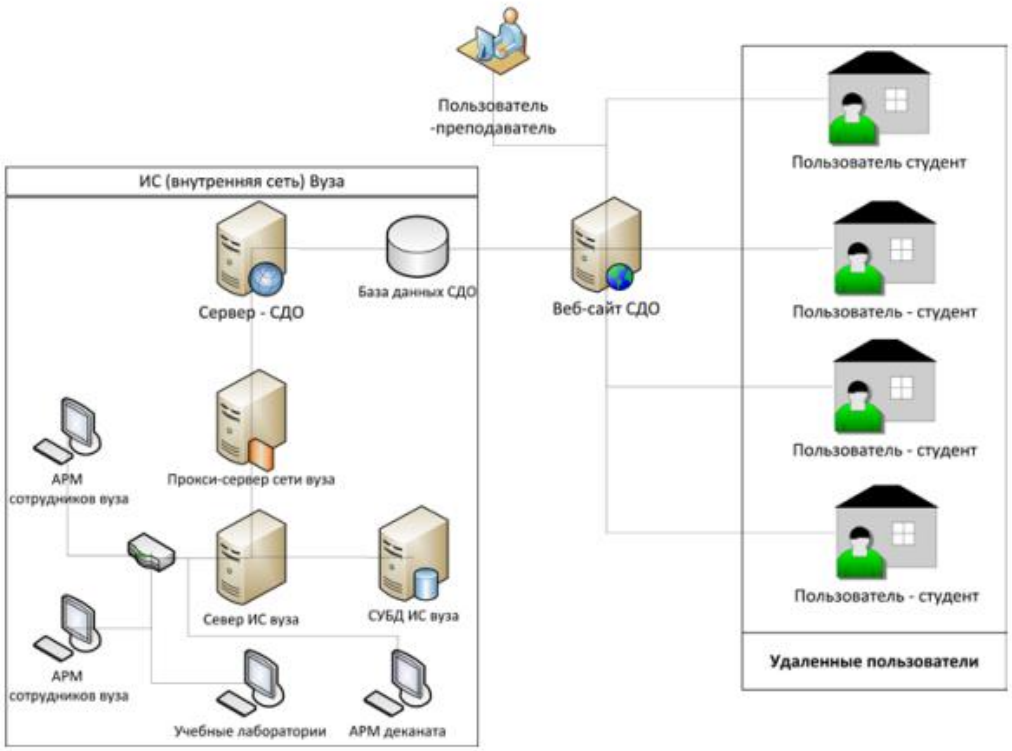

Рисунок 3.1.1 – Типовая архитектура СДО

В качестве основных функциональных компонентов СДО можно выделить:

1. веб-приложение - внешний интерфейс, предназначенный для организации удаленного доступа студентов к содержанию учебных курсов, презентациям, мультимедийным материалам, тестам и интерактивного взаимодействия с преподавателем, например посредством вебинара и/или видеоконференций;

2. база данных, в которой храниться наполнение учебных курсов, размещаются оценочные материалы, электронные учебники, информация для студентов и данные об успеваемости;

3. сервер СДО, являющийся ядром системы и обеспечивающий следующие функциональные возможности:

- регистрация и управление учетными записями пользователей СДО;
- разграничение прав доступа к функциям и наполнению СДО;
- предоставление доступа к ресурсам как удаленным пользователям из глобальной сети, так внутренним пользователям локальной сети вуза;
- администрирование и защита СДО;
- учет обучаемых;
- создание и импорт учебных материалов;
- управление каталогами курсов;
- отслеживание результатов обучения и тестирования;
- регистрация информации о событиях в СДО;
- взаимодействие с другими компонентами внутренней информационной инфраструктуры вуза.

Основными субъектами взаимодействия в рамках СДО являются внутренне и внешние пользователи, которых можно разделить на следующие группы:

1. преподаватели вуза – создают учебные курсы, контролируют учебный процесс, проводят on-line консультации;

2. методисты вуза – комплектует группы, управляет учебным процессом, наполняют содержимым и обновляют материалы курсов, осуществляет взаимодействие с преподавателями;

3. администраторы, программисты, специалисты по информационной безопасности информационных подразделений вуза – обеспечивают администрирование и защиту СДО, отслеживают события и инциденты, связанные с функционированием СДО;

4. студенты – изучают курсы, проходят тестирование, осваивают учебный план.

В соответствии с выделенными функциональными подсистемами и субъектами типовой технологический процесс обработки информации в СДО допустимо представить следующим образом:

1. подключение пользователя к веб-сайту СДО;
2. авторизация пользователя на сервере СДО;
3. запрос на сервер СДО на предоставление информации и доступа к ресурсам курсов и подсистем СДО;
4. ввод, модификация или вывод информации открытого и/или ограниченного доступа;
5. получение пользователем запрошенного материала и данных;
6. отключение пользователя от ресурсов СДО.

При таком технологическом процессе наиболее уязвимыми с точки зрения информационной безопасности будут процессы:

- передачи идентификационных и аутентификационных данных пользователя СДО;
- обмен данными между браузером удаленного пользователя и веб-сайтом СДО.
- авторизации пользователя в СДО (на сервере СДО и в ИС вуза);
- извлечение и запись данных в БД СДО и ИС вуза;
- обмен данными между сервером СДО и сервером ИС вуза.

Подобное заключение в первую очередь связано с тем, что именно в процессе выполнения данных действий, наиболее вероятна попытка злоумышленника реализовать атаку на СДО и получить доступ к ее ресурсам, сервисам и данным. Это подтверждается и статистикой [10] по нарушениям и инцидентам ИБ, которая показывает, что основным источником нарушений является сеть, включая браузер, сетевые ресурсы и сервисы, на долю которых приходиться 39,6% всех нарушений. Злоумышленник может быть как

внешним (32%), так и внутренним (61,5%) и, с учетом [11], при реализации атаки преследовать следующие цели:

- получение несанкционированного доступа к ресурсам и сервисам СДО
- превышение привилегий и получение контроля над СДО;
- получение через взломанную СДО несанкционированного доступа к внутренней ИС вуза;
- кража материалов и интеллектуальной собственности: учебных материалов, оценочных материалов и материалов, создаваемых коллективно участниками учебного процесса;
- получение доступа к персональным данным студентов и сотрудников вуза;
- кража и разглашение персональных данных студентов и сотрудников вуза;
- получение несанкционированного доступа и внесение изменений в базы данных учебных ведомостей;
- получение несанкционированного доступа к внутренней служебной и другой конфиденциальной информации, хранящейся и обрабатываемой в ИС вуза;
- получение несанкционированного доступа и кража результатов научно исследовательской и инновационной деятельности вуза;
- нарушение целостности и/или уничтожение учебных материалов и данных об учебном процессе;
- нарушение доступности веб-сайта и сервера СДО;
- нарушение доступности информации и материалов учебных курсов для пользователей СДО.

Анализ [12, 13] показывает, что при реализации атак, злоумышленник использует:

- уязвимости в веб-приложении и сервисах СДО;

- слабые пароли и недостатки процесса аутентификации пользователей на сервере СДО;
- ошибки в конфигурировании и администрировании СДО;
- вредоносное программное обеспечение (вирусы, троянские программы, руткиты, программные бомбы и закладки);
- слабости системы защиты информации.

По данным исследования PositiveTechnologies [14] более половины (57%) систем подвергшимся воздействиям со стороны злоумышленника содержали критические уязвимости, связанные с использованием устаревших версий программного обеспечения и операционных систем. Средний возраст наиболее устаревших неустановленных обновлений составляет 32 месяца. Наибольшим числом уязвимостей, в соответствии с [15], эксплуатируемых злоумышленником при атаке из внешней сети (например, интернет), обладают следующие виды прикладным программ, активно использующиеся в СДО:

- браузеры, используемые пользователями СДО при доступе к веб-сайту;
- Adobe Reader, Adobe Flash Player и OracleJava, которые используются при выполнении скриптов, а также чтении и загрузки документов и мультимедиа файлов.

В среднем для получения доступа к СДО внешнему злоумышленнику требуется использовать лишь две уязвимости. Для проведения атаки в 82% случаев злоумышленнику достаточно иметь среднюю или низкую квалификацию и лишь в 17% случаев злоумышленник должен обладать высокой квалификацией для получения доступа к критически важным ресурсам, а в половине всех систем успешные атаки возможны со стороны любого неквалифицированного пользователя, в том числе и студента

Помимо умышленных угроз и атак злоумышленника на СДО могут воздействовать угрозы и дестабилизирующие факторы случайного характера. К ним относят катастрофы природного, биолого-социального и техногенного

характера, сбои и отказы программно-аппаратного обеспечения СДО, ошибки в действиях пользователей.

Каждая потенциальная угроза безопасности информации в СДО может быть охарактеризована через такие показатели как вероятность реализации и потенциальный ущерб. Размер ущерба от реализации угрозы в отношении информации или ресурса зависит от [3]:

- стоимости информации или ресурса, который подвергается риску
- степени разрушительности воздействия на информацию или ресурс, выражаемой в виде коэффициента разрушительности. Как правило, указанный коэффициент лежит в диапазоне от 0 до 1.

Соотношение между ущербом, частотой и вероятностью возникновения определяет уровень риска от реализации угрозы и степень допустимости каждой угрозы. Значения риска указывает насколько необходимо использовать средства и механизмы, противодействующие каждой конкретной угрозы. Для этого ожидаемый риск сравнивается с затратами на внедрение и последующую эксплуатацию средства защиты, после чего принимается решение в отношении данного риска. Риск может быть принят, перенесен, устранен или снижен.

Технологии защиты СДО

Для противодействия актуальным для СДО вуза угрозам и удержания рисков в пределах допустимого, используются различные механизмы и средства защиты информации, организационно-правового, технического и программного характера, которые должны необходимо учитывать ряд особенностей связанных с процессом их функционирования СДО вуза:

- СДО вуза должна быть доступна для пользователей 24 часа 7 дней в неделю;
- межсетевые экраны и применение SSL не всегда обеспечивают защиту от взлома СДО поскольку, доступ к веб-сайту СДО из внешних сетей должен быть всегда открыт;

- СДО часто имеет прямой доступ к данным, обрабатываемым в ИС вуза: базы данных, ERP-системы, информация об инновационных разработках и научной деятельности вуза, учебные ведомости, персональные данные и др.;
- узконаправленные СДО, собственной разработки вуза, более восприимчивы к атакам, так как они не подвергаются такому длительному тестированию и эксплуатации, как общедоступные известные коммерческие СДО;
- традиционные сетевые средства защиты не предназначены для отражения специализированных атак на веб-приложения СДО, поэтому злоумышленники при помощи браузеров легко проходят через периметр ИС вуза и получают доступ к внутренним системам и серверам;
- ручное обнаружение и устранение уязвимостей в СДО часто не дает положительных результатов - разработчики могут находить и исправлять сотни уязвимостей в коде, но злоумышленнику для проведения результативной атаки достаточно обнаружить всего одну.

Следовательно, обеспечение защиты СДО должно осуществляться как на этапе проектирования и разработке самого СДО путем создания безопасного кода, так и в процессе его эксплуатации с внесением в случае необходимости своевременных корректировок. Поскольку даже если в программном коде СДО уязвимостей нет, необходима комплексная защита, учитывающая наличие базы данных, веб - приложения СДО, сервера СДО и прочих элементов ИТ-платформы вуза. Таким образом, в соответствии с требованиями стандартов:

- ФЗ «О государственной тайне» от 21.07.93 № 5485-1 (статьи 5, 8, 20, 28);
- ФЗ«О персональных данных» от 27.07.2006 №152-ФЗ; руководящие документы

- ГОСТ Р 50922—96 «Защита информации. Основные термины и определения»;
- ГОСТ Р 50739—95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»;
- ГОСТ 28147—89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»,
- ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»,
- ГОСТ Р ИСО/МЭК 17799–2005 «Информационные технологии. Практические правила управления информационной безопасностью» и др.) и регуляторов в области информационной безопасности (Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ (статья 10);
- ФСТЭК «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», «Автоматизированные системы.

Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»), защита должна строиться по трем основным направлениям:

1. контроль над безопасностью кода и наличием уязвимостей в ДО;
2. использование специализированных средств защиты информации:

- прямые и обратные прокси-сервера;
- классические межсетевые экраны и межсетевые экраны уровня приложений;
- многофакторные системы аутентификации (сертификаты, временные дополнительные паролей и ключевые слов в дополнение к паре

логин+пароль пользователя, методы статической и динамической биометрической аутентификации и др.);

- системы обнаружения атак и предотвращения вторжений;
- антивирусное программное обеспечение;
- системы регистрации и анализа событий;
- VPN и защищенные протоколы передачи данных;
- шифрование данных;
- средства резервирования и восстановления данных.

3. проведение периодического контроля защищенности СДО и выработка корректирующих действий в случае необходимости.

Существующие подходы к оценке защищенности

Анализ литературных источников [2-6, 12, 16] показывает, что исследование защищенности является важным этапом в решении задач связанных с контролем над безопасностью системы, моделированием и оптимизацией архитектуры системы защиты. В связи с этим в настоящее время существует несколько направлений теоретических и практических исследований связанных с исследованием, оценкой и управлением защищенностью:

- работы, посвященные анализу защищенности автоматизированных систем;
- работы, посвященные исследованиям в области интегрированного управления информационными и другими типами рисков;
- работы, посвященные исследованиям в области анализа комплексных нарушений в системах защиты информации и анализа безопасности в условиях неполной информации и др.
- В общем случае защищенность системы оценивается двумя основными способами:
- самостоятельная оценка, которая выполняется собственником, администраторами системы и/или службой внутреннего аудита,

независимой от подразделений информационных технологий и информационной безопасности организации;

- оценка независимым внешним исполнителем, которая, в свою очередь, имеет два распространенных варианта реализации - аудит и экспертная оценка.

Самооценка или самоконтроль - самый распространенный тип оценки защищенности, который осуществляется практически непрерывно с использованием не описанных формально процедур. Для проведения самостоятельной оценки защищенности системы, ответственное за безопасность лицо может воспользоваться стандартом ГОСТ Р ИСО/МЭК 17799–2005. Согласно данному стандарту рекомендуется проводить периодические проверки соответствия текущей защищённости, требуемому уровню, политике безопасности и техническим требованиям, однако в нем ничего не говорится о рекомендуемых методах реализации проверок. В общем случае, процедуру оценки, проводят с применением различных методов опроса. Основными этапами данного подхода являются:

- использование опросных листов на основе требований стандарта;
- формирование на основе требований и рекомендаций стандарта и/или основе мнений привлеченных специалистов – экспертов базы знаний;
- нахождение правил по анализу ответов на опросные листы

Нахождение правил по анализу ответов на опросные листы. Применение только стандартизированного подхода позволит достаточно быстро произвести оценку защищенности и получить рекомендации для исследуемой системы. Однако, основным недостатком подобного подхода является то, что реализация полученных рекомендаций практически всегда затруднена (или невозможна) из-за того, что не стандарт не учитывает информацию, накопленную самой системой в процессе ее функционирования. Поэтому помимо учета требований стандарта необходимо также учитывать специфику системы, информационные активы

и статистики по угрозам ИБ или инцидентам ИБ собранных в процессе функционирования системы.

Анализ источников показывает, что процедура оценки защищенности проводится как в «ручном» режиме так и в автоматизированном с привлечением специальных программных средств оценки защищённости и рисков, реализующих различные методики. В настоящее время наиболее распространенными являются следующие методики оценки защищенности:

- методика количественно-качественной оценки защищенности по уровням;
- методика оценки защищенности как величины предотвращенного ущерба;
- методика оценки защищенности на основе непрерывного бета распределения плотности вероятности ущерба;
- методика численной оценки уровня защищенности на основе вероятностно-статистического подхода;
- методика оценки защищенности через моделирование угроз;
- методика векторного анализа информационной безопасности.

Каждая из данных методик имеет свои достоинства и недостатки, сложность и особенности реализации, а также форму представления показателя общей защищенности систем. В рамках данной работы автором при разработке модели оценки защищенности СДО вуза будет использоваться комбинированный подход, построенный на исследовании рисков ИБ и применении методик количественнокачественной оценки защищенности по уровням и численной оценки уровня защищенности на основе вероятностно-статистического подхода.

3.3 Модель оценки защищенности СДО

Для решения задач, поставленных перед оценкой защищенности СДО вуза, необходимо, чтобы в проекте модели были предусмотрены следующие функции:

- сбор данных о СДО, ее функциях, архитектуре и техникоэксплуатационных характеристиках, категории обрабатываемой информации, видах и стоимости информационных ресурсов, количестве видах используемых средств защиты, ограничений на стоимость средств защиты и уровень допустимого риска;
- составление модели актуальных для СДО угроз, задание экспертных оценок вероятности реализации и потенциального ущерба для каждой угрозы;
- расчет рисков от реализации каждой угрозы из модели актуальных угроз, расчет общего риска;
- ранжирование угроз по уровню допустимости риска;
- оценка текущего уровня защищенности СДО
- сравнение текущего уровня защищенности с требуемым вузом уровнем защищенности;
- приятие решения о необходимости изменения состава или реконфигурации средств защиты СДО;
- составление списка рекомендаций и проекта дополнительных средств защиты информации в СДО;
- формирование отчета о результатах оценки защищенности и выдача рекомендаций о повешении защищенности СДО.

Таким образом, концептуальную схему модели оценки защищенности СДО можно представить следующим образом (рисунок 3.3.1).

Входными данными модели являются:

1. информация о СДО: архитектура, тип и название СДО;
2. информация о данных и сервисах подлежащих защите в СДО:

- тип и наивысшая категории обрабатываемой информации (информация не ограниченного доступа, ограниченного доступа: для служебного

пользования, персональные данные, конфиденциальная информация, секретная и т.п.);

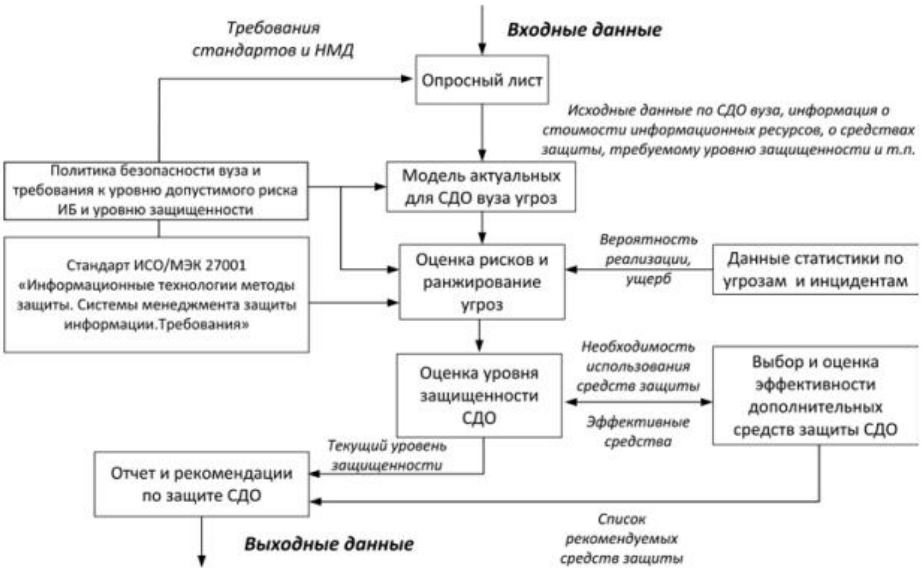

Рисунок 3.3.1 – Схема модели оценки защищенности СДО

- список информационных ресурсов и сервисов с указанием их стоимости, можно установить общую стоимость всех ресурсов или инвентаризировать все файлы и данные в СДО и оценить стоимость каждого;

3. требования к уровню защиты СДО:

- уровень допустимого риска;
- приемлемый уровень защищенности;
- ограничения на стоимость защиты СДО;

4. списки возможных для СДО угроз

5. списки используемых в СДО средств защиты.

Выходными данными оценки защищенности СДО являются:

1. рассчитанный уровень защищенности СДО;

2. степень соответствия уровня защищенности СДО требованиям безопасности вуза;

3. решение о необходимости повышения уровня защищенности;

4. рекомендации по отношению к недопустимым рискам и список потенциальных средств защиты, применение которых позволит повысить защищенность СДО.

Формализованная модель оценки защищенности СДО основывается на теории множеств, логики нечетких высказываний и лингвистических переменных. Таким образом, все элементы, участвующие в оценки защищенности СДО можно представить в виде совокупности множеств (формула 1), связанных различными отношениями.

SAM = {RE, IR, TR, SP, SL, KE, REC, STATUS},

где RE – множество требований к безопасности СДО; IR – множество информационных ресурсов и сервисов СДО, подлежащих защите; TR – множество возможных угроз безопасности СДО; SP – множество реализованных в СДО средств защиты; SL – множество уровней защищенности СДО; KE – множество критериев эффективности средств защиты; REC – множество рекомендаций, которые применяются к каждой угрозе в соответствии с допустимостью риска от ее реализации; STATUS – множество, описывающее два состояния, указывающих на защищенность или незащищенность СДО.

Множество требований к безопасности СДО состоит из следующих элементов RE={Rкрит, Rдоп, Cmax, SLдоп}, где Rкрит - критический уровень риска; Rдоп - приемлемый уровень риска; Cmax - максимально допустимые затраты на средства защиты; SLдоп - приемлемый уровень защищенности СДО вуза.

Каждый элемент IR IR,l= ..k l ∀ ∈ 1 описывается вектором IRl=(Type, Cost, A, I, C, Cy), где

- Type – это тип информационного ресурса. Описывается множеством базовых значений Type={ ED, OS, EV, CT, PD, YI, OI, SR, DB, WS}, где ED - учебные материалы, OS - фонд оценочных средств, EV – учебные ведомости, CT- коммерческая тайна, PD - персональные данные, YI -

управляющая информация, OI - общедоступная информация, SR – сервер СДО, DB – база данных СДО, WS – веб-сайт СДО;

- Cost – стоимость информационного ресурса;
- A, I, C, Cy - свойства безопасности информационного ресурса, которые необходимо обеспечивать. A - доступность, I - целостность, C - конфиденциальность, Cy – непрерывность. Принимают значение 1 если свойство необходимо обеспечить и 0 в противном случае.

Каждая возможная для СДО угроза TR TR,i= ..n i ∀ ∈ 1 описывается вектором значений TRi = (Pi, Ui, Ri), где ∈[0,1] Pi - вероятность возникновения угрозы, определяется экспертным путем или на основании статистики инцидентов ИБ, U – ущерб, наносимый вузу и пользователям СДО от реализации угрозы, Ri=UiPi - риск от каждой угрозы. Для указания типа связи и существующего отношения R между информационными ресурсами и возможными угрозами используется следующее правило, представленное на формуле 2.

$$m_{TRi}^{IRl} = \begin{cases} 1, \text{если для ресурса } IR_l \text{ актуальна угроза } TR_i \\ 0, \text{если для ресурса } IR_l \text{ не актуальна угроза } TR \end{cases}$$

Каждое средство защиты информации∀SPk ∈SP,k=1..m описывается значениями SPk={NSPk, CSPk, TSPk }, где NSPk – тип средства защиты, CSPk – стоимость внедрения и обслуживания средства защиты, TSPk – время внедрения средства защиты, m - количество используемых средств. Связь между средствами защиты SP и множеством актуальных угроз TR описывается матрицей бинарных отношений SPk TRi SP MTR = m , где SPk mTRi отображает наличие и тип связи между угрозой TRi и средством защиты SPk. По сути является матрицей перекрытия угроз безопасности СДО средствами защиты СДО.

$$m_{TRi}^{SPk} = \begin{cases} 0, \text{если } TR_i \text{ закрывается } SP_k \text{ средством защиты} \\ 1, \text{если } TR_i \text{ не закрывается } SP_k \text{ средством защиты} \end{cases}$$

Итоговое значение риска от реализации каждой угрозы, с учетом ее перекрытия существующим средствами защиты определяется по формуле 4.

$$R_{TRi} = R_i \sum_{k=1}^{m} m_{TRi}^{SPk}$$

Множество уровней защищенности СДО, описывается качественной шкалой SL={Impermissible, Low, Middle, High}, что соответствует не допустимому, низкому, среднему и высоком уровню. Чем выше уровень защищенности, тем меньше вероятность реализации угрозы и ниже риски.

Множество критериев эффективности средств защиты используются в модели для выбора дополнительных средств защиты, которые могут быть рекомендованы для повышения защищенности, в случае если текущий уровень защищенности SLT не соответствует минимально допустимому уровню SLдоп.

нности SLT не соответствует минимально допустимому уровню SLдоп. Множество рекомендаций описывается с помощью лингвистических переменных и принимает значения REC={A, B, C, D}, где A – действия, связанные с риском должны быть выполнены немедленно и в обязательном порядке; B – действия, связанные с риском, должны быть предприняты; C – требуется мониторинг ситуации, непосредственных мер по противодействию угрозе принимать не следует; D – никаких действий в данный момент предпринимать не требуется. Каждая рекомендация представляет собой функцию от риска реализации угрозы с учетом возможности ее перекрытия средством защиты и зависит от степени допустимости риска.

$$REC(TR_i) = \begin{cases} D, \text{если } R_{TRi} < R_{доп} \\ C, \text{если } R_{доп} \le R_{TRi} < \dfrac{R_{крит}}{2} \\ B, \text{если } \dfrac{R_{крит}}{2} \le R_{TRi} < Rккри \\ A, \text{если } R_{TRi} \ge Rккри \end{cases}$$

Текущий уровень защищенности АРМ - SLT зависит от значения рекомендаций по устранению риска от реализации каждой актуальной для СДО угрозы и определяется с учетом формулы 5 следующим образом.

$$SL_T = \begin{cases} High, \text{если } \forall TR_i \in TR: REC(TR_i) = D \\ Middle, \text{если } \forall TR_i \in TR: REC(TR_i) \le C \\ Low, \text{если } \forall TR_i \in TR: REC(TR_i) \le B \\ \text{Impermissible}, \text{если } \forall TR_i \in TR: REC(TR_i) = A \end{cases},$$

где A>B>C>D. В том случае если полученное значение текущего уровня защищенности СДО, ниже требуемого значения - SLдоп, то принимается решение о не защищенности и предлагается в рамках бюджета подобрать дополнительные средства защиты, применение которых позволит повысить уровень защищенности до требуемого уровня. В противном случае СДО признается защищенным и не требующим использование дополнительных средств защиты.

$$\text{STATUS} = \begin{cases} \text{protecred}, ееесли\ S_T \ge SL_{доп} \\ \text{not\_protecred}, если\ SL_T < SL_{доп} \end{cases}.$$

В случае если СДО не защищено, то при выборе дополнительных средств защиты производиться оценка их эффективности при помощи критериев эффективности из множества КЕ. Данная процедура оценки представлена и подробно описана автором в работе.

В отчет по оценки защищенности выноситься информация о текущем уровне защищенности СДО вуза (SLT), рекомендации относительно каждой угрозы (REC(TR)), решение о соответствии или не соответствии уровня текущего уровня защищенности требуемому (STATUS), а также список средств защиты, которые рекомендуется использовать для повышения защищенности СДО (SPE).

Программный прототип модели оценки защищенности СДО

Оценка защищенности является регулярным мероприятием, которое проводится ответственным за ИБ лицом и/или лицами с целью контроля над

состоянием безопасности системы. Поэтому для удобства применения, предложенной автором модели оценки защищенности, был разработан программный прототип, автоматизирующий данную модель. Программный прототип имеет модульную архитектуру и графический пользовательский интерфейс (рисунок 3.3.2), предназначенный для ввода данных, вывода результатов и организации вза-имодействия пользователя с программой. Модуль сбора характеристик о СДО и требований к защите, на основании опросного листа (анкеты) запол-няемой пользователям формирует список данных о характеристиках СДО, количестве пользователей, имеющихся средствах защиты, уровне критичного и допустимого риска, допустимого уровня защищенности, а также предельно допустимой стоимости средств защиты. Позволяет выбрать различные режимы работы модели. Активирует модуль «Инвентаризация информаци-онных ресурсов СДО» в случае если пользователем установлен в настройках режим «инвентаризация файлов и данных СДО».

Модуль инвентаризации, осуществляет поиск каталогов и файлов учебных материалов СДО, производит классификацию найденной информации по степени важности и категории доступа, позволяет установить пользователям ее стоимость и ранжировать найденные данные. Передает данные в модуль «Сбор характеристик о СДО и требований к защите».

Модуль составления модели актуальных угроз, позволяет выбрать из списка потенциально возможных угроз, угрозы которые будут наиболее актуальны для анализируемой СДО. Присвоить им такие характеристики как вероятность реализации и потенциальный ущерб. Затем на основании внесенных данных модуль рассчитывает суммарный риск и риск для каждой угрозы из списка актуальных. Передает данные в модуль «Формирование рекомендаций и отчета», где на основании данных о допустимом уровне риска для каждой угрозы вырабатываются мероприятия направленные на устранение рисков.

Рисунок 3.3.2 – Архитектура программного прототипа оценки защищенности СДО

Модуль оценки защищенности СДО на основании данных об уровне риска и рекомендациях по защите от каждой угрозы позволяет оценить и присвоить СДО один из 4 уровней защищенности. А если уровень защищенности ПК не советует допустимому, вызвать модуль по подбору и оценки эффективности дополнительных средств защиты.

Модуль оценки эффективности средств защиты позволяет отобрать из списка различные средства защиты, которые могут применяться для последующей оценки их эффективности. На основании данных о требованиях к защите, модели актуальных угроз и списка средств – претендентов, производит комплексную оценку эффективности каждого средства защиты на основании 5 взвешенных по уровню значимости частных критериев. Средства, получившие лучшие оценки и удовлетворяющие наложенным ограничениям признаются эффективными и рекомендуются для внедрения, с целью повышения защищенности СДО.

Модуль формирования рекомендаций и отчета обеспечивает взаимодействие между другими модулями и на основании данных о допустимом уровне риска вырабатывает комплекс мероприятий –

рекомендаций по защите от каждой из актуальных угроз, определяет соответствие между рассчитанным уровнем защищенности и допустимым и выносит решение о защищенности СДО или ее не защищённости. И если СДО имеет низкую защищенность, выводит список рекомендуемых средств защиты.

Пользовательский интерфейс (рисунок 3.2.3) состоит из семи вкладок, реализующих основные функциональные возможности программного прототипа:

1. характеристики;
2. информационные ресурсы;
3. модель угроз;
4. средства защиты;
5. оценка защищенности;
6. оценка эффективности;
7. отчет и рекомендации.

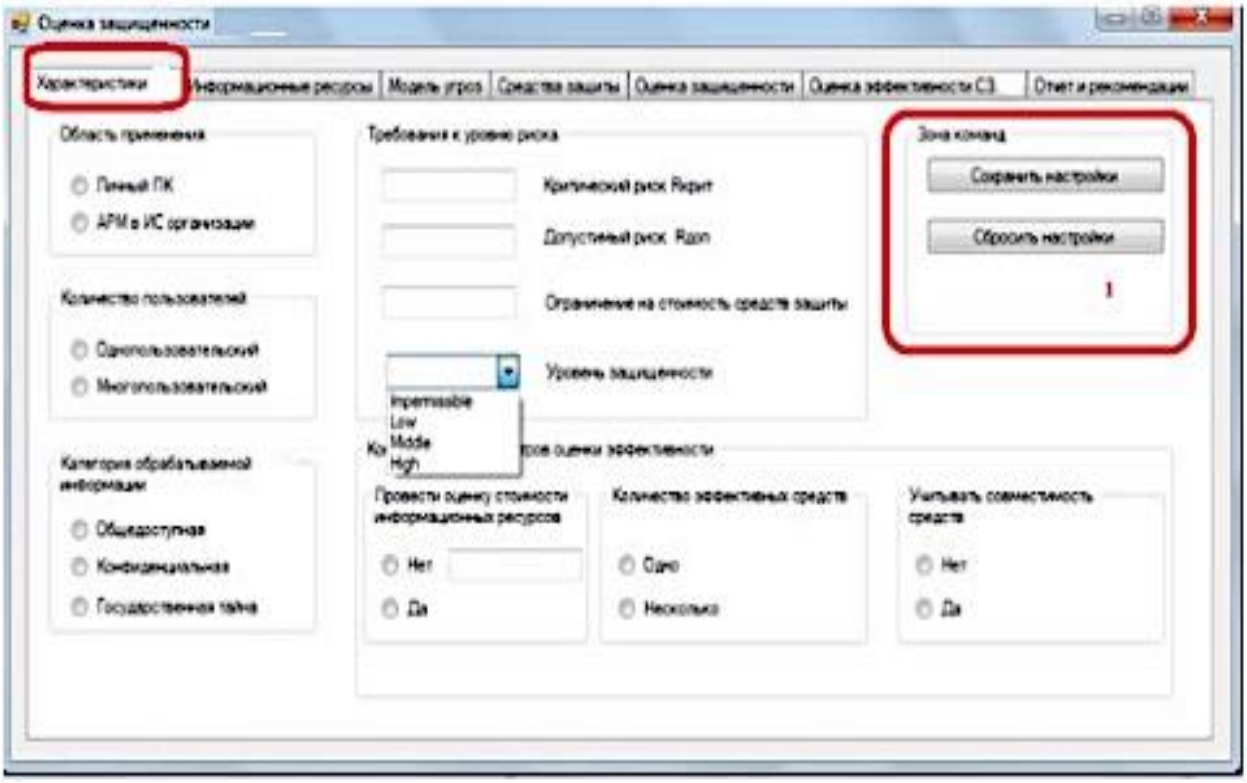

Рисунок 3.2.3 – Пользовательский интерфейс программного прототипа. Вкладка «Характеристики»

Для взаимодействия пользователей с программой при создании интерфейса использованы следующие элементы управления:

- стандартные элементы управления окном Windows;
- кнопки различных размеров и видов;
- выпадающие списки;
- поля ввода и вывода цифровых данных.

Для взаимодействия пользователя с элементами управления применяется манипулятор типа «мышь», touchpad, сенсор или др. Также возможно использование для этой цели клавиатуры ЭВМ.

Разработанный прототип является 64 – разрядным приложением, работающим под управлением ОС Windows 10. Программа имеет оконный интерфейс, разделенный контекстными вкладками - страницами. Работа пользователя с ней строится на принципах, принятых в операционной системе Windows. Написана на языке программирования VisualC# 2013 среды разработки VisualStudio .Net, Framework 4.5.1

С помощью разработанного программного прототипа модели было проведено исследование защищенности 10 различных СДО с различной конфигурацией, набором средств защиты и типом обрабатываемой информации. Полученные результаты представлены в таблице 1 и в виде диаграммы на рисунках 3.3.4 и 3.3.5.

Таблица 3 – Результаты исследования защищенности ПК различного типа

Результат оценки защищенности СДО	Количество СДО
Уровень защищенности СДО соответствует требованиям	4
Уровень защищенности СДО не соответствует требованиям	6
Рекомендации повысили уровень защищенности СДО до требуемого	4
Рекомендации повысили уровень защищенности СДО, но он остался ниже требуемого	1
Рекомендации не повысили уровень защищенности СДО	1

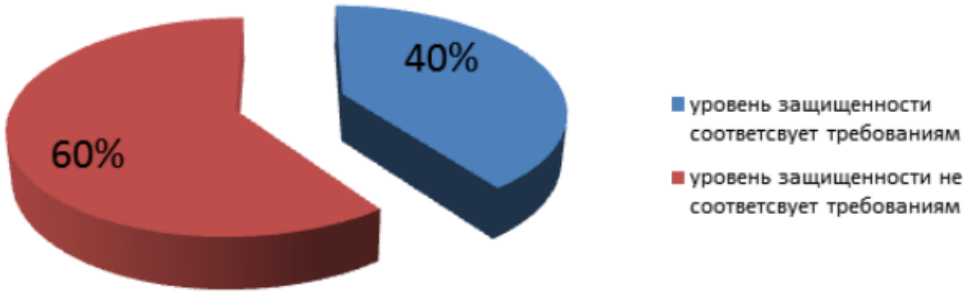

Рисунок 3.3.4 – Распределение результатов первичной проверки защищенности СДО различного вида и конфигурации

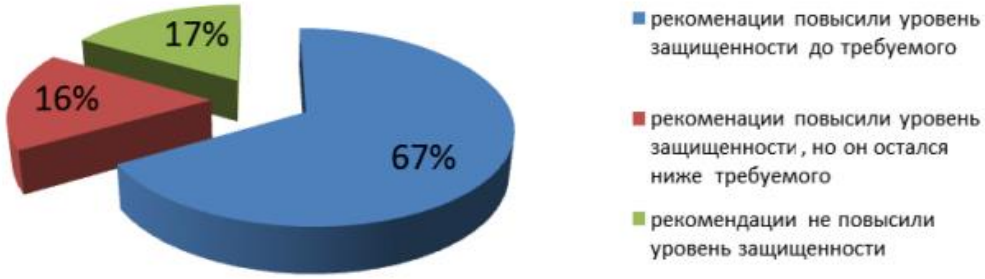

Рисунок 3.3.5 –Распределение результатов повторной оценки защищенности СДО после применения рекомендаций по повышению защищенности.

На основании полученных результатов, можно сделать вывод, что предложенные в результате первичной оценки защищенности рекомендации при их применении могут повысить общий уровень защищенности СДО и снизить остаточный риск, что было зафиксировано в 67% случаев.

Вывод по 3 главе

Данная модель оценки защищенности СДО колледжа:

1. использует комбинированный подход, построенный на применении количественно-качественной оценки защищенности, при котором защищенность представляет собой функцию от значений рекомендаций по устранению риска от реализации каждой актуальной угрозы для СДО;

2. дает возможность построить матрицу отношений между угрозами и используемыми средствами защиты и оценить риск реализации

каждой угрозы по трехфакторной модели, учитывающей вероятность реализации и ущерб, которые оцениваются экспертной оценкой и возможность перекрытия данной угрозы средством защиты СДО;

3. позволяет не только оценить уровень защищенности, но и в случае несоответствия подобрать наиболее рациональные средства защиты для СДО, применения которых позволит устранить выявленные на этапе анализа показателей защищенности несоответствия требованиям вуза и повысить уровень защищенности

Разработанный программный прототип модели оценки защищенности СДО колледжа автоматизирует процесс оценки защищенности СДО и может использоваться на практике в качестве инструментального средства поддержки принятия решений при проведении планового контроля защищенности СДО и аудите ИБ колледжа. Также данный программный прототип может быть использован в качестве обучающего стенда-макета на лабораторном практикуме при подготовке студентов в области информационной безопасности.

ГЛАВА 4. РАЗРАБОТКА МОДЕЛИ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Даная глава посвящена разработке МСУИ в форме программного комплекса, реализующего теоретические результаты предыдущих разделов. Разрабатываемый программный продукт является полностью автономным и завершенным. В его функционал входят все компоненты, необходимые для организации дистанционного учебного процесса.

4.1 Структура программного комплекса

Структура программного комплекса системы дистанционного обучения представлена на рисунке 4.1.1:

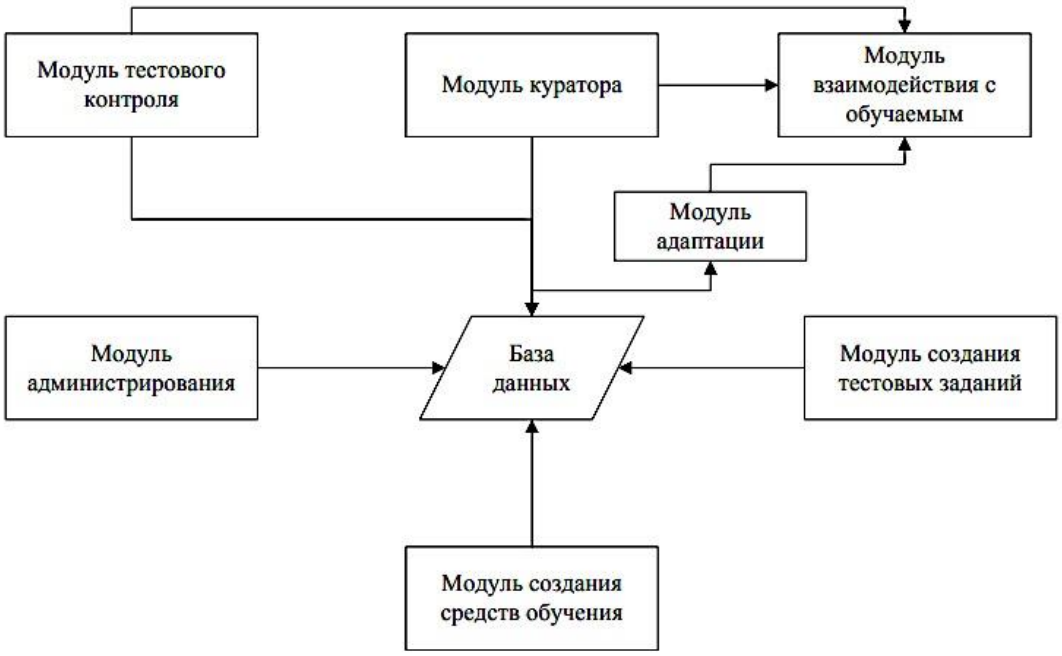

Рисунок 4.1.1 – Структура программного комплекса

Рассмотрим более подробно компоненты программного комплекса.

База данных – основной компонент системы, предназначена для хранения всей, используемой в процессе работы программы, информации.

Модуль куратора – компоненты системы, предназначенный для взаимодействия куратора с системой обучения. Данный модуль позволяет не

только просматривать результаты работы обучающихся, но и взаимодействовать непосредственно с каждым обучающимся.

Модуль взаимодействия с обучающимся – компонент системы, реализующий процесс взаимодействия системы с обучающимся на всех этапах обучения, включающих:

- предварительные испытания,
- оценка предпочтительности дисциплин,
- планирование обучения,
- обучение,
- тестовый контроль.

Модуль тестового контроля – компонент системы, используемый для контроля качества знаний обучающегося.

Модуль адаптации – модуль системы, отвечающий за адаптацию учебного материала при взаимодействии с каждый обучающимся.

Модуль администрирования – компонент системы, позволяющий управлять системой, производить ее настройку, добавлять и удалять пользователей, определять их роли.

Модуль создания средств обучения – компонент системы, используемый для формирования учебного материала. Позволяет формировать и редактировать текст с использованием иллюстраций, таблиц, диаграмм, анимации.

Модуль создания тестовых заданий – модуль системы, позволяющий создавать тестовые задания для каждого раздела дисциплин. Так же позволяет использовать в тексе иллюстрации, таблицы, диаграммы, анимации. Основными типами тестовых заданий, которые позволяет создавать данный модуль являются:

- тестовые задания с одним верным вариантом ответа,
- тестовые задания с несколькими верными вариантами ответа
- задания на указания верной последовательности вариантов ответа,

– задания с указанием соответствия элементов в обеих частях тестового задания.

Описанная структура является общим представлением разрабатываемой системы и требует подробной реализации всех ее компонентов.

Для функционирования программного комплекса необходимо определить три уровня доступа к системе: Администратор, Куратор и Обучающийся. Данные группы необходимы для разграничения доступа к средствам системы с целью повышения ее безопасности.

Администратор является наиболее привилегированной и малочисленной группой пользователей. Пользователям данной группы позволено создавать, удалять и редактировать все, без исключения группы пользователей, производить настройку системы, делать резервной копирование и восстановление базы данных.

Куратор является второй по возможностям доступа группой пользователей. Участникам данной группы позволено создавать и редактировать учебный материал и тестовые задания, а также отслеживать деятельность обучающегося, просматривать результаты его тестовых испытаний, взаимодействовать с обучающимся по средствам текстовых сообщений, при необходимости.

Обучающийся является набольшей по численности, но наименее привилегированной группой пользователей. Пользователи данной группы могут просматривать учебную информацию, проходить тестовые испытания, определять предпочтительные дисциплины.

4.2 Выбор средств разработки программного комплекса

Так как разрабатываемая модель является дистанционной, требуется определить какую web-технологию необходимо использовать

Таблица. 4.2.1 Сравнение технологий ASP.Net и PHP

Параметр сравнения	ASP.Net	PHP
Языки программирования	При создании приложений ASP Dot Net существует возможность использовать любой язык из платформы .Net – C# или Visual Basic.Net. Доступен весь функционал библиотеки Dot Net Framework.	PHP является наиболее популярным языком webпрограммирования. Используется си-подобный синтаксис, отсутствует строгая типизация переменных.
Среды разработки	Основной продукт, который используется для разработки вебприложений на ASP.Net – это Microsoft Visual Studio.	Для языка PHP сегодня существует множество различных сред разработки: родная Zend Studio, версия Eclipse для PHP, плагин под Visual Studio и т.п.
Стоимость среды разработки	Express-версия Visual Studio поставляется бесплатно и обладает широкими возможностями. Также бесплатна и Expressверсия SQL-сервера.	Весь LAMP-стек (Linux Apache Mysql PHP) бесплатен. Бесплатны Unixподобные операционные системы, бесплатен вебсервер Apache, бесплатен интерпретатор PHP и бесплатна база данных MySQL (за исключением ее коммерческого использования, в этом случае лицензией предусмотрена оплата за базу данных).
Базы данных	Зачастую ASP.Netприложения используют сервер баз данных от Microsoft – Microsoft SQL Server.	Зачастую вместе с PHP используется СУБД MySQL. Реже – PostgreSQL.

Основываясь на результатах сравнения можно сделать вывод, что в данном случае наиболее подходящей технологией является ASP.Net.

Что касается технологии построения программного продукта, то оптимальным вариантом будет использование технологии MVC (ModelView-Controller). Шаблон архитектуры Model-View-Controller (MVC) разделяет

приложение на три основных компонента: модель, представление и контроллер.

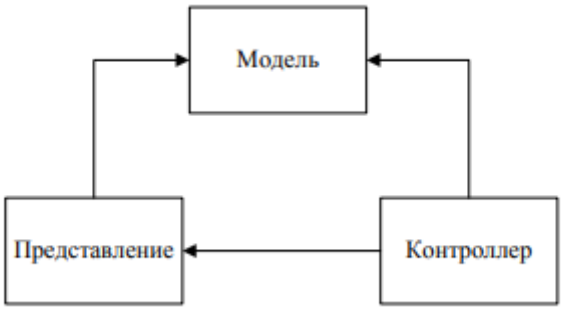

Рисунок 4.2.2 – Структура MVC - приложения

4.3 Разработка базы данных для системы дистанционного обучения

База данных является важнейшим элементом разрабатываемой системы, поэтому качество ее организации повлияет на производительность и безопасность всей системы

Так как в качестве технологии разработки программного продукта была выбрана ASP.Net MVC от компании Майкрософт, то оптимальным средством организации баз данных является MS SQL Sever 2012.

Использование СУБД MS SQL Sever 2012 дает возможность формировать запросы и осуществлять поиск необходимых данных, синхронизировать данные, а также выполнять аналитическую обработку информации и получать разнообразные отчеты. При этом базы данных и средства управления ими доступны, как с настольных компьютеров, так и с различных мобильных устройств. Важным фактором при использовании СУБД является применение надежной серверной платформы, обеспечивающей максимальные возможности

Структура базы данных, разработанная для использования в МСУИБ, представлена на рисунке 4.3.1.

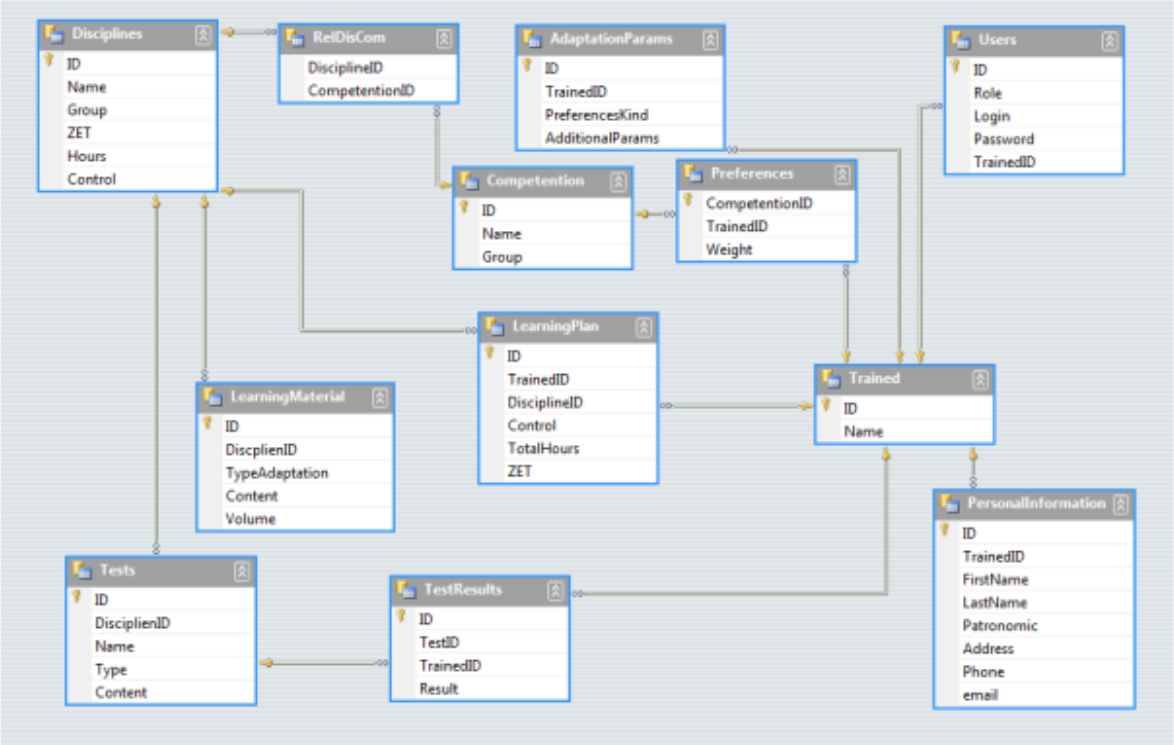

Рисунок 4.3.1 - Структура базы данных системы дистанционного обучения

Как видно, все значимые таблицы содержат поле ID – уникальный идентификатор записи, являющийся первичным ключом для связи таблиц по типу «многие к одному». Вторичными ключами являются поля составление из названия головной таблиц и окончания ID. Данные поля являются ссылками на первичные. Некоторые таблицы, такие как Preferences, не содержат первичных ключей, подобные таблицы используются для связей типа «многие ко многим».

Рассмотрим более подробно каждую из таблиц.

Первой будет рассмотрена таблица Disciplines, в которой хранятся учебные дисциплины.

Таблица 4.3.1 Поля таблицы Disciplines

Имя столбца	Назначение
Name	Используется для хранения наименования дисциплины
group	Группа в которую входит данная дисциплина
ZET	Объем дисциплины в зачетных единицах
Hours	Объем дисциплины в часов
Control	Тип итогового контроля

Следующей таблицей является Competention, она используется для хранения компетенций, которые требуется освоить обучающемуся в процессе обучения.

Табл. 4.3.2 Поля таблицы Competention

Имя столбца	Назначение
Name	Наименование компетенции
Group	Группа в которую входит компетенция

Каждая дисциплина связана с определенным множеством компетенций, которые приобретает обучающийся в процессе обучения. Для данной связи используется таблица RelDisCom.

Табл. 4.3.3 Поля таблицы RelDisCom

Имя столбца	Назначение
DisciplineID	Ссылка на дисциплину
CompetentionID	Ссылка на компетенцию

Данная таблица содержит связи «многие ко многим», так как существует множество дисциплин, реализующих одни и те же компетенции

Данные об обучающемся содержатся в таблице PersonalInformation, она включает всю личную и контактную информацию.

Табл. 4.3.4 Поля таблицы PersonalInformation

Имя столбца	Назначение
TrainedID	Ссылка на профиль обучающегося
FirstName	Имя обучающегося
LastName	Фамилия
Patronomic	Отчество
Address	Адрес проживания обучающегося
Phone	Контактный телефон
email	Адрес электронной почты

Записи в данной таблице ссылаются на профиль обучающегося в таблице Trained. Эти таблицы специально разделены для ускорения работы подзапросов.

Как говорилось ранее, каждый обучающийся определят приоритетные для себя компетенции. Для организации данной зависимости служит таблица Preferences, содержащая связи типа «многие ко многим»

Табл. 4.3.5 Поля таблицы Preferences

Имя столбца	Назначение
TrainedID	Ссылка на профиль обучающегося
CompetentionID	Ссылка на компетенцию

Для каждой дисциплины содержится учебный материал, если есть возможность – учебный материал представлен в различных видах, для последующей адаптации. Для хранения учебного материала используется таблица LearningMaterial

Табл. 4.3.6 Поля таблицы LearningMaterial

Имя столбца	Назначение
DiscplienID	Ссылка на учебную дисциплину
TypeAdaptation	Тип представления материала для адаптации
Content	Содержимое учебного материала
Volume	Объем учебного материала в часах

Для каждого обучающегося в системе формируется индивидуальный учебный план, для его хранения используется таблица LearningPlan.

Табл. 4.3.7 Поля таблицы LearningPlan

Имя столбца	Назначение
TrainedID	Ссылка на профиль обучающегося
DisciplineID	Ссылка на дисциплину
Control	Тип контроля
TotalHours	Объем учебного плана в часах
ZET	Объем учебного плана в зачетных единицах

По каждой дисциплине существует набор тестовых заданий для контроля качества знаний. Тестовые задания хранятся в таблице Tests

Имя столбца	Назначение
DiscplienID	Ссылка на учебную дисциплину
Name	Заголовок теста

После тестирования уровня знаний обучающегося результаты заносятся в таблицу TestResults. В дальнейшем данные результаты используются системой для определения качества знаний обучающегося.

Табл. 4.3.9 Поля таблицы TestResults

Имя столбца	Назначение
TestID	Ссылка на тестовое задание
TrainedID	Ссылка на профиль обучающегося
Result	Результат

Все пользователи системы (администраторы, кураторы и обучающиеся) имеют свои данные авторизации. Эти данные хранятся в таблице Users.

Табл. 4.3.10 Поля таблицы Users

Имя столбца	Назначение
Role	Роль пользователя
Login	Логин
Password	Пароль
TrainedID	Ссылка на обучающегося. Если пользователь не является обучающимся, то ссылка равна NULL.

После того, как база данных спроектирована, необходимо определить способ взаимодействия с ней программного комплекса. Существует два основных подхода к реализации доступа к базам данных:

1. прямые SQL запросы,
2. объектно-реляционная проекция (Object Relational Mapping – ORM).

При разработке программного комплекса адаптивной системы дистанционного обучения оптимальным вариантом является использование объектно-реляционной проекции.

Так как в качестве технологии разработки программного комплекса выбрана ASP.Net MVC, а в качестве системы управления базами данных Microsoft SQL Server, то оптимальным вариантом объектно-реляционной проекции является технология Microsoft ADO.NET Entity Framework. Данная технология является составной частью платформы Microsoft .NET Framework

4.4 Реализация интерфейса программной модели системы дистанционного обучения

В качестве технологии разработки нами была выбрана технология ASP.Net MVC, поэтому в соответствии со спецификацией необходимо создать представление для каждой из станиц. Создание страниц происходит на языке HTML.

Каждый пользователь системы должен быть авторизован, для определения его роли и прав доступа. Для этого служит страница авторизации (рис. 4.4.1).

Для кураторов пароли могут быть созданы администраторами, а для обучающихся как администраторами, так и кураторами. Данные процедуры будут рассмотрены позже. Администраторский пароль, необходимый для

первоначального доступа предоставляется при установке системы. Поэтому форма регистрации как таковая не требуется.

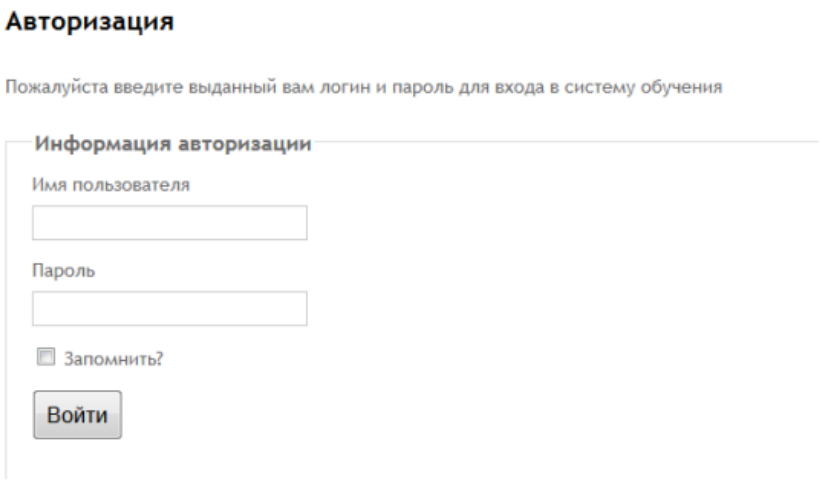

Рис. 4.4.1. Страница авторизации

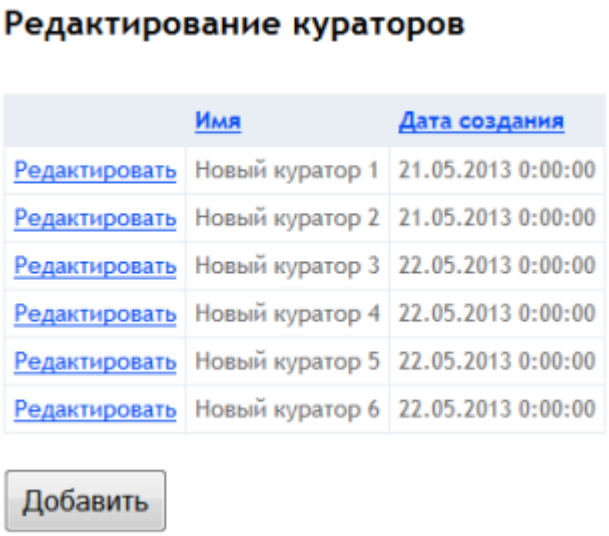

Рисунок 4.4.2 Форма создания и редактирования кураторов

Так как в базе данных храниться лишь результат вычисление функции пароля – нет смысла выводить его на редактирование. При регистрации нового пользователя, а так же при редактировании данных – новый пароль будет выслан на адрес электронной почты. Данный подход позволит ограничить круг лиц, имеющих доступ к паролю – тем самым увеличить безопасность системы.

Аналогичным образом происходит редактирование обучающихся, однако, для каждого обучающегося куратор может видеть подробную информацию о текущем состоянии изученности каждой учебной дисциплины и т.д..

При нажатии на кнопку «подробней» появляется форма отображения профиля текущего обучающегося. В данном разделе отображается информация о текущих дисциплинах, по которых он проходит обучение, процент изученности дисциплины, количество пройденных этапов промежуточного контроля знаний, а так же тип итогового контроля, предусмотренный каждой дисциплиной (зачет или экзамен)

Рис. 4.4.3. Форма создания и редактирования обучающихся

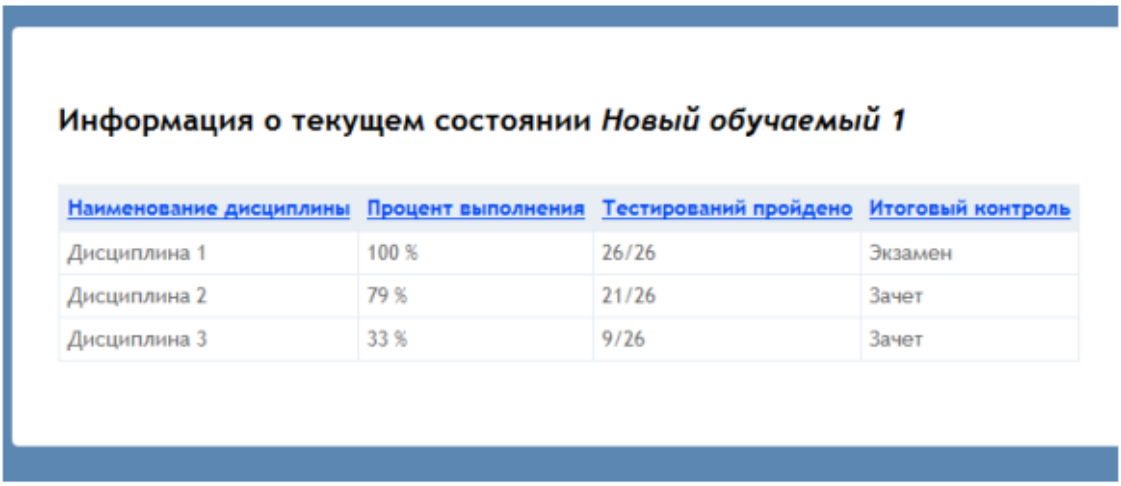

Рис. 4.4.4. Информация о прогрессе обучающегося

Для создания учебного материала существует специальный редактор, который позволяет создавать учебный материал с использованием широкого наборы средств редактирования текста, создания и использования изображений, диаграмм, графиков. Данный редактор создан на основе свободной библиотеки FreeTextBox (http://www.freetextbox.com/).

Все учебные материалы, созданные с использованием данного редактора сохраняются в виде XML-разметки в базе данных. Изображение хранятся в бинарном виде.

Разрабатываемая система адаптивного дистанционного образования в сфере информационных технологий поддерживает формат хранения учебного материала SCORM. Для сохранения учебного материала в формате SCORM необходимо открыть редактор, и заполнить все поля соответствующие стандарту SCORM:

1. идентификатор учебного курса;
2. версия
3. пространства имен, используемые в процессе изучения учебного материала;
4. схема и ее версия;
5. язык, на котором написан учебный материал;
6. заголовок учебного материала;

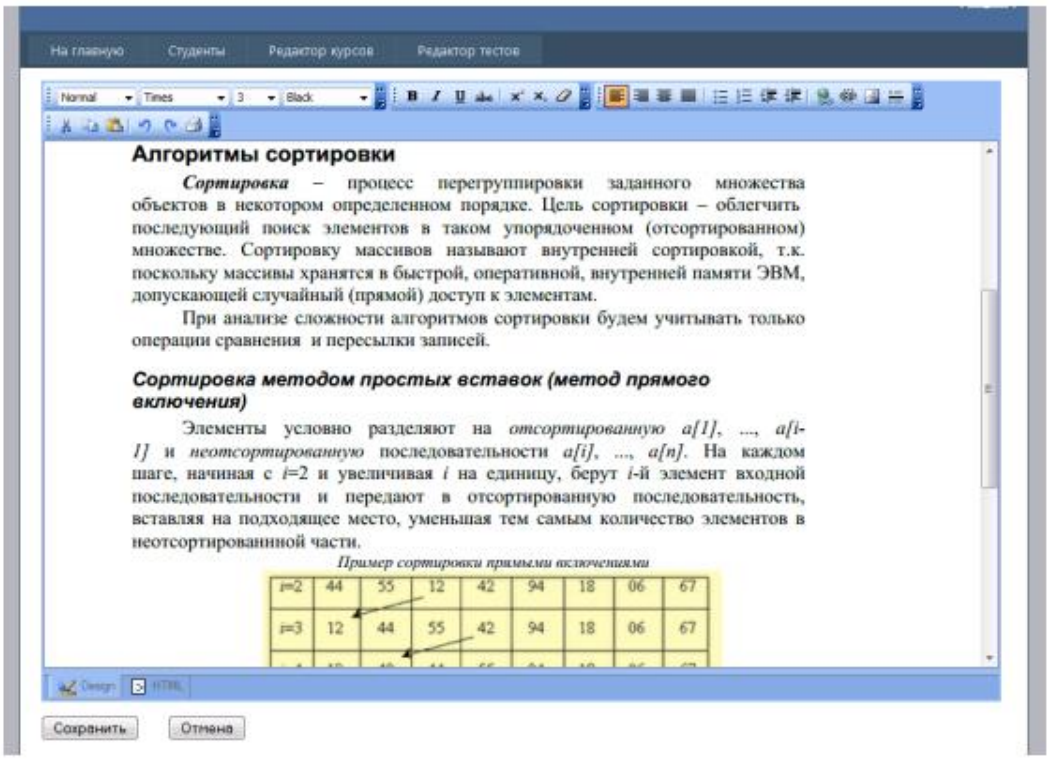

Рис. 4.4.5. Редактор для создания учебного материала

7. описание учебного материала;
8. ключевые слова учебного материала;
9. формат данных, заключенных в SCORM-пакет;
10. Права на копирование;
11. Количество описанных в манифест-файле ресурсов;
12. Тип содержимого;
13. Adlcp:scormType учебного материала;
14. Иерархическое дерево ресурсов;
15. Дерево зависимых файлов;
16. Общая информация о файле.

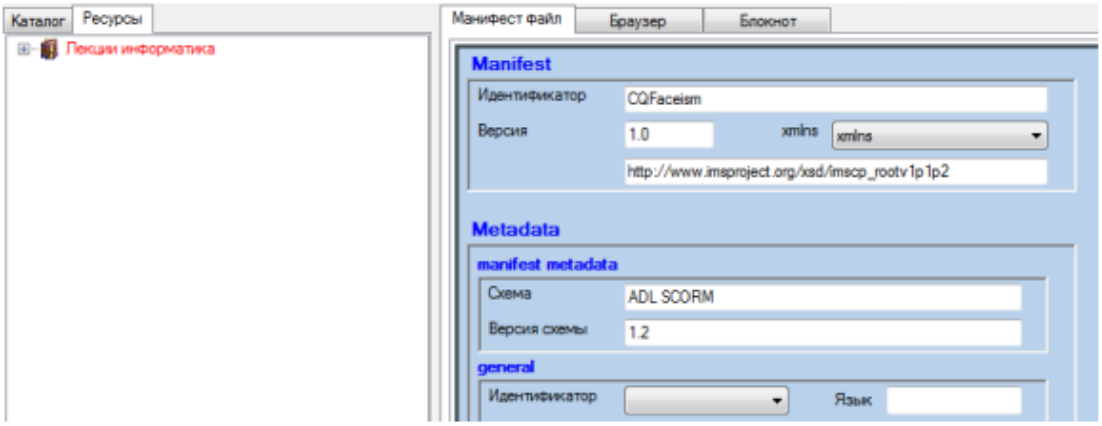

Рис. 4.4.6. Параметры пакета SCORM

После заполнения всех необходимых параметров будет сформирован SCORM –пакет, доступный для экспорта в другие системы дистанционного обучения, поддерживающие данный формат.

Фактически SCORM-пакет представляет собой ZIP-архив, содержащий учебный материал, а так же всю необходимую информацию для экспорта в другие системы

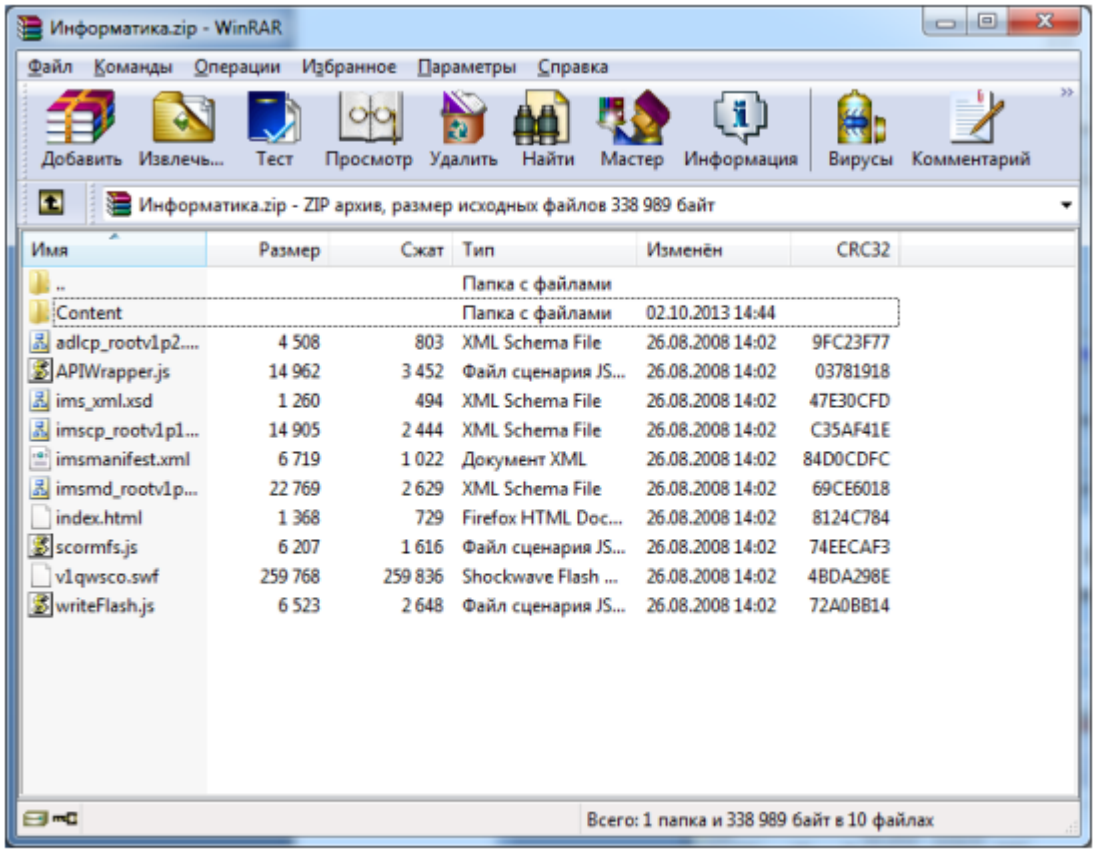

Рис. 4.4.7. Содержимое SCORM-пакета

Поддержка стандарта скорм дает программному средству ряд функциональных возможностей:

- Совместимость со стандартами SCORM 2004 третьего и четвертого поколения;
- Возможность интегрирования спецификации RTE;
- Описание документации;
- Возможность поиска файла и моментального его отображения;
- Структурирование основных элементов учебного материала;
- Построение иерархичной модели учебных материалов;
- Возможность работы с учебным материалом посредством графического интерфейса, исключая возможность работы с исходным кодом.

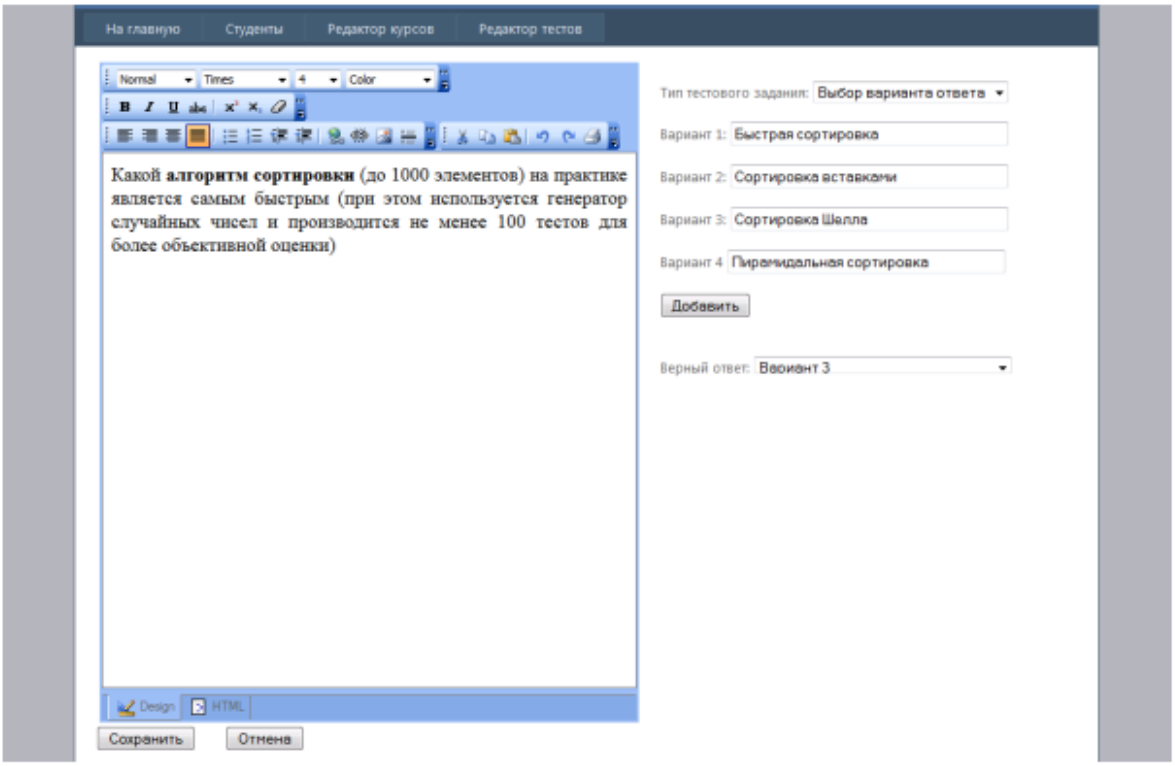

Рис. 4.4.8. Редактор тестовых заданий

Еще одним важным элементом программного комплекса является редактор тестовых заданий. Функциональные возможности данного редактора позволяют создавать тестовые задания с использованием не только текста, но и иллюстраций и диаграмм. Существует возможность создавать

тестовые задания следующих видов: задание с одним верным ответом, несколькими верными ответами, задание на последовательность, задание за соответствие вариантов.

Теперь перейдем к рассмотрению интерфейса обучающегося. Если профиль обучающегося создан заново, то перед началом обучения необходимо составить для него учебный план, при этом обучающийся должен определить приоритетные компетенции. Данные о предпочтениях обучающегося будут учтены в процессе создания учебного плана.

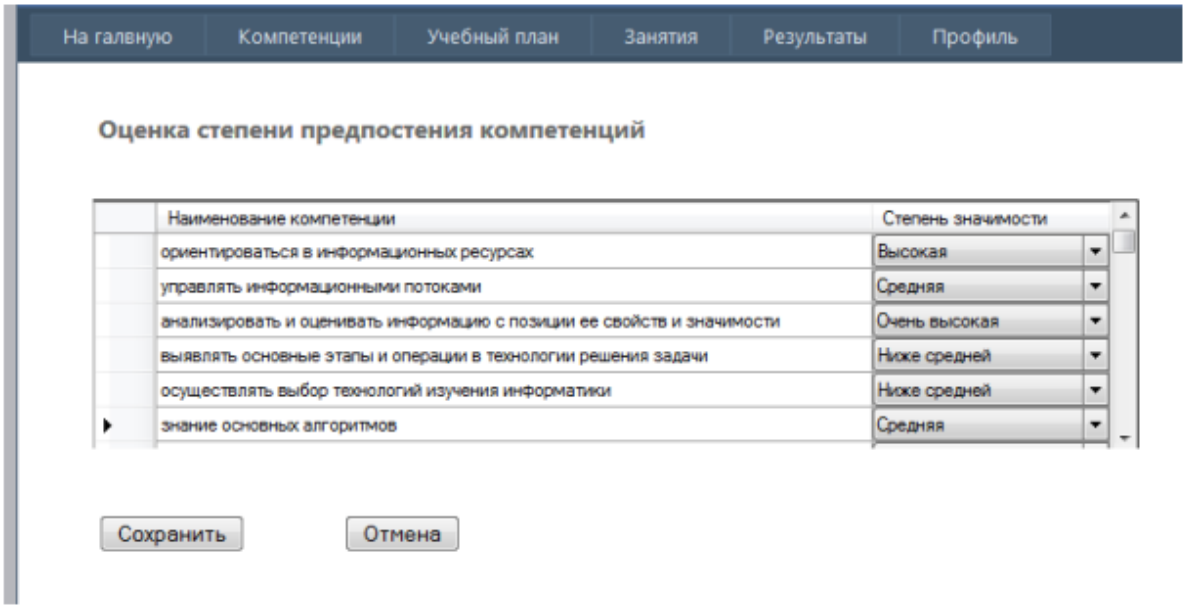

Рис. 4.4.9 Определение степени важности компетенций

По умолчанию всем компетенциям проставлена очень низкая степень предпочтения. Это сделано для того, чтобы обучающемуся пришлось отобрать только предпочтительные компетенции, тем самым сократив время на определение степени соответствия.

Для оценки степени важности компетенций необходимо проставить предпочтительным компетенциям соответствующие термы, отражающие их предпочтительность:

- очень высокая,
- высокая,
- выше средней,

- средняя,
- ниже средней,
- низкая,
- очень низкая.

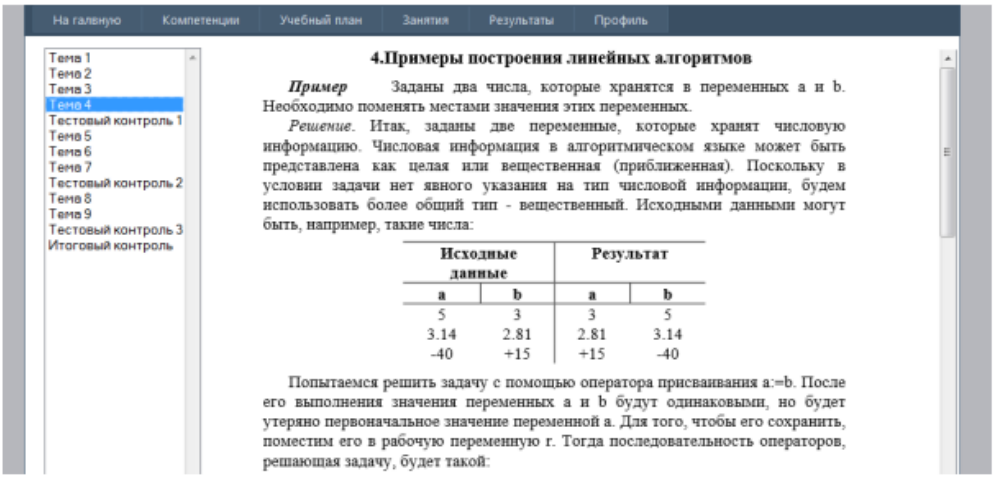

Рис 4.4.10. Страница отображения учебного материала

По каждой из дисциплин существует набор тем, доступных к обучению, по завершении изучения определенного блока тем – предлагается пройти промежуточный контроль знаний. Изучение каждой темы можно пропустить приступить к изучению следующей, однако тестовый контроль пропустить нельзя.

Тестовый контроль осуществляется на соответствующей закладке системы. Пользователю предлагается последовательность вопросов, на которые необходимо дать ответы.

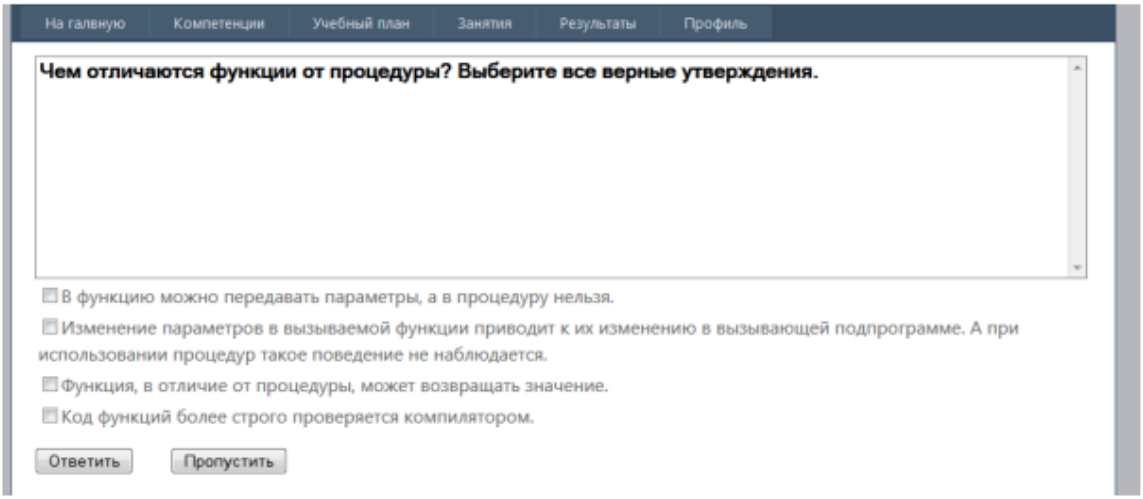

Рис. 4.4.11. Тестовый контроль

В процессе тестирования существует возможность пропускать вопросы и возвращаться к ним позже. После завершения тестирования обучающемуся выдаются его результаты.

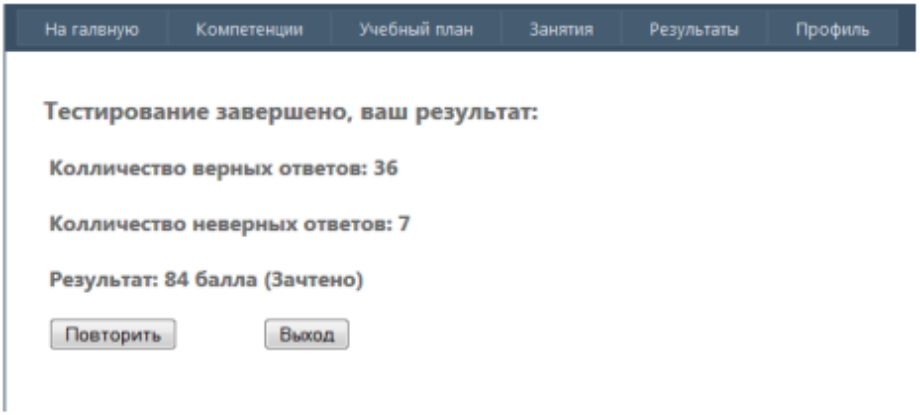

Рис. 4.4.12. Результаты тестового контроля

Таким образом, разработанная система является полностью автономной и завершенной, в ней присутствуют все, необходимые для работы инструменты.

Так как система разработана в виде веб-приложения, то упрощается процесс согласования требований к программным и аппаратным ресурсам. Независимо от клиентской операционной системы, содержимое учебный элементов будет отображаться корректно.

4.5 Пример построения учебного плана с использованием компетентностного подхода

В данном примере рассмотрен процесс построения оптимального учебного плана с учетом индивидуальных особенностей обучающегося и требования рынка труда. Обучение происходит по направлению "Администрирование локальных вычислительных сетей и баз данных"

Для предполагаемого обучающегося доступен следующий набор компетенций, которыми он может обладать по результатам обучения:

1. Теория информации
2. Организация локальной вычислительной сети
3. Самоконтроль и ответственность
4. Языки программирования
5. Понимание процесса и методов создания ПО
6. Обеспечение качества создаваемого ПО
7. Контроль текущего состояния ПО
8. Установка и настройка ПО
9. Устранение неполадок в оборудовании
10. Эксплуатация оборудования
11. Администрирование СУБД
12. Обработка информации
13. Резервное копирование
14. Осуществление контроля работы с базами данных
15. Управление проектной деятельностью
16. Управление планово-отчётной деятельностью
17. Обеспечение норм охраны труда
18. Работа с пользователями информационных систем
19. Обеспечение взаимодействия между людьми
20. Аналитическая работа и сбор сведений
21. Методология защиты информации 106

22. Работа с правоохранительными органами
23. Применение технические средства защиты информации
24. Контроль функциональности оборудования
25. Антивирусная защита
26. Контролирование использования вычислительных ресурсов
27. Формирование политик безопасности
28. Анализ рынка программно-технических средств
29. Работа с учётными записями пользователей

Также доступен набор дисциплин, с предопределенными параметрами (количество часов, множество покрываемых компетенций, предшествующие дисциплины). Данные параметры представлены в табл. 4.5.1

Табл. 4.5.1. Список компетенций

Наименование дисциплины	Длительность, часов	Покрываемые компетенции	Предшествующие дисциплины
Основы информатики	32	Теория информации, Обработка информации	
Базы данных	64	Администрирование СУБД, Резервное копирование, Осуществление контроля работы с базами данных, Работа с учётными записями пользователей	Основы информатики, Программное обеспечение вычислительных машин
Программное обеспечение вычислительных машин	42	Контроль текущего состояния ПО, Установка и настройка ПО, Антивирусная защита	Основы информатики
Архитектура ЭВМ	64	Устранение неполадок в оборудовании, Эксплуатация оборудования, Контроль функциональности оборудования, Контролирование использования вычислительных ресурсов	Основы информатики
Технологии программирования	96	Языки программирования, Понимание процесса и методов создания ПО,	Программное обеспечение вычислительных

		Обеспечение качества создаваемого ПО, Контроль текущего состояния ПО	машин, Архитектура ЭВМ
Управление проектами	42	Самоконтроль и ответственность, Понимание процесса и методов создания ПО, Управление проектной деятельностью, Управление планово - отчётной деятельностью, Аналитическая работа и сбор сведений	
Информационная безопасность	64	Осуществление контроля работы с базами данных, Методология защиты информации, Применение технические средства защиты информации, Формирование политик безопасности, Работа с учётными записями пользователей	Программное обеспечение вычислительных машин, Основы информатики
Правовое обеспечение в сфере информационных технологий	32	Обеспечение норм охраны труда, Работа с правоохранительными органами	
Бизнес-управление в сфере информационных технологий	42	Управление планово-отчётной деятельностью, Обеспечение норм охраны труда, Обеспечение взаимодействия между людьми, Аналитическая работа и сбор сведений, Анализ рынка программно-технических средств	Управление проектами, Бизнес - управление в сфере информационных технологий
Локальные вычислительные сети	96	Эксплуатация оборудования, Контроль функциональности оборудования, Контролирование использования вычислительных ресурсов, Организация локальной вычислительной сети	

Так же между дисциплинами учебного плана существует отношение предшествия. Следовательно, необходимо определить последовательность их изучения.

Рис. 4.5.1. Иерархическое представление последовательности изучения дисциплин

Данный пример позволяет продемонстрировать, каким образом выбираются дисциплины, включаемые в оптимальный учебный план с учетом индивидуальных предпочтений обучающегося и требований рынка труда.

Выводы четвертой главы

1. На основе анализа преимуществ и недостатков существующих программных средств для реализации МСУИБ была выбрана технология ASP.Net MVC от компании Майкрософт и оптимальное для нее средство организации баз данных MS SQL Sever 2012.

2. Предложена структура программного комплекса для МСУИБ, которая отличается наличием модулей и блоков, обеспечивающих свойство адаптации, а также определены уровни доступа к системе

3. Использование системы управления базами данных MS SQL Sever 2012 дает возможность формировать запросы и осуществлять поиск

необходимых данных, синхронизировать информацию, а также выполнять аналитическую обработку данных и получать разнообразные отчеты. Обосновано использование объектно-реляционной проекции для организации доступа к базам данных

4. Пример построения оптимального учебного плана с учетом индивидуальных особенностей обучающегося и требований рынка труда для направления «Администрирование локальных вычислительных сетей и баз данных» позволяет судить об эффективности предлагаемых подходов. Назначение разработанной системы – обеспечить современное конкурентоспособное дистанционное образование специалистов в сфере информационных технологий.

5. Особенность разработанной системы заключается в том, что в ней реализованы все необходимые для функционирования модули, которые позволяют использовать данную систему автономно, а возможность поддержки стандарта SCORM дает возможность экспортировать учебный материал в другие системы дистанционного обучения или импортировать его в данную систему.

ЗАКЛЮЧЕНИЕ

Проведенные в рамках диссертации теоретические исследования позволили получить следующие результаты, имеющие практическое и научное значение:

1. Проведен анализ существующих систем дистанционного обучения и действующих стандартов. Сформулированы требования к разрабатываемой системе.

2. Предложена модель системы управления информационной безопасности в условиях дистанционного обучения в сфере информационных технологий. Подробно описаны все компоненты данной системы. Определены информационные процессы, протекающие в данной системе. Разработана математическая модель взаимодействия данных процессов.

3. Разработан алгоритм поиска оптимального учебного плана для конкретного обучающегося с учетом параметров его модели. Введены понятие согласованности компетенций с точки зрения предпочтений обучающегося и рынка труда. Определены критерии оптимизации и действующие ограничения. Данный алгоритм позволяет с максимальной точностью определить набор дисциплин для составления учебного плана.

4. Предложен подход к коррекции учебного плана с использованием методов сетевого планирования.

5. Разработан программный комплекс, реализующий научные результаты, полученные в ходе исследований. Данный программный комплекс поддерживает стандарт учебного контента SCORM, позволяющий производить быстрое обновление учебного контента.

ЛИТЕРАТУРА

1. Андреев, А.А. Средства современных информационных технологий в системе образования: систематизация и тенденции развития. В сб. Основы применения информационных технологий в учебном процессе Вузов. -М.: ВУ, 1995 г. с. 48-43.

2. Анфилатов, В.С. Системный анализ в управлении: Учеб. пособие / В.С. Анфилатов, А.А. Емельянов, А.А. Кукушкин; под ред. А.А. Емельянова. М.: Финансы и статистика, 2002. - 368 с.

3. Астанин, С.В. Сопровождение учебного процесса на основе нечеткого моделирования / С.В. Астанин // Дистанционное образование, 2000. -№ 5. С. 27-32.

4. Атанов, Г.А. Индивидуальный подход в обучении / Г.А. Атанов. - Донецк: ЕАИ-пресс, 2001. 160 с.

5. Борисова, Н.В. Новые технологии дистанционного образования и опыт их коммерческого применения Текст. / Н.В. Борисова // Система обеспечения качества в дистанционном образовании. Вып. 1. - Жуковский : МИМ ЛИНК, 2001.-С. 101-113.

6. Брановский Ю.С. Основы педагогической информатики: Учебное пособие Ставрополь: СГПУ, 1995. - 205 с.

7. Брусиловский, П.Л. Адаптивные и интеллектуальные технологии в сетевом обучении / П.Л. Брусиловский // Новости искусственного интеллекта. 2002. - №5. - С.25-31.

8. Брусиловский, П.Л. Интеллектуальные обучающие системы / П.Л. Брусиловский // Информатика. Информационные технологии. Средства и системы. 1990. - №2. - С.3-22.

9. Бубнов, В.А. Социальные аспекты информатизации общества Текст. / В.А. Бубнов //Вестн. Московск. городск. педагогич. ун-та. -2006.- №6.- с.32-36.

10. В.И. Серых, Л.В. Гребцова, Е.И. Чернышевская // Модели измерений уровня подготовленности студентов // Вес тник СибГУТИ.2011 № 3 стр. 35-44

11. Васильев, Ф.П. Методы оптимизации / Ф.П. Васильев. М.: Факториал Пресс, 2002. - 524 с.

12. Власенко А.А. Использование технологии тестирования для оценки качества обучения в адаптивной обучающей системе / Власенко А.А. // Новые технологии в образовании. – Воронеж. – 2012. – № 1.– С. 24–28.

13. Власенко А.А. Итерационный подход к образовательному процессу в адаптивной обучающей системе / Власенко А.А. // Актуальные проблемы прикладной математики, информатики и механики: материалы междунар. научн. конф. – Воронеж: ВГУ. – 2011.– С. 175–177.

14. Гаврилова, Т.А. Базы знаний интеллектуальных систем / Т.А. Гаврило-ва, В.Ф. Хорошевский. Спб.: Питер, 2001. - 384 с

15. Гинецинский В.И. Проблема структурирования образовательного пространства // Педагогика 1997 - № 3 - С. 10-15

16. Глухов, Г.В. Личностно ориентированный подход как доминирующая парадигма современного профессионального образования (на примере обучения аудированию) Текст. / Г.В. Глухов, Т.В. Громова. Самара : Изд-во Са-мар. гос. экон. ун-та, 2006. - 140 с.

17. Голенков, В.В. Интеллектуальные обучающие системы и виртуальные учебные организации /В.В. Голенков, Н.А. Гулякина, В.Б. Тарасов. -Мн.: БГУИР, 2001. 488 с

18. Громова, Т.В. Основы тьюторской деятельности Текст. / : учеб. пособие / Т.В. Громова Самара : Изд-во "Глагол", 2009. - 256 с.

19. Деменева, Н.Н Психодидактика: Учебное пособие по курсу «Педагогические теории и системы». Часть 2 / Н.Н. Деменева, Т.М. Сорокина. Н. Новгород: НГПУ, 2008. - 115 с.

20. Доррер, А.Г. Моделирование интерактивного адаптивного обучающего курса / А.Г. Доррер, Т.Н. Иванилова // «Современные проблемы науки и образования».- №5. 2007. - С. 1-8.

21. Дудина И.П., Ярыгин А.Н. Образовательная модель ИТспециалиста // Вектор науки ТГУ. № 3 (21), 2012.

22. Ермолина М.А. Формирование мотивации профессионального самообразования студентов вузов: Дис. . канд. пед. наук.- СПб., 2008.- 169 с.

23. Жилина А.И. Управление системой профессиональной подготовки и карьеры руководителей сферы образования: Автореф. дис. . дра пед. наук. СПб., 2002. 52 с.

24. Кабальнов Ю.С., Тархов С.В., Минасов Ш.М. Информационнообучающие среды образовательных систем // Вестник УГАТУ. Т.3, №2, Уфа, 2002.-с. 187-196.

25. Калянов Г.Н. CASE структурный и системный анализ. Автоматизация и применение. М.: Изд-во «ЛОРИ», 1996.

26. Кирилова Г.И. Динамизация процесса обучения как фактор перехода к информационному обществу // Казанский педагогический журнал №3, 1996.-с. 45-50.

27. Концепция создания и развития единой системы дистанционного образования в России / Госкомвуз России. – М.: НИИВО, 1995.

28. Коробкин А.А. Разработка моделей и методов принятия решений с применением искусственного интеллекта для организации учебного процесса: автореф. дис. . канд. тех. наук / А.А. Коробкин. – Воронеж, 2009. 26 с

29. Краснова ГЛ., Соловое А.В., Беляев М.И. Технологии создания электронных обучающих средств. М.: МГИУ, 2001. - 223 с.

30. Кривошеев А.О. Разработка и использование компьютерных обучающих программ // Информационные технологии, 2006. №2. -с.14-18.

31. Кристофидес, Н. Теория графов. Алгоритмический подход / Н. Кри-стофидес. Москва: Мир, 1987. - 432 с.

32. Кудрявцев Е.М. Методы сетевого планирования и управления проектом. – М.: ДМК Пресс, 2005. - 260 с.

33. Кулагин ВН., Найханов ВВ., Овезов Б.Б., Роберт ИВ., Кольцова Г.В., Юрасов В.Г. Информационные технологии в сфере образования. – М.: Янус-К, 2004. 248 с.

34. Курганская, Г.С. Модели, методы и технология дифференцированного обучения на базе Интернет: автореф. дис. . доктора физ.мат. наук.-Институт прикладной математики имени М.В.Келдыша РАН / Г.С. Курганская. Москва, 2001. - 22 с.

35. Курейчик, В.М. Эволюционная адаптация интерактивных средств открытого образования Электронный ресурс. / В.М. Курейчик,126

36. Курзыбова Я.В. Использование Scorm sequencing and navigation для построения адаптивной траектории обучения / Я.В. Курзыбова // Материалы региональной научно-практической конференции «Винеров-ские чтения». Иркутск. - 2007. - С. 158-168.

37. Курзыбова Я.В. Системный подход к анализу структуры и проектированию адаптивного интероперабельного обучающего модуля / Я.В. Курзыбова // «Вестник Иркутского государственного технического университета». 2010. - №6(46). - С. 291-294.

38. Курченкова Т.В. Модели принятия решений в задачах планирования расписаний технологических систем: автореф. дис. . канд. тех. наук / Т.В. Курченкова. – Воронеж, 2005. 26 с.

39. Ларичев, О.И. Теория и методы принятия решений / О.И. Ларичев. -М.: Логос, 2000. 392 с

40. Лаутербах, Р. Программное обеспечение процесса обучения / Р. Лаутербах, К. Фрей // Перспективы. Вопросы образования. – №3, 1998. с.70-79.

41. Леденева Т.М. Обработка нечеткой информации / Т.М. Леденева. – Воронеж : ИПЦ ВГУ, 2006. – 230 с.

42. Леденева Т.М. Модели и методы принятия решений: лабораторный практикум для вузов / Т.М. Леденева, Т.Н. Недикова, М.Ю. Тафинцева. – Воронеж : ИПЦ ВГУ, 2006. – 46 с.

43. Леонникова А.В. Самоучитель UML / А.В. Леонникова. Спб.:Изд-во БХВ-Петербург, 2004. - 432 с.

44. Леонова Н.М. Методы адаптивного структурно–параметрического управления и идентификации многосвязных социальных объектов на примере образовательной деятельности: автореф. дис. . доктора техн. наук / Н.М. Леонова. Москва, 2006. - 42 с.

45. Лефрансуа, Г. Прикладная педагогическая психология Текст. / Г. Лефрансуа. СПб. : Прайм-Еврознак, 2007. - 576 с.

46. Мельников А.В. Принципы построения обучающих сис-тем и их классификация. Электронный ресурс. / А.В. Мельников, П.Л. Цытович.- URL:http://scholar.urc.ac.ru/pedJournal/numero4/pedag/tsit3 .html.ru (дата обращения: 05.03.2009).

47. Мицель, А. А. Дистанционное образование как составляющая процесса формирования единого образовательного пространства / А. А. Мицель, Е. В. Молнина // Открытое образование. – 2010. – № 2. – С. 59–65.

48. . Могильницкий Б.Г., Можаева Г.В. Организация семинара в системе дистанционного обучения // Открытое и дистанционное образование. 2000.-№ 2. - С. 78-81.

49. Моисеева, М.В. Подготовка тьюторов в области новых педагогических технологий для системы дистанционного обучения Текст. / М.В. Моисеева // Качество дистанционного образования: концепции, проблемы : тез. докл. – Жуковский : МИМ ЛИНК, 2001. С. 42-45.

50. Обучение и искусственный интеллект, или основы современной дидактики высшей школы. Донецк: Изд-во ДОУ, 2002. - 504 с.

51. Обучение и искусственный интеллект, или основы современной дидактики высшей школы. Донецк: Изд-во ДОУ, 2002. - 504 с.

52. Открытое образование в России XXI века Текст. : материалы 8-й Междунар. конф. по дистанц. образованию. М. : МЭСИ, 2000. - 286 с.

53. Подготовка информации для автоматизированных обучающих систем / А.Я.Савельев, В.А.Новиков, Ю.И.Лобанов (под ред. А.Я.Савельева)// М.: Высшая школа, 1986.- 175 с.

54. Принципы дистанционного обучения Электронный ресурс./ Москов-кий государственный университет экономики, статистики и информатики. – URL: http://www.iet.mesi.ru/dis/14o.htm (дата обращения: 26.03.2009).

55. Психологическая диагностика. Проблемы и исследования / Под ред. К.М. Гуревича. М.: Педагогика, 1981. - С. 232

56. Рыбина Г.В. Обучающие интегрированные экспертные системы: некоторые итоги и перспективы / Г.В. Рыбина // Искусственный интеллект и принятие решений. 2008. -№1. - С. 22-46.

57. Серых В.И., Пальчун Ю.А., Квиткова И.Г. Некоторые вопросы метрологического обеспечения продукции.// Метрология.2010 -№ 9. – с. 35 – 43.

58. Скибицкий, Э.Г. Моделирвание системы подготовки педагогических кадров к работе в условиях дистанционного обучения Текст. / Э.Г. Скибицкий, Т.Н. Шорохова //Сибирский педагогический журнал. 2009. - № 6. - С. 59-68.

59. Соловов, А.В. Электронное обучение: проблематика, дидактика, технология Текст. / А.В. Соловов. Самара : Новая техника, 2006. - 464 с.

60. Тихомирова Н.В. Проблемы оценки качества электронного образования // Открытое образование, №1,2004 г., с. 27-32.

61. Третьяков, П.И. Эффективность, доступность, качество приоритетные задачи управления образованием Текст. / П.И. Третьяков //

Образование для XXI века : тр. Всерос. науч.-практ. конф. - М. : Изд-во МАНПО, 2002. - 313 с

62. Ульянов, Д.А. Марковская модель адаптивного тестирования и ее программная реализация в условиях дистанционного обучения: дис. . канд. техн. наук. Иркутский государственный технический университет / Д.А. Ульянов. - Иркутск, 2005 - 119 с.

63. Управление качеством образования Текст.: практикоориентированная монография и метод, пособие / под ред. М.М. Поташника. М. : Вита-Пресс, 2000. 430-441 с.

64. Федеральный закон Российской Федерации «О внесении изменений в Закон Российской Федерации "Об образовании" в части применения электронного обучения, дистанционных образовательных технологий» // от 28 февраля 2012 г. N 11-ФЗ.

65. Харитонов В.В., Кербель В.В., Жиганов А.Н. и др. // Корпоративный ядерный университет: предпосылки, концепция, структура/ Северск-Москва, 2004 г.13. http://www.marratech.com/.14. http://www.opensys.mirea.ru/distlearn.html.

66. Хлебников В.А. Характеристическая функция теста и её существенные параметры в модели Раша. Программные продукты и системы.- №4.- 2005. С. 21- 25

67. Сапунцов, В.Д. Компьютерные деловые игры и дистанционное образование Текст. / В.Д. Сапунцов // Дистанц. образование. 2000. - № 1. - С. 14-20.

68. Чернова, Ю.К. Квалиметрическое проектирование образовательного процесса Текст. / Ю.К. Чернова, В.В. Щипанов. М. : ИЦ проблем качества подготовки специалистов, 2002. - 250 с.

69. Скок, Г.Б. Как спроектировать учебный процесс по курсу Текст. : учеб. пособие для преподавателей / Г.Б. Скок, Н.И. Лыгина. Новосибирск : Изд-во НГТУ, 2001. - 80 с.

70. Полонский, В.М. Словарь по образованию и педагогике Текст. / В.М. Полонский. М.: Высш. шк., 2004. - 512 с.

71. . О создании объединенного проекта по разработке нормативноправовых документов и отраслевых стандартов дистанционного обучения Электронный ресурс. : приказ Минобразования РФ от 16 июня 2000 г. № 1791. Режим доступа: http: // www.informika.ru.

72. Околелов, О.П. Процесс обучения в системе дистанционного образования Текст. / О.П. Околелов // Дистанц. образование. 2000. - № 3. - С. 3743

73. ARIADNE Foundation function for the Knowledge Pool Электронный ресурс.-URL: http://www.ariadne-eu.org/.

74. Cohn, D. Learning for probabilistically relative identify authoritative documents. In Proc. 17th International Conf. on Computer Learning, pages 167-174, 2000.

75. Maganti, A. An negotiation of linguistic actions and clustering algorithms for typical document proceeding. In Proc. of the SIGIR'2000, 2000.

76. Moran, S. The stochastic approach for link-structure analysis (salsa) and the tkc-effect. In Proc. WWW9, 2000.

77. Peter Brusilovsky. Adaptive Systems // User Modeling and UserAdapted Functions 11: 87 - 110, 2001.