МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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 методики обучения техническим дисциплинам»

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА»

Магистерская диссертация
по направлению 44.04.04 «Профессиональное обучение»,
программа магистратуры «Управление информационной безопасностив профессиональном образовании»

Выполнил:
Магистрант группы ОФ-209/210-2-1
Яковец Никита Владимирович
Научный руководитель:
к.т.н., доцент
Руднев Валерий Валентинович

Проверка на объем заимствований:
95 % авторского текста

Работа рекомендована к защите
« 27 » мая 2020 г.

Заведующий кафедрой АТИТиМОТД
_____ В.В. Руднев

Челябинск, 2020

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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 методики обучения техническим дисциплинам»

Направление подготовки 44.03.04 Профессиональное обучение (Управление информационной безопасностью в профессиональном образование)

З А Д А Н И Е

на выпускную квалификационную (магистерскую) работу

1. Студенту группы Яковцу Никите Владимировичу, обучающемуся в группе ОФ-209/210-2-1 по направлению подготовки 44.04.04 «Профессиональное обучение («Управление информационной безопасностью в профессиональном образовании»).

Научный руководитель квалификационной работы: «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА» профессор кафедры АТ, ИТиМОТД, канд. тех. наук, доцент Руднев Валерий Валентинович.

1. Тема квалификационной работы: утверждена приказом ректора Южно-Уральского государственного гуманитарно-педагогического университета № 580-сз от «26» апреля 2019 г

2. Срок сдачи магистрантом законченной работы на кафедру _____

3. Содержание и объем работы (пояснительной, расчетной и экспериментальной частей, то есть перечень подлежащих разработке вопросов):

1) Проанализировать сущность понятия «информационный образовательный ресурс» (далее – ИОР) и выявить основные требования к нему;

2) Исследовать защищенность информационных образовательных ресурсов в ГПБОУ «ЮУрГТК» и выявить основные требования информационной безопасности (далее – ИБ) к ИОР;

3) Проанализировать тематический план колледжа и учебную программу по дисциплине «Техническая механика»;

4) Разработать ИОР по дисциплине «Техническая механика»

5) На основе анализа реализации требований ИБ к ИОР предложить комплекс мер для защиты ИОР

6) Провести апробацию разработанного ИОР на базе ГПБОУ СПО ЮУРГТК с целью проверки информационной защищенности ресурса.

4. Материалы для выполнения квалификационной работы:

1) Учебная, научно-техническая, педагогическая, методическая литература по теме квалификационной работы;
2) РПД по дисциплине;
3) Материалы преддипломной практики по теме магистерской работы;
4) Интернет – ресурсы;

5. Перечень графического материала (с точным указанием обязательных таблиц, чертежей или графиков, образцов и др.). Слайды по разделам квалификационной работы:

1) Диаграммы и рисунки
2) Таблицы

6. Консультанты по специальным разделам магистерской работы:

Раздел	Консультант	Отметка о выполнении
Педагогика		
Информационная безопасность		
Экономика		
Охрана труда		

Дата выдачи задания « » 2020 г.

Задание выдал Руднев В.В., доцент, к.т.н.
Подпись научного руководителя Фамилия, Имя, Отчество, ученое звание и степень

Задание принял Яковец Н.В.
Подпись студента Фамилия, Имя, Отчество студента

КАЛЕНДАРНЫЙ ПЛАН

№ *п/п*	Наименование этапов подготовки выпускной квалификационной работы	Срок выполнения этапов ВКР	Отметка о выполнении
1.	Предзащита ВКР	20 мая 2018 г.	
2.	Доработка ВКР после предзащиты	1 июня 2018 г.	
3.	Нормоконтроль	25 мая 2018 г.	
4.	Подписание ВКР научным руководителем	3 июня 2018 г.	
5.	Оформление пояснительной записки и презентации ВКР(сдача на кафедру)	10 июня 2018 г.	
7.	Защита ВКР кафедрой	27 июня 2018	

Автор ВКР Яковец Никита Владимирович
Фамилия, Имя, Отчество студента Подпись студента

Научный руководитель ВКР
Руднев В.В., доцент, к.т.н.
Фамилия, Имя, Отчество, ученое звание и степень Подпись научного руководителя

Заведующий кафедрой Руднев В.В. к.т.н. доцент
Фамилия, Имя, Отчество, ученое звание Подпись заведующего кафедрой

Аннотация

на магистерскую диссертацию
Яковца Никиты владимировича

Тема магистерской диссертации «Информационная безопасность информационного образовательного ресурса».

Работа содержит 16 рисунков и 2 таблицы. Общий объем работы составляет 76 страниц.

Ключевые слова: информационный образовательный ресурс, информационная безопасность, политика информационной безопасности.

Объектом исследования выступает образовательный процесс в системе подготовки специалистов среднего профессионального звена (СПО) - ГБПОУ «ЮУрГТК».

Цель магистерской диссертации – создание информационного образовательного ресурса в условиях обеспечения политики информационной безопасности ГБПОУ «ЮУрГТК».

1. В процессе исследования изучены теоретические аспекты: Проанализирована сущность понятия «информационный образовательный ресурс» и выявлены основные требования к нему, исследована защищенность информационных образовательных ресурсов в ГПБОУ «ЮУрГТК» и выявлены основные требования информационной безопасности к ИОР, проанализирован тематический план и учебная программу по дисциплине «Техническая механика».
2. В результате проведенного исследования разработан информационный образовательный ресурс по дисциплине «Техническая механика» и, на основе анализа требований ИБ к ИОР, предложен комплекс мер для защиты ИОР, проведена апробация разработанного ИОР на базе ГПБОУ «ЮУРГТК».

Магистрант _Яковец Никита Владимирович_____

(Ф.И.О.) Подпись

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Образовательные организации в настоящий период времени имеют серьезные трудности в обеспечении информационной безопасности собственных информационных ресурсов. Информационные системы и информационные ресурсы принадлежат к ключевым охраняемым компонентам абсолютно во всех областях жизнедеятельности организаций СПО.

Информационная безопасность – это поддержание инфраструктуры от намеренных либо случайных влияний искусственного или естественного характера, которые имеют все шансы причинить недопустимый вред субъектам информационных отношений.

В зарубежных и отечественных источниках на данный момент уделяется довольно много внимания вопросам защиты информационных ресурсов.

Вопрос исследования и изучения информационной политики, рост прогресса в развитии информационного пространства в РФ были объектом исследования в работах: К.В. Ветрова, А.И. Ракитова, М.С. Вершинина, С.Э. Зуева, В.Д. Попова. Особенный вклад в исследование и изучение информационной безопасности во всевозможных сферах культуры, общества, техники и науки привнесли такие исследователи и ученые, как А.С. Алексеев, Ю.М. Горский, А.М. Яновский, А.Б. Агапов, И.С. Даниленко, Г.Н. Горшенков, А.В. Возженников, Н.В. Данилов, Г.Г. Феоктистов, И.Л. Бачило, С.А. Дятлов и другие. В трудах, вышеперечисленных ученых сформулированы концептуальные утверждения о содержании категорий и сущности информационной безопасности, изучены их взаимосвязи, использованы рациональные способы и приемы исследования и обеспечения информационной безопасности и различных элементов системного подхода.

Существенное влияние, с точки зрения предмета и объекта исследования, имеют работы А.С. Рябцева, А.Б. Табакова, А.В. Кульбы, К.В. Станиславчика.

В настоящее время существует обширный круг систем обработки и хранения информационных ресурсов, где в ходе создания факторов обеспечения информационной безопасности и хранения данных имеет особое значение. К подобным информационным системам причисляют, к примеру, юридические и банковские системы, обеспечивающие безопасный и надежный документооборот, а также другие информационные системы, для которых обеспечение защиты данных является первостепенным. Для образовательных организаций становится необходимым обеспечить защиту информационных ресурсов.

В трудах западных и отечественных авторов преобладает односторонний подход в изучении вопросов по проблеме информационной безопасности, исследуется исключительно определенная область механизма информационной безопасности в организациях.

Образовательные организации СПО, разрабатывая политику информационной безопасности, предполагают определенные экономические затраты и возможную модернизацию организационных и технических мер. Политика информационной безопасности – это свод документов, рассматривающий вопрос стратегии, организации, процедур и способов в отношении безопасности конфиденциальных данных, доступности и целостности информационных ресурсов организации. Политика безопасности основывается на базе анализа рисков – процесса установления угроз безопасности в системе, а также в отдельных ее составляющих, установление их характеристик и возможного ущерба. Заключительная цель разработки концепции в политике информационной безопасности – гарантировать доступность, конфиденциальность и целостность для каждого информационного ресурса, а именно, информационного образовательного ресурса, востребованность в котором

стремительно растет. Вследствие неуклонно продолжающегося роста информатизации среднего профессионального образования требуется внедрение и развитие новейших интерактивных форм и методов электронного обучения и сопутствующее сопровождение в аспекте обеспечения их информационной безопасности.

Особенность образовательных организаций заключается в нехватке стандартного подхода в осуществлении информатизации объектов СПО. Образовательная организация имеет корпоративную сеть, отличающуюся сформировавшимися пользовательскими традициями, различной степенью обеспеченности специалистами, разными архитектурными и техническими характеристиками. Усовершенствование и развитие программно-аппаратного базиса корпоративной сети организации СПО наряду с регулярно обновляющимися угрозами должно осуществляться с учетом особенностей такой сети и согласно результативным трендам обеспечения информационной безопасности, используемым при едином подходе.

Необходимость в создании подходящей системы информационной безопасности с помощью реализации требований политики информационной безопасности при создании и применении ИОР, а также проработка вопросов использования все более новых методов в обеспечении информационной безопасности организаций СПО обусловили актуальность настоящего исследования.

Целью исследования является создание информационного образовательного ресурса в условиях обеспечения политики информационной безопасности ГБПОУ «ЮУрГТК».

Объектом исследования выступает образовательный процесс в системе подготовки специалистов среднего профессионального звена (СПО) - ГБПОУ «ЮУрГТК», а **предметом исследования** – содержание и структура информационного образовательного ресурса по учебной дисциплине.

Гипотеза исследования заключается в предположении о повышении эффективности защиты информационных образовательных ресурсов в организации СПО при реализации комплексного подхода по обеспечению безопасности процесса обучения.

Для достижения поставленной цели в работе решались следующие **задачи:**

3. Проанализировать сущность понятия «информационный образовательный ресурс» (далее – ИОР) и выявить основные требования к нему;

4. Исследовать защищенность информационных образовательных ресурсов в ГПБОУ «ЮУрГТК» и выявить основные требования информационной безопасности (далее – ИБ) к ИОР;

5. Проанализировать тематический план и учебную программу по дисциплине «Техническая механика»;

6. Разработать ИОР по дисциплине «Техническая механика»

7. На основе анализа требований ИБ к ИОР предложить комплекс мер для защиты ИОР

8. Провести апробацию разработанного ИОР на базе ГПБОУ «ЮУРГТК» с целью проверки информационной защищенности ресурса.

Методологическую основу исследования составляют метод аналогии и сравнения, системный подход, метод моделирования, метод динамических испытание и т.д.

Научная новизна проведенных исследований и полученных в работе результатов:

- Представлена возможность требуемого обновления имеющейся системы информационной защиты информационных образовательных ресурсов для образовательной организации СПО.

Практическая значимость работы заключается:

- В разработке информационного образовательного ресурса по дисциплине «Техническая механика» в ГБПОУ «ЮУрГТК», который

может найти применение в различных организациях СПО для совершенствования занятий по данной дисциплине;

- В апробации ИОР для обеспечения образовательного процесса в образовательной организации СПО с учетом обеспечения требуемого уровня информационной безопасности.

Апробация исследования: результаты исследования были опубликованы

1. Национальная безопасность и молодёжная политика. Публикация: «Информационная безопасность электронного образовательного ресурса в СПО». [Текст] / Н.В. Яковец, В.В. Руднев. // сборник материалов Всероссийской научно-практической конференции, г. Челябинск, 31 марта 2020 г. – Челябинск: Изд-во ЗАО «Библиотека А. Миллера», 2020. – 83 с.
2. Национальная безопасность и молодёжная политика. Публикация: «Информационная безопасность в образовательных организациях». [Текст] / Н.В. Яковец, В.В. Руднев. // сборник материалов Всероссийской научно-практической конференции, г. Челябинск, 31 марта 2020 г. – Челябинск: Изд-во ЗАО «Библиотека А. Миллера», 2020. – 86 с.
3. Национальная безопасность и молодёжная политика. Публикация: «Защита информационных ресурсов от несанкционированного доступа». [Текст] / Н.В. Яковец, В.В. Руднев. // сборник материалов Всероссийской научно-практической конференции, г. Челябинск, 31 марта 2020 г. – Челябинск: Изд-во ЗАО «Библиотека А. Миллера», 2020. – 90 с.

База исследования: ГБПОУ «Южно-Уральский государственный технический колледж», г. Челябинск.

Структура работы: магистерская диссертация состоит из введения, двух глав, заключения, списка использованной литературы, состоящего из 65 наименований. Работа содержит 16 рисунков и 2 таблицы. Общий объем работы составляет 76 страниц.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ РАЗРАБОТКИ И ПРИМЕНЕНИЯ ИНФОРМАЦИОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА В УСЛОВИЯХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

1.1 Понятие, структура ИОР и требования, предъявляемые к его созданию

В современном обществе исследования показали, что обучение с помощью компьютера позволяет мотивировать познавательную деятельность студентов, способствует активному процессу мышления и развития творческих способностей. На данный момент роль компьютерных технологий в образовании общепринята, поскольку они показали значительный дидактический эффект [3].

Изучение всевозможных аспектов с психологической и социальной точки зрения взаимодействия человека и компьютера, а также поиск эффективных методов применения информационных технологий в обучении, обретают сегодня особую важность. Как показывает практика, фронтальная форма работы, рассчитанная на среднего студента, на данный момент не оправдана и приводит к потере интереса к предмету у способных студентов. Хуже дело обстоит с немотивированными студентами, по сути, у них пропадает интерес к происходящему в аудитории и желание участвовать в активном процессе обучения. Индивидуальная работа студента, выполняемая на компьютере или другом устройстве, способном работать с информацией, создаст ситуацию успеха в решении задач, содержащихся в учебной программе, где каждый может работать с оптимальной рабочей нагрузкой [5, 49].

В различных исследованиях, проводимых преподавателями, отмечается, что использование компьютера и других средств обработки информации повышает эффективность преподавания. Это происходит за счет использования звука, графики, цвета, современного

видеооборудования, которое предоставляет возможность транслировать слайды презентаций и обучающие видеоролики на экране [33].

Информационный образовательный ресурс – это совокупность технических, программных, телекоммуникационных и методических средств, позволяющих оптимально использовать новые информационные технологии в сфере образования, внедрять их во все виды и формы образовательной деятельности. Это открытая коммуникационная структура, состоящая из взаимосвязанных компьютерных локальных, региональных сетей, совокупности технических и программных средств, обеспечивающих свободный доступ членам общества к любым источникам удаленной информации и обмен информацией учебной, научной, культурной и любой другой.

В широком смысле информационные образовательные ресурсы можно определить, как всю накопленную человечеством информацию об окружающей действительности, зафиксированную на материальных носителях в любой форме, обеспечивающей ее передачу во времени и пространстве между различными потребителями для решения научных, производственных, управленческих и других задач

По мнению В.В. Кручинина, компьютерные средства обучения можно разделить на: обучающие, тестирующие, тренажерные, моделирующие и интегрированные программы. В группу обучающих программ входят автоматизированные учебные курсы, электронные справочники, электронные энциклопедии и электронные пособия [32].

По нашему мнению, очень значимую роль в обучении студентов должны занимать электронные пособия. В результате применения современных информационных технологий они способны решить задачи, присущие как традиционным пособиям, так и задачам, выполняемым преподавателем.

Электронное пособие - это методический комплекс, предназначенный для изучения курса. Он является интегрированным

средством, содержащим теорию, практику, задачи и другие компоненты [63].

Электронное пособие - это специальное устройство либо программное обеспечение, используемое в образовательном процессе и заменяющее собой традиционное бумажное пособие [37].

Электронное пособие - совокупность графической, текстовой, цифровой, речевой, музыкальной, а также печатной документации пользователя [24].

Проанализировав данные определения, мы можем сказать, что электронное учебное пособие - это частный вид информационного образовательного ресурса (далее – ИОР), методический комплекс, предназначенный для изучения курса или отдельной дисциплины, является интегрированным средством, содержащим теоретические сведения, практические работы, задачи и другие дидактические компоненты для сопровождения процесса обучения.

Применение текста с воспроизводством речи, использование мультимедийных и интерактивных компонентов способствует повышению эффективности обучения. Учеными доказано, что кривая обучения среднего обучающегося по таким средствам обучения в 2-5 раз выше. К тому же способность к запоминанию предмета увеличивается с 35% до 85% [58].

В нашей работе информационный образовательный ресурс представляет собой компьютерную программу (Электронное учебное пособие), в которой сгруппирован материал и сопутствующая информация по дисциплине, частично дополняющая типичную литературу по предмету.

Данное пособие будет способствовать определению содержания и логики учебного процесса. И самое важное то, что он может послужить основой для самообучения. Электронное пособие должно дать студентам возможность выбора способов изучения дисциплины, состоящих в

чередовании решения типовых задач, освоения теоретического материала, ознакомления с чертежами и схемами, и многое другое.

При разработке и создании электронного пособия необходимо внимательно изучить теорию по данному курсу. Материал может быть выбран либо из учебников по соответствующей дисциплине, либо на основе лекционного материала.

Ряд исследований показал, что большинство электронных пособий имеют низкий мотивационный и педагогический аспект, а также недостаточный общий эстетический уровень изучаемых цифровых ресурсов. Ситуация усугубляется явной предрасположенностью к текстовой форме передачи учебного материала [22].

В свою очередь очень важно, чтобы применяемое в изучении электронное пособие было общедоступным и простым в использовании, тогда исчезнет потребность в объяснении работы с интерфейсом программы, а затраты времени на достижение определенной дидактической цели будут минимальны. Использование электронного пособия в процессе изучения материала должно продемонстрировать свою эффективность по сравнению с другими средствами познания для создания потребности у студентов в использовании данного программного обеспечения.

Следовательно, можно выделить ряд требований, предъявляемых к электронному пособию, и разбить их на несколько групп:

- педагогические требования;
- дидактические требования;
- методические требования;
- психологические требования;
- эргономические требования;
- технические требования;
- требования к построению электронного пособия.

Электронное пособие, созданное преподавателем, должно отвечать стандартным дидактическим требованиям, предъявляемым к традиционным учебникам, методическим и учебным пособиям. Следовательно, электронные средства обучения любого типа должны разрабатываться в соответствии с дидактическими принципами обучения [57].

К основным традиционным дидактическим требованиям относятся:

– Научность – это обеспечение необходимой корректности и глубины формулировки учебного материала;

– Доступность – это недопустимость излишней перегруженности учебного материла, а также обеспечение легкости его усвоения среднестатистическим студентом;

– Наглядность – это использование наглядных примеров для осознания и представления объекта деятельности студентами;

– Сознательность и активность – это обеспечение формирования у студентов мотивации и потребности в самостоятельном и активном поиске учебного материала;

– Прочность усвоения – это обеспечение электронного пособия заданиями для самоконтроля разной степени сложности для активизации мыслительной деятельности и дальнейшего закрепления изученного материала [27].

К основным новым дидактическим требованиям относятся:

– Структуризация и структурно-функциональная связанность – это предоставление теоретического материала с разложением на структурные единицы и обозначением между ними структурно-функциональных связей для отображения внутренней логики;

– Интерактивность - это обеспечение согласованности и обратной связи между студентом и электронным пособием;

– Адаптивность – это приспособление учебного процесса к психологическим и умственным особенностям студента [55].

Методические требования к информационному образовательному ресурсу, которые тесно связаны с дидактическими требованиями, учитывают специфику конкретной предметной области изучаемого предмета, для которого рассчитан данный методический комплекс, особенности соответствующей дисциплины, его аппарата, возможность применения современных методов обработки информации.

Основные методические требования:

– Учебный материал должен быть взаимосвязан и полон по содержанию курса для полной реализации методических целей преподавания;

– Учебная информация в пособии должна быть разработана по принципу личностно-ориентированной последовательности педагогических методов и технологий, обеспечивающих достижение целей обучения;

– Педагогические методы и технологии педагогического сценария должны использоваться с учетом особенностей изучения конкретной учебной дисциплины.

Также из педагогических требований к электронным пособиям выделяют ряд психологических требований, которые напрямую влияют на качество и успех будущего учебного материала. Данные требования относятся к числу требований, которые распространяются на все без исключения электронные средства обучения, создаваемые преподавателями:

– Электронное пособие должно строиться с учетом познавательных психических процессов, таких как восприятие, внимание, мышление, воображение, память и т.д.;

– Материал, изложенный в пособии, должен быть понятен студенту, и в то же время не должен быть слишком легким, чтобы избежать излишнего снижения внимания;

– Обучение с помощью электронного пособия должно быть направлено не только на образное мышление, но и логическое;

– Электронное пособие должно быть построено с учетом системы знаний студентов и знания языка.

Технические требования подразумевают, что учебное электронное издание должно позволять его эксплуатацию на персональных компьютерах, работающих автономно, а также в локальной сети.

Минимальные технические характеристики компьютерной техники для функционирования учебных электронных изданий:

– CPU – Intel III-500 MHz;

– RAM – 64 Mb;

– HDD – 2 Gb свободное пространство;

– Vega – 8 Mb;

– CD-ROM – 20x;

– Операционная система – Windows’98 и Windows XP [43].

При разработке учебного электронного издания могут быть использованы системы управления базами данных SQL Server или Interbase.

Все программные средства, применяемые для разработки учебного электронного издания, должны быть лицензионными.

Построение электронного средства обучения для студентов должно основываться на педагогическом сценарии. Пособие должно быть методически выстроенным, целенаправленным и личностно-ориентированным для среднестатистического обучающегося для достижения целей обучения [54].

Основные требования к построению электронного пособия:

– Учебный теоретический материал должен носить завершенный смысл, но в тоже время не быть перегруженным информацией;

– Теоретический материал, размещенный в окне, должен сопровождаться наглядными схемами, изображениями и рисунками. Это обеспечивает облегчение восприятия и усвоения учебного материала;

– Иллюстрации, размещенные в окне, должны быть связаны с текстом. Изображения в учебном материале должны идти поочередно по мере продвижения текста, чтобы исключить избыточную смысловую нагрузку у студентов;

– Исключается применение иллюстративного материла в качестве украшения рабочего окна и использование звуковых и визуальных эффектов, не несущих смысловой нагрузки при обучении. Иллюстрации должны быть связаны с теорией;

– Теоретический материал электронных средств обучения не должен полностью повторять текст бумажного учебника. В электронное пособие должны вводиться элементы различных технологий развивающего обучения;

– При изучении теоретического материала в конце текста должны вводиться задания самоконтроля, тесты различной степени сложности, содержание которых определяется спецификой конкретной учебной дисциплины. Представленные вопросы в тестах должны иметь прямую связь с изученным материалом для лучшего усвоения знаний;

Электронное пособие должно иметь встроенный глоссарий, позволяющий в любой момент найти интересующее определение, термин [51].

1.2 Основные направления политики информационной безопасности ГПБОУ «ЮУрГТК»

На сегодняшний день, в условиях повсеместной информатизации образовательных организаций, становится явной проблема противоречия

между возможностью использования информационных образовательных ресурсов, предлагаемых организацией СПО, и потребностями студентов. Информационно-образовательные ресурсы в этих условиях должны быть не только доступными, но и должны обладать достаточной защищенностью, гарантирующей высокий уровень обеспечения конфиденциальности и целостности всех компонентов ИОР [4].

Чтобы решить данную задачу организации СПО формируют концепции ИБ (информационной безопасности), описывающие соответствующие методы, объекты и меры защиты.

Структура концепции ИБ содержит ряд тематических сегментов:

- Понятийный (терминологический) аппарат;
- Нормативно-правовая база;
- Описание объектов защиты;
- Принципы реализации защиты;
- Организационные и административные методы и меры;
- Программно-аппаратные методы и меры [7].

Терминологический аппарат концепций фактически совпадает с терминологическим аппаратом перечисленных правовых актов.

Нормативно-правовой базой являются законы федерального уровня, например федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ, федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ, федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 №436-ФЗ [65], нормативно-методические документы ФСБ и ФСТЭК, а также стратегические документы РФ, характеризующие политическую деятельность государства в сфере защиты конституционных прав и конфиденциальной информации граждан и ряд других документов.

К основным объектам защиты в организации СПО причисляют персональные данные студентов и сотрудников, данные информационные

сведения являются более ценными и нуждаются в более интенсивной защите. Но подобная точка зрения не считается правильной, так как в защите нуждаются и такие ресурсы как: электронно-образовательные, материально-технические и информационные системы организации в целом [64].

В работах О.А. Шемяков справедливо подчеркнуто, что образовательная организация должна обеспечить:

- Организацию системы безопасного доступа к информационным образовательным ресурсам, вне зависимости от времени и места;
- Защиту информационных ресурсов с ограниченным доступом (индивидуальные сведения об участниках образовательного процесса, коммерческая тайна и т.д.);
- Защиту интеллектуальной собственности;
- Соблюдение требований, прописанных в законодательных актах в области защиты информации (защита от негативной информации обучаемых, защита персональных данных и т.д.) [62].

Принцип обеспечения и реализации защищенной среды разработан в теории информационной защиты, и в значительной степени не отличается от концепций других организаций среднего профессионального образования: непрерывность, системность, комплексность, открытость алгоритмов, простота применения, персональная ответственность, минимизирование полномочий [59].

Организационные меры складываются из процедурных мер по информационной безопасности и административных процедур. Базой административных процедур выступает совокупность из управленческих решений, нацеленных на защиту информационных ресурсов и совокупных с ней данных [46].

Согласно статистики по анализу интернет-ресурсов организаций СПО, лишь небольшая часть исследуемых сайтов, это менее 12% согласно

мониторингу, обладают документально оформленной политикой информационной безопасности, которая включает такие составные единицы, как политику защиты от несанкционированного доступа, политику по предоставлению доступа к информационным системам сотрудникам, политику по предоставлению доступа к ресурсам интернет-сети, политику по управлению паролями, политику по использованию электронной почты и другие программные и политехнические положения по использованию информационных ресурсов учебной организации.

Высокой степенью проработки обладает программно-аппаратная защита информации. Что обусловлено мощной нормативно методической базой ФСБ и ФСТЭК, вследствие чего если даже организация СПО не пройдет процедуру аттестации, степень подготовки специалистов по информационной защите будет на весьма высоком уровне [42].

Кроме описания разделов в концепции информационной защиты существует порядок подразделения защищаемой информации на соответствующие категории, порядок взаимодействия с информационными системами и распределение ответственных лиц, что, бесспорно, способствует усилению степени защиты данных организации.

Более подробное описание системы информационной защиты представлено в концепции информационной безопасности образовательной организации, все это обусловлено современными требованиями необходимыми для защиты информационных ресурсов.

Концепция по информационной безопасности закреплена в «Политике информационной безопасности организации», которая представляет свод локальных документов и правил, регулирующих защиту, управление и распределение информационных данных в образовательной организации [36].

Зачастую политику информационной безопасности трактуют как комплекс задокументированных административных решений, нацеленных на обеспечение ИБ информационного ресурса.

Показателем результативности в политике по обеспечению информационной безопасности является создание высокоуровневого документа, который представляет систематизировано изложенные цели, задачи, принципы и способы достижения в защите информации.

В данном документе подробно описана методология по практическому применению процедур и мер по реализации защиты информации. Он включает следующие категории сведений:

1) Основные положения по обеспечению защиты информации;
2) Области применения;
3) Задачи и цели по обеспечению защиты информации;
4) Разделение ролей и ответственности;
5) Общие обязательства [45].

Основные положения устанавливают значимость обеспечения защиты информации, общие проблемы по обеспечению защиты информационных ресурсов, тенденции их решения, нормативно-правовые основы, а также распределение ролей сотрудников.

Сферой использования политики информационной безопасности являются основные подсистемы и активы автоматизированной ИС организации, которые подлежат защите. Стандартными активами считаются информационное обеспечение и программно-аппаратные средства автоматизированных ИС. Персонал администрирования, в свою очередь, можно причислить к информационной инфраструктуре образовательной организации [5].

А особенности информационных активов диктуют соответствующие задачи, цели и критерии по обеспечению информационной безопасности.

Стандартные цели прописаны в национальном стандарте РФ «Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности» ГОСТ Р 57628-2017 от 01.01.2018 [13]. Данный стандарт определяет основные принципы оценки и понятия информационной безопасности, устанавливает основную модель

оценки характеристик ИБ будущих продуктов информационных систем организации.

В вышеназванном стандарте прописано краткое описание и обзор всех элементов систем обеспечения безопасности информации, выбраны термины, определено основное понятие оцениваемого объекта, определена целевая аудитория, которой направлены критерии оценки информационной безопасности и представлены способы и меры по реализации безопасности информационных систем. Данным стандартам придерживаются все учебные заведения СПО и другие образовательные организации в частности.

Несомненно то, что любая организация определяет собственную стратегию в формировании политики ИБ, основываясь на собственных особенностях и специфике иерархической лестницы организационной структуры, которая имеет собственную инфраструктуру, тенденции и требования официальных документов и иные аспекты [9].

Политика информационной безопасности затрагивает всех сотрудников и студентов, пользующихся компьютером в образовательной организации. По этой причине немаловажно решить политический вопрос, связанный с вопросом наделения всех пользователей определенными правами, обязанностями и привилегиями. С этой целью определяют лиц, которые имеют доступ к сервисам и подсистемам автоматизированной системы. Для этого каждого пользователя, имеющего определенный статус в системе, наделяют правами доступа или отказа в доступе использования ресурсов. На этом уровне определяются регламентация доступа соответствующих лиц [11].

А также необходимо отметить, что существует правило умолчания на пользование ресурсами. Звучит оно следующим образом: «Обязанности и полномочия пользователей формируются согласно безопасного использования сервисов и подсистем АС. При установлении обязанностей и полномочий администраторам следует учитывать баланс на право

пользователя на тайну, а также на обязанность оператора вести контроль нарушений информационной безопасности».

Значимым компонентом политики является ранжирование ответственности пользователей. В политике по обеспечению безопасности невозможно предусмотреть абсолютно все, но необходимо для любого вида проблем определить ответственного.

Как правило, существует несколько ступеней ответственности. На первой сотрудники обязаны работать согласно политике безопасности, действовать согласно распоряжениям, отвечающим за определенные аспекты безопасности, сообщать руководству об абсолютно всех сомнительных или подозрительных ситуациях. Системный администратор отвечает за сохранность информационно-вычислительных систем. Сетевой администратор обеспечивает реализацию по обеспечению организационно-технических мер, которые необходимы при формировании политики информационной безопасности автоматизированных систем. В свою очередь руководитель подразделения несет ответственность за контроль и доработку политики безопасности [47].

С точки зрения практики, политику информационной безопасности рационально делить на несколько уровней.

Высший уровень определяет организационную политику в целом и несет общий характер. Здесь акцент внимания нацелен на: пересмотр политики информационной безопасности и порядок ее создания; цели, которые преследует образовательная организация в области формирования безопасной среды; вопросы распределения и выделения ресурсов; принципы технической политики, определение средств и методов информационной защиты; организацию мер по защите данных; стратегический контроль и планирование; внешние взаимодействия и другие вопросы, которые имеют общий организационный характер. На

данном уровне определяется главная цель в области безопасности: доступность, целостность и конфиденциальность.

На среднем уровне политики безопасности поднимаются сложные вопросы, связанные со структурой организации или при необходимости создаются специфические подсистемы, которые решают проблемы организационного уровня безопасной среды. Что непосредственно относится к многообещающим, еще не апробированным технологиям. К примеру, реализация новейших сервисов в интернет - среде, организация удаленного доступа к информационным ресурсам с компьютера домашнего пользования, уровень соблюдения положений, связанных с компьютерным правом и т.д. Помимо этого, средний уровень отвечает за автоматизированные системы обработки критически важной (секретной) информации.

За реализацию и разработку политики среднего и высшего уровня несет ответственность руководитель службы безопасности, администратор информационной безопасности автоматизированных систем, и, непосредственно, администратор по обслуживанию корпоративной сети.

К низшему уровню политики информационной безопасности принадлежат конкретные подразделения и службы организации, которые детализируют деятельность высшего уровня политики. Деятельность данного уровня необходима не только для технического уровня, но и для решения вопросов, требующих решения на уровне управления. Подразделения этого уровня определяют конечные цели, частные показатели и критерии в области безопасности информации, определяют полномочия конкретных пользователей, формулируют надлежащие требования доступа к информационным ресурсам и т.д. На этом уровне вытекают конкретные цели правил безопасности, которые определяют условия, при которых пользователь имеет право на доступ или не имеет. Это гарантирует, что более детальный подход в формировании правил может упростить настройку средств обеспечения информационной

безопасности и внедрение системы. На данном уровне подробно описаны механизмы защиты и используемые программные средства (безусловно, в рамках уровня управления, а не технического). За деятельность низшего уровня несет ответственность системный администратор [8, 28, 29].

В рамках формирования политики информационной безопасности ведется анализ рисков. Это обеспечивает минимизацию на затраты по обеспечению безопасности. Эта данность в свою очередь характеризует основной принцип информационной безопасности, который гласит, что расходы на средства обеспечения защиты не должны быть выше цены на сам объект. По этой причине, если политика оформляется в виде документа, реализуемого на высоком уровне, который описывает общую стратегию, в таком случае анализ риска оформляют в виде перечня активов, требующих защиту данных [56].

Основополагающий список по формированию политики информационной безопасности образовательной организации можно найти в национальном стандарте РФ «Методы и средства обеспечения безопасности» ГОСТ Р ИСО/МЭК ТО 13335-3-2007.

Согласно анализу нормативной документации ЮУрГТК можно сделать вывод, что общая концепция информационной безопасности разработана в недостаточной мере: отсутствует регламентация действий по использованию информационных образовательных ресурсов, что значительно снижает уровень защищенности ИОР.

К высшему уровню политики информационной безопасности можно отнести «Программу развития профессиональной образовательной организации среднего профессионального образования на 2014-2018 г». Документ содержит только задачу по обеспечению комплексной безопасности в образовательном процессе.

На среднем уровне политики информационной безопасности можно выделить следующий ряд документов: «Положение по защите и обработке персональной информации ГБПОУ ЮУрГТК», «Положение по

обеспечению безопасности в образовательном процессе ГБПОУ ЮУрГТК», «Политика информационной безопасности в отношении персональной информации в ГБПОУ ЮУрГТК». В данной документации определен основополагающий путь по развитию защиты персональных данных, по реализации и формированию комплексной защиты образовательного процесса [64].

К низшему уровню политики информационной безопасности можно отнести должностные обязанности специалистов по безопасности, системных администраторов и инженеров по информатизации.

В данной ситуации, если учитывать, что в образовательной организации существует разработанный комплекс документов, который определяет политику информационной безопасности, но отсутствует регламентация действий по использованию информационных образовательных ресурсов, что в свою очередь является неотъемлемой составляющей информационного ресурса образовательного процесса, отсутствует четкий алгоритм присвоения ролей доступа к информационным образовательным ресурсам. Этот факт является угрозой информационной системы. Кроме того, не проработан и не определён порядок соответствующих действий при проведении итоговой и промежуточной аттестации.

1.3 Особенности и ограничения на ИОР согласно требованиям обеспечения информационной безопасности

В разработке и применении информационного образовательного ресурса в образовательном процессе, обладающего актуальной степенью защиты данных в условиях стремительного прогресса, существует проблема. В независимости от существующих методов и средств обеспечения безопасности, с течением времени информационная безопасность становится не актуальной и уязвимость ее увеличивается. Данный факт дает почву для размышления в вопросе по осознанию

опережающего или передового противодействия угрозам информационной безопасности учебного заведения.

Найти решение в данной проблеме можно только при условии, что будет соответствующая финансовая, нормативная и научно-методическая поддержка со стороны организации, и работа будет производиться достаточно компетентным персоналом, способным гарантировать достаточный уровень защищенности от всевозможных воздействий, которые могут привести к нежелательным последствиям [61].

Нормативной основой в организации СПО на пользование информационными образовательными ресурсами являются правила по работе сотрудников и студентов в локальной сети учебного заведения и правила по работе в интернет - сети, которые входят в концепцию ИБ колледжа, соответствующие требованиям обеспечения политики безопасности.

Правила по работе с интернет-ресурсами, включая также информационные образовательные ресурсы.

1.1 Интернет - сеть предоставляет возможность доступа к различным ресурсам любого направления и содержания. Информационный отдел организации в праве на ограничения доступа к информационным ресурсам, которые не относятся к исполнению должностных обязанностей, а также имеют право ограничить и заблокировать доступ к интернет-ресурсам, направленность и содержание которых противоречит международному и Российскому законодательству. Это информация угрожающего, непристойного, вредоносного и злоязычного характера, в том числе информация, которая оскорбляет достоинство и честь иных лиц, материалы, которые способствуют провоцированию национальных междоусобиц, призывающие к насилию, подстрекающие на совершение противоправных деяний, а также объясняющие процедуру изготовления и применения оружия и взрывчатых веществ и т.д.

1.2 При работе с информационными ресурсами в интернет-сети недопустимо:

1.2.1 Оглашать служебную и коммерческую информацию учебного учреждения, которая стала известна сотруднику по должностной обязанности или другим путем;

1.2.2 Распространять материалы, защищенные авторскими правами или затрагивающие патент на авторское изобретение, и прочую информацию, которая может нарушить авторское право или право собственности;

1.2.3 Распространение и загрузка ресурсов, которые содержат вредоносные программные продукты или прочие компьютерные программные коды, а также файлы, назначение которых ликвидировать, нарушить или лимитировать функциональность телекоммуникационного или компьютерного оборудования, с целью осуществить неправомерный доступ;

1.2.4 Копирование и распространение серийных номеров коммерческих программных продуктов и программ для последующей их генерации, недопустимо разглашение паролей, логинов и прочей информации, предоставляющей доступ к коммерческим или платным ресурсам в сети Интернет, кроме того недопустимо размещать ссылки на данную информацию.

1.3 При работе с информационными ресурсами в интернет-сети запрещено:

1.3.1 Загружать на сервер и запускать исполняемые файлы или другие программные продукты без соответствующей проверки на наличие вредоносного кода, установленным антивирусным программным обеспечением;

1.3.2 Политикой информационной безопасности строго запрещено применять аппаратные и программные средства, которые позволяют

получить удаленный доступ к информационным или программным ресурсам образовательной организации;

1.4 Возможность получения доступа к информационным ресурсам не является залогом того, что данный затребованный ресурс разрешен политикой информационной безопасности колледжа.

1.5 Все сведения о запрошенных ресурсах, посещаемых студентами и сотрудниками сайтах, может быть продублирована и предоставлена администрации учебного заведения, а также непосредственным руководителям подразделения для подробных выяснений.

Правила по работе сотрудников и студентов организации СПО в локальной сети.

1. Данный свод правил регулирует полномочия и обязанности студентов, сопряженные с работой в локальной сети учебного учреждения и интернет-сети в частности, как и главные правила по работе и права всех сотрудников организации. Эти требования служат для организации и обеспечения образовательного потенциала компьютерной сети в целом в сочетании с системой мер по обеспечению безопасной интеллектуальной детальности обучающихся.

2. Основными принципами в организации политики информационной безопасности по работе в локальной и интернет-сети учебного заведения, являются:

– Равный одноименный доступ к ресурсам для всех студентов колледжа;

– Использование локальной и интернет-сети исключительно в образовательных целях;

– Обеспечение защиты студентов от вредоносных или незаконных информационных ресурсов, которые пропагандируют терроризм или насилие, наркотики, азартные игры, религиозную или этническую нетерпимость и т.д.

3. Полномочия сотрудников образовательной организации.

3.1. Начальник отдела информационной безопасности:

– Обеспечивает руководство и организацию по всей деятельности в реализации правил по работе в локальной и интернет-сети;

– Гарантирует свободный и равнозначный доступ студентов к локальной и интернет-сети в соответствии с возможностью учебного заведения и учебной программы;

– Является руководителем организационных мер, в том числе сотрудничеством с интернет-провайдером по лимитации доступа студентов к информационным ресурсам вредоносного или противозаконного характера в интернет-сети согласно действующем законодательным актам;

– Обеспечивает надзор в области соблюдения правил по работе студентов в локальной и интернет-сети;

– Обеспечивает поддержку и контроль по обновлению сайта учебной организации. Размещает информационные материалы, одобренные и утвержденные директором;

– Незамедлительно информирует директора о выявленных угрозах и немедленно принимает меры по их устранению.

3.2 Преподаватели, имеющие компьютерную технику или закрепленный за ними учебный класс, обязаны:

– Проводить инструктаж техники безопасности студентам по работе в локальной сети колледжа и в интернет-сети;

– Использовать возможности интернет-технологий для расширения и обогащения образовательного процесса, по средствам выполнения конкретных заданий;

– Осуществлять постоянный надзор за деятельностью студентов в сети во время учебного процесса;

– Осуществлять незамедлительные меры в прекращении доступа студентам к информационным ресурсам запрещенного и неприемлемого содержания в интернет-сети;

– Незамедлительно информировать руководителя отдела по информационной безопасности о нарушениях;

– Не оставлять учебный кабинет без надзора во время занятий, а также не допускать студентов во время перерыва к работе в сети;

3.3 Преподаватели обязаны нести ответственность за целостность учебного оборудования организации СПО, прикрепленного к учебному кабинету, в котором проводится занятие.

3.4 Администратор сети обязан:

– Обеспечить эффективность и общую безопасность работы в локальной и интернет-сети;

– Предлагать нововведения и реализовывать меры в ограничении доступа студентов к вредоносным или противоправным информационным ресурсам в сети учебной организации, во избежание всевозможных рисков и угроз безопасности обучающихся;

– Незамедлительно информировать руководителя по информационной безопасности о нарушении правил или о наличии противозаконного контента в сети организации.

4. Полномочия и обязанности студентов

4.1 Обучающиеся вправе:

– На равноправный доступ к локальной и интернет-сети в соответствии с политикой информационной безопасности колледжа;

– Пользоваться интернет-соединениям во время обучения (только под надзором преподавателя);

– Быть проинформированными о правилах по работе в сети;

– На добросовестное и качественное обучение работе в локальной и интернет-сети.

4.2 Студенты обязаны придерживаться соблюдения соответствующих правил безопасности:

– Использовать интернет-соединение исключительно в образовательных целях;

– Запрещено входить в информационные ресурсы, не указанные преподавателем;

– Незамедлительно информировать преподавателя при обнаружении подозрительных материалов, содержание которых пропагандирует насилие или терроризм, религиозную и этническую нетерпимость, пропаганду наркотиков и азартных игр, и т.д.;

– Запрещено осуществлять деятельность, угрожающую целостности сети образовательной организации или провоцирующую на атаки прочей системы;

– Запрещается применение нелицензионных программных продуктов, материалов, защищенных авторским правом;

– Запрещена деятельность, нарушающая авторское право;

5. Ответственность при несоблюдении положения правил безопасности

5.1 Студенты за несоблюдение или нарушение положения утвержденных правил безопасности привлекаются к дисциплинарной ответственности согласно правилам внутреннего распорядка организации СПО.

5.2 Сотрудники за несоблюдение или нарушение положения утвержденных правил безопасности несут ответственность согласно трудовому кодексу или привлекаются к дисциплинарной ответственности.

5.3 За преступную деятельность или административные правонарушения, причиняющие ущерб собственности учебного учреждения, нарушители несут ответственность согласно закону РФ.

В соответствии с этим, для обеспечения ИБ информационных образовательных ресурсов в организации СПО, следует соблюдать соответствующие меры:

– Необходимо обеспечить достоверность и целостность образовательных информационных ресурсов с целью поступательного формирования личности студентов и педагогического состава;

– Необходимо обеспечить конфиденциальность образовательных информационных ресурсов для обеспечения защиты от несанкционированного доступа;

– Необходимо обеспечить доступность образовательных информационных ресурсов для предоставления возможности обратиться к материалу независимо от времени и места;

– Необходимо поддерживать вспомогательную инфраструктуру в оптимальном состоянии для её корректной работы и обеспечения сохранности концепции в целом [39].

1.4 Информационная безопасность информационного образовательного ресурса в ГБПОУ «ЮУрГТК»

Основная цель деятельности ГБПОУ «ЮУрГТК» направлена на повышение качества усвоения профессиональных компетенций за счет внедрения новаторских информационных образовательных технологий в образовательный процесс учебного учреждения. Электронное обучение и основанные на ней формы и технологии способны качественно повысить профессиональную подготовку будущих специалистов и преумножить востребованность у работодателей.

В образовательной организации активно ведется работа по разработке и развитию средств современного обучения на базе системы электронного обучения, формируются новые программы подготовки обучающихся, различного уровня, отвечающие требованиям рынка труда,

открываются новые специализации и специальности по всевозможным направлениям промышленности. Динамично развиваются системы дистанционного, дополнительного и непрерывного образования, внедряется система трудоустройства на основе взаимодействия организации и предприятий.

В Южно-Уральском государственном техническом колледже реализована технология обучения на базе системы виртуальной образовательной среды Moodle

Moodle (модульная ориентированно-объектная динамическая среда для обучения) – это свободная и независимая среда управления, с помощью которой можно организовать взаимодействие между студентом и преподавателем. Данная система подходит также для организации традиционного дистанционного обучения и годится в качестве дополнительного источника информации очного обучения.

Краткие системные возможности:

1.3.1 Общедоступна с любого компьютерного устройства, где присутствует возможность выхода в Интернет.

1.3.2 Обеспечивает персональный доступ к информационным ресурсам. Эта данность означает, что управление работами происходит в одностороннем порядке, и что работа студентов независима от других лиц. За каждым обучаемым закреплен личный электронный журнал, который заполняется по результат выполненных работ;

1.3.3 Существует система автоматического контроля выполнения различных заданий. Данный инструмент облегчает работу с одаренными студентами, самостоятельно изучающими образовательную программу, также с обучаемыми, которые отстают по учебной программе.

1.3.4 Различные инновационные инструменты дают возможность более продуктивно организовывать учебную работу и осуществлять контроль за выполнением контрольных и курсовых работ, семинаров и т.д.

Тем самым более эффективно и рационально использовать учебное время студентов и преподавателей [2].

Применяя систему Moodle, преподаватель способен разрабатывать и внедрять различные курсы, наполняя их теоретическим материалом в виде текста, презентаций, тестов и т.д. Для использования учебной среды Moodle достаточно обладать любым браузером, благодаря этому свойству пользование данной средой удобно как преподавателям, так и студентам. Согласно итогам выполненных студентами заданий, преподаватель способен выставить соответствующую оценку и написать комментарий.

С точки зрения информационной безопасности учебная среда Moodle обладает достаточной защитой от всевозможных угроз из вне, хакерских атак и спама. Для того чтобы оградить образовательный курс от несанкционированного доступа, достаточно в настройках убрать галочку «разрешить» в окне самостоятельной регистрации пользователя.

Но определенные опции безопасности данных могут быть весьма полезными для комфортной работы пользователей и при администрировании системы.

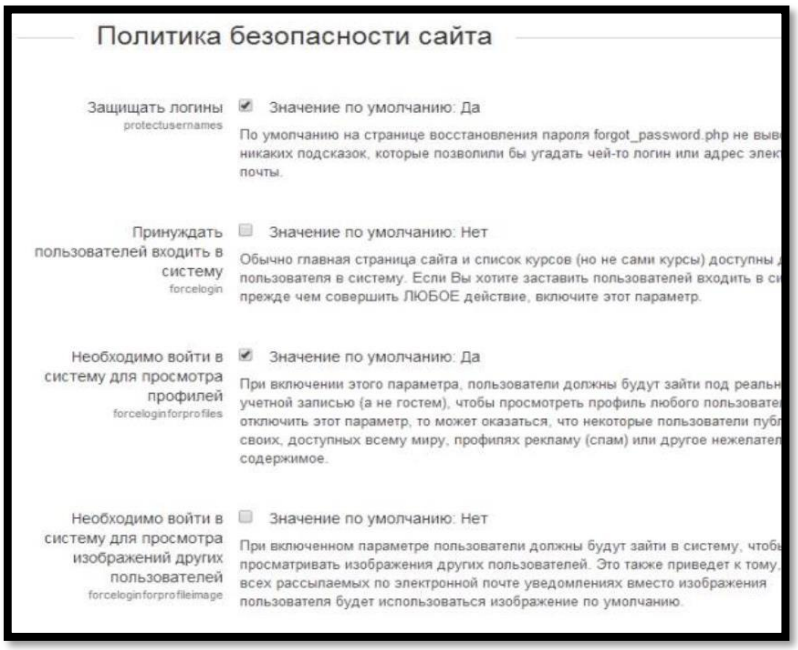

Рис.1.1 - Политика информационной безопасности сайта Moodle

Политика информационной безопасности образовательной среды Moodle:

Здесь мы проанализируем только определенные опции безопасности, на которых необходимо сосредоточить внимание администратора. Другие опции рекомендуется сохранить без изменений.

Чтобы пройти в раздел политики безопасности сайта, необходимо пройти в раздел администрирования и найти вкладку «безопасность», а после пройти по соответствующей ссылке (рис.1.1).

На первом этапе следует настроить систему для пользователей, во всех пунктах содержатся подробные комментарии, которые можно отредактировать на собственное усмотрение.

Следующий шаг — это установка ограничений для студентов при работе с файлами загрузки и системой на сайте (рис 1.2):

Рис.1.2 - Окно настройки ограничений

Политика паролей определяет уровень сложности при входе для пользователя. Согласно настройке «по умолчанию» — это достаточно непростое сочетание символов и знаков, для комфортного входа в систему доступ можно упростить.

Данных настроек достаточно для безопасной работы информационного ресурса на сайте (рис 1.3). С иными настройками необходимо обращаться с осторожностью, так как при неверной регулировке можно нанести ущерб курсу.

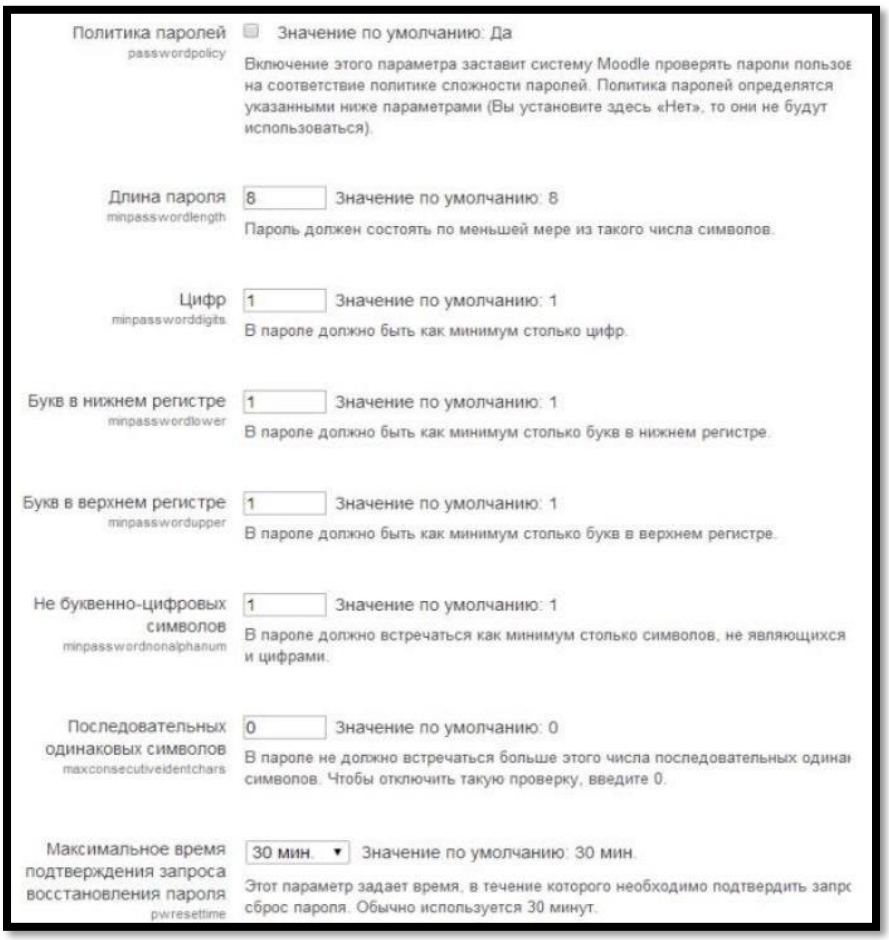

Рис.1.3 - Окно политики безопасности пароля

Согласно настройке «по умолчанию» в системе Moodle предусмотрена только ручная регистрация. Что, в свою очередь, обязывает администратора системы самостоятельно регистрировать студентов на сайте.

Однако эта мера весьма эффективна с точки зрения информационной безопасности сайта. Регистрация потусторонних лиц станет невозможна. Это означает, что на сайте будут отсутствовать заброшенные аккаунты и различный спам.

Помимо данного способа регистрации существуют и другие. В первую очередь стоит отметить самостоятельную регистрацию пользователя по электронной почте. В случае если этот тип регистрации разрешен со стороны администратора сайта, то пользователь может самостоятельно пройти регистрацию на сайте с дальнейшим его подтверждением, которое осуществляется при переходе по гиперссылке в e-mail.

Данный вид регистрации является абсолютно приемлемым.

Среда Moodle обладает несколькими вариантами записи на курсы. Наиболее популярный и востребованный это тот, который включен по умолчанию – ручная запись и гостевой доступ.

В том случае, если гостевой доступ разрешен, зарегистрироваться в системе может абсолютно любой пользователь, и тем самым сможет просматривать информационные материалы курса. Однако в гостевом режиме нет возможности работы с тестами, заданиями и т.д.

При ручной регистрации пользователя преподаватель должен самостоятельно записывать студентов на свои курсы, производя работу по поиску обучающихся в списке зарегистрированных пользователей сайта.

Из этого можно сделать вывод, что обеспечение информационной безопасности ИОР напрямую зависит от политики информационной безопасности образовательной среды Moodle.

ВЫВОД ПО ГЛАВЕ I

В процессе исследования литературных источников было подтверждено, что создание информационного образовательного ресурса по дисциплине «Техническая механика» актуально, так как является востребованным продуктом для повышения эффективности обучения будущих специалистов.

Нами было проанализировано понятие: Информационно-образовательные ресурсы – это совокупность технических, программных,

телекоммуникационных и методических средств, позволяющих оптимально использовать новые информационные технологии в сфере образования, внедрять их во все виды и формы образовательной деятельности. Электронное учебное пособие - это частный вид информационного образовательного ресурса (далее – ИОР), методический комплекс, предназначенный для изучения курса или отдельной дисциплины, является интегрированным средством, содержащим теоретические сведения, практические работы, задачи и другие дидактические компоненты для сопровождения процесса обучения. В нашей работе информационный образовательный ресурс представляет собой электронное учебное пособие, в которой сгруппирован материал и сопутствующая информация по дисциплине «Техническая механика».

Был установлен и определен ряд требований к информационному образовательному ресурсу: педагогические, дидактические, методические, психологические, эргономические, технические и структурные.

Также мы провели анализ концепции информационной безопасности организации СПО. Подробно проанализировали каждый из сегментов концепции информационной безопасности. Определили, по каким направлениям образовательная организация обеспечивает защиту своих информационных ресурсов, и в частности. – ИОР, для чего проанализировали нормативно-правовую базу на различных уровнях политики ИБ в ГПБОУ «ЮУрГТК»

К высшему уровню политики информационной безопасности можно отнести «Программу развития профессиональной образовательной организации среднего профессионального образования на 2014-2018 г».

На среднем уровне политики информационной безопасности можно выделить следующий ряд документов: «Положение по защите и обработке персональной информации ГБПОУ ЮУрГТК», «Положение по обеспечению безопасности в образовательном процессе ГБПОУ

ЮУрГТК», «Политика информационной безопасности в отношении персональной информации в ГБПОУ ЮУрГТК».

К низшему уровню политики информационной безопасности можно отнести должностные обязанности специалистов по безопасности, системных администраторов и инженеров по информатизации.

Согласно анализу нормативной документации ЮУрГТК можно сделать вывод, что общая концепция информационной безопасности разработана в недостаточной мере: отсутствует регламентация действий по использованию информационных образовательных ресурсов, что значительно снижает уровень защищенности ИОР.

Также в рамках исследовательской работы были изучены основные ограничения и особенности по работе с информационными образовательными ресурсами. Были проанализированы правила по работе с образовательными интернет-ресурсами и правила по работе в локальной сети СПО, а также степень ответственности за несоблюдение прописанных норм.

В ходе работы мы выяснили, что в Южно-Уральском государственном техническом колледже реализована технология электронного обучения на базе системы виртуальной образовательной среды Moodle

Moodle (модульная ориентированно-объектная динамическая среда для обучения) – это свободная и независимая среда управления, с помощью которой можно организовать взаимодействие между студентом и преподавателем. Данная система подходит также для организации традиционного дистанционного обучения, и годится в качестве дополнительного источника информации очного обучения.

С точки зрения информационной безопасности учебная среда Moodle обладает достаточной защитой от всевозможных угроз извне, хакерских атак и спама при должной настройки политики безопасности курса.

ГЛАВА 2. РАЗРАБОТКА И ПРИМЕНЕНИЕ ИНФОРМАЦИОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА ПО ДИСЦИПЛИНЕ «ТЕХНИЧЕСКАЯ МЕХАНИКА» В УСЛОВИЯХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЮУрГТК

2.1 Анализ учебной документации по дисциплине «Техническая механика» в ГБПОУ «ЮУрГТК»

Согласно ФГОС СПО по специальности 230207 «Техническое обслуживание и ремонт двигателей, систем и агрегатов автомобиля» выпускник обладает профессиональными компетенциями: ПК 1.1. Осуществлять диагностику систем, узлов и механизмов автомобильных двигателей; ПК 1.2. Осуществлять техническое обслуживание автомобильных двигателей согласно технологической документации; ПК 1.3. Проводить ремонт различных типов двигателей в соответствии с технологической документацией.

В таблице 2.1 приведен фрагмент учебного плана по специальности 230207 «Техническое обслуживание и ремонт двигателей, систем и агрегатов автомобиля».

Квалификация – специалист. Уровень подготовки – базовый.

Учебные практики проводятся на базе учебно-производственных мастерских техникума, остальные виды практик – в автотранспортных предприятиях города.

Стандартом предусмотрено получение рабочей специальности для студентов очной формы обучения: слесарь по ремонту двигателя, систем и агрегатов автомобиля.

Область профессиональной деятельности выпускников: организация процессов и осуществление диагностирования, ремонт и обслуживание современных автотранспортных средств, ремонт систем и электрооборудования автомобилей, осуществление кузовного ремонта,

организация процессов модификации и модернизации автомобилей, владение методикой тюнинга авто.

Объектами профессиональной деятельности выпускников являются:

– Автотранспортные средства;

– Техническая документация;

– Технологическое оборудование для технического обслуживания и ремонта автотранспортных средств;

– Первичные трудовые коллективы.

Техник готовится к следующим видам деятельности:

– Техническое обслуживание и ремонт автотранспорта;

– Организация деятельности коллектива исполнителей;

– Выполнение работ по профессии.

Таблица 2.1

Фрагмент учебного плана по специальности 230207 «Техническое обслуживание и ремонт двигателей, систем и агрегатов автомобиля».

Наименование циклов, дисциплин, профессиональных модулей, МДК, практик	Формы промежуточной аттестации	Учебная нагрузка обучающихся (час.)	
		Максимальная	Самостоятельная работа
Общепрофессиональный цикл		612	153
Инженерная графика		90	29
Техническая механика		122	61
Материаловедение		60	21
Метрология, стандартизация и сертификация		60	21

Программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности 230207 «Техническое обслуживание и ремонт двигателей, систем и агрегатов автомобиля» (базовый уровень).

Место дисциплины в структуре основной профессиональной образовательной программы: дисциплина входит в профессиональный модуль (общепрофессиональные дисциплины).

Цели и задачи дисциплины – требования к результатам освоения дисциплины:

В результате освоения дисциплины обучающийся должен уметь:

– определять напряжения в конструкционных элементах;

– читать кинематические схемы;

– производить расчеты механических передач и простейших сборочных единиц.

В результате освоения дисциплины обучающийся должен знать:

– основы технической механики;

– методику расчета элементов конструкций на прочность, жесткость и устойчивость при различных видах деформации;

– виды механизмов, их кинематические и динамические характеристики;

– основы расчетов механических передач и простейших сборочных единиц общего назначения.

В результате освоения учебной дисциплины «Техническая механика» обучающийся должен овладеть:

Общими компетенциями:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Профессиональными компетенциями:

ПК 1.1. Использовать конструкторскую документацию при разработке технологических процессов изготовления деталей

ПК 1.2. Выбирать метод получения заготовок и схемы их базирования.

ПК 1.3. Составлять маршруты изготовления деталей и проектировать технологические операции.

ПК 1.4. Разрабатывать и внедрять управляющие программы обработки деталей.

ПК 1.5. Использовать системы автоматизированного проектирования технологических процессов обработки деталей.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Курс «Техническая механика» позволяет повысить у студентов интерес к технике, сформировать понимание основных терминов, встречающихся в технической литературе, а также понять социальную значимость выбранной профессии. Преподавание ведется посредством использования электронного пособия «Техническая механика», что позволяет индивидуализировать образование студентов и увеличить эффективность учебной работы.

Обучение данному курсу имеет практическую направленность и проводится в тесной взаимосвязи с другими специальными и общепрофессиональными дисциплинами: «Материаловедение», «Инженерная графика», «Метрология, стандартизация и сертификация».

Цель программы – предоставить учащимся комплекс базовых знаний необходимых для будущей профессии и для повышения общей и технической культуры. Сформировать у студентов навыки работы с компьютером, как со средством обучения.

Отличительной особенностью данной образовательной программы от уже существующих программ является то, что данная программа создана в соответствии с современными требованиями общества. Программа способствует развитию навыков самостоятельной работы, индивидуализирует обучение и способствует обеспечению развития аналитического ума.

Таблица 2.2

Тематический план по теме «Техническая механика»

№ п/п	Наименование и содержание темы	Количество часов		
		Теория	Практика	Всего
Раздел 1. Теоретическая механика				
1.1	Глава 1. Статика, основные понятия и аксиомы.	2	2	4

1.2	Глава 2. Условия равновесия систем сил.	2	2	4
1.3	Глава 3. Кинематика точки.	2	4	6
1.4	Глава 4. Простые и сложные виды движения тела.	2	2	4
1.5	Глава 5. Основные законы, теоремы и принципы динамики.	2	4	6
Раздел 2. Сопротивление материалов				
2.1	Глава 6. Основные понятия и допущения. Растяжение и сжатие.	2	4	6
2.2	Глава 7. Срез и смятие.	2	2	4
2.3	Глава 8. Кручение.	2	2	4
2.4	Глава 9. Изгиб.	2	2	4
2.5	Глава 10. Гипотезы прочности. Расчет валов.	2	4	6
2.6	Глава 11. Устойчивость сжатых стержней	2	2	4
Раздел 3. Детали машин				
3.1	Глава 12. Соединение деталей. Разъемные и неразъемные соединения.	2	2	4
3.2	Глава 13. Передачи вращательного движения.	2	2	4
3.3	Глава 14. Валы и оси. Опоры валов и осей.	2	2	4
3.4	Глава 15. Муфты и редукторы	2	2	4
ИТОГО за первый год обучения:		30	38	68

Материально-техническое обеспечение дисциплины

Занятия по дисциплине должны проходит в специализированной аудитории, оборудованной современными компьютерами или ноутбуками с операционной системой Windows. Число рабочих мест должно быть таким, чтобы обеспечить каждому студенту индивидуальную работу над информационным образовательным ресурсам.

2.2 Выбор средств разработки информационного образовательного ресурса по дисциплине «Техническая механика»

На первом этапе нам нужно определиться с фундаментом ИОР, который будет построен в виде обучающего приложения. Главным инструментом построения будет служить система программирования Delphi 7. Это продукт Borland International был создан с целью быстрой разработки приложений. Процесс выстраивания будущего интерфейса программы напоминает игру с конструктором, поэтому RAD-среды иначе называют визуальными средами разработки. Данная программа считается самой удобной, мощной и быстрой средой разработки приложений для операционной системы Windows по средствам языка программирования Object Pascal. Интегрированная среда разработки Delphi 7 имеет отладчик программного кода, подсветку синтаксиса, предоставляет возможность навигации по исходному коду с системой закладок [33].

Delphi 7 содержит в себе огромную библиотеку визуальных компонентов VCL, что дает возможность создавать приложения баз данных с применением данных компонентов, кроме того подключать компоненты других разработчиков и создавать собственные. Также программа содержит компилятор командной строки и дает возможность создавать приложения на основе BDE (Borland Database Engine), поддерживает форматы локальных баз данных Paradox и BDF. А также содержит драйвер SQlink для серверов баз данных Oracle, Informix, InterBase и MS SQL.

Данное приложение кроме того дает возможность формировать сервера приложений на базе Remote Data Module и технологии MIDAS/DataSnap, содержит лицензию разрешающую их распространять. В этом приложении интегрированы средства моделирования разработки и развертывания приложений электронной коммерции и Web-сервисов.

Достоинства Delphi 7 по сравнению с другими подобными программными продуктами:

– Скорость разработки;

– Высокопроизводительность программных продуктов;

– Незначительные требования программных продуктов к компьютерным ресурсам;

– Успешная проработка иерархии предметов;

– Потенциал разработки собственных инструментов и компонентов.

Но также программа имеет и ряд недостатков:

– Высокая стоимость программного обеспечения;

– Узкая форматоемкость в браузерном окне [20].

Концепция программирования Delphi предназначена для конструирования любых приложений, при этом предоставляет широкий выбор инструментов для решения различных задач. Но главным преимуществом данной среды разработки является скорость и качество созданной программы. Эти характеристики обеспечивает среда визуального проектирования. Способности Delphi полностью отвечают возложенным требованиям и подойдут для создания приложений различной сложности.

Следующая программа отвечает за разработку и составление теоретического материала электронного пособия. Это всем известная программа Microsoft Word, входящая в пакет офисных приложений Microsoft Office. Данная программа предоставляет интуитивно понятный

интерфейс для работы с текстом, обеспечивает быстрый доступ к командам. Обладает рядом преимуществ, таких как надежность, экономичность и защита от сбоев. В частности, это приложение может использоваться на компьютерах с установленной операционной системой Windows Vista и старше.

Для корректной работы программе необходимы следующие технические параметры:

- Размер оперативной памяти – от 512 Мбайт;
- Свободное место на жестком диске – от 2 Гбайт;
- Частота процессора – от 667 МГц.

Документы в данном текстовом редакторе можно легко конвертировать из формата Word в PDF, что обеспечит корректную работу в оболочке электронного пособия [40].

Для создания тренировочных тестов мы использовали программный продукт, созданный группой разработчиков Ispring Solutions для платформы Windows. Ispring Suite - это пакет программ, в который входят приложения Ispring Pro, Ispring Kinetikl и Ispring QuisMake. Данный пакет служит дополнением к Microsoft PowerPoint и расширяет его функции. Программы обеспечивают быстрое создание тестов, диалоговых тренажеров, видео-лекций и электронных учебных курсов. Кроме того, данные приложения поддерживают весь функционал PowerPoint (гиперссылки, анимации, шрифты, темы, эффекты перехода и т.д.). А также предоставляет набор специальных функций:

- Запись экрана для создания видео-лекций;
- Разработка опросов и тестов;
- Оригинальное оформление тестов;
- Создание видео-опросов и аудио-опросов;
- Тонкая настройка прохождение тестирования;
- Защита созданных учебных файлов от злоумышленников.

Для разработки тренировочных тестов мы использовали программу Ispring QuisMake, с помощью которой можно с легкостью создать тестирование разного уровня сложности и загрузить в оболочку будущего электронного пособия, предварительно скачав и установив на компьютер flash-плеер для просмотра тестов. В тесты можно добавлять различные изображения и формулы. Приложение нацелено на среднестатистического пользователя ПК для реализации сложных педагогических задач.

Для работы программы необходимо:

– Оперативная память – от 1 Гбайт;

– Частота процессора – от 1 ГГц;

– Свободное место на жестком диске – от 1,5 Гб;

– Операционная система – от Windows XP и старше [1].

Плюсы программы:

– Легкое освоение программы;

– Возможность дополнения внешними ресурсами и медиафайлами;

– Широкий выбор видов тестирования.

Минусы программы:

– Высокая стоимость;

– Мало интерактивностей.

Также для нашего пособия понадобится краткий словарь технических терминов – глоссарий. Для его создания можем использовать приложение Microsoft FrontPage. Эта программа используется при разработке веб-страниц в формате HTML, в нее заложен html-движок Trident, лежащий в основе браузера Internet Explorer. Приложение FrontPage обладает обширным спектром возможностей и удобным интерфейсом при создании веб-сайтов [60].

Плюсами данного программного обеспечения являются:

– Трехрежимный вид работы: визуальный редактор, код и смешанный;

– Простота использования;

– Имеет встроенную инструкцию по эксплуатации приложением.

Минусы данной программы:

– Некорректность и избыточность кода;

– Ориентация на технологии IIS.

Для эстетического оформления кнопок и фона электронного пособия мы использовали программу Photoshop. Это универсальный графический редактор для обработки изображений. Он имеет огромный ассортимент инструментов для обработки растровых изображений. Продукт считается фаворитом в своем классе и самой известной программой фирмы Adobe. Этот фоторедактор имеет право называться цифровой фотолабораторией. Photoshop может открывать и редактировать цифровые изображения, накладывать эффекты, а также изменять размеры получившегося проекта [19]. Может похвастаться высокой скоростью по обработке среди фоторедакторов. На данный момент приложение может работать с операционными системами Windows и macOS и с мобильными системами Android и IOS.

Для работы программы необходимо:

– Оперативная память – 2 Гбайт (рекомендуется 8 Гбайт);

– Частота процессора – от 2 ГГц;

– Свободное место на жестком диске – от 2,5 Гб;

– Операционная система – Windows, macOS, Android и IOS [35].

К основным плюсам данной программы можно отнести:

– Высокая производительность;

– Стабильная работа;

– Широкий функционал.

Минусы программы:

– Высокая стоимость продукта;
– Сложная в освоении.

2.3 Описание структуры и содержания разработанного ИОР по дисциплине «Техническая механика»

На первоначальной стадии разработки учебного пособия были определены задачи по его созданию для работы студентов колледжа по дисциплине «Техническая механика». Учебное пособие должно включать:

– Теоретический материал;
– Тесты для самоконтроля;
– Глоссарий (словарь терминов);
– Сведения о разработчике программы.

Программа должна быть нацелена на среднестатистического пользователя и основываться на использовании меню и гиперссылок в интерфейсе. Теоретический материал, тестовые задания и глоссарий должны быть выполнены в виде подключаемых файлов и в дальнейшем скомпилированы в приложение [38, 10].

На второй стадии разработки учебного пособия «Техническая механика» был проведен анализ литературных источников, содержащих информацию согласно выбранной теме. Материал, используемый в электронном пособии, был обработан и систематизирован.

Основные определения, термины и сведения о разработчике были включены в раздел справочной системы электронного пособия.

На третьей стадии была выполнена разработка будущей модели учебного пособия. Были спроектированы содержание и дизайн пособия, включающего следующие разделы;

– Лекции;
– Тестирование;
– Словарь;

– Сведения об авторе.

Четвертая стадия – разработка учебного электронного пособия по дисциплине: «Техническая механика».

Данный вид работы наиболее продолжительный и сложный. На этой стадии заранее отобранный материал для разделов пособия переводится в язык гипертекстовой разметки HTML и помещается в определенные папки, расположенные в основном каталоге учебного пособия. После все данные компилируются в исходный файл.

Пятая стадия одна из самых важных и заключительных - это тестирование полученного электронного пособия «Техническая механика». Испытание программы проходило посредством проверки возможности программы в стандартных ситуациях. По результатам испытания мы можем сказать, что программа справляется с поставленными задачами и сбоев не обнаружено.

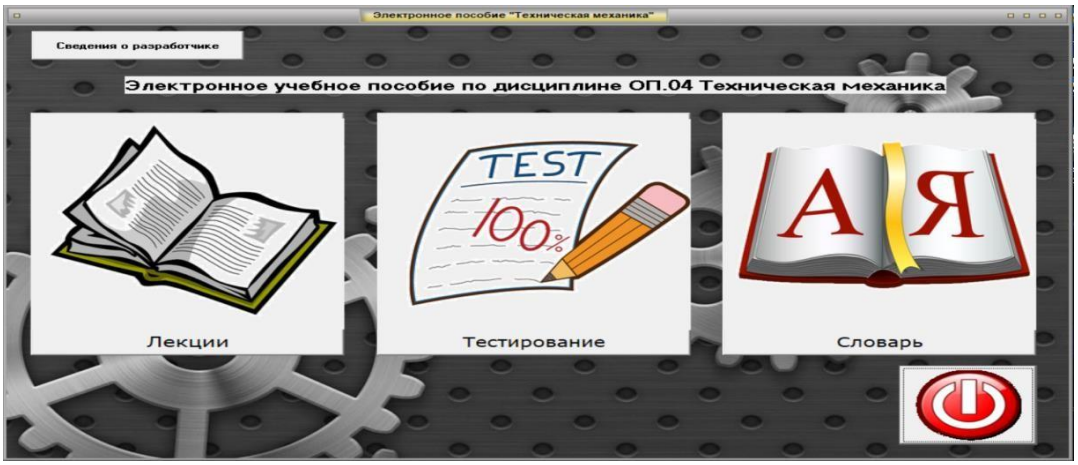

Рис.2.1 - Стартовая страница

При запуске учебного электронного пособия открывается стартовая страница, содержащая ряд гиперссылок для перехода к теоретическому материалу «Лекции», для перехода к тестовым заданиям «Тестирование» и для перехода к терминологическому минимуму «Словарь» (рис. 2.1).

При нажатии на гиперссылку «Лекции» перед глазами студента открывается окно учебного пособия (рис.2.2).

Слева в окне приложения мы можем увидеть меню разделов пособия, а справа - окно трансляции учебного пособия. При нажатии стрелкой на раздел открывается меню глав. Выбор главы происходит по средствам нажатия на соответствующую гиперссылку.

Сверху есть панель быстрого доступа. С помощью данной панели студент может сохранить копию любой главы из пособия или сразу же распечатать на бумажный носитель.

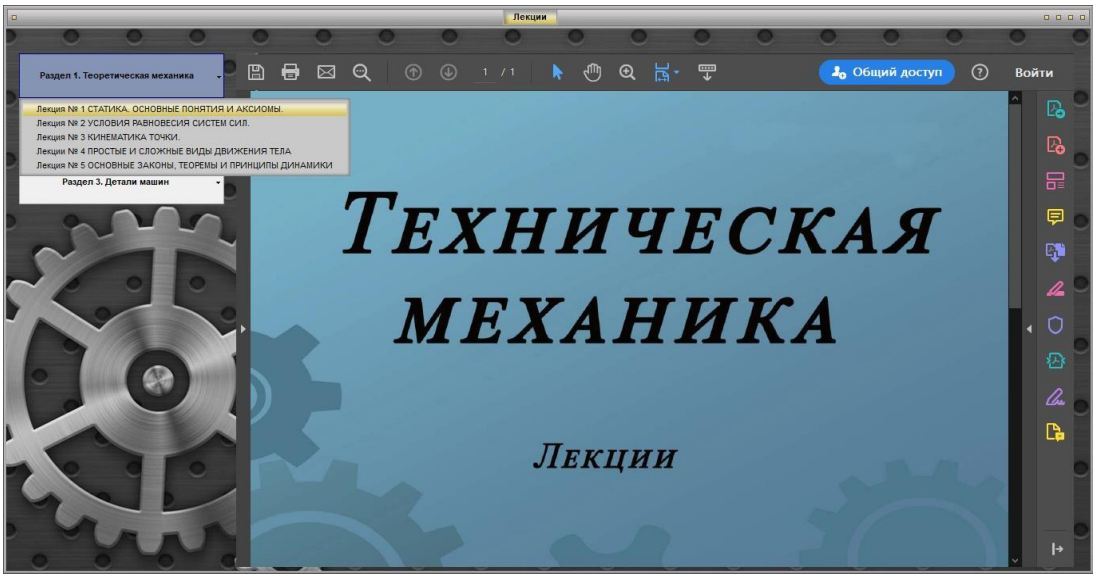

Рис.2.2 –страница «Лекции»

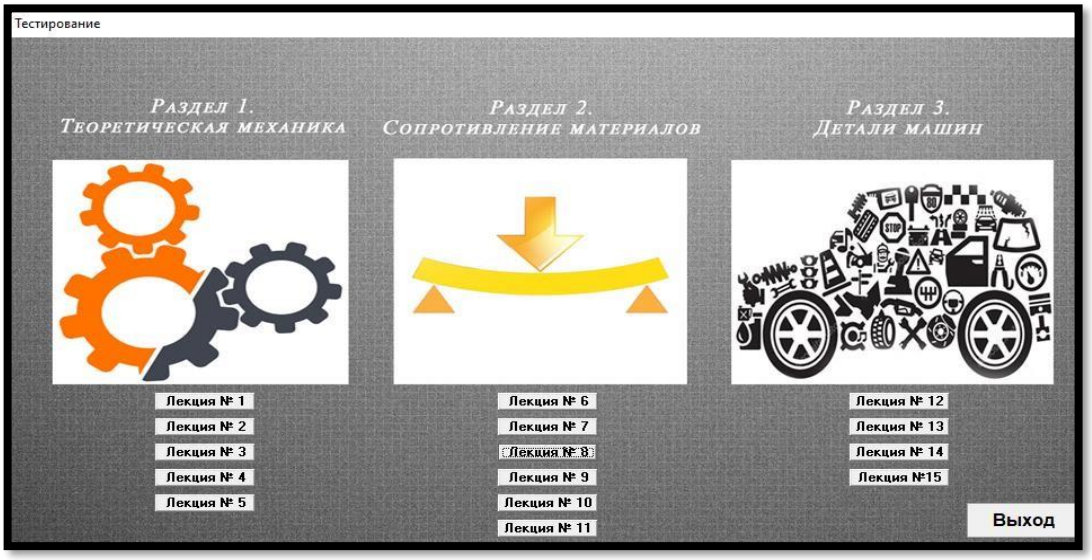

Рис.2.3 –раздел «Тестирование»

При переходе в раздел «Тестирование» мы видим кнопки с соответствующими лекциями. При нажатии на нужную лекцию

открывается тест для самоконтроля (рис.2.3). Тест содержит задания разного уровня сложности, такие как:

– Выбор одного правильного ответа;
– Выбор нескольких правильных ответов;
– Задания на соответствия;
– Ввод правильного ответа с помощью клавиатуры.

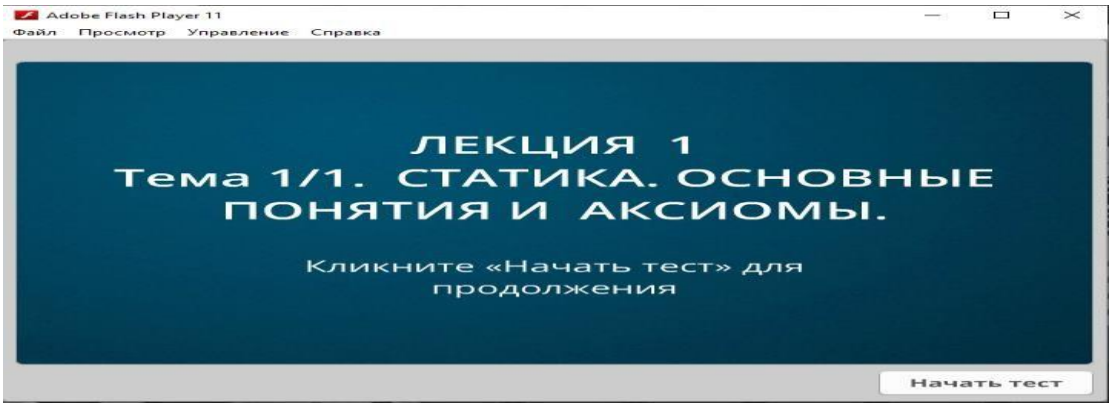

Рис. 2.3 - Тест

После перехода к тесту программа предложит студенту пройти регистрацию для прохождения (рис.2.4). В соответствующих полях необходимо ввести группу, ФИО и электронную почту студента. Приложение не позволит приступить к тестированию, если хотя бы одно поле останется не заполненным.

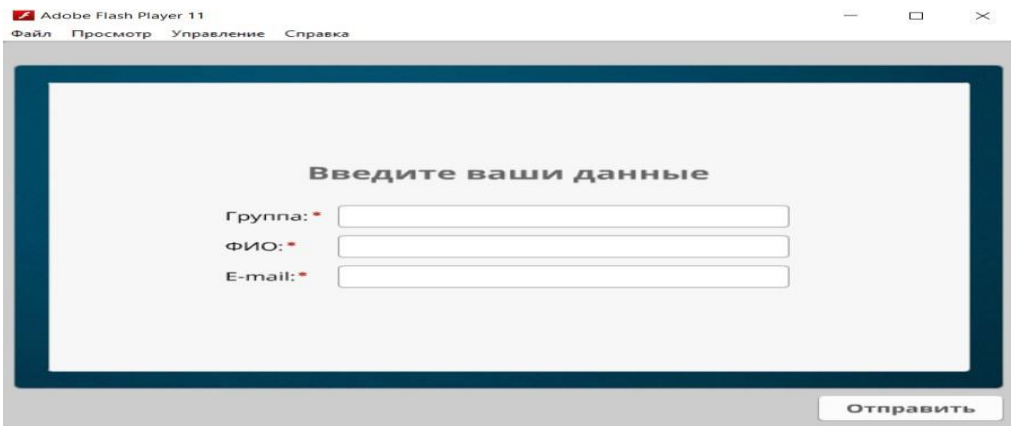

Рис. 2.4 – Окно регистрации

При завершении тестирования в окне отображается результат (рис.2.5). За каждое правильно выполненное задание начисляется 1 балл. Результат прохождения теста показан по центру в процентном и бальном соотношении, а также показан и проходной бал для успешной сдачи теста. После завершения работы над тестом программа автоматически отправляет результаты на электронную почту преподавателя, где можно увидеть полную информацию результатов тестирования (рис.2.6). А студент в свою очередь может посмотреть результат на ПК и провести работу над ошибками.

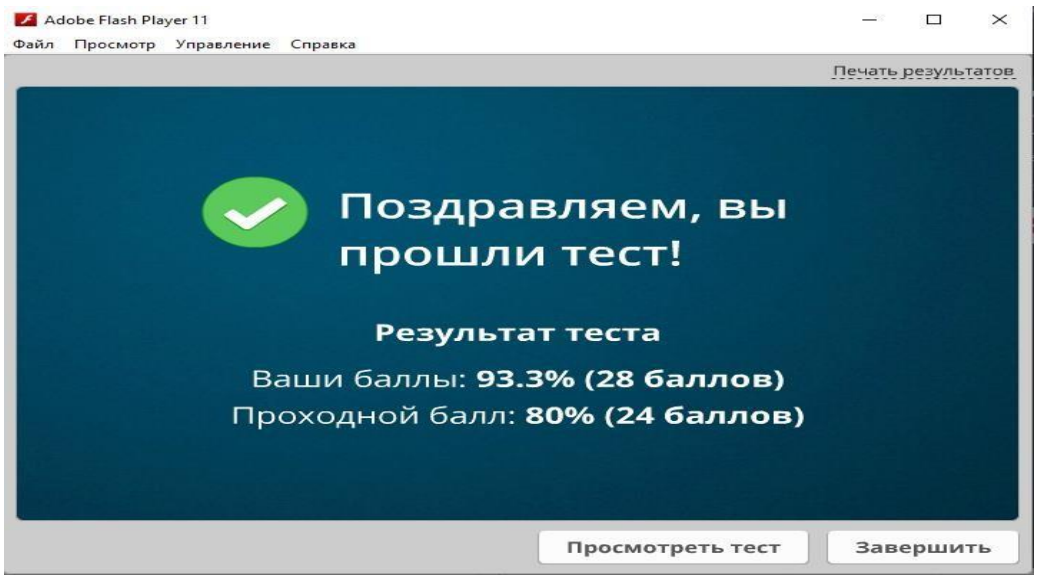

Рис. 2.5 - Результат тестирования

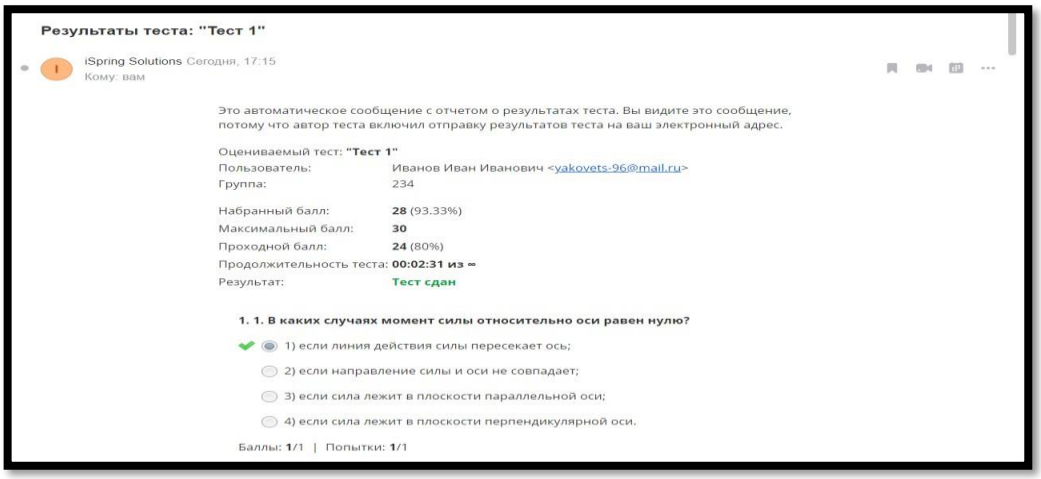

Рис. 2.6 - Результат тестирования на электронной почте

В данном пособии также существует раздел «Словарь», содержащий все главные определения и термины, встречающиеся в учебном пособии по дисциплине «Техническая механика» (рис. 2.7). Быстрый переход к термину можно осуществить при клике на первую букву интересующего вас слова, а также мгновенно осуществить возврат в начальное положение с помощью гиперссылки «Возврат в начало».

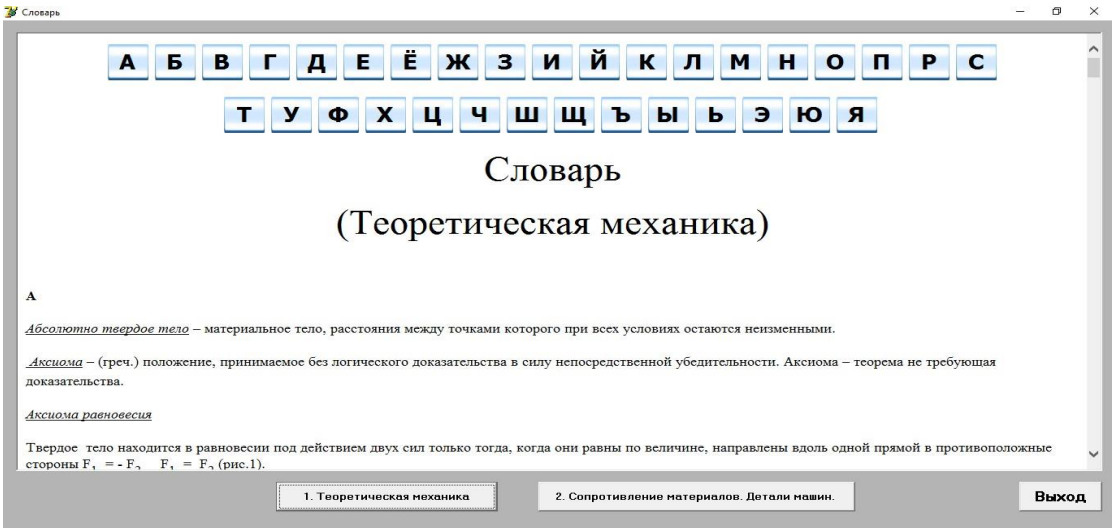

Рис.2.7 - Терминологический словарь

Познакомиться с информацией о разработчике и посмотреть его контактные данные можно в разделе «Сведения о разработчике» (рис. 2.8).

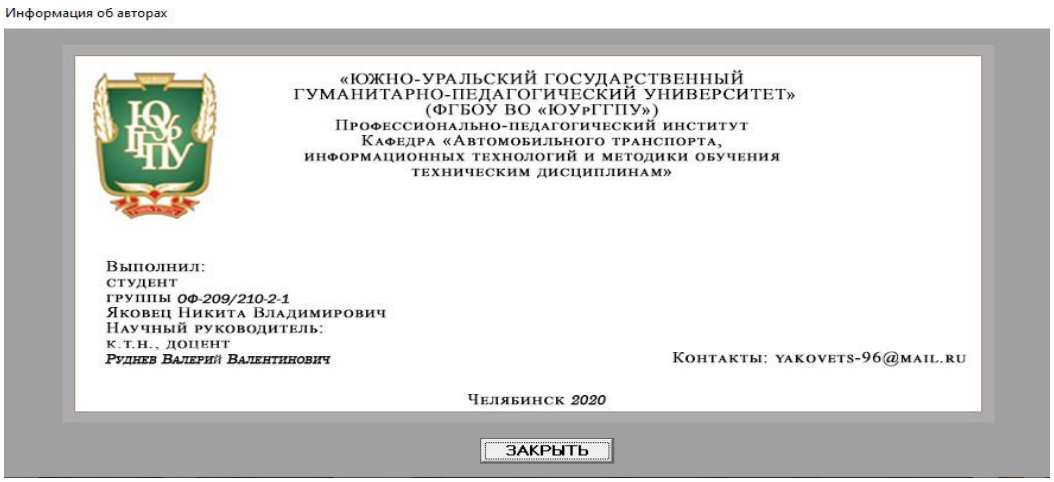

Рис.2.8 - Сведения о разработчике

Следующей стадией разработки электронного пособия является создание окна авторизации при входе на информационный ресурс. Прежде чем войти в электронное учебное пособие, студент обязан авторизоваться в программе, для этого необходимо ввести соответствующий логин и пароль (рис. 2.9).

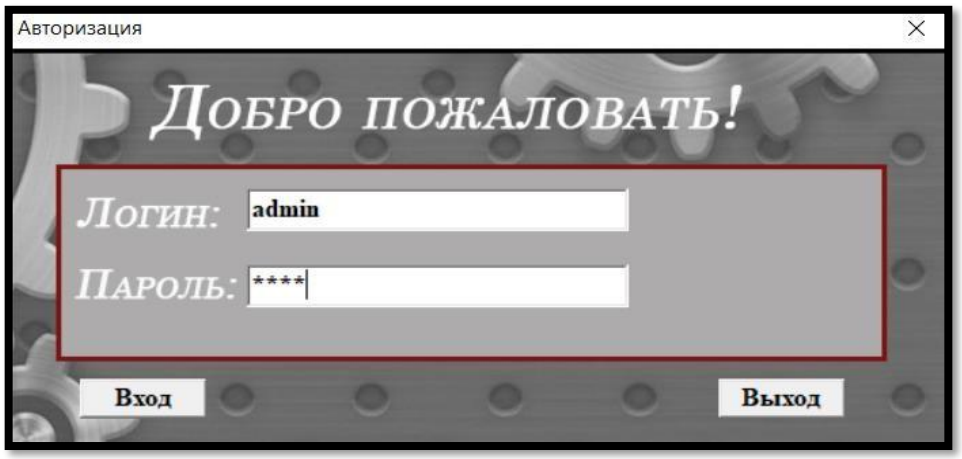

Рис.2.9 – Окно авторизации

При проведении альфа-тестирования были выявлены ошибки при выводе рабочих окон и запуске правильной последовательности форм, в дальнейшем данные недостатки были устранены.

2.4 Апробация разработанного информационного образовательного ресурса по дисциплине «Техническая механика»

Для того чтобы обеспечить информационную безопасность ИОР, нами был разработан комплекс мер по защите данных образовательного ресурса.

Лимитирование допуска к файлам ИОР, находящихся на жестком диске ПК со стороны пользователя.

Процесс лимитирования допуска делится на несколько этапов:

1) Необходимо создать новую политику конфиденциальности для учебной группы при помощи программного продукта Folder Lock (рис 2.10)

Folder Lock – это весьма надежный и эффективный программный продукт, обеспечивающий защиту конфиденциальных данных, файлов и папок благодаря функциям установки пароля, шифрования и сокрытия.

Для более продуктивного обеспечения безопасности данных на персональном компьютере рекомендуется одновременное использование шифрования и блокировки. В таком случае файлы, защищенные с помощью этой функции, не обнаружатся в приложениях и проводнике. Что делает их полностью недоступными. Таким образом, получить доступ к данным невозможно без соответствующего пароля даже при сторонней загрузке в DOS файл в безопасном режиме или на другой компьютерной технике.

Рис 2.10 – Программа Folder Lock

Исходные информационные ресурсы, требующие защиты, могут храниться не только в корневой папке на жестком диске, но и на картах памяти, ноутбуках и дисках. А процесс установки предусмотренных программных средств, обеспечивающих безопасность, может осуществлять в автономном режиме при неактивности ПК.

2) В режиме Stealth Mode следует скрыть историю, указывающую сведения об установке средств по защите информационных ресурсов на

компьютере. Данный метод скрывает информацию о деинсталляции и инсталляции в панели управления, препятствует отображению соответствующих ярлыков в меню «Пуск» и на рабочем столе, очищает данные из буфера обмена и историю и т.д.

Помимо этого, программа ведет учет всех попыток неудачного входа, а также регистрирует попытки снятия защиты, что дает возможность администратору своевременно зафиксировать потустороннюю активность в файлах и папках со стороны пользователя.

Порекомендованная мера необходима для исключения акта несанкционированного доступа к системным и исполняемым файлам информационного образовательного ресурса.

3) Для повышения уровня информационной безопасности необходимо также установить программу удаленного администрирования RMS (рис 2.11). Установка данного программного продукта предоставляет возможность преподавателю вести контроль над деятельностью студентов во время выполнения контрольного тестирования по закреплению полученных теоретических знаний.

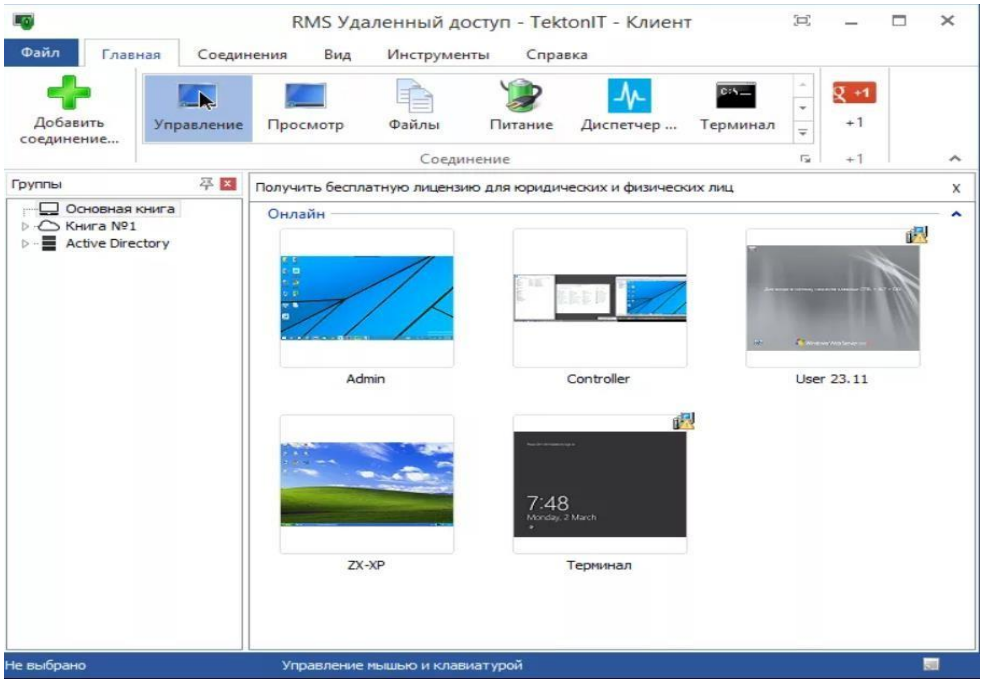

Рис 2.11 – Программа удаленного администрирования RSM

4) Еще одним важным обстоятельством по обеспечению ИБ при работе с электронным учебным пособием является компетентность и квалификация преподавателя в данном аспекте. С целью решить данный вопрос нами были скорректированы соответствующие рекомендации для преподавательского состава организации СПО:

- Нельзя покидать рабочее место в том случае, если был произведен вход в систему под личной учетной записью. В данном случае при уходе всегда необходимо производить выход из системы;
- Пароль к учетной записи следует изменять с периодичностью, сроком не менее 30 дней, кроме того не следует использовать распространённый вид пароля, такие как «0000», «1234» и т.д. А также не следует применять в качестве пароля личные сведения, например, фамилию, дату рождения, имя и подобную информацию. Игнорирование данной рекомендации способно спровоцировать несанкционированный вход в учетную запись пользователя методом подбора.
- При распространении исполняемого файла электронного учебного пособия не рекомендуется раздавать приложение при помощи общей папки в локальной сети организации, так как данный способ способствует образованию уязвимости, благодаря которой студент может скопировать или удалить ценные файлы. Распространение ведется по средствам модуля «Server», данный способ позволит студентам получить доступ к локальной сети, но в свою очередь ограничит доступ к исходным данным.

Перечисленные порекомендованные меры могут существенно повысить уровень информационной безопасности в процессе обучения при работе с информационным образовательным ресурсом «Техническая механика».

Введение рекомендуемых мер безопасности привело к повышению уровня информационной защищенности при применении

информационного образовательного ресурса в ГБПОУ «Южно-Уральский государственный технический колледж».

Главным показателем уровня обеспечения информационной безопасности ИОР является вторичный анализ числа обращений к программному продукту и файлам обобщения и сбора результатов контрольного тестирования.

Созданные и внедренные меры, такие как: разработка комплекса рекомендаций для педагогического коллектива организации СПО, ориентированные на развитие и формирование компетенций в области безопасности информационных ресурсов, лимитирование доступа к исходным файлам учебного пособия, настройка и установка удаленного доступа для контроля обучающихся во время прохождения тестирования знаний в реальном времени. Данные меры позволили существенно уменьшить показатель обращений к минимальным значениям благодаря тому, что у студентов доступ к исходным и системным файлам стал недоступен.

Благодаря использованию среды разработки Delphi 7, нам удалось добиться полной автономности программного продукта, даже в условиях отсутствия интернет – соединения, что обеспечивает работу с информационными ресурсами изолированной. Кроме того, при внедрении системы авторизации, информационными образовательными ресурсом можно воспользоваться только при обращении к преподавателю, у которого находится исходный логин и пароль, который периодически меняется в базе данных, защищенной паролем.

Рис 2.12 – Динамика количества обращений к файлам

Доступ к исполняемому файлу производится при переходе через ярлык электронного учебного пособия. Это позволило нам закрыть доступ как к файлам исходникам, так и к корневым файлам самого пособия. Данная мера позволила сократить риск реконструкции продукта по средствам изолированной среды. При вторичном анализе было выявлено 12 обращений к исполняемому файлу, подробная статистика изменений показана на диаграмме (рис 2.12).

Также благоприятно отразились рекомендации для педагогического состава в вопросе обеспечения защиты информационных данных. Преподаватели заменили собственные пароли на более надежные и активировали функцию, напоминающую изменять учетную запись с периодичностью раз в тридцать дней.

А благодаря внедрению программы удаленного доступа преподаватели стали более результативно осуществлять контроль над работой студентов во время прохождения тестирования, что положительно сказалось на качестве усвоения знаний, навыков и умений.

Итоги бета-испытаний разработанного нами информационного образовательного ресурса для организации занятий в организации СПО по дисциплине «Техническая механика» показали высокий уровень защищенности и эффективность внедренных мер, что доказывает гипотезу нашего исследования.

ВЫВОД ПО ГЛАВЕ II

Во второй главе была проанализирована рабочая программа по дисциплине «Техническая механика» Программа была создана с опорой на современные тенденции общества. Провели анализ тематического плана и определились с материально-техническим обеспечением по дисциплине «Техническая механика».

Был проведен анализ имеющихся программных приложений, подходящих для проектирования и разработки учебного пособия, среди

которых программная среда разработки Delphi 7. Данная программа считается самой удобной, мощной и быстрой средой разработки приложений для операционной системы Windows по средствам языка программирования Object Pascal. Текстовой редактор Microsoft Word был выбран для составления теоретического материала преимущественно из-за простоты использования и надежности, а также за возможность конвертирования файлов в PDF формат, что обеспечило корректную работу в оболочке электронного учебного пособия. Для создания тренировочных тестов был использован Ispring QuisMake. Данная программа позволила с легкостью создать тестирование разного уровня сложности. При создании словаря использовано приложение Microsoft FrontPage за обширный спектр возможностей при создании HTML документов, за удобный и продуманный интерфейс. Для эстетического оформления кнопок и фона электронного учебного пособия была выбрана программа для обработки изображений Photoshop. С помощью этой программы можно редактировать изображения и изменять его размеры согласно необходимым требованиям. Также выявлены основные достоинства и недостатки используемых программ.

Было представлено описание основных этапов разработки электронного учебного пособия по дисциплине «Техническая механика».

Было спроектировано содержание и дизайн учебного пособия, включающий следующие разделы:

- Теоретический материал;
- Тесты для самоконтроля;
- Глоссарий (словарь терминов);
- Сведения о разработчике программы.

Для того чтобы обеспечить информационную безопасность информационных образовательных ресурсов нами был разработан комплекс мер по защите данных образовательного ресурса, к ним отнесено:

1. Лимитирование допуска к файлам электронного учебника, находящихся на жестком диске ПК со стороны пользователя;

2. Активация режима Stealth Mode устраняющая следы установки программного продукта;

3. Установка программы удаленного администрирования RMS, для ведения контроля за деятельностью обучающихся;

4. Рекомендации по повышению компетентности и квалификации преподавателей в вопросе ИБ при работе с учебным пособием.

При проведении альфа-тестирования были выявлены ошибки при выводе рабочих окон и запуске правильной последовательности форм, в дальнейшем данные недостатки были устранены.

На последнем этапе были изложены итоги бета-испытаний по оценке эффективности внедренных мер, обеспечивающих информационную безопасность учебного пособия в ГБПОУ «ЮУрГТК». Результаты бета-испытаний, разработанного нами информационного образовательного ресурса для занятий в организации СПО по дисциплине «Техническая механика» показали высокий уровень защищенности и эффективность внедренных мер. Показатель числа обращений к исполняемому файлу снизился, что доказывает гипотезу нашего исследования.

ЗАКЛЮЧЕНИЕ

Вследствие анализа многочисленных информационных источников по теме магистерской диссертации можно сделать вывод о практической важности создания ИОР по дисциплине «Техническая механика».

В первой главе магистерской диссертации мы провели анализ структуры ИОР и требований, предъявляемых к его созданию.

Нами были изучены основные направления политики информационной безопасности в образовательной организации ГБПОУ «ЮУрГТК». Подробно проанализировали каждый из сегментов концепции информационной безопасности. Определили, по каким направлениям образовательная организация должна обеспечивать защиты и т.д. Согласно анализу нормативной документации ЮУрГТК можно сделать вывод, что общая концепция информационной безопасности разработана в недостаточной мере и требует определенной доработки. Были изучены основные ограничения и особенности по работе с ИОР. Были проанализированы правила по работе с образовательными Интернет-ресурсами и правила по работе в локальной сети СПО, а также степень ответственности за несоблюдение прописанных норм.

В ходе работы выяснили, что в Южно-Уральском государственном техническом колледже реализована технология электронного обучения на базе системы виртуальной образовательной среды Moodle. С точки зрения информационной безопасности данная среда обладает достаточной защитой от всевозможных угроз.

Во второй главе магистерской диссертации была проанализирована рабочая программа по дисциплине «Техническая механика» Программа была создана с опорой на современные тенденции общества. Провели анализ тематического плана и определились с материально-техническим обеспечением по дисциплине «Техническая механика».

Провели анализ имеющихся программных приложений, подходящих для проектирования и разработки ИОР.

В рамках исследования спроектировали и разработали учебное пособие по дисциплине «Техническая механика» для студентов ГБПОУ «ЮУрГТК». Разработали комплекс мер по защите данных образовательного ресурса, которые могут ограничить доступ к информационным ресурсам учебного пособия, обеспечить контроль за деятельность студентов во время проведения занятий и существенно повысить компетентность и квалификацию преподавателей в вопросе ИБ при работе с учебным пособием.

При проведении альфа-тестирования были выявлены ошибки при выводе рабочих окон и запуске правильной последовательности форм, в дальнейшем данные недостатки были устранены.

На последнем этапе были изложены итоги бета-испытаний по оценке эффективности внедренных мер, обеспечивающих информационную безопасность учебного пособия в ГБПОУ «ЮУрГТК». Результаты бета-испытаний, разработанного нами информационного образовательного ресурса для занятий в организации СПО по дисциплине «Техническая механика» показали высокий уровень защищенности и эффективность внедренных мер. Показатель числа обращений к исполняемому файлу снизился, что доказывает гипотезу нашего исследования.

Таким образом, цель работы достигнута, задачи выполнены, гипотезы нашего исследования подтверждены.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. iSpringSuite. База знаний [Электронный ресурс]// Режим доступа: https://www.ispring.ru/ispring-suite/knowledge. Дата обращения 17.04.2020.
2. Андреев А.В. Практика электронного обучения с использованием Moodle [Текст] / А.В. Андреев, С.В. Андреева, И.Б. // Доценко. Изд-во. ТТИ ЮФУ, 2018. - 146 с.
3. Абдулина, Е.Л. Общесистемные требования к электронным учебным материалам: лекция [Электронный ресурс] /Е.Л. Абдулина / Режим доступа: http: //www.cctpu.edu.ru/conf/sec7/tez02.htm. Дата обращения 12.03.2020.
4. Бадарчев Д.А. Информационные и коммуникационные технологии в образовании [Текст] / Д.А Бадарчев – М.: ИИТО ЮНЕСКО, 2017 – 318 с.
5. Баранова, Ю.Ю. Методика использования электронных учебников в образовательном процессе [Текст] / Ю.Ю. Баранова // Информатика и образование. - 2016. - 47 с.
6. Бекетов Н. Информационная безопасность развития государства [Текст] / Н. Бекетов // Информационные ресурсы России, № 8, 2017. – 35 с.
7. Белов, Е.Б. Основы информационной безопасности. [Текст] // Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов.– М.: Горячая линия – Телеком, 2016. – 534 с.
8. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс. -2018. - 454 с.
9. Белов, Е.Б. Основы информационной безопасности. //Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком. - 2016. – 243 с.

10. Вишнякова А.Ю. Разработка электронного образовательного ресурса в составе информационно-методического обеспечения учебного курса [Электронный ресурс] / А.Ю. Вишнякова. /Режим доступа: http://elar.urfu.ru/bitstream/10995/ 54385/1/m_th_a.y.vishnyakova_2017.pdf. Дата обращения: 28.03.2020.

11. Галатенко В.А. Стандарты информационной безопасности: курс лекций [Текст] / В.А. Галатенко //. Учебное пособие. - 2-ое издание. М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий». - 2017. - 264 с.

12. Гафарова Е.А. К вопросу проектирования онтологий предметной области при подготовке магистров по направлению информационная безопасности [Текст] / Е.А. Гафарова Ф.В. Синицын // Сборник научных трудов. 2016. С. 54-57.

13. ГОСТ Р 57628-2017 «Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности». [Электронный ресурс] / Режим доступа: http://docs.cntd.ru/ document/1200146707 Дата обращения 24.04.2020.

14. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. [Электронный ресурс] / Режим доступа: http://docs.cntd.ru/document/1200146707 Дата обращения 17.03.2020.

15. ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». [Электронный ресурс] / Режим доступа: http://docs.cntd.ru/document/1200146707 Дата обращения 10.03.2020.

16. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий». [Электронный ресурс] /

Режим доступа: http://docs.cntd.ru/document/1200146707 Дата обращения 21.04.2020.

17. Дарахвелидзе, П.Г., Марков Е.П. Программированиев Delphi. [Текст] / П.Г. Дарахвелидзе, Е.П. Марков. - М.: СПБ.: БХВ-Петербург. - 2018 – 113 с.

18. Доктрина информационной безопасности Российской Федерации. [Электронный ресурс] / Режим доступа: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html Дата обращения 29.04.2020.

19. Дунаев, В.В. Понятный самоучитель Photoshop CS6. [Текст] / В.В. Дунаев - М.: Питер. – 2017. – 205 с.

20. Дьяченко, В.К. Организационная структура учебного процесса и ее развитие. [Текст]/ В.К. Дьяченко. - М.: Педагогика, 2018. - 160 с.

21. Заика, А. И. Photoshop для начинающих. [Текст] / А.И. Заика. - М.: Питер. – 2017. – 130 с.

22. Зайнутдинова, Л.Х. Психолого-педагогические требования к электронным учебникам. [Текст] / Л.Х. Зайнутдинова. — Астрахань: АГТУ, 2016. - 71 с.

23. Зеер Э.Ф. Психология профессионального образования [Электронный ресурс] / Э.Ф. Зеер. Учеб. пособие. – М.: Академия, 2016. - 416 с. – URL:http://www.academiamoscow.ru/ftp_share/_books/fragments /fragment_23598.pdf. Дата обращения 14.03.2020.

24. Зимина, О.В. Рекомендации по созданию электронного учебника. [Электронный ресурс] / О.В. Зимина. // Режим доступа: http://www.academiaxxi.ru Дата обращения 24.03.2020.

25. Зимняя, И. А. Педагогическая психология. Учебник для вузов. Изд. второе. [Текст]/ И. А. Зимняя. – М.: Издательская корпорация «Логос», 2016. -384 с.

26. Знакомство со средой программирования Delphi. [Электронный ресурс] / Режим доступа: http://1aya.ru/paper/art-290899.php. Дата обращения: 09.05.2020.

27. Изергин, Н.Д. Разработка электронных учебных изданий. [Текст] / Н.Д. Изергин, А.А. Кудряшов, А.Ю. Руднев, В.А. Тегин // Учеб пособие для студентов вузов. - СПб.: СПбГУП, 2018. - 157 с.

28. Информационная безопасность: Учебное пособие [Текст] / В.В. Гафнер. - Рн/Д: Феникс, 2016. - 324 с.

29. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности. [Электронный ресурс] / Режим доступа: http://citforum.ru /security/articles/categorizing/3.shtml. Дата обращения: 02.05.2020.

30. Коджаспирова, Г. М. Педагогический словарь [Текст] / Г. М. Коджаспирова, А. Ю. Коджаспиров. — М.: Academia, 2016. - 176 с.

31. Костромина, С.Н. Эффективность усвоения учебной информации студентами в условиях электронного учебника. [Текст]/ С.Н. Костромина. -М.: СПБ.: БХВ-Петербург, 2016 – 134с.

32. Кречетников, К.П. Особенности проектирования интерфейса средств обучения. Информационные и коммуникационные технологии в образовании. [Текст] / К.П. Кречетников // Информатика и образование. – 2016 -55 с.

33. Кузьмина, Н.Н. Развитие мотивационных факторов учебно-трудовой деятельности студентов как средство повышения ее продуктивности. [Электронный ресурс] / Н.Н. Кузьмина. / Режим доступа: http://www.dissercat.com/ Дата обращения 12.03.2020.

34. Культин, Н.Б. Основы программирования в Delphi 7. [Текст] / Н.Б Культин. - М.: СПБ.: БХВ-Петербург. – 2018. -595 с.

35. Лисовский, В.Т. Духовный мир и ценностные ориентации молодежи России [Текст] / В.Т. Лисовский, А.В. Дмитриев. // Учеб., пособие для студентов вузов. - СПб.: СПбГУП, 2017. - 508 с.

36. Лукацкий А. Обеспечение информационной безопасности современного ВУЗа. [Электронный ресурс] / А. Лукацкий // Режим доступа: http://www.comprice.ru/articles/detail Дата обращения 9.03.2020.

37. Материал из Википедии — свободной энциклопедии. Электронный учебник. [Электронный ресурс] // Режим доступа: https://ru.wikipedia.org/wiki/ Дата обращения 02.04.2020.

38. Матыкин В.Ю. Создание и использование электронных учебных пособий [Электронный ресурс] / В.Ю. Матыкин. / Режим доступа: http://e-lib.gasu.ru/konf/nit/archiv/2005/3/4.html. Дата обращения 16.03.2020.

39. Мешкова Е.В. Обеспечение информационной безопасности при работе с электронными образовательными ресурсами [Электронный ресурс] / Е.В. Мешкова. / Режим доступа: http://vio.uchim.info/Vio_104/cd_ site/articles/a rt_2_1.htm. Дата обращения: 13.04.2020.

40. Несен, А.В. MicrosoftWord: от новичка к профессионалу. [Текст] / А.В. Несен. - М.: Солон-Пресс. – 2016. – 416 с.

41. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. №149-ФЗ, в ред. от 06.04.2011 г. № 149-ФЗ]. - Режим доступа: www.consultant.ru. Дата обращения: 01.03.2020.

42. Обеспечение информационной безопасности в образовательной организации. [Электронный ресурс] / Режим доступа: http://www.iccwbo.ru/blog/2016/obespehenie-informatsionnoy-bezopasnosti/. Дата обращения: 10.04.2020.

43. Осин, А.В. Основные положения концепции образовательных электронных изданий и ресурсов. [Текст] / А.В. Гиглавый, М.Н. Морозов, А.В. Осин, О.И. Руденко-Моргун, Ю.М. Тараскина. – М.: Республиканский мультимедиа центр, 2018. – 108 с.

44. Основы программирования в среде Delphi 7.0. [Электронный ресурс] / Режим доступа: http://fan5.ru/fan5-reply/reply-27589.php. Дата обращения: 24.04.2020.

45. Особенности защиты информации в образовательном учреждении. [Электронный ресурс] / Режим доступа: http://pandia.ru/text/79/076/98286.php. Дата обращения: 13.05.2020.

46. Партыка Т.Л. Информационная безопасность: Учебное пособие [Текст] / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2016. - 432 с.

47. Петров С.В. Информационная безопасность: Учебное пособие [Текст] / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2017. – 296 с.

48. Пилкасинского П. И. Педагогика: учеб. пособие для студентов пед. вузов и пед. колледжей [Текст] / П. И. Пилкасинского. – М.: Пел. О-во России, 2018. – 640с.

49. Полат Е.С. Новые педагогические и информационные технологии в системе образования: учебное пособие [Электронный ресурс] / Е.С. Полат, М. Ю. Бухаркина, М.В. Моисеева, А.Е. Петров // Под ред. Е. С. Полат. -6-е изд. — М.: Академия, 2019. 252 с. – Режим доступа: http://library.kpi.kharkov.ua/NEW/NewPiITvSO. Дата обращения 17.03.2020.

50. Положение об организации работы по охране труда, обеспечению безопасности образовательного процесса в ГБПОУ [Электронный ресурс] / Режим доступа: SUOT-PP-02-01-Ob-organizacii-raboty-po-OT-obespecheniyu-bezopasnosti-obrazovatelnogo-processa. Дата обращения 17.03.2020

51. Прессман, Л.П. Методика и техника эффективного использования средств обучения в учебно-воспитательном процессе. [Текст] / Л.П. Прессман. - СПб.: СПбГУП, 2016. - 219 с.

52. Программа развития ЮУрГТК [Электронный ресурс] / Режим доступа: [http://sustec.ru/svedeniya-o-kolledzhe/dokumenty/PROGRAMMA-RAZVITIYA-YUUrGTK-na-2014-2018gg-dlya-chirpo.pdf/ Дата обращения 26.03.2020.

53. Ранних В.Н. Электронный практикум как дидактическое средство повышения качества образования в вузе [Электронный ресурс] /

В.Н. Ранних/ Режим доступа:http://cyberleninka.ru/article. Дата обращения 02.03.2020.

54. Роберт И. Современные информационные технологии в образовании: дидактические проблемы; перспективы использования [Текст] / И. Роберт. - М: Школа-Пресс, 2018 -292 с.

55. Роберт, И.В. Теория и методика информатизации образования (психолого-педагогические и технологические аспекты). [Текст] / И.В. Роберт. - М.: ИИО РАО, 2017. - 234с.

56. Сабанов А.Г. О проблеме достоверности идентификации пользователя при удаленном электронном взаимодействии [Электронный ресурс] / А.Г. Сабанов / Режим доступа: https://cyberleninka.ru/article/n/o-probleme-dostovernosti-identifikatsii-polzovatelya-pri-udalennom-elektronnom-vzaimodeystvii. Дата обращения 12.04.2020.

57. Селевко Г.К. Современные образовательные технологии [Текст] / Г.К. Селевко. - М: Народное образование, 2016 -255 с.

58. Тихомиров, А.А. Компьютерные технологии в науке, практике и образовании. [Электронный ресурс] / А.А. Тихомиров. / Режим доступа: http://нэб.рф/catalog/ Дата обращения 19.03.2020.

59. Тихонов В.А. Информационная безопасность. Концептуальные, правовые, организационные и технические аспекты [Текст] /В.А. Тихонов, В.В. Райх // Гелиос АРВ.- 2019г. - 528 с.

60. Хестер, Н. Microsoft Front Page для Windows. [Текст] / Н. Хестер - М.: ДМК Пресс. – 2017. – 450с.

61. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений/ П.Б. Хорев.–М.:Издательский центр «Академия», 2017.–256 с.

62. Шемяков О.А. Научно-методический аппарат оценки уязвимости системы обеспечения безопасности информации в современном вузе - диссертация на соискании степени канд. техн. наук, 2013 Серпухов. [Электронный ресурс] / О.А. Шемяков. / [Электронный

ресурс]: http://www.dissercat.com/content/nauchno-metodicheskii-apparat-otsenki-uyazvimosti-sistemy-obespecheniya-bezopasnosti-informa Дата обращения 03.03.2020.

63. Явич, М.П. Концепции обучения информационных технологий ElMI- metodikjournal. [Текст] / М.П. Явич, Ц.Г. Мишеладзе, М.Т. Тхелидзе. Азербаджанский педагогический университет. 2016.-42 с.

64. «Южно-Уральский государственный колледж» Официальный сайт ГБПОУ [Электронный ресурс]: / Режим доступа: http://sustec.ru. Дата обращения 27.03.2020.

65. «Консультант плюс» - законодательство РФ, кодексы, законы, указы, постановления Правительства РФ [Электронный ресурс] / Режим доступа: http://www.consultant.ru/ Дата обращения 27.03.2020.