



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

Разработка мультимедийной системы обучения в условиях
обеспечения информационной безопасности в организации
профессионального образования

Выпускная квалификационная работа
по направлению 44.04.04 Профессиональное обучение
Направленность программы магистратуры
«Управление информационной безопасности в профессиональном
образовании»

Проверка на объем
заимствований:
_____ % авторского текста

Выполнил: магистрант 3 курса,
гр. 309/210-2-1
Смык Ольга Васильевна

Работа рекомендована к защите
«__» _____ 201__ г.
Зав. кафедрой АТ, ИТ и МОТД
ППИ Руднев В.В.

Научный руководитель:
к.т.н., доцент кафедры АТ, ИТ и МОТД ППИ
ЮУрГГПУ
Дмитриев Михаил Сергеевич

Челябинск, 2017

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: 44.04.04. «Профессиональное обучение»
Программа подготовки магистров «Управление информационной безопасностью
в профессиональном образовании»

ЗАДАНИЕ

на выпускную квалификационную работу
(магистерскую диссертацию)

Магистранту Смык Ольге Васильевне, обучающегося в группе ЗФ 309/210-2-1 по направлению подготовки “Профессиональное обучение (Управление информационной безопасностью в профессиональном образовании)”

Научный руководитель квалификационной работы: Дмитриев М.С. д.т.н., профессор кафедры АТ, ИТ и МОТД

1. Тема квалификационной работы: «Разработка мультимедийной системы в условиях обеспечения информационной безопасности в организации профессионального образования», утверждена приказом Южно-уральского государственного гуманитарно-педагогического университета № 539-сз от «10» 03 2016 г.

2. Срок сдачи магистрантом законченной работы на кафедру «__» ____201__ г.

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

- Проанализировать теоретические аспекты создания и защиты мультимедийных систем.

- Рассмотреть возможность использования мультимедийных систем в образовательных учреждениях в условиях информационной безопасности.

- Разработать мультимедийную систему по дисциплине с учетом информационной безопасности образовательного учреждения.

- Создать техническую документацию по выбранной дисциплине.

- Проверить эффективность использования созданной мультимедийной системы.

4. Материалы для выполнения квалификационной работы:

- Учебная, научно-техническая, педагогическая, методическая, нормативно-правовая литература по теме выпускной квалификационной работы (магистерской диссертации).

- Материалы научно-исследовательской работы, педагогической и преддипломной практики.

5. Перечень графического материала (с точным указанием обязательных таблиц, чертежей или графиков, образцов и др.) Таблица, таблицы и диаграммы результатов экспериментальной проверки внедрения в организации СПО и экспертной проверки действующих педагогов и руководителей СПО и ВО, а также технических специалистов.

6. Консультанты по специальным разделам ВКР:

Раздел	Консультант	Отметка о

Дата выдачи задания «_____» _____ 2017 года

Задание выдал, к.т.н., доцент,
зав. кафедрой АТ,ИТиМОТД _____ В.В. Руднев

Задание приняла _____ Смык О.В.

КАЛЕНДАРНЫЙ ПЛАН

выполнения выпускной квалификационной работы (магистерской диссертации)

№ n/n	Наименование этапов подготовки выпускной квалификационной работы	Срок выполнения этапов ВКР	Отметка о выполнении
1	Предзащита ВКР	21.11. 2017 г.	
2	Доработка ВКР после предзащиты		
3	Нормоконтроль		
4	Подписание ВКР научным руководителем		
5	Оформление пояснительной записки и презентации ВКР		
6	Подписание рецензии на ВКР		
7	Защита ВКР на заседании ГАК	14 .12. 2017.	

Автор _____ Смык О.В.

Научный руководитель,

д.т.н., профессор,

каф.АТ,ИТиМОТД _____ М. С. Дмитриев

Заведующий кафедрой АТ,ИТиМОТД,

к.т.н., доцент

_____ В.В. Руднев

Содержание

Введение	4
1.1 Что такое мультимедийная система	8
1.1.1 Понятие мультимедиа	8
1.1.2 Мультимедиа технологий	14
1.1.3 Мультимедиа в образовании	17
1.2 Требования к разработке мультимедийной системы. Этапы проектирования мультимедийной системы	24
1.2.1. Требования к разработке мультимедийной системы	24
1.2.2. Этапы проектирования мультимедийных систем	32
1.3 Программы разработки мультимедийной системы	36
1.3.1. Обзор и анализ существующих программных средств разработки мультимедийных программных продуктов	36
Выводы по первой главе	46
Глава 2. Практические аспекты создания мультимедийной системы	47
2.1. Нормативная документация по дисциплине «Информатика и программирования»	47
2.1.1. Пояснительная записка	47
2.1.2. Содержание дисциплины, структурирование по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	48
2.1.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	55
2.1.4. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	56
2.2. Разработка и структура мультимедийной системы	61
Выводы по второй главе	68
Глава 3. Теоретические и практические методы информационной безопасности и защиты информатики	73

3.1. Информационная безопасность в образовательной организации	73
3.1.1. Сущность понятия информационная безопасность	73
3.1.2. Основные угрозы информационной безопасности	75
3.1.3. Методы защиты информации	81
3.1.4. Информационная безопасность образовательной организации	91
3.2. Реализация информационной безопасности в колледже	97
3.2.1. Информационные технологии при организации учебного процесса в колледже	97
3.2.2. Политика информационной безопасности колледжа	102
3.3. Место в системе электронных образовательных ресурсов и меры защиты от угроз	116
3.3.1. Место в системе	116
3.3.2. Меры защиты	117
Выводы по третьей главе	118
Заключение	119
Библиографический список	120

Введение

Актуальность темы. Проблема защиты информации от постороннего доступа и нежелательных воздействий на нее возникла практически на заре человечества. С развитием общественных отношений, появлением частной собственности, государственного строя, борьбой за власть и дальнейшим расширением масштабов человеческой деятельности информация приобретает все большую ценность. С переходом на использование технических средств связи информация подвергается воздействию неблагоприятных случайных процессов: неисправностей и сбоев аппаратуры, ошибок операторов и т.п., которые могут привести к ее разрушению, изменениям, потере, а также создать предпосылки для доступа к ней посторонних лиц.

С появлением автоматизированных систем и информационно-вычислительных сетей проблема защиты информации приобретает еще большее значение. Автоматизированные информационно-документационные системы (АИС) играют все более значимую роль в обеспечении потребностей как общества, организации, так и отдельного человека.

Процессы информатизации современного общества и тесно связанные с ними процессы информатизации всех форм образовательной деятельности характеризуются процессами совершенствования и массового распространения современных информационных и коммуникационных технологий (ИКТ).

Актуальность разработки мультимедийной системы обусловлена радикальными переменами в социальной, политической и экономической жизни общества под влиянием информатизации. В настоящее время наблюдается процесс перехода общества к качественно новому состоянию, названными учёными информационным обществом.

Образование в Информационном обществе перестаёт быть способом усвоения готовых и общепринятых знаний, оно становится способом

информационного обмена человека с окружающими людьми, который предполагает также генерирование информации в обмен на полученную.

Различие между знанием и информацией, относительность знаний вследствие их быстрого устаревания, превращение образования в непрерывное - все эти процессы ведут к вытеснению знаний информацией в качестве основного элемента образовательного процесса, превращению знания в информацию о мире. В связи с этим, одной из основных задач образования становится обучение работе с информацией.

Актуальность безопасности в информационной сфере определяется, с одной стороны, действием объективно возникающих в современном обществе и образовании ситуаций цивилизованных изменений, с другой стороны, наличием проблемной ситуации в связи с необходимостью изменения приоритетов в науке, образовании, общественном сознании и социальной практике и перехода от традиции значимости безопасности общества к значимости безопасности человека. В частности, в системе образования данная проблема определяется противоречием между существующей необходимостью обеспечения информационной безопасности, используя интернет в образовательном процессе, и отсутствием механизма ее реализации в образовательном пространстве.

В частности, в системе образования данная проблема определяется противоречием между существующей необходимостью обеспечения. Закон Российской Федерации «О безопасности» (1992 г.), Конституция Российской Федерации (1993 г.) (ст. 2 и 7), Закон Российской Федерации «Об информации, информатизации и защите информации» (1995 г.), Концепция национальной безопасности Российской Федерации (2000 г.), Доктрина информационной безопасности Российской Федерации (2000 г.) создают правовую основу безопасности человека.

Базовым концептуальным документом, определяющим политику государства в этой области, является Доктрина информационной безопасности Российской Федерации, в которой обозначены интересы личности и общества в

целом. В качестве интересов личности, определяющих состояние ее безопасности, выделены реализация конституционных прав и свобод, обеспечение личной безопасности, повышение качества и уровня жизни, духовное, интеллектуальное и свободное развитие человека и гражданина.

В настоящее время общество находится на пороге смены образовательной парадигмы - переход от образования в условиях ограниченного доступа к информации к образованию в условиях неограниченного доступа к информации. Необходимость ее смены означает осознание несоответствия ранее сложившихся и ставших традиционными представлений нынешней педагогической практике (по Г. Л. Ильину). В связи с переходом к Информационному обществу и внедрением Инновационных компьютерных технологий в образовательный процесс, с изменением целей обучения возрастает роль самостоятельной деятельности с использованием ресурсов Интернета.

Цель исследования – разработка мультимедийной системы в условиях информационной безопасности.

Гипотеза – внедрение системы защиты мультимедийных образовательных ресурсов от несанкционированного копирования позволит повысить уровень информационной безопасности в организации профессионального образования.

Объект исследования – процесс использования и защиты мультимедийных систем от несанкционированного копирования в образовательных учреждениях.

Предмет исследования – совершенствование мультимедийных образовательных ресурсов и систем защиты от их несанкционированного копирования.

Задачи исследования:

1. Проанализировать теоретические аспекты создания и защиты мультимедийных систем.

2. Рассмотреть возможность использования мультимедийных систем в образовательных учреждениях в условиях информационной безопасности.

3. Разработать мультимедийную систему по дисциплине с учетом информационной безопасности образовательного учреждения.

4. Создать техническую документацию по выбранной дисциплине.

5. Проверить эффективность использования созданной мультимедийной системы.

Методы исследования:

1. Изучение основной и методической литературы.

2. Сбор информации.

3. Анализ собранной информации.

4. Создание продукта.

Практическая значимость исследования – возможность использования разработанной мультимедийной системы в учебном процессе организаций СПО и ВО.

Диссертация состоит из введения, трех глав, заключения, списка использованной литературы, включающего 64 источника, 4 таблиц, 19 рисунков. Общий объем работы составляет 121 с.

Глава 1. Теоретические аспекты создания мультимедийных систем.

1.1 Что такое мультимедийная система.

1.1.1. Понятие мультимедиа.

Термин мультимедиа появился в 80-х годах прошлого столетия. До этого мультимедиа ограничивалась пишущей машинкой «Консул», которая не только печатала, но и могла привлечь внимание оператора мелодичным треском. Новым веянием в развитии мультимедиа явился компьютерный гороскоп 1980 года, который при помощи динамика и программируемого таймера синтезировал расплывчатые устные прогнозы на каждый день, а, кроме того, ещё перемещал по экрану звёзды.

В конце 80-х годов интересы производителей оборудования для электронных коммуникаций совпали с потребностями нарождающегося информационного общества. Сама по себе теория мультимедийных технологий появилась как ответ на возможное решение серьезных проблем, возникших в различных отраслях: телерадиовещании, информатике и связи. До этого момента различные производители занимали свои сектора на рынке, однако все они одновременно встали перед задачей: изобрести, развить и внедрить в жизнь новый рынок мультимедийных технологий, способный расти быстрыми темпами.

Если говорить о революции, которую произвело появление компьютера, то она затронула абсолютное меньшинство населения, т.к. все первые ЭВМ концентрировались на производстве, на рабочих местах. Если говорить о телефоне, кино, звукозаписи и телевидении – то даже они, отдельно взятые, не обладали потенциалом мультимедийных технологий. Последние сочетают в себе огромные возможности для развлечения, потребления, информирования, образования, трудовой деятельности, культуры и коммуникации.

Последние индустриальные революции показали – в основе каждого серьезного изменения общества лежали и лежат технологические новшества.

Наступление информационной эры развития человечества было вызвано цифровыми технологиями обработки, передачи и воспроизведения информации. Мультимедиа появились на конечном этапе цифровых коммуникационных технологий.

Современный, мультимедийный персональный компьютер напоминает домашний стереофонический Hi-Fi комплекс, объединённый с дисплеем–телевизором. Он укомплектован активными стереофоническими колонками, микрофоном и дисководом для оптических компакт – дисков – CD-ROM. Кроме того, данный агрегат содержит новое для ПК устройство – аудиоадаптер. Он позволяет перейти к прослушиванию чистых стереофонических звуков через акустические колонки с встроенными усилителями. На сегодняшний день мультимедиа-технологии являются одним из наиболее перспективных и популярных направлений информатики.

В представлении информации активно используются следующие возможности мультимедиа:

- увеличивать (детализировать) на экране изображение или его фрагменты, при сохранении качества изображения. Данная возможность актуальна в процессе презентаций произведений искусства и уникальных исторических документов;
- хранить большой объём разнообразной информации на одном носителе;
- сравнивать и обрабатывать изображения разнообразными программными средствами с научно-исследовательскими или познавательными целями;
- использовать технологии гипертекста и гипермедиа;
- осуществлять непрерывное аудио-сопровождение (музыкального или любого другого), соответствующего статичному или динамичному визуальному ряду;
- использование видеофрагментов из фильмов, видеозаписей, функции «стоп – кадра», покадрового «пролистывания» видеозаписи и т. д.; □ подключение к глобальной сети Internet;

- работа с различными приложениями: текстовыми, графическими и звуковыми редакторами, картографической информацией;

- включение в состав мультимедийного продукта игровых компонентов с информационными составляющими. [13]

Приведем несколько имеющихся определений термина «мультимедиа»:

Мультимедиа - это:

- технология, описывающая порядок разработки, функционирования и применения средств обработки информации разных типов;

- информационный ресурс, созданный на основе технологий обработки и представления информации разных типов;

- компьютерное программное обеспечение, функционирование которого связано с обработкой и представлением информации разных типов;

- компьютерное аппаратное обеспечение, с помощью которого становится возможной работа с информацией разных типов;

- особый обобщающий вид информации, которая объединяет в себе как традиционную статическую визуальную (текст, графику), так и динамическую информацию разных типов (речь, музыку, видео фрагменты, анимацию и т.п.).[10]

- современная компьютерная информационная технология, позволяющая объединить в компьютерной системе текст, звук, графическое изображение, видеоизображение и анимацию (мультипликацию).

- сумма технологий, позволяющих компьютеру вводить, обрабатывать, хранить, передавать и отображать (выводить) такие типы данных, как текст, графика, анимация, оцифрованные неподвижные изображения, видео, звук, речь.

- интерактивные системы, обеспечивающие работу с неподвижными изображениями и движущимся видео, анимированной компьютерной графикой и текстом, речью и высококачественным звуком. [13]

Если обобщить эти определения, то мультимедиа является одним из наиболее перспективных и популярных направлений развития информационных

технологий. Их цель — создание приложений, содержащих «коллекции изображений, текстов и данных, сопровождающихся звуком, видео, анимацией и другими визуальными эффектами, включающими интерактивный интерфейс и другие механизмы управления» [34]

Идейной предпосылкой возникновения технологии мультимедиа считают концепцию организации памяти «MEMEX». Она предусматривала поиск информации в соответствии с ее смысловым содержанием, а не по формальным признакам (порядку номеров, индексов или по алфавиту и т. п.). Эта идея нашла свое выражение и компьютерную реализацию сначала в виде гипертекста (системы работы с комбинациями текстовых материалов), а затем и в виде гипермедиа (системы, работающей с комбинацией графики, звука, видео и анимации). Особый интерес к применению мультимедиа-технологии связан с именем Билла Гейтса, которому принадлежит идея создания и успешной реализации на практике мультимедийного продукта на основе служебной музейной инвентарной базы данных для «National Art Gallery» в Лондоне, с использованием в нем всех возможных «сред»: изображений, звука, анимации, гипертекстовой системы.

Именно этот продукт интегрировал в себе три основных принципа мультимедиа [20]:

- 1) представление информации с помощью комбинации множества воспринимаемых человеком сред;
- 2) наличие нескольких сюжетных линий в содержании продукта;
- 3) художественный дизайн интерфейса и средств навигации.

Мультимедиа-продукты можно разделить на несколько групп в зависимости от того, на какие категории потребителей они ориентированы.

Одна группа программ — это обучающие, развивающие программы, всевозможные энциклопедии и справочники, графические программы, простые музыкальные редакторы и т.п.

Другая категория – это бизнес-приложения. Здесь мультимедиа служит для иных целей. С ее помощью оживают презентации, становится возможным организовать видеоконференции «вживую», а голосовая почта настолько хорошо заменяет офисную АТС, что обычный телефон начинает восприниматься как архаизм.

Третья группа продуктов ориентирована на профессионалов. Для них предлагаются средства производства видеофильмов, компьютерной графики, а также домашние музыкальные студии. [13]

Применение средств мультимедиа в компьютерных приложениях стало возможным благодаря прогрессу в разработке и производстве новых микропроцессоров и систем хранения данных:

- возросший объем памяти, характеристики внешней памяти;
- быстродействие;
- графические возможности;
- достижения в области видеотехники, лазерных дисков, их массовое внедрение;
- разработка методов быстрого и эффективного сжатия/развертки данных.

[23]

Благодаря применению мультимедиа в средствах информатизации за счет одновременного воздействия графической, звуковой, фото и видео информации, такие средства обладают большим эмоциональным зарядом и активно включаются в индустрию развлечений, практику работы различных учреждений, домашний досуг, образование.

Появление систем мультимедиа произвело революцию во многих областях деятельности человека. Одно из самых широких областей применения технология мультимедиа получила в сфере образования, поскольку средства информатизации, основанные на мультимедиа способны, в ряде случаев, существенно повысить

эффективность обучения. Экспериментально установлено, что при устном изложении материала обучаемый за минуту воспринимает и способен переработать до одной тысячи условных единиц информации, а при "подключении" органов зрения до 100 тысяч таких единиц. [8]

Мультимедиа-технологии используют разные способы представления информации различного вида. Рассмотрение видов и форм представления информации начнем с определения понятия информации. Термин информация уходит корнями к латинскому *information* – разъяснение, изложение. Изначально в это слово вкладывался смысл, соответствующий сведениям, передаваемым одними людьми другим людям, устным, письменным или другим способом, а также сам процесс передачи или получения этих сведений.

На сегодняшний день существует три основных направления развития научных исследований, связанных с понятием информация.

Первое из них обеспечивает разработку математического аппарата, отражающего основные свойства информации. В этой связи уместно вспомнить деятельность таких выдающихся ученых как Г. Крамер, Б. Ван-дер-Варден, С. Кульбак и других. Благодаря подобным исследованиям информация разделена на типы, изучены свойства и основные признаки каждого вида информационных процессов.

Второе направление научной деятельности, посвященной информации, осуществлялось А. Харкевичем, Р. Карнапом и другими учеными. Оно привело к теоретической разработке различных аспектов понятия информация на базе уже имеющихся математических средств в исследовании основных свойств информации. Практически решена сложнейшая проблема измерения ценности и полезности информации с точки зрения ее использования, проблемы измерения количества информации и другие вопросы.

Третий вид исследований проводится большим количеством ученых из различных научных областей и посвящен использованию информационных методов в лингвистике, биологии, психологии, социологии, педагогике, медицине и многих других областях. Подобное разнообразное использование понятия информация побудило У. Эшби, Л. Бриллюэна, А. Урсула и некоторых других ученых придать этому понятию общенаучное значение. [13]

1.1.2 Мультимедиа технологий.

Формальный подход к определению средств мультимедиа, говорит о том, что ими могут являться практически любые средства, способные привнести в обучение и другие виды деятельности информацию разных видов. В таком случае под понятие средств мультимедиа могут попасть и ставшие традиционными устаревающие аналоговые средства.

Однако чаще всего к средствам мультимедиа относят компьютеры и их соответствующее периферийное оборудование. Компьютер, является универсальным средством обработки информации. Универсальность компьютера состоит в том, что, с одной стороны, он один в состоянии обрабатывать информацию разных типов (мультимедиа информацию), с другой стороны, один и тот же компьютер в состоянии выполнять целый спектр операций с информацией одного типа. Благодаря этому компьютер в совокупности с соответствующим набором периферийных устройств в состоянии обеспечить выполнение всех функций технических мультимедиа средств.

«Мультимедийный компьютер» – это такой компьютер, на котором мультимедийные приложения могут в полной мере реализовать все свои возможности. Мультимедийный компьютер должен уметь многое: отображать на экране монитора графическую и видео-информацию, анимацию, воспроизводить с высоким качеством различное звуковое сопровождение, музыку, в том числе и с музыкальных компакт-дисков, и многое другое...

Обычно под набором комплектующих, объединенных понятием «мультимедийный компьютер», понимают следующий их состав:

- Корпус с блоком питания
- Системная (материнская) плата
- Центральный процессор
- Оперативная память
- Видеоадаптер
- Монитор
- Накопитель на жестких дисках
- Клавиатура
- Мышь
- Дисковод CD-ROM
- Дисковод гибких дисков
- Звуковая карта
- Дисковод DVD
- Модем
- Телевизионный и УКВ тюнер.

Но даже самый современный компьютер не будет работать без программного обеспечения.

Программное обеспечение можно условно разделить на прикладную часть (мультимедиа-энциклопедии, компьютерные игры, аудио и видеоплееры и т.п.) и специализированную, к которой можно отнести программы, предназначенные для создания прикладных программ (профессиональные графические редакторы, редакторы 3D-графики, звуковые редакторы и т.д.)

Рассмотрим основные части программного обеспечения мультимедиа-компьютера:

- Операционная система
- Прикладные мультимедийные приложения

Сейчас мультимедийные приложения стали одним из наиболее быстро растущих сегментов рынка программного обеспечения. Большинство современных компьютеров продаются с установленными приводами, звуковыми картами и мощными графическими адаптерами. Чтобы иметь возможность воспользоваться всеми этими аппаратными средствами поддержки мультимедиа на компьютере должна быть установлена операционная система, поддерживающая все эти устройства. Наиболее яркими примером являются ОС Microsoft Windows XP, Windows Vista, Windows 7, Linux.

К прикладным можно отнести мультимедийные приложения, с которыми непосредственно работает обычный пользователь мультимедийного компьютера. В первую очередь это компьютерные игры. Также сюда можно отнести мультимедиа-энциклопедии, видео и аудиоплееры, программы для создания и просмотра презентаций и многие другие.[6].

1.1.3. Мультимедиа в образовании.

Мультимедиа-приложения используются во многих областях деятельности человека.

- Образование — медиаобразование (виртуальные университеты, система дистанционного обучения (ДО), курсы).
- Промышленность (авиация, автомобилестроение, судостроение, кибернетика и др.), особенно в механической и автомобильной промышленности, мультимедиа, прежде всего, используется на стадии проектирования. Это позволяет, например, инженеру рассматривать изделие в различных перспективах,

производить другие манипуляции, прежде чем приступить к производству (автоматизированное проектирование).

- Экономика (системы управления).
- Медицина (диагностика, лечение) мультимедиа применяется в процессе обучения хирургов (виртуальная хирургия).
- СМИ (виртуальная студия, цифровое и аналоговое телевидение, радио, телетекст, Интернет).
- Коммерция (реклама, виртуальные предприятия, киоски и супермаркеты).
Возможности технологии мультимедиа безграничны. В бизнес-приложениях мультимедиа в основном применяются для обучения и проведения презентаций. В сфере бизнеса фирма по продаже недвижимости уже используют технологию мультимедиа для создания каталогов продаваемых домов.
- Военные цели (космические, авиация, корабли, танки, штабы и тренажеры).
Технологические мультимедиа пользуется большим вниманием военных. Так, Пентагон реализует программу перенесения на интерактивные видеодиски всей технической, эксплуатационной и учебной документации по всем системам вооружений, создания и массового использования тренажеров на основе таких дисков.
- Наука (моделирования различных процессов).
- Культура и искусство (кино, музеи, виртуальные личности и объекты, энциклопедии). В искусстве наиболее яркими примерами мультимедиа являются специальные эффекты в кино, компьютерная мультипликация и трехмерная графика.
- Игры (развлечения, отдых, туризм, знакомство).

- Создание сайтов — наиболее популярная сфера использования. Сайт, содержащий звук, видео, анимированные изображения и текст, позволит наглядно и доступно представить информацию любого содержания.

- Виртуальная реальность — получение почти реальных ощущений человеком от нереального мира.[23]

Одно из самых широких областей применения технология мультимедиа получила в сфере образования, поскольку средства информатизации, основанные на мультимедиа способны, в ряде случаев, существенно повысить эффективность обучения.

Мультимедийные технологии позволяют сделать обучение более эффективным, вовлекая в процесс восприятия учебной информации большинство чувственных компонент обучаемого. Сегодня мультимедиа-технологии – это одно из перспективных направлений информатизации учебного процесса.

Перспектива успешного применения современных информационных технологий в образовании состоит в совершенствовании программного и методического обеспечения, материальной базы, а также в обязательном повышении квалификации преподавателей.

Мультимедиа-технологии позволяют интегрировать мощные распределенные образовательные ресурсы, обеспечить среду формирования и проявления ключевых компетенций, таких, как информационная и коммуникативная. Мультимедиа и телекоммуникационные технологии открывают принципиально новые методические подходы в системе образования. Интерактивные технологии на основе мультимедиа позволяют организовывать дистанционные формы обучения на базе Интернет-коммуникаций и интерактивных CD-курсов. [13]

Средства и технологии мультимедиа повышают мотивацию студентов к учению за счет применения современных способов обработки аудиовизуальной информации, таких, как:

- «манипулирование» (наложение, перемещение) визуальной информацией;
- контаминация (смещение) различной аудиовизуальной информации;
- реализация анимационных эффектов;
- деформирование визуальной информации (увеличение или уменьшение определенного линейного параметра, растягивание или сжатие изображения);
- дискретная подача аудиовизуальной информации;
- многооконное представление аудиовизуальной информации на одном экране с возможностью активизировать любую часть экрана (например, в одном «окне» – видеофильм, в другом - текст);
- демонстрация реально протекающих процессов, событий в реальном времени (видеофильм). [22]

Современный процесс обучения должен постоянно интенсифицироваться, так как вследствие накопленного человечеством объема знаний и поставленными обществом задачами, современный студент должен усваивать огромные объемы информации за меньшую единицу времени. На помощь приходят мультимедийные и интерактивные технологии.

Мысль о том, чтобы рассказать о технологиях, строении объектов, рельефных картах и процессов в динамике без их демонстрации вызывает улыбку. При этом возможности и эффект восприятия динамического видео или 3D изображений не сравнимы с печатными статичными изображениями.

Мультимедиа в образовании позволяют подключить максимум каналов человека к восприятию информации, так как более 70% информации мы воспринимаем с помощью зрения, и менее 30% - с помощью слуха. Мультимедиа позволяют создавать информационно насыщенную среду погружения для участников образовательного процесса, используя текстовые и графические

данные, видео, аудио, возможности объемного моделирования и интерактивные инструменты.

Эффективность применения интерактивных методик в обучении давно изучена и доказана. Известно, что интерактивные инструменты позволяют увеличивать степень усвоения материала до 90%. Методика интерактивного обучения с использованием современного мультимедиа оборудования позволяет использовать новые возможности по предоставлению большего объема знаний и формированию необходимой фокусировки внимания учащихся. [22]

Современная организация обучения ученика имеет следующие методические особенности:

Применение мультимедийных презентаций с использованием мультимедиа проекторов, электронных справочников, автоматизированных обучающих систем, видеозаписей работы различных программ и т.д.

Закрепление за каждым обучаемым на практических занятиях отдельного компьютера, на котором целесообразно создать его личную папку.

Использование индивидуального подхода, включающего использование индивидуализированных обучающих программ, банка многоуровневых заданий для практических и лабораторных работ и тестов.

Целесообразность проведения значительной части занятий в форме деловых игр; в качестве заданий должны выдаваться реальные жизненные многовариантные и непоставленные задачи, особенно те, с которыми выпускники будут встречаться в профессиональной деятельности.

Использование метода проектов, в рамках которого необходимо соблюдать принципы последовательности и преемственности; это значит, что одно глобальное задание должно последовательно выполняться во всех практических, лабораторных и расчетно-графических работах, дополняться и расширяться, воплощаясь в стройную завершенную систему.

Возможность параллельного и концентрического изучения основных разделов программы, что позволяет обучающимся по мере усвоения курса получать все более глубокие знания по каждому из разделов, не теряя при этом целостности изложения всего материала.

Использование следующих взаимосвязанных принципов обучения: мотивации познания; разностороннего восприятия; межпредметной координации.

Использование проблемного метода обучения, предусматривающего создание обучающимися реальных информационных продуктов (презентаций, документов, таблиц, баз данных), которые могут быть использованы в процессе обучения.

Применение мультимедиа-технологий в образовании обладает следующими достоинствами по сравнению с традиционным обучением:

- возможность использования цветной графики, анимации, звукового сопровождения, гипертекста;
- возможность обновления учебного материала; □ небольшие затраты на публикацию и размножение;
- возможность использования в учебном материале интерактивных веб-элементов, тестов и рабочих тетрадей;
- возможность копирования и переноса частей для цитирования;
- возможность нелинейного прохождения учебного материала, содержащего гиперссылки;
- гиперсвязи с дополнительной литературой в электронных библиотеках или образовательных сайтах.

Организация аудиторных занятий с применением мультимедиа-технологий дает возможность экономить время, тем самым интенсифицируя изложение учебного материала, за счет использования простых и доступных средств.

В ходе занятий обучающиеся могут создавать визуализированные красочные учебно-игровые среды, что значительно повышает восприятие изучаемого предмета. Мультимедийные компьютерные технологии дают преподавателю возможность оперативно сочетать разнообразные средства, способствующие более глубокому и осознанному усвоению изучаемого материала, экономить время занятий, насыщая его информацией. Включение информационных мультимедийных технологий делает процесс обучения технологичнее и результативнее и способствует повышению интереса к обучению.

При использовании мультимедиа на занятиях через интерактивность, структуризацию и визуализацию информации происходит усиление мотивации обучающегося, активизация его познавательной деятельности, как на уровне сознания, так и подсознания. Однако внедрение в образование мультимедиа технологий требует дополнительной подготовки мультимедийных учебных материалов и соответствующей организации занятий. [13]

Мультимедиа-средства могут применяться в самых различных стилях обучения и восприниматься людьми с различными психо-возрастными особенностями восприятия и обучения: некоторые учащиеся предпочитают учиться только посредством чтения, другие – посредством восприятия материала на слух, третьи – посредством просмотра видеофильмов.

Мультимедийные программные средства способствуют повышению эффективности следующих видов образовательной деятельности:

- просмотра аудиовизуальной информации;
- тренажера по теории с использованием практических упражнений;
- педагогического контроля и измерения результативности обучения;
- работы со словарем терминами и понятиями;
- интерактивного общения учащегося с преподавателем. [15]

Из всех каналов получения информации человека визуальный является наиболее мощным, поэтому его использование в области образования средствами

мультимедиа более разработано. Эффективность усвоения материала значительно повышает создание для каждого мультимедийного учебника своей ритмической доминанты с помощью оптимального подбора музыкального сопровождения. Продуманное взаимодействие клавиатуры и мыши в мультимедийных учебных материалах в сочетании с другими информационными каналами добавляет еще одно преимущество данной образовательной технологии. Оно основано на том, что мануальные упражнения существенно развивают память. [13]

Использование мультимедийных средств обучения позволяет реализовать совершенно новые высокоэффективные методы для самостоятельного обучения, значимые с точки зрения новой системы открытого образования. Предпосылками к применению мультимедиа в образовании служат цели, преследующие самообразование. Так, Ф. И. Вейнерт к этим целям относит построение усвоенного знания и выстраивание значимого, прикладного знания и знания об обучении. Достигнуть выше упомянутых целей образования помогает использование мультимедийных средств обучения. Для достижения поставленных целей необходимо: – в процессе обучения необходимо активизировать не один канал восприятия, а несколько, что делает возможной интеграцию информации, доставляемую разными органами чувств; – визуально представлять все динамические процессы и абстрактную информацию; – формировать у учащегося системность построения изучаемого материала. [15]

1.2. Требования к разработке мультимедийной системы. Этапы проектирования мультимедийной системы.

1.2.1. Требования к разработке мультимедийной системы.

Современные информационные технологии имеют огромные возможности для совершенствования учебного процесса и системы образования в целом. Одним из средств, обладающих значительным развивающим потенциалом, является мультимедиа. Она представляет собой совокупность программных средств, реализующих обработку аудиовизуальной информации с использованием анимации, графики, фотографий, видео, звука и текста, что создает комплексную информационную среду.

Мультимедиа является эффективной образовательной технологией благодаря присущим ей качествам интерактивности, гибкости и интеграции различных типов учебной информации, а также благодаря возможности учитывать индивидуальные особенности учащихся и способствовать повышению их мотивации.

Возможности мультимедиа технологий позволяют создавать:

- электронные учебники,
- мультимедиа-энциклопедии,
- обучающие системы,
- деловые игры,
- лингвистические мультимедиа-системы,
- интерактивные мультимедиа-презентации и многое другое.

В настоящее время в образовании используются образовательные ресурсы, выполненные на основе мультимедийных технологий.

В большом многообразии этих ресурсов выделим:

- мультимедиа-энциклопедии;
- мультимедиа-презентации;
- обучающая мультимедиа-система;
- лингвистическая мультимедиа-система;

- мультимедиа-учебники;
- мультимедийные базы данных;
- бизнес-игры;
- справочные мультимедиа-системы;
- электронный журнал;
- мультимедиа-каталоги.

При создании мультимедийных образовательных ресурсов в первую очередь встает вопрос о формировании системы требований к этим ресурсам. Учитывая, что каждый ресурс имеет свои особенности, проведем анализ этих требований. Результаты анализа представлены в таблице 1.

Таблица 1 – Требования к разработкам мультимедиа систем.

Наименование	Требование к разработке
Мультимедиа-энциклопедии	<ol style="list-style-type: none"> 1. Полнота информации; 2. Системность изложения материала; 3. Научность языка энциклопедии; 4. Объективность при характеристике понятий, событий, объектов и биографических данных; 5. Фактологическая точность; 6. Лаконичность и популярность изложения; 7. Наличие определения в каждой статье; 8. Схематичность изложения; 9. Изложение фактов без эмоциональных личностных оценок.

<p>мультимедиа-презентации</p>	<ol style="list-style-type: none"> 1. Соответствие содержания презентации поставленным дидактическим целям и задачам; 2. Соблюдение принятых правил орфографии, пунктуации, сокращений и правил оформления текста; 3. Отсутствие фактических ошибок, достоверность представленной информации; 4. Лаконичность текста на слайде; 5. Завершенность; 6. Объединение семантически связанных информационных элементов в целостно воспринимающиеся группы; 7. Сжатость и краткость изложения, максимальная информативность текста; 8. В текстовых блоках необходимо использовать короткие слова и предложения; 9. Рекомендуется минимизировать количество предлогов, наречий, прилагательных; 10. Презентация должна дополнять, иллюстрировать то, о чем идет речь на занятии.
<p>обучающая мультимедиа-система;</p>	<ol style="list-style-type: none"> 1. Интуитивно понятный интерфейс за счет применения графики, цвета, и прочего; 2. Многоуровневые разветвления обучающей программы; 3. Возможность использования учеником различных вспомогательных средств при возникновении проблем в процессе обучения такие как: системы подсказок, ссылок на дополнительные обучающие

	<p>материалы, выходы на иные информационные материалы и так далее;</p> <ol style="list-style-type: none"> 4. Многообразие вариаций в постановке заданий, разнообразные возможности взаимодействия с обучающей программой, как системный принцип ее построения; 5. Обеспечение постоянной привязки времени и темпа обучения к уровню результатов каждого отдельного обучающегося и его психофизическим возможностям восприятия материала обучения, что предполагает наличие в системе разнообразия стратегий обучения в зависимости от типа ученика; 6. Возможность прерывания процесса обучения в любой момент времени с сохранением достигнутых к этому моменту результатов обучения студента. 7. Обеспечение возможности продолжения занятия с места, на котором оно было прервано или возврата к началу.
<p>лингвистическая мультимедиа-система;</p>	<ol style="list-style-type: none"> 1. Единый язык общения пользователей с системой; 2. Единая терминологическая система, включающая единую систему унификации терминов, имеющих одинаковую смысловую нагрузку; 3. Обеспечение единых методов формализации текстов, нормализации и редактирования данных.
<p>мультимедиа-учебники;</p>	<ol style="list-style-type: none"> 1. Информация по выбранному курсу должна быть хорошо структурирована и представлять собою

	<p>законченные фрагменты курса с ограниченным числом новых понятий;</p> <p>2. Каждый фрагмент, наряду с текстом, должен представлять информацию в аудио- или видео виде;</p> <p>3. Текстовая информация может дублировать некоторую часть живых лекций;</p> <p>4. На иллюстрациях, представляющих сложные модели или устройства, должна быть мгновенная подсказка, появляющаяся или исчезающая синхронно с движением курсора по отдельным элементам иллюстрации;</p> <p>5. Текстовая часть должна сопровождаться многочисленными перекрестными ссылками, позволяющими сократить время поиска необходимой информации, а также мощным поисковым центром;</p> <p>6. Видеоинформация или анимации должны сопровождать разделы, которые трудно понять в обычном изложении;</p> <p>7. Наличие аудиоинформации, которая во многих случаях является основной и порой незаменимой содержательной частью учебника.</p>
<p>мультимедийные базы данных;</p>	<p>1. Интеграция – возможность избежать дублирования данных для обращения к ним из различных программ;</p> <p>2. Независимость данных – отделение функций СУБД и администрирования от прикладных программ;</p>

	<p>3. Управление одновременным доступом – обеспечение непротиворечивости данных в БД мультимедиа с помощью правил, регулирующих порядок выполнения параллельных транзакций;</p> <p>4. Сохранение текущего состояния между сеансами – способность объектов данных продолжать существовать на протяжении ряда различных транзакций и сеансов работы программы;</p> <p>5. Защищенность – ограничение на неавторизованный доступ к хранимым данным и их модификацию;</p> <p>6. Контроль целостности – обеспечение непротиворечивости состояния БД в процессе обработки транзакций путем наложения на них определенных ограничений;</p> <p>7. Восстановление – методы, служащие гарантией того, что неудачно завершившиеся транзакции не повлияют на постоянно хранимые данные;</p> <p>8. Поддержка обработки запросов – распространение механизмов обработки запросов на мультимедиа-данные;</p> <p>9. Управление версиями – организация хранения различных версий объектов и управление ими.</p> <p>10. Поддержка мультимедийных типов данных;</p>
<p>бизнес-игры;</p>	<p>1. Организация совместной деятельности игроков;</p> <p>2. В основу разработки должна быть положена деятельность, отражающая согласование различных интересов;</p>

	<p>3. Ситуация должна предполагать неоднозначность решений, содержать элемент неопределенности, что обеспечивает проблемный характер игры и личностное проявление игроков;</p> <p>4. Возможность каждому игроку принимать решения и обеспечить осознание этого участниками;</p> <p>5. Наличие стимулов, обеспечивающих высокую вовлеченность участников;</p> <p>6. Хорошо продуманная последовательность действий и взаимосвязи участников.</p>
<p>справочные мультимедиа-системы;</p>	<p>1. Каждый раздел должен представлять собой самостоятельную статью, при ограниченном объеме в целом понятную читателю в отрыве от остального материала;</p> <p>2. Если полное понимание раздела невозможно без ознакомления с другими разделами справки, на них должны быть сделаны ссылки;</p> <p>3. Исключение неявных ссылок из одного раздела в другой.</p>
<p>электронный журнал;</p>	<p>1. Электронный Журнал должен быть общедоступным — бесплатным и возможным для неограниченного числа пользователей;</p> <p>2. В публикуемых материалах не должно быть информации, содержащей сведения, относящиеся к государственной, служебной или коммерческой тайне;</p> <p>3. Предоставляемые статьи должны быть оригинальными – неопубликованными ранее в других печатных или электронных изданиях;</p>

	<p>4. Разделы статьи должны быть пронумерованы;</p> <p>5. При ссылках на литературу в тексте указываются фамилии авторов и год издания (в круглых скобках);</p> <p>6. Выпускные данные должны включать в себя следующие сведения: наименование издателя журнала, его почтовый и электронные адреса, телефон; наименование изготовителя, его адрес и другое.</p>
<p>мультимедиа- каталоги</p>	<p>1. Каталогизация документов в соответствии с нормативными требованиями;</p> <p>2. Предоставление доступа к базе данных через сеть Интернет в режиме on-line;</p> <p>3. Обеспечение сохранности информации через резервное копирование, рабочие и страховые архивы;</p> <p>4. Оказание необходимой помощи пользователю при самостоятельном проведении информационного поиска (навигационные услуги в информационном пространстве, подсказки).</p>

Проанализировав требования, приходим к выводу, что из всего многообразия этих требований базовые, которые можно условно разделить на 2 группы.

К требованиям к контенту относятся:

1. Соответствие содержания поставленным целям и задачам;
2. Системность изложения материала;
3. Научность изложения материала;
4. Полнота информации;

5. Достоверность представленной информации;
6. Единая терминологическая система.

В требованиях к программной реализации выделяем:

1. Интуитивно понятный интерфейс;
2. Единый язык общения пользователей с системой;
3. Многоуровневые разветвления обучающей программы;
4. Возможность использования вспомогательных средств;
5. Интеграция;
6. Независимость данных;
7. Обеспечение единых методов формализации текстов, нормализации и редактирования данных;
8. Управление одновременным доступом;
9. Защищенность.

Следования этим требованиям позволит создать высококлассный образовательный ресурс. [30]

1.2.2. Этапы проектирования мультимедийных систем.

Приступая к работе над проектом, необходимо выбрать модель представления данных, которая должна отвечать следующим требованиям:

- наглядность представления информации;
- простота ввода информации;
- удобство поиска, просмотра и отбора информации;
- возможность использования информации из других программных продуктов;
- возможность перенастройки проекта (добавление новой информации или ее удаление);
- дружественный интерфейс, обеспечивающий интерактивный режим.

При разработке мультимедийного проекта желательно соблюдать определенную последовательность этапов работы:

I этап.

Выбор темы и постановка проблемы. Определившись с темой, вы должны четко написать задание для создания мультимедийного продукта, где должны быть указаны его назначение и цель.

II этап.

Анализ объекта. На этом этапе рассматривается, из каких объектов может состоять проект, а также какими параметрами характеризуются эти объекты.

III этап.

Разработка сценария и синтез модели. При разработке сценария необходимо предусмотреть последовательность работы с продуктом, возможность изменения хода работы и выход из него (завершение работы). Важно просчитать потенциальные аварийные ситуации с целью их предотвращения, а также проверить степень инвариантности работы, то есть возможность достижения одного и того же результата разными путями. В сценарии должно быть заложено звуковое оформление процесса работы.

Используя результаты анализа на втором этапе, необходимо выбрать определенную модель будущего проекта. Это может быть, например, иерархическая модель, обеспечивающая вызов отдельных программных продуктов или элементов проекта. После выбора модели необходимо нарисовать ее схему с указанием связей между приложениями или узлами.

IV этап.

Форма представления информации и выбор программных продуктов. После разработки сценария и создания модели необходимо определить программные продукты для реализации проекта.

На этом этапе необходимо обеспечить себя двумя видами программных продуктов:

- для подготовки и обработки материалов, составляющих проект: графических объектов, аудио- и видеозаписей, текста;
- для создания мультимедийного продукта, то есть непосредственный инструментарий работы.

После выбора программных средств необходимо выбрать форму представления информации и инструменты для ее реализации.

V этап.

Синтез компьютерной модели объекта. После рассмотрения возможностей, которыми располагают выбранные вами программные продукты, можно приступить к реализации проекта на компьютере.

В процессе создания компьютерной модели предстоит пройти две стадии.:

Стадия 1. Подготовка материала для работы. На этой стадии подготавливается графический, текстовый, гипертекстовый (документ, содержащий ссылки на другие документы), аудио- и видеоматериал при помощи выбранных программных продуктов. Работа по подготовке материала требует хороших навыков.

Стадия 2. на этой стадии создается и тестируется компьютерная модель мультимедийного проекта на базе подготовленного материала и выбранных программных средств.

VI этап.

Работа с мультимедийным продуктом. Теперь можно работать с созданным приложением: осуществлять просмотр, поиск, отбор информации и т.д.

Процесс создания мультимедийного продукта.

Процесс создания мультимедиа-информационных систем может рассматриваться как состоящий из двух основных фаз:

- фазы проектирования
- фазы реализации

Фаза проектирования.

1. Проектирование концептуальной модели сценария для мультимедиа-информационной системы.

2. Проектирование медиа-зависимых представлений информации.

3. Проектирование информационных структур.

4. Проектирование медиа-комбинаций и синхронизаций (звук - видео)

5. Проектирование структур узел-связь (ссылки)

6. Проектирование информационных топологий (общая среда)

7. Проектирование интерфейса пользователя

8. Проектирование пользовательского интерфейса

9. Проектирование методов навигации

Фаза реализации.

Реализация должна сопровождаться инструментами и методами создания.

1. Первичная интеграция - создание фрагментов, создание структуры
2. Полная интеграция мультимедиа-продукта монтаж, т.е. соединение всех элементов в единый продукт, в соответствии с определенной структурой и заданными средствами навигации.
3. Производство мультимедиа-продукта (определяется носителем)
4. Распространение мультимедиа-продукта [1]

1.3. Программы разработки мультимедийной системы.

1.3.1. Обзор и анализ существующих программных средств разработки мультимедийных программных продуктов.

Создание мультимедийного приложения начинается вовсе не с выбора необходимого средства разработки. Прежде всего нужно определить, какую информацию и каким образом нужно будет использовать. И только после этого можно переходить к выбору инструмента, который позволит наиболее полно выразить понравившиеся идеи.

Предположим, что вопрос о том, что за приложение необходимо создать, уже решен и наступил момент отбора необходимых средств реализации проекта. Руководствуясь рекомендациями, необходимо найти наиболее подходящий для выполняемой задачи тип авторской системы.

На выбор авторской системы влияют следующие факторы:

- тип платформы разработки;

- подход к программированию;
- наличие инструментов отладки и тестирования приложений;
- возможности форматирования текста и печати;
- интерактивные возможности;
- возможность управления внешними устройствами;
- возможности встроенного редактора компонентов мультимедиа;
- наличие средств организации проекта;
- поддержка баз данных;
- контроль над синхронизацией воспроизведения элементов мультимедиа;
- техническая поддержка;
- наличие обучающей программы;
- качество печатной документации.[26]

После выбора авторской системы и создания отдельных частей мультимедийной системы необходимо соединить эти части воедино. Средства, которые позволяют объединить созданные отдельные части в единое законченное целое можно условно разделить на три группы:

- системные программные средства;
- инструментальные программные средства;
- прикладные программные средства.

1. Системные программные средства включают комплекс программ, входящие в состав операционной системы компьютера и осуществляющие

управление устройствами мультимедиа. Управление осуществляется на двух уровнях:

Первый уровень – физический, на котором происходит управление вводом-выводом информации.

Второй – низкий уровень, управление происходит с помощью машинных команд и пользователем, который управляет характеристиками устройств с помощью графического интерфейса, изображающего пульт управления устройством, например регулировки громкости звука, тембра, стерео баланса и так далее.

2. Инструментальные программные средства позволяют модифицировать файлы мультимедиа, расширять возможности управления мультимедийными устройствами, а так же облегчают процесс создания новых мультимедийных приложений.

Создание мультимедийных приложений осуществляется с помощью следующих пакетов программ [17]:

- редакторов неподвижных графических изображений;
- средств создания анимированных GIF-файлов;
- средств аудио- и видеомонтажа;
- средств создания презентаций;
- средств распознавания отсканированных текстов;
- средств создания обучающих программ;
- систем распознавания голоса и преобразования звуковых файлов в текстовые;
- системы создания приложений виртуальной реальности и другие.

Инструментальные средства являются платными продуктами, некоторые из них имеют высокую стоимость.

3. Прикладные программные средства – это комплекс прикладных программ предназначенных для различных видов деятельности [18].

В России наибольшей популярностью пользуются персональные компьютеры с операционными системами Windows. Далее будут рассмотрены некоторые программные средства для разработки различных мультимедийных систем.

Adobe Flash Professional – это мощный современный инструмент для создания яркой анимации и мультимедийного контента для компьютеров, смартфонов, планшетов, телевизоров и других устройств, доступных современным пользователям. Его обновленная версия позволяет оптимизировать рабочий процесс, создавать наиболее яркие анимационные проекты. Она также имеет поддержку технологии HTML5.

Программа имеет усовершенствованные возможности для работы с текстами, расширены возможности рисования. В программу добавлена глобальная поддержка языков, преобразование объектов в 3D с их трехмерной анимацией. Имеет удобный интерфейс.

Adobe Flash позволяет работать с векторной, растровой и ограниченно с трёхмерной графикой. Также он поддерживает двунаправленную потоковую трансляцию аудио и видео. Формат .swf является стандартным расширением для готовых flash-файлов. Расширение .flv используется для видеороликов в формате Flash. Для рабочих файлов в среде разработки соответствует расширение .fla. Загруженный из Интернета код flash-программы выполняется на виртуальной машине, которая представляет собой Flash Player.

Основой анимации во Flash служит векторный морфинг – плавное «перетекание» одного ключевого кадра в другой, что позволяет создавать сложные мультипликационные сцены. Flash-контент способны воспроизводить многие плееры иных производителей [32].

SunRay BookReader – программа, предназначенная для создания и редактирования различных электронных книг и учебников. Любая книга может состоять из неограниченного количества глав, разделов и подразделов.

Возможности программы:

- текст с визуальными эффектами;
- параграфы могут содержать: нумерованные/ маркированные/ алфавитные списки, бордюры, цвет фона, выравнивание, отступы, межстрочные интервалы и так далее;
- использование изображений; таблиц; аудио- и видео- файлов; GIF-анимации;
- экспорт и импорт разделов в формат HTML и RTF;
- импорт всех документов из одной директории с автоматическим созданием разделов;
- импорт и экспорт различных форматов: DOC, HTML, RTF, XLS, TXT и так далее из Microsoft Office.

Одним из преимуществ является использование в книгах современных мультимедийных форматов: аудио и видео файлов, изображений (PNG, JPEG, GIF, Flash, любые OLE объекты и так далее).

Программа для создания и редактирования оборудована встроенной системой проверки орфографии.

Недостатком программы является то, что книги, созданные с помощью этой программы, сохраняются только во внутреннем формате программы и недоступны для редактирования [37].

REDCLASS Course – это комплекс программ, предназначенный для создания и модификации учебных материалов дистанционных курсов.

Система REDCLASS Course функционирует в автономном режиме, не требующем подключения к сети Интернет, и позволяет выполнять следующие операции:

- создавать курсы обучения, включающие в себя лекционные страницы, тестовые задания, упражнения, мультимедийные объекты;
- автоматически создавать курсы (импортировать) на основе структурированного документа Word;
- экспортировать курс в документ формата Word;
- формировать пакеты курсов в международных стандартах представления контента SCORM 1.2 и SCORM 2004.

Это позволяет использовать учебные материалы, созданные в Системе REDCLASS Course, в сторонних системах обучения, поддерживающих данные стандарты:

- производить полнотекстовый поиск;
- создавать стили оформления и единый шаблон оформления страниц;
- автоматически проверять корректность курса;
- просматривать созданный курс в браузере.

Курс, создаваемый в Системе REDCLASS Course, может состоять из комбинаций следующих учебных элементов [20]:

- лекционных материалов в различных форматах, в том числе и мультимедийных объектов;
- тестовых заданий, состоящих из вопросов;
- практических упражнений.

Приложение **Learning Content Development System (LCDS)** — это бесплатный инструмент, позволяющий создавать интерактивные курсы высокого качества для работы в сети и презентации Microsoft Silverlight Learning Snacks.

С помощью системы LCDS любой участник образовательного сообщества Microsoft может публиковать курсы электронного обучения и презентации Learning Snacks путем заполнения удобных форм LCDS, позволяющих без затруднений формировать материалы с широкими возможностями пользовательской настройки, интерактивные задания, опросники, игры, проверочные работы, анимационные и демонстрационные видеоролики и другие мультимедийные ресурсы.

Особенности LCDS [36]:

- возможность создавать интерактивное приложение с интересным содержанием и различными ссылками;
- возможность предварительного просмотра;
- возможность публикации готового курса в Интернете;
- возможность изменения структуры курса в любое время;
- поддержка форматов: MP3 для аудио, SWF и WMV для видео, JPEG и PNG для изображений;
- возможность использования различных языков написания.

Adobe Premiere – профессиональная программа нелинейного видеомонтажа компании Adobe Systems.

При развитии к приложению Adobe Premiere присоединялись новые модули: фильтры и эффекты для управления видео и звуком, разные аппаратные средства, инструменты для создания и редактирования титров с оригинальными возможностями оформления и прочие. Наряду с этим, расширялся список поддерживаемых форматов, увеличивался перечень предустановленных шаблонов и стилей, улучшался алгоритм предосмотра в реальном времени наложенных слоев и аудио/видео эффектов.

С выходом новой версии пользователь получил возможность подстраивать его под собственные требования, вплоть до создания определенных клавишных сочетаний и яркости внутри конкретных окон.

В последние версии Adobe Premiere был интегрирован инструмент Project Manager, посредством которого происходит управление проектом. Кроме быстрого удаления неприменяемых материалов, он позволяет организовать их хранение и результативное управление файлами во время работы с большим количеством HD-материала.

При создании проекта пользователь имеет возможность сохранять предпочтенные спецэффекты в виде комбинаций на клавиатуре с целью их быстрого вызова, проводить автоматическую корректировку цвета изображения с применением фильтров Adobe Photoshop.

Adobe Premiere тесно взаимодействует с иными продуктами компании (Audition, Photoshop, Encore). Наличие в программе встроенного движка Adobe After Effects, позволяет выполнять копирование клипов в утилиту After Effects простым сочетанием клавиш. После этого, они аналогичным образом возвращаются в приложение уже в обработанном виде [23].

Поддерживаемые форматы файлов:

- видео: RAM, AVI, MPG, RM, MPEG, MPE, WMA, MOV, WMV, MOOV;
- изображения: TIF, AI, PSD, EPS, GIF, FLI, FLC, BMP, RLE, DIB, FLM, JPE, JFIF, PIC, PCT, JPG, TGA, ICB, PCX, VST, VDA;
- аудио: MP3, AIF, WAV;
- прочие: PBL, PSQ, PPJ, PTL, PRTL, AAF, CSV, TXT, TAB.

Microsoft PowerPoint – программа, входящая в пакет Microsoft Office, предназначенная для создания презентаций с использованием упорядоченного набора слайдов, позволяющего графически пояснить выступление на конференции, прокомментировать лекционный материал и тому подобное.

Содержит средства для создания гибкого сценария презентации и записи звукового сопровождения каждого слайда. Наличие русскоязычной версии

позволяет успешно работать с текстами на русском языке. Встроенная поддержка Интернета позволяет сохранять презентации в формате HTML, однако анимированные компоненты требуют установки специального дополнения PowerPoint Animation Player.

Позволяет создавать сложные программные надстройки на языке программирования Visual Basic for Application, что существенно расширяет возможности программы. Специальная надстройка Custom Soundtracks Add-In дополняет презентацию фоновым музыкальным сопровождением с широким выбором мелодий [21].

Недостатками программы является:

- презентации, имеющие пароль, не открываются;
- редактирование и сохранение может привести к потере нескольких образцов. Прозрачность при сплошной заливке отображается менее четко;
- настройки на отображение не влияют;
- сглаживание не поддерживается, текст и графика отображаются менее гладкими. Примечания не отображаются. Диаграммы преобразуются в группы фигур.

Основным недостатком продукта Microsoft PowerPoint является наличие ограниченного, по сравнению с существующим на сегодняшний день рядом программ для разработки ресурсов, набора мультимедийных инструментов, которые не дают возможности создавать полноценные мультимедийные проекты.

Help&Manual - программа для создания файлов справочной системы.

Главным преимуществом программы является ее универсальность. С ее помощью можно получить файл справочной информации в любом из наиболее распространенных на сегодняшний день форматов (CHM, HLP, HXS, HTML, PDF, RTF, EXE, XML). Интуитивно понятный интерфейс делает программу простой в

освоении. Основной блок программы составляет текстовый редактор, мало отличимый от MS Word как по интерфейсу, так и по количеству возможностей.

Интерфейс состоит из двух областей. Первая – это панель Navigation с древовидной структурой содержания файла. Вторая – редактор страниц.

В дереве задается вся структура файла содержания, так как его будет видеть пользователь. Здесь задаются заголовки папок и страниц. Для каждого элемента дерева можно задать собственную иконку и статус. В зависимости от статуса элемент выделяется своим цветом (желтый - редактируется, голубой - требует доработки, белый - готов), тем самым делая работу по наполнению страниц более наглядной.

Редактор страниц состоит из трех закладок: Topic Options (опции), Page Editor (редактор страницы), XML Source Code (исходник в формате XML).

На первой закладке определяются основные параметры текущей страницы: идентификатор страницы, идентификатор окна, в котором она будет открываться, ключевые слова, якорь по умолчанию, компиляторы, включающие данную страницу в конечный файл.

Вторая закладка – это непосредственно сам редактор, на котором пользователь пишет текст, форматирует его, добавляет таблицы, рисунки, медиафайлы, ссылки, якоря и прочее.

Третья закладка – это исходный текст страницы в формате XML. При желании пользователь имеет возможность редактировать страницу прямо в исходнике или добавлять сюда код, который невозможно ввести с помощью редактора (хотя такое трудно себе представить).[25]

Выводы по первой главе.

Проанализированы теоретические основы мультимедиа и мультимедийных систем, их использование в образовательной деятельности, а так же требования к разработке электронных ресурсов.

Глава 2. Практические аспекты создания мультимедийной системы.

2.1. Нормативная документация по дисциплине «Информатика и Языки программирования».

2.1.1. Пояснительная записка.

Цель дисциплины - формирование четкого представления понятия информатика, ее места и роли в современном обществе; выработка и закрепление устойчивых навыков работы на персональном компьютере с использованием современных программных средств; изучение основные понятий языков программирования, принципов анализа синтаксиса и семантики, формальных способов описания языков программирования; типов данных, способов и механизмов управления данными, методов и основных этапов трансляции; разработка и представление алгоритма с использованием существующих стандартов, реализацию алгоритма на языке программирования высокого уровня, отладку и тестирование программы.

Задачи дисциплины:

- изучение основных понятий информатики; методов сбора, преобразования, передачи, хранения и обработки информации; принципов функционирования компьютера и управления им; структуры программного обеспечения, основных видов программ и методов работы с ними; алгоритмизацию и управляющие конструкции алгоритмических языков; переменные и типы данных алгоритмических языков; принципы компилирования и трансляции программ в исполняемый код; различные структуры данных;
- формирование умения работать в различных операционных системах, пользоваться распространенными офисными приложениями; составлять алгоритмы решения задач; правильно использовать типы данных и управляющие конструкции алгоритмических языков при решении задач; рационально использовать структуры данных при решении задач; реализовать программу на алгоритмическом языке по заданному алгоритму, отладить программу в изучаемой

среде программирования, составить план и провести тестирование, написать программную документацию;

- формирование навыков работы с компьютерами в современных средах и оболочках; алгоритмического мышления; работы в интегрированных средах программирования; практические навыки решения задач от построения алгоритма ее решения, до выполнения ее на компьютере. [32]

Предмет освоения дисциплины - информатика; информация; данные; способы обработки, передачи, хранения данных; компьютер; персональный компьютер (ПК); архитектура и структура ПК; характеристики основных устройств ПК; алгоритм; способы представления алгоритма; графическая схема алгоритма; программа; язык программирования; алфавит; лексемы; типы данных; константы; переменные; операции; выражения; операторы; подпрограммы; модули; процессы: создания и корректировки программы, ее трансляции, отладки, сборки, тестирования, запуска, эксплуатации.[31]

2.1.2 Содержание дисциплины, структурирование по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий.

Таблица 2 - Разделы дисциплины, виды, объем занятий и формы контроля.

[30]

Номер раздела	Наименование разделов дисциплины	Семестр	Объем в часах по видам учебной работы		
			Лекции	Самостоятельные работы	Всего
1	Общие сведения об информатике	I	8	10	18
2	Основы алгоритмизации	I	24	10	34

3	Формальные языки и грамматики	I,II	6	9	15
4	Рекурсивные данные и алгоритмы	II	8	8	16
5	Сортировка и поиск	II	26	8	34
6	Основы объектно-ориентированного проектирования и анализа	III	26	45	71
Всего					188

Таблица 3 - Темы лекций, их содержание, трудоемкость. [30]

Тема лекции	Содержание	Кол-во часов
Предмет и методы информатики	Информатика как наука и как вид практической деятельности. Основные сведения из истории информатики. Поколения ЭВМ. Современные персональные компьютеры.	4
Математические основы информатики	Методы и модели оценки количества информации; системы счисления. Энтропия. Представление чисел в различных системах счисления. Перевод чисел из одной системы в другую. Общая характеристика процессов сбора, передачи, обработки и хранения информации.	4

Введение в теорию алгоритмов	Интуитивное понятие алгоритма. Свойства алгоритмов. Понятие об исполнителе алгоритма. Уточнение понятия алгоритма. Основные алгоритмические конструкции. Способы записи алгоритмов.	6
Машины Тьюринга	Алгоритм как преобразование слов из заданного алфавита. Машина Тьюринга. Формат команды и программа машины Тьюринга. Способы записи программы: таблицы, диаграммы. Примеры. Композиция машин Тьюринга. Примеры. Тезис Тьюринга и его обоснование.	4
Нормальные алгорифмы Маркова	Нормальные алгорифмы Маркова. Формулы подстановки и схемы. Выполнение алгоритма. Примеры. Принцип нормализации и его обоснование.	2
Вычислимые функции	Понятие вычислимой функции. Суперпозиция, примитивная рекурсия, минимизация. Примеры.	2
Алгоритмическая неразрешимость	Понятие об алгоритмической неразрешимости. Доказательство существования алгоритмически неразрешимых задач. Примеры.	2
Методы разработки алгоритмов	Основные методы разработки алгоритмов. Рекурсия и математическая индукция. Реализация механизма	2

	рекурсии. Рекурсия и итерация. Реализация. Сравнение.	
Развитие понятия алгоритма	Развитие понятия алгоритма: параллельное программирование и распределенные алгоритмы, объектно - ориентированный подход к разработке программ, методы искусственного интеллекта. Конструкции языков высокого уровня для организации ветвлений и циклов, конструкции распределенного и параллельного программирования.	2
Понятие сложности алгоритма и классы сложности задач	Понятие вычислительной сложности (по времени и памяти) алгоритма и его применение для анализа алгоритмов. Асимптотические верхние и средние оценки для итеративных и рекурсивных алгоритмов; сравнение алгоритмов по времени и памяти. Основные методы и приемы анализа сложности. Сложность алгоритмов с ветвлениями, циклами. Сложность рекурсивных алгоритмов. Оптимизация алгоритмов. Основы доказательства правильности. Разрешимые и неразрешимые задачи. Сложность задачи. Задачи полиномиальной и экспоненциальной сложности (трудно решаемые задачи). Сводимость и другие классы сложности.	4

	Класс задач NP, NP-сложные и NP - полные задачи. Примеры.	
Формальные языки и понятие грамматики	Понятие о формальных языках. Основные понятия: алфавит, лексика, синтаксис и семантика, прагматика языка. Понятие грамматики. Классификация формальных языков.	4
Способы описания алгоритмических языков	Способы строгого описания формальных языков, понятие о метаязыках. Алфавит, синтаксис и семантика алгоритмического языка. Формальные способы описания языков программирования: описание синтаксиса языка с помощью металингвистических формул и синтаксических диаграмм. Примеры.	2
Рекурсивные данные	Конструирование типов. Понятие рекурсивно определенного типа данных и динамическое распределение памяти. Линейные списки, деревья, графы: определение и способы представления.	2
Операции над линейными списками	Создание списков, включение элементов в голову и конец списка, на указанное место. Просмотр списков. Поиск элемента в списке. Удаление элемента списка. Сравнение списков.	2
Операции над бинарными деревьями	Создание деревьев, включение элементов в бинарное древо. Просмотр деревьев и поиск элементов. Удаление элемента	2

	списка. Сравнение деревьев. Применение бинарных деревьев в программировании.	
Представление графов и операции над графами	Способы представления графов. Сравнение. Создание графа (добавление вершин и дуг). Поиск вершины и дуги. Удаление вершин и дуг. Алгоритмы на графах.	2
Основные понятия, задачи сортировки и поиска	Формулировка задач сортировки и поиска. Основные понятия. Связь между задачами.	2
Сортировка массивов	Основные подходы к разработке алгоритмов сортировки массивов, классификация алгоритмов сортировки. $O(n)$ алгоритмы сортировки (например, выбором и вставкой); оценки сложности, лучшие и худшие случаи. $O(n \log n)$ алгоритмы сортировки (например, быстрая сортировка, метод слияния); оценка сложности; другие методы сортировки (метод Шелла и т.д.); сравнение алгоритмов сортировки.	10
Внешние сортировки	Понятие файла. Представление деревьями, В-деревья. Особенности сортировки файлов. Общие подходы и основные методы сортировки файлов (двухпутевое слияние и пр.).	4
Поиск	Подходы к решению задач поиска. Последовательный и бинарный поиск, оценки сложности, лучшие и худшие	6

	случаи. Поиск в массивах. Использование деревьев в решении задач поиска. Исчерпывающий поиск: перебор с возвратом, метод ветвей и границ, динамическое программирование.	
Хеширование	Понятие хеш-функции и возможность эффективной реализации, проблема коллизий. Основные методы разрешения коллизий: устранение коллизий с помощью рехеширования (линейное и случайное рехеширование), метод цепочек. Сравнение.	4
Основы объектно-ориентированного анализа	Итеративная технология разработки программного обеспечения. Модель прецедентов - модель способов взаимодействия пользователей с системой. Концептуальная модель (модель предметной области) – скелет создаваемой системы. Паралич анализа. Демонстрация реализации этапа объектно-ориентированного анализа на примере разработки проектов рассмотренных на предыдущих лекциях.	8
Основы объектно-ориентированного проектирования	создание исходного списка объектов; определение и уточнение назначений объектов при помощи карточек CRC; разработка точек взаимодействия; детализация отношений между	6

	объектами; построение объектной модели. Паралич проектирования.	
Тестирование объектно-ориентированного программного обеспечения	Два метода испытания программного кода: тестирование методом «прозрачного ящика» и испытание методом «черного ящика». Четыре формы тестирования: тестирование элементов программы (блочное тестирование); проверка взаимодействия и функционирования компонентов системы (комплексные испытания, компоновочные испытания, совместные испытания); испытание системы (системное тестирование); регрессивное тестирование. Обработка исключений. Создание эффективной документации.	10
Итого		96

2.1.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине.

Для полноценного освоения дисциплины необходимо электронное учебно-методическое обеспечение для самостоятельной работы обучающихся, в том числе обучающиеся из числа лиц с ограниченными возможностями здоровья.

1. Программа дисциплины «Информатика и программирование».
2. Слайдовые презентации лекций по темам дисциплины
3. Карточки с заданиями разного уровня сложности для СРС на практических занятиях.
4. Фонд оценочных средств.

5. Основная и дополнительная литература.[32]

2.1.4. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.

Таблица 4 – Описание показателей оценивания обучающихся. [30]

№ п/п	Контролируемые разделы	Наименование оценочного средства
1	Общие сведения об информатике	Домашняя работа по систематизации Информации. Компьютерное тестирование.
2	Основы алгоритмизации	Самостоятельная работа по решению задач.Тест. Дискуссия. Решение задач; домашняя работа; самостоятельная работа.
3	Формальные языки и грамматики	Решение задач. Компьютерное тестирование Домашняя работа; самостоятельная работа.
4	Рекурсивные данные и алгоритмы	Решение задач. Компьютерное тестирование Решение задач.Компьютерное тестирование. Самостоятельная работа.
5	Сортировка и поиск	Опрос; реферат по методам сортировки. Решение задач; домашняя работа; самостоятельная работа;

		разработка программ сортировки и поиска
--	--	---

Критерии оценки знаний студентов на экзамене:

- «Отлично» выставляется студенту в том случае, если он:
глубоко и правильно усвоил программный материал, последовательно, грамотно и логически стройно его излагает; владеет основными алгоритмами решения задач; умеет строить алгоритмы, связывать теорию с практикой, показывает умение применять знания.
- «Хорошо» выставляется студенту, если:
он твердо знает программный материал, грамотно и по существу его излагает; владеет основными математическими методами, методами алгоритмизации и программирования; не допускает существенных ошибок, но и испытывает затруднения в выводах и доказательствах; умеет применять основные положения и формулы для решения задач.
- «Удовлетворительно» выставляется студенту в том случае, если он:
имеет знания только основного материала, но не умеет делать выводов и доказательств; допускает ошибки, недостаточно правильные формулировки; с трудом увязывает основные положения с практикой.
- «Неудовлетворительно» выставляется студенту в том случае, если он: не знает основополагающих вопросов изучаемого курса или значительной части программного материала; допускает ошибки, обнаруживает неумение их исправлять; не может увязать теорию с практикой. [31]

Примерные темы рефератов:

1. Поколение ЭВМ.
2. Перевод из одной системы в другую.
3. Способы записи алгоритмов.
4. Методы разработки алгоритмов
5. Машины Тьюринга.

6. Разработка алгоритмов.
7. Методы оптимизации алгоритмов.
8. Методы генерации кодов.
9. Формальные языки.
10. Алгоритмы сортировки.
11. Алгоритмы поиска.

Вопросы к экзамену.

1. Информатика как наука и как вид практической деятельности
2. Основные сведения из истории информатики.
3. Поколения ЭВМ. Современные персональные компьютеры.
4. Методы и модели оценки количества информации; системы счисления.

Энтропия.

5. Представление чисел в различных системах счисления. Перевод чисел из одной системы в другую.

6. Общая характеристика процессов сбора, передачи, обработки и хранения информации.

7. Интуитивное понятие алгоритма. Свойства алгоритмов.

8. Понятие об исполнителе алгоритма. Уточнение понятия алгоритма.

9. Основные алгоритмические конструкции. Способы записи алгоритмов.

10. Алгоритм как преобразование слов из заданного алфавита. Машина Тьюринга.

11. Формат команды и программа машины Тьюринга. Способы записи программы: таблицы, диаграммы. Примеры.

12. Композиция машин Тьюринга. Примеры. Тезис Тьюринга и его обоснование.

13. Нормальные алгорифмы Маркова. Формулы подстановки и схемы.

14. Выполнение алгорифма Маркова. Примеры. Принцип нормализации и его обоснование.

15. Понятие вычислимой функции.
16. Суперпозиция, примитивная рекурсия, минимизация. Примеры.
17. Понятие об алгоритмической неразрешимости.
18. Доказательство существования алгоритмически неразрешимых задач.

Примеры.

19. Основные методы разработки алгоритмов.
20. Рекурсия и математическая индукция.
21. Реализация механизма рекурсии.
22. Рекурсия и итерация. Реализация. Сравнение.
23. Развитие понятия алгоритма: параллельное программирование и распределенные алгоритмы, объектно-ориентированный подход к разработке программ, методы искусственного интеллекта.
24. Конструкции языков высокого уровня для организации ветвлений и циклов, конструкции распределенного и параллельного программирования.
25. Понятие вычислительной сложности (по времени и памяти) алгоритма и его применение для анализа алгоритмов.
26. Асимптотические верхние и средние оценки для итеративных и рекурсивных алгоритмов; сравнение алгоритмов по времени и памяти.
27. Основные методы и приемы анализа сложности. Сложность алгоритмов с ветвлениями, циклами.
28. Сложность рекурсивных алгоритмов. Оптимизация алгоритмов. Основы доказательства правильности.
29. Разрешимые и неразрешимые задачи. Сложность задачи.
30. Задачи полиномиальной и экспоненциальной сложности (трудно решаемые задачи). Сводимость и другие классы сложности.
31. Класс задач, сложные и полные задачи. Примеры.
32. Понятие о формальных языках. Основные понятия: алфавит, лексика, синтаксис и семантика, прагматика языка.
33. Понятие грамматики. Классификация формальных языков.

34. Способы строгого описания формальных языков, понятие о метаязыках.
35. Алфавит, синтаксис и семантика алгоритмического языка.
36. Формальные способы описания языков программирования: описание синтаксиса языка с помощью металингвистических формул и синтаксических диаграмм. Примеры.
37. Конструирование типов. Понятие рекурсивно определенного типа данных и динамическое распределение памяти.
38. Линейные списки, деревья, графы: определение и способы представления.
39. Создание списков, включение элементов в голову и конец списка, на указанное место. Просмотр списков.
40. Поиск элемента в списке. Удаление элемента списка. Сравнение списков.
41. Создание деревьев, включение элементов в бинарное дерево.
42. Просмотр деревьев и поиск элементов. Удаление элемента списка. Сравнение деревьев. Применение бинарных деревьев в программировании.
43. Способы представления графов. Сравнение. Создание графа (добавление вершин и дуг).
44. Поиск вершины и дуги. Удаление вершин и дуг. Алгоритмы на графах.
45. Формулировка задач сортировки и поиска. Основные понятия. Связь между задачами.
46. Основные подходы к разработке алгоритмов сортировки массивов, классификация алгоритмов сортировки.
47. Алгоритмы сортировки (например, выбором и вставкой); оценки сложности, лучшие и худшие случаи.
48. Алгоритмы сортировки (например, быстрая сортировка, метод слияния); оценка сложности;
49. Другие методы сортировки (метод Шелла и т.д.); сравнение алгоритмов сортировки.

50. Особенности сортировки файлов. Общие подходы и основные методы сортировки файлов (двухпутевое слияние и пр.).

51. Подходы к решению задач поиска. Последовательный и бинарный поиск, оценки ложности, лучшие и худшие случаи.

52. Поиск в массивах. Использование деревьев в решении задач поиска.

53. Понятие хеш-функции и возможность эффективной реализации.

54. Проблема коллизий. Основные методы разрешения коллизий: устранение коллизий с помощью рехеширования (линейное и случайное рехеширование), метод цепочек. Сравнение. [30]

2.2. Разработка и структура мультимедийной системы.

При разработке мультимедийной системы использовалась программа Help&Manual - программы для создания файлов справочной системы. Данная мультимедийная система создана в виде Web - справочника для самостоятельного изучения дисциплины «Информатика и программирование».

Справочник состоит из 3 разделов:

Раздел 1 – Лекции. В данном разделе описываются темы, которые используются для изучения материала.

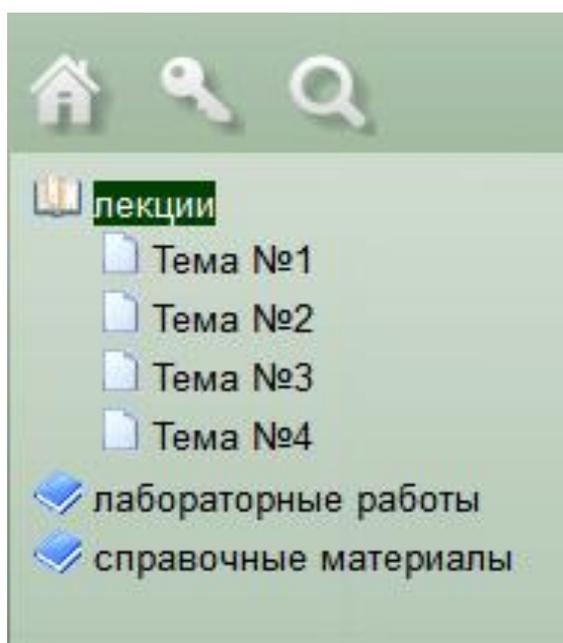


Рисунок 1 – Раздел «Лекции»

Раздел 2 – Лабораторные работы. В данном разделе собраны практические задания, которые используются для закрепления пройденного материала.

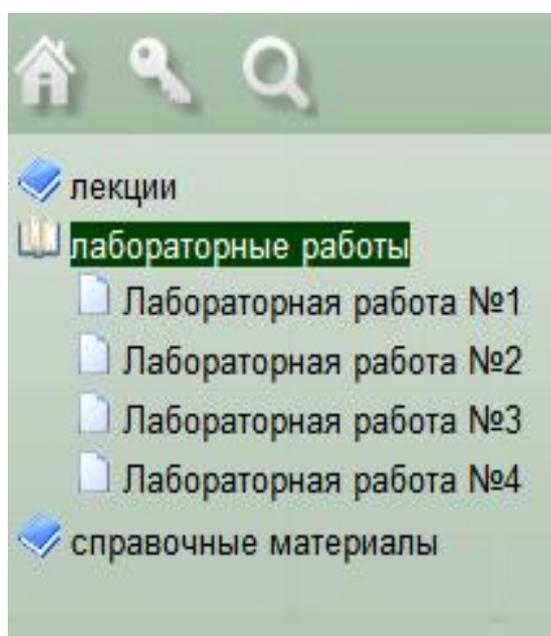


Рисунок 2 - Раздел «Лабораторные работы»

Раздел 3 – Справочные материалы. В данном разделе описаны основные элементы Pascal для лучшего усвоения программы и правильного выполнения лабораторных работ, а так же виды языков программирования.

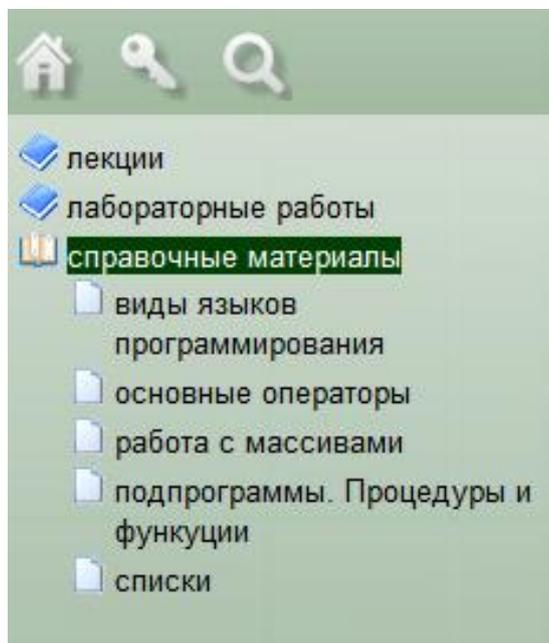


Рисунок 3 – Раздел «Справочные материалы»

Рассмотрим подробнее каждый из разделов.

В разделе Лекции каждая тема представлена в виде текстового файла в котором кратко объясняются основные понятия изучаемого материала.

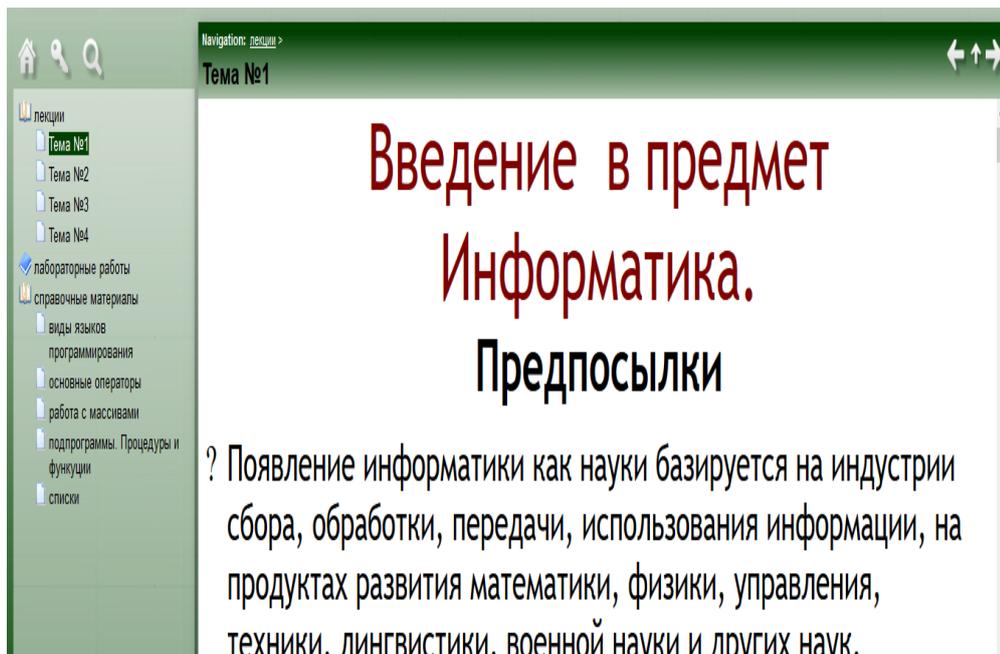


Рисунок 4 – Тема №1 «Введение в предмет»

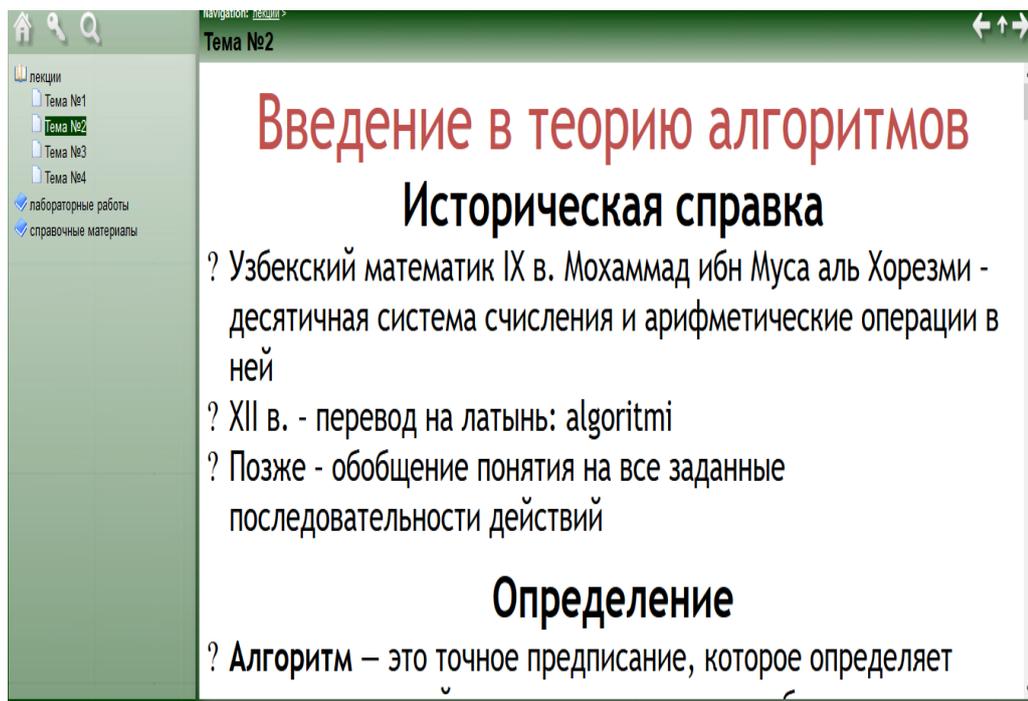


Рисунок 5 – Тема №2 «Введение в теорию алгоритмов»

Navigation: лекции >
Тема №3

Машина Тьюринга

? **Машина Тьюринга** - абстрактная вычислительная машина (абстрактный исполнитель), предложенная для формализации понятия алгоритма.

? **Автор** - английский математик Алан Тьюринг (1912-1954).

Назначение:

- ? не стала реально действующим устройством;
- ? постоянно используется в качестве основной модели для выяснения сущности таких понятий, как "вычислительный процесс", "алгоритм";

Рисунок 6 – Тема № 3 «Машина Тьюринга»

Navigation: лекции >
Тема №4

Нормальные алгорифмы Маркова

Историческая справка

? **Дата создания** - 1951 г.

? **Автор** - советский математик А.А. Марков

Определение

Нормальный алгорифм Маркова (НАМ) - вербальный (предназначенный для применения к словам в различных алфавитах) алгоритм, который задается с помощью пары **Алфавит алгорифма** (к словам которого алгорифм будет применяться) **Схема алгорифма** - конечный упорядоченный набор формул

Рисунок 7 – Тема №4 «Нормальные алорифмы Маркова»

В разделе Лабораторные работы каждое практическое задание так же представлено в виде текстового документа, в котором расписано каким образом необходимо выполнить те или иные задачи.

Navigation: лабораторные работы >

Лабораторная работа №1

Тема: системы счисления.

Задание: выполнить перевод указанных значений из исходной системы счисления в целевую.

Основание исходной системы	Основание целевой системы	Значение 1	Значение 2	Значение 3
10	2	12	123	12345
2	10	101b	1111011b	1010101010101b
10	8	12	123	12345
8	10	7o	12o	123o
10	16	12	123	12345

Рисунок 8 – Лабораторная работа №1 «Системы счисления»

Navigation: лабораторные работы >

Лабораторная работа №2

Лабораторная работа №2

Тема: простые программы для машины Тьюринга.

Задание 1: На ленте записано целое десятичное число. В начальном состоянии МТ обозревает правую цифру числа. Построить МТ, которая умножает заданное число на 10.

Задание 2: На ленте записано целое десятичное число. В начальном состоянии МТ обозревает левую цифру числа. Построить МТ, которая умножает заданное число на 10 и заканчивает работу в исходной позиции считывающей головки.

Задание 3: На ленте записано целое десятичное число. В начальном состоянии МТ обозревает левую цифру числа. Построить МТ, которая вычитает единицу из заданного числа, при этом в выходном слове старшая цифра не должна быть 0. Например, если входным словом было "100", то выходным должно быть "99", а не "099".

Рисунок 9 – Лабораторная работа №2 «Простые программы для машины Тьюринга»

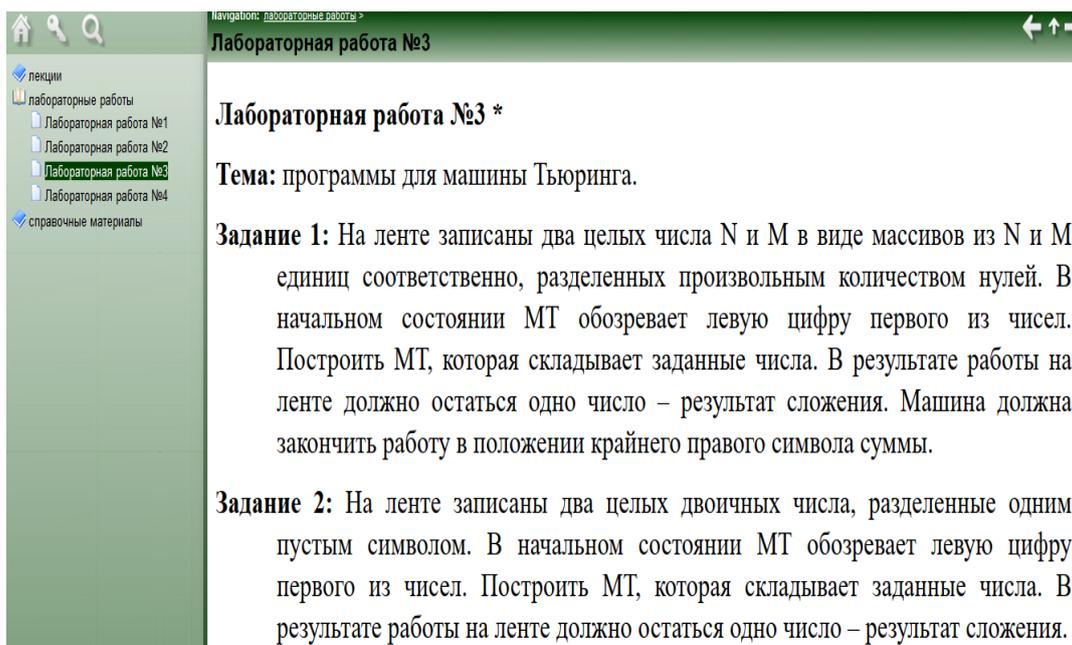


Рисунок 10 – Лабораторная работа №3 «Программы для машины Тьюринга»

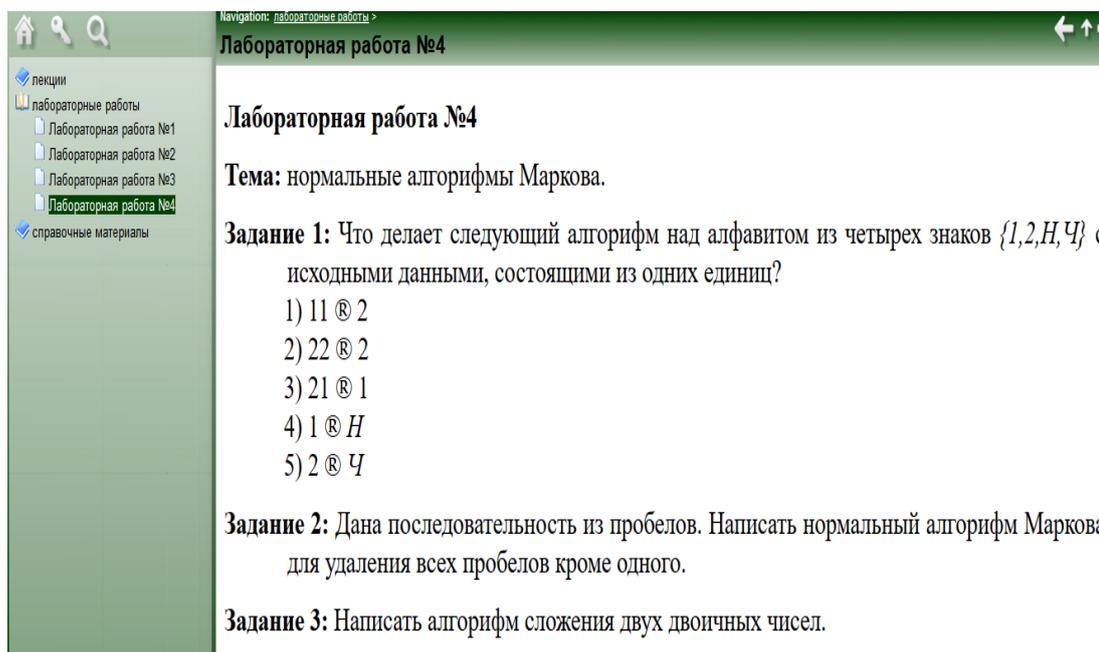


Рисунок 11 – Лабораторная работа №4 «Нормальные алгоритмы Маркова»

В разделе Справочные материалы представлены основные элементы, необходимые для написания элементарных программных продуктов на основе лабораторных работ, а так же виды языков программирования. Для более лучшего понимания дисциплины описание каждого элемента сопровождается видео с наглядным примером.

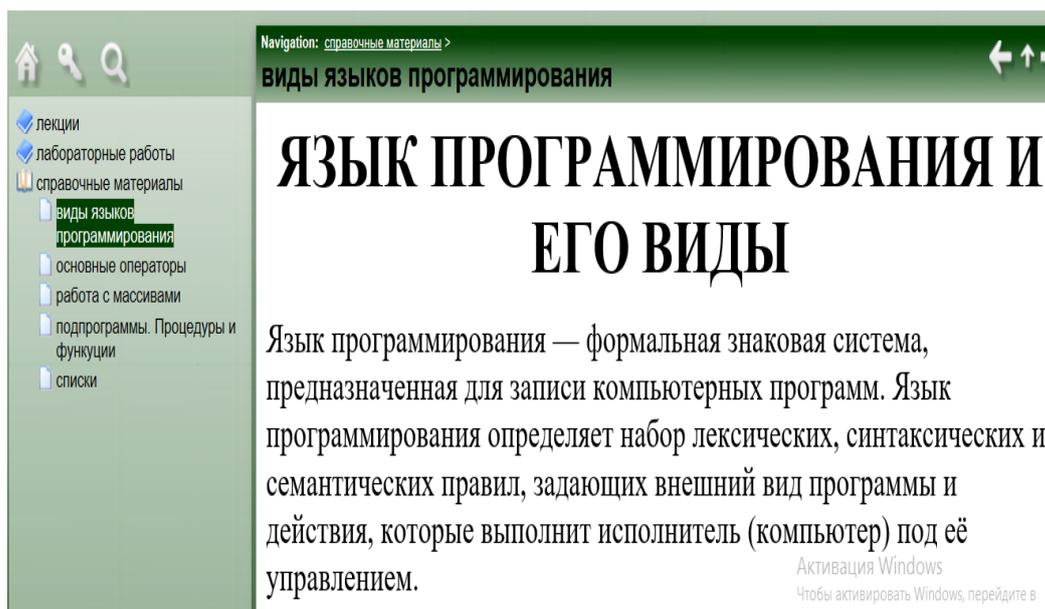


Рисунок 12 – Виды языков программирования

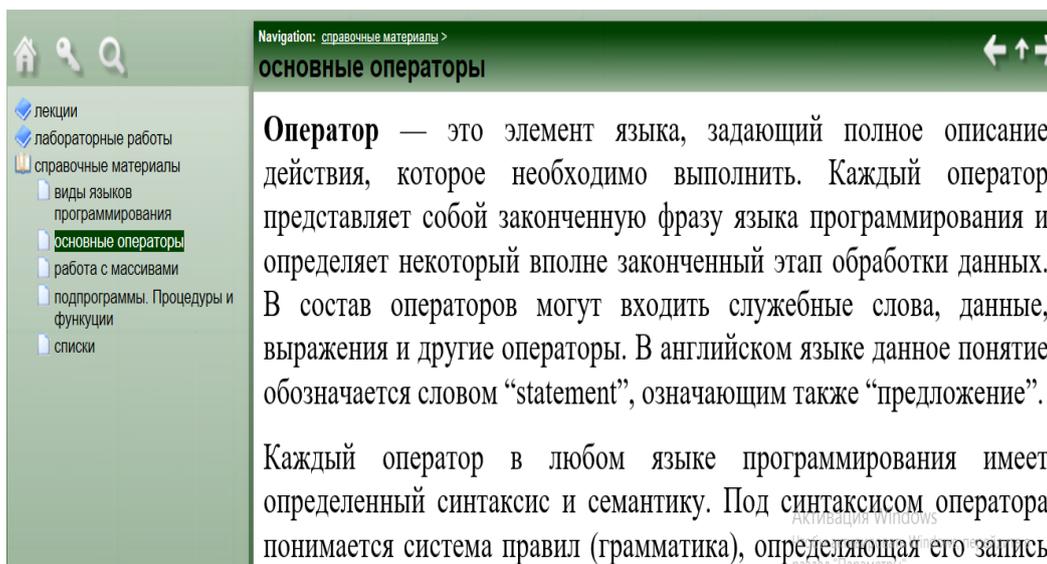


Рисунок 13 – Основные операторы

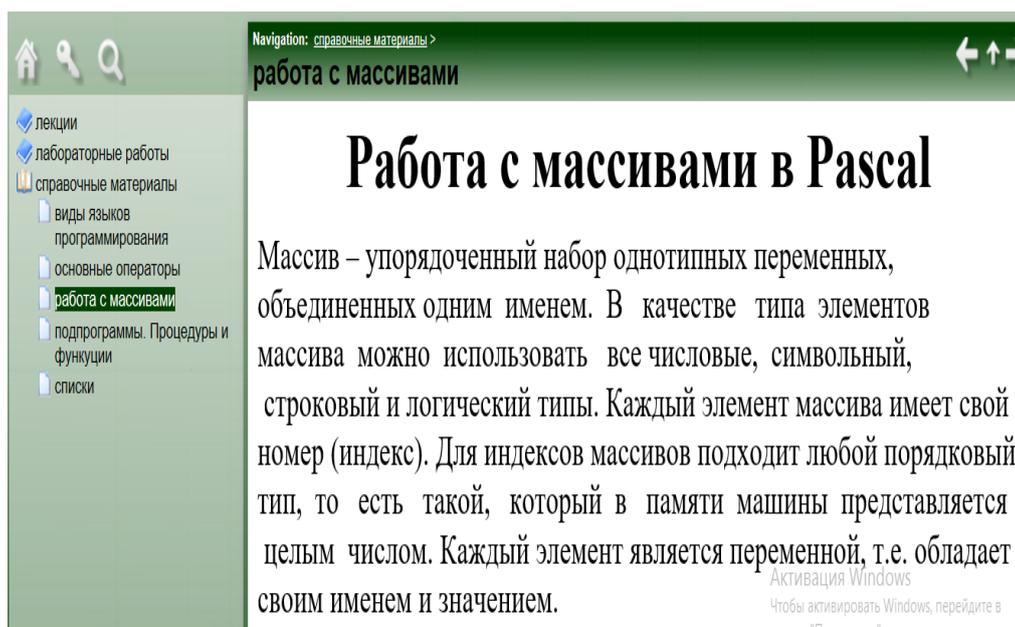


Рисунок 14 – Работа с массивами

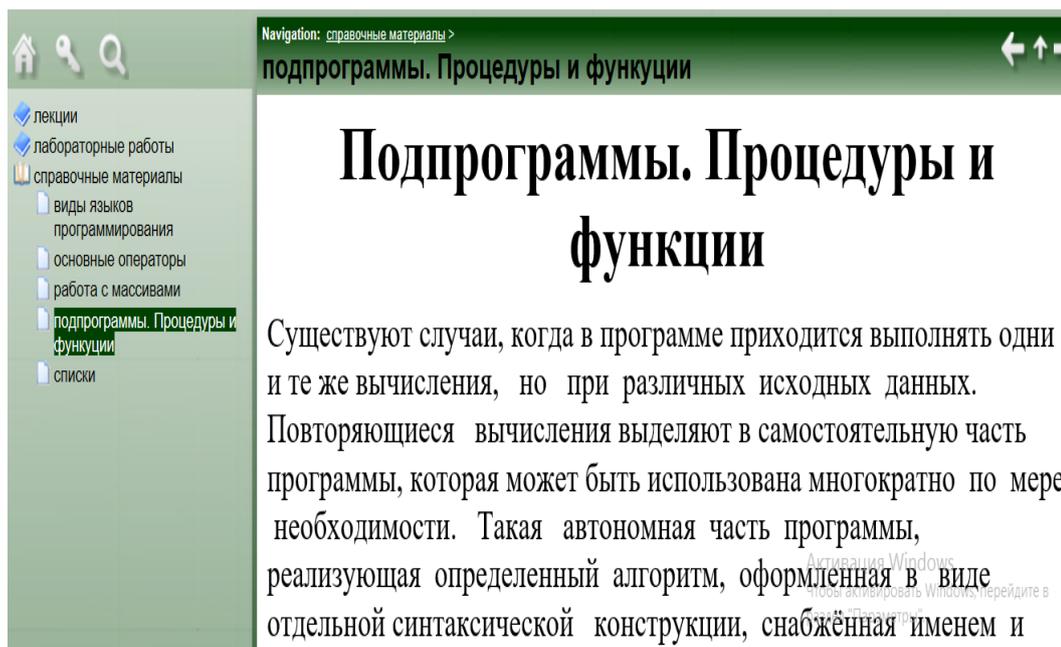


Рисунок 15 – Процедуры и функции

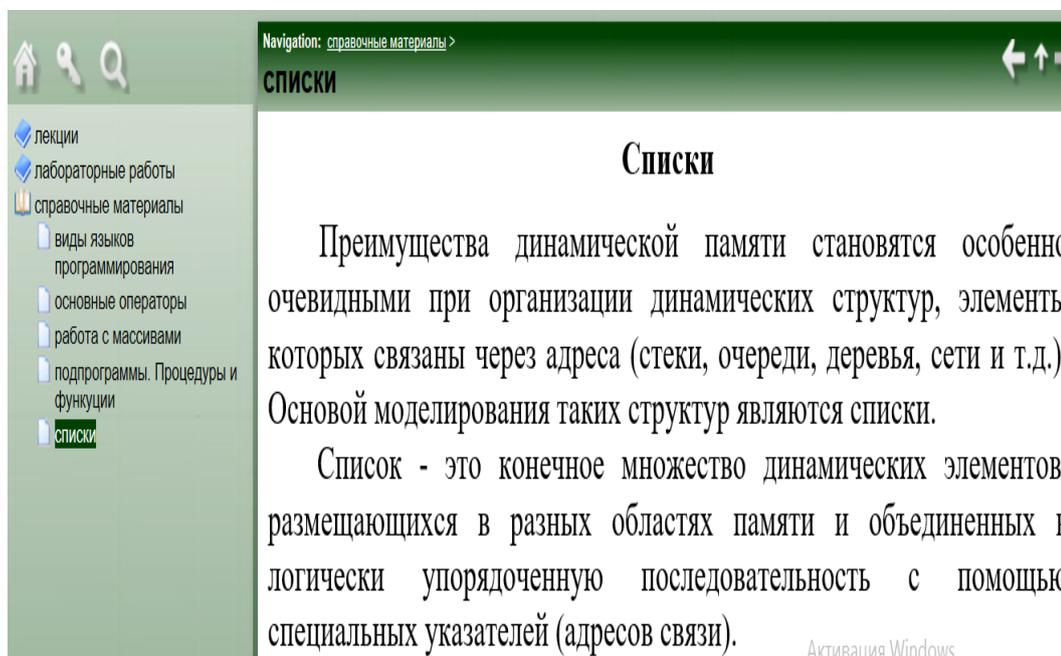


Рисунок 16 – Работа со списками

The screenshot shows a web application interface with a green header and a light green sidebar. The header contains navigation icons (home, search, magnifying glass) and the text "Navigation: справочные материалы >" and "работа с массивами". The sidebar lists various categories, with "работа с массивами" highlighted. The main content area features a large black video player with a white play button icon. Below the video player, the title "Сортировка массивов" is displayed in a bold serif font, followed by the subtitle "Сортировка массивов – это упорядочение их элементов" in a regular serif font.

Рисунок 17 – предоставление видео материала.

Выводы по второй главе.

Приведена разработка мультимедийной системы и подробно изложено ее содержание с выносками и иллюстрациями для лучшего понимания структуры электронного ресурса, а так же описаны основные нормативные документы по дисциплине «Информатика и программирование».

Глава 3. Теоретические и практические методы информационной безопасности и защиты информатики.

3.1. Информационная безопасность в образовательной организации.

3.1.1. Сущность понятия информационная безопасность.

Проблема защиты информации в последнее время превращается из гипотетической в полнее реальную. Количество угроз возрастает с каждым днем, изменяется нормативно правовая база, в соответствии с этим должны изменяться и методы обеспечения защиты информации.

Информация — результат и отражение в человеческом сознании, многообразии внутреннего и окружающего миров (сведения об окружающих человека предметах, явлениях, действия других людей).

Информационная безопасность может рассматриваться в следующих значениях:

1. Состояние (качество) определённого объекта (в качестве объекта может выступать информация, данные, ресурсы автоматизированной системы, автоматизированная система, информационная система предприятия, общества, государства, организации и т. п.);

2. Деятельность, направленная на обеспечение защищённого состояния объекта (в этом значении чаще используется термин «защита информации»).

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

1. Конфиденциальность – свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц.

2. Целостность – неизменность информации в процессе ее хранения и передачи.

3. Доступность – свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц.

Выделяют и другие не всегда обязательные категории модели безопасности:

- неотказуемость или апеллируемость — способность удостоверить имевшее место действие или событие так, что эти события или действия не могли быть позже отвергнуты;
- подотчётность — обеспечение идентификации субъекта доступа и регистрации его действий;
- достоверность — свойство соответствия предусмотренному поведению или результат;
- аутентичность или подленность — свойство, гарантирующее, что субъект или ресурс идентичны заявленным.[8]

Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе.

Безопасность информации (при применении информационных технологий) — состояние защищённости информации (данных), обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована.

В то время как информационная безопасность — это состояние защищённости информационной среды, защита информации представляет собой

деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Ценность информации — является важнейшим критерием при принятии решений о защите информации.

Уровень секретности — административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю секретной конкурентной информации, регламентируемой специальным документом с учетом государственно-военно стратегических, коммерческих, служебных или частных интересов.

Статистика защиты информации показывает, что защищать нужно не только секретную информацию, но и связанную с ней не секретную.[29]

3.1.2. Основные угрозы информационной безопасности.

Современная информационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя.

Компоненты автоматизированной информационной системы можно разбить на следующие группы:

Аппаратные средства. Это компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства - принтеры, контроллеры, кабели, линии связи и т.д.);

Программное обеспечение. Это приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.;

Данные, хранимые временно и постоянно, на дисках, флэшках, печатные, архивы, системные журналы и т.д.;

Персонал. Пользователи, системные администраторы, программисты и др.

Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы. Причинами случайных воздействий при эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия - это целенаправленные действия нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами:

- недовольством служащего своей карьерой;
- взяткой;

- любопытством;
- конкурентной борьбой;
- стремлением самоутвердиться любой ценой.

Можно составить гипотетическую модель потенциального нарушителя:

- квалификация нарушителя на уровне разработчика данной системы;
 - нарушителем может быть как постороннее лицо, так и законный пользователь системы;
 - нарушителю известна информация о принципах работы системы;
- нарушитель выбирает наиболее слабое звено в защите.

Наиболее распространенным и многообразным видом компьютерных нарушений является несанкционированный доступ. Несанкционированный доступ использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке.

Проведем классификацию каналов несанкционированного доступа, по которым можно осуществить хищение, изменение или уничтожение информации:

Через человека:

- хищение носителей информации;
- чтение информации с экрана или клавиатуры;
- чтение информации из распечатки.

Через программу:

- перехват паролей;

- дешифровка зашифрованной информации;
- копирование информации с носителя.

Через аппаратуру:

- подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т.д.

Особо следует остановиться на угрозах, которым могут подвергаться компьютерные сети. Основная особенность любой компьютерной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Компьютерные сети характерны тем, что против них предпринимают так называемые удаленные атаки. Нарушитель может находиться за тысячи километров от атакуемого объекта, при этом нападению может подвергаться не только конкретный компьютер, но и информация, передающаяся по сетевым каналам связи.[25]

Анализируя возможные угрозы с точки зрения наибольшей опасности, изощренности и разрушительности, следует выделить вредоносное программное обеспечение. Вредоносное программное обеспечение – это любая программа, написанная с целью нанесения ущерба или для использования ресурсов атакуемого компьютера. О вредоносном программном обеспечении известно больше, чем о каких-либо других опасностях и повреждениях компьютерной техники.

Вредоносное программное обеспечение можно разделить на три группы:

- компьютерные вирусы;
- хакерское ПО;
- спам.

Вирус – программа, которая может заражать другие программы, включая в них модифицированные копии, обладающие способностью дальнейшего распространения.

Программный вирус – исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение или данные, хранящиеся в автоматизированных системах. [18]

Вредоносное действие вируса может проявиться в следующем:

- появление в процессе работы компьютера неожиданных эффектов (падение символов на экране, неожиданные звуковые эффекты, появление неожиданных картинок и т.п.);
 - замедление работы компьютера;
 - сбои и отказы в работе прикладных программ;
 - порча или исчезновение файлов с магнитного диска;
 - вывод из строя операционной системы;
 - разрушение файловой системы компьютера;
 - вывод из строя аппаратуры компьютера.

Хакерское ПО — это инструмент для взлома и хищения конфиденциальных данных. Существуют инструменты для сбора данных о потенциальных жертвах и поиска уязвимостей в компьютерных сетях. К ним относятся программы для сканирования сети с целью определения IP-адресов компьютеров и «открытых» портов. Программы «прослушивания» сетевого трафика незаметно перехватывают IP-пакеты в сети и анализируют их в целях определения адресов отправителей и

получателей и, может быть, выявления секретных данных типа имен и паролей, передаваемых в открытом виде. Формат почтовых сообщений является открытым, следовательно, электронное письмо может быть легко прочитано.

Есть инструменты хакеров, предназначенные для взлома компьютеров и сетей. К ним относятся программы подбора паролей, фальсификации IP-пакетов путем подмены адреса отправителя/ получателя. Отдельного рассмотрения требуют программы-троянцы (трояны), представляющие в настоящее время главную угрозу и занимающие лидирующее положение среди вредоносного ПО.

Спам заслуженно считается одной из важных проблем Интернета. Более 80% всех получаемых электронных писем являются спамом, т.е. ненужными пользователю. Природа спама такая же, как у телевизионной рекламы, и пока рассылка спама приносит деньги, вряд ли он может быть искоренен. Пользователю спам причиняет гораздо меньший вред, чем ранее рассмотренные вредоносные программы. В конечном итоге, удаление ненужных писем занимает не очень много времени — обычно несколько минут. Побочный эффект спама — удаление в общей массе мусора «нужных» писем. Но методы рассылки спама заслуживают внимания, так как в этот процесс может быть произвольно вовлечен компьютер пользователя. [8]

3.1.3 Методы защиты информации.

Любые способы утечки информации могут привести к значительному материальному и моральному ущербу, как для организации, так и для пользователей. Большинство из перечисленных путей несанкционированного

доступа поддаются надежной блокировке при правильно разработанной и реализуемой на практике системе обеспечения безопасности.

Острота проблемы защиты информационных технологий в современных условиях определяется следующими факторами:

- высокими темпами роста парка средств вычислительной техники и связи, расширением областей использования ЭВМ, многообразием и повсеместным распространением информационно-управляющих систем, подлежащих защите;
- вовлечением в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей;
- отношением к информации, как к товару, переходом к рыночным отношениям, с присущей им конкуренцией и промышленным шпионажем, концентрацией больших объемов информации различного назначения и принадлежности на электронных носителях;
- наличием интенсивного обмена информацией между участниками этого процесса;
- количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам.

Естественно, в такой ситуации возникает потребность в защите вычислительных систем и информации от несанкционированного доступа, кражи, уничтожения и других преступных и нежелательных действий.

Наблюдается большая разнородность целей и задач защиты - от обеспечения государственной безопасности до защиты интересов отдельных организаций, предприятий и частных лиц, дифференциация самой информации по степени ее уязвимости. Рассмотрим некоторые методы защиты информации в целом.

Организационно-правовая защита информации

Такая подсистема предназначена для регламентации деятельности пользователей ИС и представляет собой упорядоченную совокупность организационных решений, нормативов, законов и правил, определяющих общую организацию работ по защите информации в ИС.

Достижение высокого уровня безопасности невозможно без принятия должных организационных мер. С одной стороны, эти меры должны быть направлены на обеспечение правильности функционирования механизмов защиты и выполняться администратором безопасности системы. С другой стороны, руководство организации, эксплуатирующей средства автоматизации, должно регламентировать правила автоматизированной обработки информации, включая и правила ее защиты, а также установить меру ответственности за нарушение этих правил.

Организационно-правовую защиту структурно можно представить так:

Организационно-правовые вопросы:

- органы, подразделения и лица, ответственные за защиту;
- нормативно-правовые, методические и другие материалы;
- меры ответственности за нарушение правил защиты;
- порядок разрешения спорных ситуаций.

Регистрационные аспекты:

- фиксация "подписи" под документом;
- фиксация фактов ознакомления с информацией;
- фиксация фактов изменения данных;
- фиксация фактов копирования содержания.

Юридические аспекты:

- Утверждение в качестве законов:
- правил защиты информации;
- мер ответственности за нарушение правил защиты;
- регистрационных решений;
- процессуальных норм и правил.

Морально-психологические аспекты:

- подбор и расстановка кадров;
- обучение персонала;
- система моральных и материальных стимулов;
- контроль за соблюдением правил.

Для организации и обеспечения эффективного функционирования СЗИ должны быть разработаны документы, определяющие порядок и правила обеспечения безопасности информации при ее обработке в ИС, а также документы, определяющие права и обязанности пользователей при работе с электронными документами юридического характера (договор об организации обмена электронными документами).

План защиты информации может содержать следующие сведения:

- назначение ИС;
- перечень решаемых ею задач;
- конфигурация;
- характеристики и размещение технических средств и программного обеспечения;
- перечень категорий информации (пакетов, файлов, наборов и баз данных, в которых они содержатся), подлежащих защите в ИС;
- требования по обеспечению доступности, конфиденциальности, целостности различных категорий информации;
- список пользователей и их полномочий по доступу к ресурсам системы;
- цель защиты системы и пути обеспечения безопасности ИС и циркулирующей в ней информации;
- перечень угроз безопасности ИС, от которых требуется защита, и наиболее вероятных путей нанесения ущерба;
- основные требования к организации процесса функционирования ИС и мерам обеспечения безопасности обрабатываемой информации;

- требования к условиям применения и определение ответственности, установленных в системе технических средств защиты от НСД;
- основные правила, регламентирующие деятельность персонала по вопросам обеспечения безопасности ИС (особые обязанности должностных лиц ИС);
- цель обеспечения непрерывности процесса функционирования ИС, своевременность восстановления ее работоспособности и пути ее достижения;
- перечень и классификация возможных кризисных ситуаций;
- требования, меры и средства обеспечения непрерывной работы и восстановления процесса обработки информации (порядок создания, хранения и использования резервных копий информации и дублирующих ресурсов и т.п.);
- обязанности и порядок действий различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий, минимизации наносимого ущерба и восстановлению нормального процесса функционирования системы;
- разграничение ответственности субъектов, участвующих в процессах обмена электронными документами;
- определение порядка подготовки, оформления, передачи, приема, проверки подлинности и целостности электронных документов;
- определение порядка генерации, сертификации и распространения ключевой информации (ключей, паролей и т.п.);
- определение порядка разрешения споров в случае возникновения конфликтов.

Так же стоит проводить организационные и организационно-технические мероприятия по созданию и поддержанию функционирования комплексной системы защиты

Они включают:

- разовые (однократно проводимые и повторяемые только при полном пересмотре принятых решений) мероприятия;

- мероприятия, проводимые при осуществлении или возникновении определенных изменений в самой защищаемой АС или внешней среде (по необходимости);
- периодически проводимые (через определенное время) мероприятия; постоянно (непрерывно или дискретно в случайные моменты времени) проводимые мероприятия.[32]

Методы инженерно-технической защиты информации.

Теория инженерно-технической защиты информации описывает основные принципы, средства и методы обеспечения информационной безопасности объектов. Она включает в себя следующие вопросы:

- систему защиты информации;
- оценку угроз;
- принцип построения системы защиты информации.

Инженерно-техническая защита состоит из таких компонентов, как специальные органы, технические средства и мероприятия по их использованию для защиты конфиденциальной информации.

Постоянная и эффективная техническая защита информационных ресурсов является обязательной составляющей комплексной системы обеспечения информационной безопасности и способствует оптимизации денежных расходов на организацию защиты информации. Техническая защита информации предполагает целый комплекс мероприятий по защите информации от несанкционированного доступа по различным видам каналов, а также исключения специальных воздействий на нее, таких как, уничтожение, искажение или блокирование доступа.

Основными целями и задачами технической защиты являются:

- защита носителей информации от полного уничтожения в результате различных природных и техногенных воздействий;
- предотвращение проникновения злоумышленника к источникам

информации с целью уничтожения, хищения или изменения;

- предотвращение утечки информации по различным техническим каналам.

При проектировании систем технической защиты необходимо выполнять следующие принципы:

- непрерывность защиты информации в пространстве и во времени, постоянная готовность и высокая степень эффективности по ликвидации угроз информационной безопасности;
- многозональность и многорубежность защиты, задающее размещение информации различной ценности во вложенных зонах с контролируемым уровнем безопасности;
- избирательность в выборе первоочередности защиты наиболее важной информации;
- интеграция (взаимодействие) различных систем защиты информации с целью повышения эффективности многокомпонентной системы безопасности;
- создание централизованной службы безопасности в интегрированных системах.

По своему функциональному назначению средства инженерно-технической защиты подразделяются на следующие группы:

- инженерные средства, представляющие собой различные сооружения и устройства, предотвращающие физическое проникновение злоумышленников на защищаемые объекты;
- аппаратные средства, представляющие собой измерительные приборы и устройства, программно-аппаратные комплексы, предназначенные для выявления каналов утечки информации, оценки их характеристик по защите информации;
- программные комплексы и средства системы защиты информации в информационных системах различного назначения и в основных средствах обработки данных;

- криптографические средства защиты компьютерной информации, передаваемой по открытым каналам передачи данных и сетям связи.

В концепции инженерно-технической защиты информации кроме целей и задач системы безопасности, определяются принципы ее организации и функционирования; правовые основы; виды угроз и ресурсы, подлежащие защите, а также основные направления разработки системы безопасности.

К основным целям защиты информации относятся: предотвращение утечки, утраты, хищения, искажения, подделки информации и применение других несанкционированных негативных воздействий.

Разработка и создание новой системы защиты, а также оценка эффективности существующей системы безопасности объекта начинается с анализа наиболее возможных угроз и оценки их реального появления. Для получения данных такого рода, необходимо произвести обследование объекта на наличие уязвимостей в защите, а так же учесть особенности расположения, инженерных конструкций, коммуникаций и тому подобного. Следующим этапом выполняется выбор соответствующих методов и средств адекватной защиты объекта.

При рассмотрении вероятных угроз объекту нельзя забывать про угрозу безопасности здоровья персонала; угрозу целостности и сохранности оборудования и материальных ценностей; безопасность информации и сохранность государственной или коммерческой тайны.

При проектировании защиты в комплексную систему должно вписываться все-то разнообразие возможных информационных угроз, так как она должна обеспечивать надежное перекрытие всех опасных каналов утечки информации.

Эффективность всей системы защиты от утечки информации по техническим каналам оценивается по разнообразным критериям, которые определяются физической природой информационного сигнала, но чаще всего по соотношению «сигнал/шум».

Все способы защиты согласно руководящей документации делятся на две группы, такие как, скрытие и дезинформация.

К группе скрытие относятся:

- пассивное скрытие – заключается в исключении или значительном затруднении обнаружения объектов;
- активное скрытие – в создании техническим средствам разведки маскирующих шумовых помех различной физической природы и ложной обстановки по физическим полям;
- специальная защита – заключается в скремблирование телефонных переговоров, кодирование цифровой информации криптографическими методами, программные методы модификации информации.

К группе дезинформация относятся:

- техническая дезинформация;
- имитация;
- легендирование.

К принципам инженерно-технической защиты информации относятся:

- скрытность защиты информации;
- надежность защиты информации;
- непрерывность защиты;
- рациональность защиты;
- комплексное применение различных способов и средств защиты;
- многообразие способов защиты;
- экономичность защиты.[33]

Научно-методологический базис защиты информации

Научно-методологический базис защиты информации можно представить как совокупность трех иерархически взаимосвязанных компонентов следующего содержания:

- первый (верхний) уровень — общеметодологические принципы формирования любой науки, обобщенные до уровня мировоззренческих основ;

- второй (средний) уровень — общая методологическая база того фундаментального направления, составной ветвью которого является рассматриваемая;

- третий (низший) уровень — методы решения задач, учитывающие специфику конкретного направления.

Что касается общеметодологических принципов формирования науки, то они представляются следующим перечнем:

- строгое следование главной задаче науки — выявлению за внешними проявлениями внутренних движений, которые, как правило, — скрыты;

- упреждающая разработка общих концепций решения проблем;

- формирование концепций на основе реальных фактов, а не на основе абстрактных умозаключений;

- учет диалектики взаимосвязей количественных и качественных изменений в изучаемом фрагменте действительности;

- своевременное видоизменение постановок изучаемых задач;

- радикальная эволюция в реализации разработанных концепций;

- максимально возможная структуризация компонентов разработанных концепций и систем;

- унификация и типизация предлагаемых решений.

Для формирования структуры и содержания второго уровня научно-методологического базиса отправной точкой должна служить та посылка, что защита информации к настоящему времени уже выросла в достаточно серьезное и относительно самостоятельное научное направление, составляющее одну из ветвей того фундаментального научного направления информатики. Отсюда следует, что в качестве данного уровня для защиты информации должна выступать методологическая база информатики.

Существует еще одна проблема, связанная с формированием научно-методологического базиса современной информатики и имеющая непосредственное отношение к защите информации.

По мере расширения фронта решаемых задач защиты информации, управления качеством информации, обеспечения информационной безопасности, информационного обеспечения освоения информационного поля человечества и других подобных задач все более настойчивой становится необходимость накопления, хранения и аналитико-синтетической переработки сверхбольших объемов информации, характеризующейся повышенным уровнем неопределенности и противоречивости.

Современные методы и средства обработки не полностью удовлетворяют этим потребностям даже при нынешнем состоянии упомянутых задач.

Третий уровень научно-методологического базиса защиты информации составляют методы и модели не-посредственного решения задач. Как известно из теории систем, все задачи, связанные с изучением, созданием, организацией и функционированием больших систем, разделены на три класса:

- анализ, состоящий в определении текущих и прогнозировании будущих значений, представляющих интерес характеристик изучаемых систем;
- синтез, состоящий в проектировании систем и их компонентов, оптимальных по заданной совокупности критериев;
- управление, состоящее в определении оптимальных управляющих воздействий, необходимость в которых может возникнуть в процессе функционирования систем. [32]

3.1.4. Информационная безопасность образовательной организации.

Когда речь заходит об информационной безопасности, обычно мы начинаем думать о компьютерах, сетях, интернете, киберпреступности и хакерах. Но для образовательной среды проблема стоит шире: в ограждении учащегося от информации, которая может негативно повлиять на его формирование и развитие, то есть о пропаганде различной направленности.

Кроме того, все еще слабо осознана та часть проблемы, которая связана с общением в социальных сетях, которые сегодня все чаще подменяют собой живое общение. В виртуальном пространстве действуют совершенно иные правила, где психически неокрепшая личность не может эффективно противостоять угрозам, запугиванию, откровенным попыткам растления. И сегодня именно этот фактор начинает выходить на первые роли в обеспечении информационной безопасности в ее широком понимании: не только технической, но и когнитивной сферы во всей ее полноте.[26]

Скачкообразное насыщение компьютерами системы образования, случившееся в начале 2000-ых годов в России породило целый ряд насущных проблем, связанных с внедрением информационных технологий в образовательный процесс. В результате последнее время основной задачей стало выстраивание информационной образовательной среды. Эта чрезвычайно нужная и важная проблема отодвинула все более частные проблемы на второй план. Сейчас, когда уже можно говорить, о существующей информационной среде в образовательных учреждениях, начинают всплывать важнейшие проблемы, оставленные ранее до лучших времен. Один из самых важных вопросов стоящих сейчас перед образовательными учреждениями с точки зрения информационных технологий – это вопрос информационной безопасности образовательного учреждения. [27]

Зарубежный и отечественный опыт позволяет определить следующие угрозы информационной безопасности, которые стоят перед образовательными учреждениями:

1. Несанкционированный доступ к данным. Эта группа угроз включает в себя подмену данных в электронных журналах, архивах, хищение информации экзаменационных билетов, личных данных учащихся и их родственников и т.п. В большинстве рекомендаций по организации схем обеспечения информационной безопасности специалисты ограничиваются только этой, технической сферой.

2. Фильтрация нежелательной информации. Эта группа угроз напрямую связана с противодействием экстремистской идеологии, но не ограничивается только ей. При рассмотрении угроз доступа к нежелательной информации следует также учитывать вопросы распространения порнографии, провокационных материалов, пропаганды наркотиков и алкоголя и т.п.

3. Проблемы регулирования использования социальных сетей. Именно в этой зоне осуществляется активное давление на учащихся, запугивание, а также сравнительно новый феномен киберхулиганства.

4. Кибертерроризм. Несмотря на то, что эта группа угроз находится в ведении соответствующих силовых ведомств, частично она может решаться и на уровне учебных заведений. Создание безопасной информационно-технологической среды серьезно осложняет возможные кибератаки на объекты образования, которые могут привести к нарушению функционирования управляющих автоматических систем и последующему повреждению инфраструктуры. Следует, впрочем, отметить, что эта группа угроз остается пока во многом гипотетической, так как учебные заведения в силу низкой их насыщенности автоматизированными управляющими системами не рассматриваются в качестве приоритетных целей для кибератак. [26]

Современные образовательные учреждения широко используют в своей деятельности информационные технологии для ведения журналов, контроля успеваемости, административно-хозяйственной деятельности и т.п. К сожалению не все информационные системы, используемые в образовательных учреждениях, отвечают требованиям, предъявляемым к безопасным системам.

Большинство информационных систем не проходят какой-либо сертификации, стандартизации, создаются очень часто на основе устаревших решений.

Перечисляя проблемы, характерные для таких информационных систем, можно отметить:

- Использование разнородных, устаревших и заведомо небезопасных платформ. Уязвимости в информационных системах, базах данных и других информационных средствах выявляются регулярно, и любая устаревшая платформа должна считаться заведомо небезопасной, если не проведены работы по устранению этих проблем. Во многих случаях информационные системы не связаны между собой, используют разные платформы, что резко осложняет их использование и поддержку.

- Отсутствие стандартизации. Несмотря на предпринятые попытки разработать унифицированные информационно-технические решения, большинство учебных заведений используют те решения, которые оказались под рукой.

- Использование публичного открытого соединения. Любая информационная система, претендующая на безопасность, должна организовывать передачу данных с использованием зашифрованных соединений по умолчанию во избежание перехвата данных.

- Отсутствие практики регулярного аудита безопасности. Без постоянной проверки и выявления потенциальных проблем даже качественно спроектированные информационные системы могут стать небезопасными при обнаружении новых видов уязвимостей.

- Низкая квалификация обслуживающего персонала или отсутствие должности специалиста по поддержке информационных систем в принципе. Качественная поддержка информационных систем требует регулярного мониторинга их работы и превентивного устранения неполадок.

- Использование пиратского программного обеспечения. Многие образцы «взломанных» программ могут содержать в себе троянский код, упрощающий внедрение в информационные системы. Кроме того, пиратское программное обеспечение часто исключает возможность его обновления, что не позволяет противостоять вновь возникающим угрозам.

- Недофинансирование. Эта проблема является корнем всех вышеперечисленных. [26]

Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно подразделить на пять уровней:

1. Законодательный . Это законы, нормативные акты, стандарты и т.п.

Нормативно-правовая база определяющая порядок защиты информации:

- Ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях по защите информации» .

В соответствии с данной статьей защита информации представляет собой принятие правовых, организационных и технических мер. Меры должны быть направлены на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

- Ст. 9 Федерального закона № 149-ФЗ, п. 5 гласит "Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению такой информации. Такая обязанность возлагается Трудовым кодексом РФ (далее – ТК РФ), гл. 14 которого определяет защиту персональных данных работника. В соответствии со статьей ТК РФ: "Лица, виновные в нарушении норм,

регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами. Для развития данных положений в РФ принят Федеральный закон № 152-ФЗ РФ «О персональных данных», который вступил в силу с 1 января 2008 г. Его основной целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайны. Статья 3 данного закона определяет: "Персональные данные - любая информация, относящаяся к определенному или неопределенному на основании такой информации лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, другая информация"

- Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию", согласно которому содержание и художественное оформление информации, предназначенной для обучения детей в дошкольных образовательных учреждениях, должны соответствовать содержанию и художественному оформлению информации для детей данного возраста. А также в соответствии с Федеральным законом «Об основных гарантиях прав ребенка» образовательные учреждения обязаны ограничивать доступ учащихся к ресурсам сети Интернет, пропагандирующим насилие и жестокость, порнографию, наркоманию, токсикоманию, антиобщественное поведение.

2. Морально-этический. Всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации.

3. Административный. Действия общего характера, предпринимаемые руководством организации.

Таковыми документами могут быть:

- приказ руководителя о назначении ответственного за обеспечение информационной безопасности;
- должностные обязанности ответственного за обеспечение информационной безопасности;
- перечень защищаемых информационных ресурсов и баз данных;
- инструкцию, определяющую порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников организации.

4. Физический. Механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей.

5. Аппаратно-программный (электронные устройства и специальные программы защиты информации). [25]

К решению всех вышеописанных проблем можно подходить на различных уровнях. Оптимальным вариантом решения данных проблем могла бы стать разработка единой платформы для всех образовательных учреждений и ее централизованная удаленная поддержка высококвалифицированными специалистами, которые обладают необходимыми знаниями в области обеспечения безопасности информационных систем. Однако такой вариант возможен только в дальнейшей перспективе и выглядит идеалистическим. В реальности все возникающие проблемы учебные заведения вынуждены решать самостоятельно. [26]

3.2. Реализация информационной безопасности в колледже.

3.2.1. Информационные технологии при организации учебного процесса в колледже.

Организация образовательной деятельности колледжа с использованием электронных информационных ресурсов предполагает использование новейших педагогических технологий, стимулирующих развитие внутренних резервов каждого ученика и одновременно способствующих формированию социальных качеств учащихся, т. е. использование новых информационных технологий обучения, позволяет решать дидактические проблемы, управляя процессом обучения. [3].

В современном колледже информация, информационная инфраструктура – один из главных компонентов учебного процесса. Учебные классы оснащаются компьютерной техникой и её качественное бесперебойное функционирование существенно определяет качество полученных знаний, способствует формированию профессиональных компетенций студентов. Вот поэтому-то обеспечение информационной безопасности учебного процесса, в том числе непрерывного функционирования компьютерных и информационных ресурсов, является весьма важной для его качества.[28].

Сегодня актуальной задачей колледжа является в поиске новых форм и средства при переходе от традиционного к инновационному образованию в учебном процессе, необходимостью повышения эффективности обучения, дать возможность учащимся проявлять самостоятельность в планировании, организации и контроле своей деятельности. Организации учебного процесса в колледже с применением новых информационных технологий содержит два тесно связанных между собой слагаемых. Во-первых, огромные возможности современные информационные технологии несут в себе несравнимый с ранее применявшимися техническими средствами обучения, дидактический материал, который может и должен быть реализован в учебно-воспитательном процессе. Во-вторых, широкое применение компьютеров в учебном процессе зависит от подготовки кадров на уровне современных требований. Поэтому изучение и использование информационной и компьютерной технологии в учебном процессе

— важнейший компонент подготовки учащихся к дальнейшей трудовой деятельности. [3]

В настоящее время информационные технологии широко применяются для организации учебно-воспитательного, научно-исследовательского и управленческого процесса колледжа, которые основными характеристиками являются возможность дифференциации и индивидуализации обучения, а также возможность развития творческой познавательной активности учащихся. Для организации учебного процесса с применением информационных технологий могут применяться пять основных методов обучения:

- объяснительно-иллюстративный;
- репродуктивный;
- проблемный;
- исследовательский;
- частично — поисковый, или эвристический метод.

Применение этих методов с использованием информационных технологий позволяет существенно улучшить качество организации процесса обучения, но не позволяет радикально изменить учебный процесс по сравнению с применяемой традиционной обучением. При использовании информационных технологий формальный компонент процесса обучения игнорировать невозможно, следовательно, невозможно и избежать использования этих методов с их однозначным пониманием и усвоением учебной информации, точным воспроизведением способов действий.

Организация учебного процесса в колледже с применением информационных технологий должны обеспечивать:

- доставку учащимся основного объема изучаемого материала;
- интерактивное взаимодействие учащихся и преподавателей в процессе обучения;

- предоставление учащимся возможности самостоятельной работы по усвоению изучаемого материала;

- контроль знаний и навыков, полученных ими в процессе обучения.

Для этих целей в учебном процессе колледжа применяются следующие средства информационные технологии:

- предоставление учебников и другого печатного материала;

- пересылка изучаемых материалов по компьютерным телекоммуникациям;

- дискуссии и семинары, проводимые через компьютерные телекоммуникации;

- современные прикладные программы (Word, Excel, PowerPoint, Access);

- интернет, в том числе электронная почта;

- двусторонние видео-телеконференции;

- электронные информационные ресурсы.

В компьютерном классе колледжа имеет возможность применять электронных ресурсов на различных этапах урока:

- при изложении нового материала

- визуализация знаний с помощью программы PowerPoint;

- проведение виртуальных лабораторных работ с использованием обучающих программ;

- закрепление изложенного материала с помощью разнообразных обучающих программ и лабораторных работ;

- система контроля и проверки знаний студентов с помощью контролируемых программ;

- при проведении интегрированных уроков по методу проектов, результатом которых будет создание Web

- страниц, проведение телеконференций.[3]

В проблеме обеспечения информационной безопасности четко выделяются технический, организационный и документационный аспекты. Технический аспект

связан с выбором программного обеспечения, организационный – с проведением мероприятий для реализации закона № 152-ФЗ «О персональных данных», а документационный – с созданием локальных актов колледжа. Однако в современном информационном обществе организационный и документационный аспекты в значительной мере перекрываются.

В первую очередь рассмотрим технические вопросы. Для студентов и преподавателей главным способом поиска информации является использование глобальной сети Интернет. Какие угрозы существуют в Интернете? Это компьютерное мошенничество, компьютерные вирусы, хакерские атаки, вандализм, хищение, разглашение конфиденциальной информации и так далее. Противостоять им можно с помощью программы, осуществляющей фильтрацию входящего трафика (прокси-сервера). Это удачное комплексное решение для организации общего доступа в Интернет из локальной сети, учета трафика и защиты от внешних угроз, а сетевой экран надежно защищает сеть от внешних атак. По необходимости можно подключать к Интернету компьютерные классы или отключать их, задавать временные отрезки для работы в Интернете, блокировать нежелательные ресурсы по-отдельности, либо по категориям сайтов. Использование прокси-сервера также позволило контролировать и объем скачиваемых из сети данных, что значительно уменьшило нагрузку на локальную сеть. Кроме того, использование грамотно настроенной антивирусной программы, с автоматическим обновлением и сформированным дополнительным списком угроз дает, в свою очередь, качественную антивирусную защиту.

Еще один канал распространения угроз – электронная почта, которой пользуются практически все. Самый надежный способ контроля - организация собственного почтового сервера, с помощью которого проще отслеживать почтовые протоколы, фильтровать нежелательные или сомнительные «послания».

Еще одной технической стороной проблемы бесперебойной работы компьютеров является разграничение доступа к информации и к ресурсам

компьютера. Наличие как минимум двух учетных записей (одна с ограниченными правами – основная, а вторая с правами администратора – только для настроек и обе обязательно под паролем) позволяет намного дольше сохранить работоспособность компьютерного парка в целом, контролировать установку программного обеспечения. Таким образом, установка контрафактного и «зловредного» ПО, в большинстве случаев, просто невозможна (не достаточно полномочий).

Второй аспект проблемы информационной безопасности – организационный. Это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба. Для успешной работы все участники образовательного процесса должны четко осознавать проблему информационной безопасности. Пока же пользователи нередко нарушают порядок обработки информации, не соблюдают требования нормативно-правовых документов, регламентирующих информационную безопасность. Безопасность информации может быть обеспечена только при комплексном использовании всех средств защиты. Процесс построения системы информационной безопасности не может быть разовым мероприятием, равно как исполнение и контроль не может быть возложен на одного ответственного за информационную безопасность. Этот процесс должен быть управляемым, постоянно совершенствуемым. Такой подход – стратегическое звено во всей системе информационной безопасности, также как информация – главный защищаемый элемент.[28]

Применение информационных технологии для организации учебного процесса значительно расширяют возможности предъявления учебной информации, позволяет существенно повысить мотивацию учащихся к обучению, вовлекают учащихся в учебный процесс, увеличивает возможности постановки учебных задач и управления процессом их решения, а также позволяют качественно изменять контроль деятельности учащихся.

Одним из преимуществ использования электронного информационного ресурса является повышенный интерес учащихся к преподаваемой дисциплине, т. к. он обладает высокой наглядностью, в нем можно использовать анимации, видеосюжеты, звуковое сопровождение, дополнительный материал и другое. [3]

3.2.2. Политика информационной безопасности колледжа.

Общие положения

1. Политика ИБ колледжа направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников; уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников колледжа, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора хранения, обработки, предоставления и распространения информации; защиту несовершеннолетних обучающихся от информации, причиняющей вред их здоровью и развитию и обеспечение эффективного и бесперебойного процесса деятельности.

2. Объектами защиты с точки зрения ИБ являются информационный процесс профессиональной деятельности и информационные активы колледжа.

3. К защищаемой информации относится информация по финансово-экономической деятельности колледжа, персональные данные.

4. Основными мерами обеспечения ИБ являются:

- постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов колледжа;

- своевременное обнаружение проблем, потенциально способных повлиять на ИБ колледжа, корректировка моделей угроз и нарушителя;

- разработка и внедрение защитных мер;

- блокирование недопустимого контента интернет-траффика;

- контроль эффективности принимаемых защитных мер;

- персонафикация и разделение ролей и ответственности между сотрудниками колледжа за обеспечение ИБ колледжа исходит из принципа персональной и единоличной ответственности за совершаемые операции.

5. Управление ИБ колледжа включает в себя:

- разработку и поддержание в актуальном состоянии Политики информационной безопасности;

- разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению ИБ;

- обеспечение бесперебойного функционирования комплекса средств ИБ;

- осуществление контроля (мониторинга) функционирования системы ИБ;

- оценку рисков, связанных с нарушениями ИБ.

6. В отношении всех собственных информационных активов колледжа, активов, находящихся под контролем колледжа, а также активов, используемых для получения доступа к инфраструктуре колледжа, устанавливается ответственность соответствующего сотрудника колледжа.

Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами колледжа должна доводиться до сведения директора колледжа.

7. Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, и согласованы с заведующим сектором по информационно-техническому обеспечению.

8. Все работы в пределах колледжа должны выполняться в соответствии с должностными обязанностями только на компьютерах, разрешенных к использованию в колледже.

9. Внос в здание и помещения колледжа личных портативных компьютеров и внешних носителей информации, а также вынос их за пределы колледжа производится только при согласовании с заведующим сектором по информационно-техническому обеспечению.

10. Все данные, составляющие тайну колледжа и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

11. В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

12. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети колледжа, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

13. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

14. Компьютерное оборудование, предоставленное колледжем, предназначено для использования исключительно в производственных целях.

15. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования.

16. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

17. Все программное обеспечение, установленное на предоставленном управлении компьютерном оборудовании, является собственностью колледжа и должно использоваться исключительно в производственных целях.

18. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Сотрудникам запрещается направлять конфиденциальную информацию колледжа по электронной почте без использования систем шифрования. Конфиденциальная информация колледжа, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

19. Использование сотрудниками колледжа публичных почтовых ящиков электронной почты осуществляется только при согласовании с заведующим сектором по информационно-техническому обеспечению.

20. Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

21. Перед отправкой сообщений пользователи должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать заведующего сектором по информационно-техническому обеспечению.

22. Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

23. Не допускается при использовании электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- рассылка рекламных материалов не связанных с производственной деятельностью;
- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит стандартам в области этики.[22]

Политика пользования электронной почтой и доступа к ресурсам сети Интернет.

Настоящая политика предоставляет персоналу разрешенные правила пользования ресурсами электронной почты (e-mail) и порядок доступа к ресурсам сети Интернет. Политика охватывает e-mail, проходящий или отправляемый через все принадлежащие колледжу персональные компьютеры, ноутбуки, сотовые телефоны и любые другие ресурсы, способные посылать или принимать e-mail.

Мониторинг.

ИТ специалист контролирует использование e-mail, каналы доступа к ресурсам сети Интернет, чтобы гарантировать текущую доступность и надежность систем.

Политика.

1. Персонал должен сохранять конфиденциальность своих паролей и, независимо от обстоятельств, никогда не передавать в пользование и не раскрывать их никому.

2. Персонал должен использовать электронную почту для любой переписки, касающейся деятельности колледжа.

3. Персонал должен ограничивать объемы пересылаемой по e-mail информации, чтобы по возможности не перегружать и не блокировать каналы связи.

4. Пересылаемая текстовая информация при необходимости должна сжиматься стандартными архиваторами. Пересылаемая графическая информация должна сжиматься стандартными средствами пакета Microsoft Office - Picture Manager (или аналог).

5. Персонал должен готовить e-mail сообщения, соответствующие по виду и содержанию официальному статусу колледжа.

6. Персонал должен удалять подозрительные сообщения и сообщения от незнакомых адресатов, при этом заботиться о ежедневном обновлении антивирусной базы.

7. Приветствуется использование технологии считывания только заголовков почтовых сообщений, что резко сокращает вирусную опасность и трафик, связанный со спамом. Этика поведения и ответственное пользование.

Колледж обеспечивает персонал каналами доступа к сети Интернет для облегчения коммуникаций и поддержки ежедневных рабочих операций.

Этично и приемлемо

- связываться и обмениваться информацией согласно с целями, характером и задачами колледжа;
- использовать общепринятую лексику и ограничения в словесных описаниях, принятых в колледже;
- уважать легальную защиту, которую предусматривают различные права пользования и лицензии на ПО и данные;
- придерживаться грамотного ведения e-mail, удалять устаревшие сообщения. Запрещено
- нарушать требования, политики ИБ колледжа;
- публиковать, показывать или передавать любую информацию или данные, содержащие клевету, ложь, неточности, оскорбления, непристойности, порнографию, богохульство, сексуальные домогательства, угрозы, расовые и национальные обиды и агрессивные комментарии, дискриминацию по полу, цвету волос и пр. или неверный материал;

- нарушать приватность персонала, данных и/или использовать информацию, содержащуюся в колледже, в личных интересах или выгоды;
- заниматься рассылкой и пересылкой писем других лиц, не связанной с исполнением должностных обязанностей, распространением недозволенной и другой рекламы и пр.;
- намеренное размножение, разработка или использование вредоносного программного обеспечения в любых формах (вирусы, черви, трояны и пр.);
- просмотр, перехват, раскрытие или помощь в просмотре, перехвате, раскрытии e-mail, не адресованной пользователю;
- использование для ведения служебных переговоров интернет-сервиса Skype;
- посещать социальные сети «Одноклассники», «В контакте», «Facebook» и аналогичные при работе на компьютерах колледжа, если это не предусмотрено должностными обязанностями;
- просматривать, скачивать информацию развлекательного, рекламного характера, видео и музыкальные файлы, если это не предусмотрено должностными обязанностями или поручениями руководителя.

Антивирусная политика.

Настоящая политика устанавливает требования, которым должны удовлетворять все компьютеры, подключенные к сети колледжа, требования к пользователям по антивирусной защите, гарантирующие эффективное определение и защиту от деструктивного воздействия вирусов.

Область применения.

Настоящая политика применяется ко всем компьютерам сети колледжа, каталогам общего пользования, к которым относятся персональные компьютеры,

ноутбуки, терминалы, любое сетевое оборудование. Источниками вирусов могут быть e-mail, Интернет-сайты со скрытыми вредоносными активными элементами, носители информации (флоппи-диски, CD-диски, flash-диски и пр.), открытые для общего доступа папки и файлы и т. д.

Политика.

Защита от внешних угроз и вирусов имеет несколько уровней:

- а) защита от внешних вторжений, вирусов с Интернет-сайтов;
- б) антивирусный контроль файлов и почтовых вложений с помощью антивирусных программ на рабочих местах пользователей;
- в) стандартные средства операционных систем.

На всех компьютерах сети должно быть установлено антивирусное программное обеспечение, а в некоторых случаях в сочетании с персональным брэндмауэром. Антивирус контролирует жесткий диск и память компьютера на проникновение вируса, а брэндмауэр контролирует данные, попадающие и покидающие «внутренний периметр» через Интернет-соединение.

Это программное обеспечение должно выполняться постоянно, а также настроено для регулярного исполнения по расписанию для проверки всего содержимого жесткого диска. Кроме того, антивирусные базы должны обновляться в срок (автоматически) и содержаться в актуальном состоянии. Инфицированные вирусами компьютеры должны удаляться из сети до полного уничтожения вирусов. Работы по уничтожению вирусов, настройке запуска антивирусных процедур по расписанию выполняются специалистами системного администрирования (СА).

Все сотрудники, допущенные к работе с информационно - технологическими ресурсами колледжа, должны неукоснительно соблюдать требования инструкции по антивирусной защите, владеть навыками работы с антивирусными

инструментами. Антивирусное сканирование конечные пользователи выполняют самостоятельно.

Любая деятельность по намеренному созданию и/или распространению вредоносных программ внутри сети колледжа (вирусы, черви, трояны, почтовые бомбы и пр.) запрещена.

Ответственность.

К сотруднику, нарушившему эту политику, применяются меры дисциплинарной ответственности.

Политика подготовки, обмена и хранения документов и данных.

Настоящая политика устанавливает требования к содержанию, копированию, порядку обмена, хранению электронных и бумажных документов, файлов и информации внутри колледжа, между управлениями и их удаленными подразделениями, предоставлении прав пользования общими данными.

Область применения.

Настоящая политика охватывает все подразделения, службы, отделы, чья деятельность связана с подготовкой, копированием, хранением, обменом документами, информацией, данными с использованием информационно-технологических ресурсов.

Политика.

Персонал колледжа должен придерживаться следующих требований по подготовке, копированию, хранению, обмену документами, информацией, данными, файлами:

- по содержанию:

- документы по виду и содержанию должны соответствовать официальному статусу колледжа, следует употреблять общепринятую деловую лексику;
- по хранению электронных документов:
 - документы офисных, почтовых, графических и др. стандартных приложений (Word, Excel, PowerPoint, Outlook, PhotoShop и пр. или аналоги) должны создаваться и храниться в папках Мои Документы (или аналогичной)\ все папки должны иметь понятную вложенную структуру и наименования по темам;
 - не допускается хранение файлов, информации личного характера, не относящейся к деятельности колледжа, на персональных компьютерах;
 - документы, предназначенные для общего пользования, после создания и обработки следует хранить в общедоступной папке — на компьютере;
 - не допускается работа с документами без извлечения из общей папки на локальный ПК пользователя;
 - периодически, раз в неделю удалять устаревшие версии файлов с компьютера - из папок для обмена и Мои Документы,
- по обмену электронными документами:
 - разрешено считывать, передавать, изменять только данные, на которые у пользователя есть права и которые пользователю положено знать, включая ошибочно доступные папки и электронную почту;
 - внутриофисный обмен файлами может выполняться через общедоступную папку на компьютере; внутриофисный обмен по электронной почте через Интернет не ограничивается;
- по хранению электронных носителей информации:
 - оберегать и содержать электронные носители, когда они не в работе, в предназначенных для этого контейнерах, полках, стеллажах, сейфах;
 - не держать электронные носители на столе в пределах визуальной доступности во время отсутствия на рабочем месте.

Ответственность

К сотруднику, нарушившему эту политику, применяются меры дисциплинарной ответственности.

Политика информационно-технической поддержки.

Настоящая политика устанавливает правила, уровни предоставления и получения персоналом информационно -технической поддержки своей работы. Доступ персонала к информационно-техническим ресурсам обеспечивается программистом на непрерывной основе, поддержкой всех технологических ресурсов в рабочем состоянии. Поддержка требует:

а) работ по обслуживанию и развитию технологических ресурсов;

б) работ по реагированию и устранению причин этих заявок (инцидентов),

т.е. работ непосредственно по поддержке. Повторяющиеся инциденты, переходят в разряд проблем и требуют выполнения внеплановых работ. Область применения.

Настоящая политика охватывает и описывает все уровни поддержки персонала, выполняемые специалистами системного администрирования. Выделяется уровень самопомощи и три уровня поддержки:

Самопомощь - когда конечный пользователь самостоятельно выполняет действия по устранению проблемы, не нарушающие безопасность сети и других пользователей, такие как перезапуск приложения или компьютера, проверка подключения всех кабелей и сетевых ресурсов, антивирусное сканирование и пр.

Поддержка 1-го уровня - выполняется реализация работ общего профиля:

- решение оперативных проблем персонала, задач доступа и безопасности;
- первичная диагностика сложных проблем, причин неработоспособности программ;

- устранение проблемы или переадресация по сложности на следующий уровень. Поддержка 2-го уровня - выполняется реализация по работе приложений и систем.

- углубленные, содержательные консультации и обучение;
- поиск решений имеющимися средствами (без вмешательства в логику приложений), помощь в выборке и восстановлении данных и документов, (раз)доработка отчетных форм;
- обслуживание контента и администрирование.

Поддержка 3-го уровня - выполняется реализация работ по развитию приложений, систем, инфраструктуры:

- работа с поставщиками приложений и разработчиками;
- планирование и развертывание новых приложений, реорганизация процессов и пр.

Политика.

Поддержка закрепляется по уровням за техническими специалистами.

Персонал должен использовать Поддержку 1-го уровня только после выполнения разрешенных процедур самопомощи. Многократное обращение за помощью по

инцидентам, устраняемым самопомощью, указывает на несоответствие персонала занимаемой должности.

ИТ обслуживание персонала осуществляется по заявкам. Содержание заявки передается программисту любым доступным способом (телефон, почта, бумажный носитель). Конечный пользователь должен быть информирован о порядке, времени исполнения заявки, ее движении, и, по возможности, обеспечен альтернативными

ресурсами. Приоритет исполнения заявки устанавливается в связи с текущими задачами.

Работы по Поддержке 3-го уровня должны выполняться на проектной основе с привлечением специалистов, консультантов, подрядчиков. Внешние консультанты и подрядчики должны иметь максимально ограниченный доступ к информационно-техническим ресурсам колледжа, но достаточный для выполнения проектов. Для ведения проектов со стороны колледжа назначаются ответственные лица.

Ответственность.

К сотруднику, нарушившему эту политику, применяются меры дисциплинарной ответственности.

3.3. Место в системе электронных образовательных ресурсов и меры защиты от угроз.

3.3.1. Место в системе.

Созданная мультимедийная система внедрялась в образовательное учреждение ГБПОУ "ЮУГК" где проводилось исследование эффективности электронного ресурса. Система использовалась для самостоятельного изучения материала группой студентов, после чего был проведен контрольный срез по изученной дисциплине. Обучающиеся были разбиты на 2 группы. Одна группа выполняла задания с использованием справочника, а вторая без использования. Результаты исследования представлены в диаграммах.

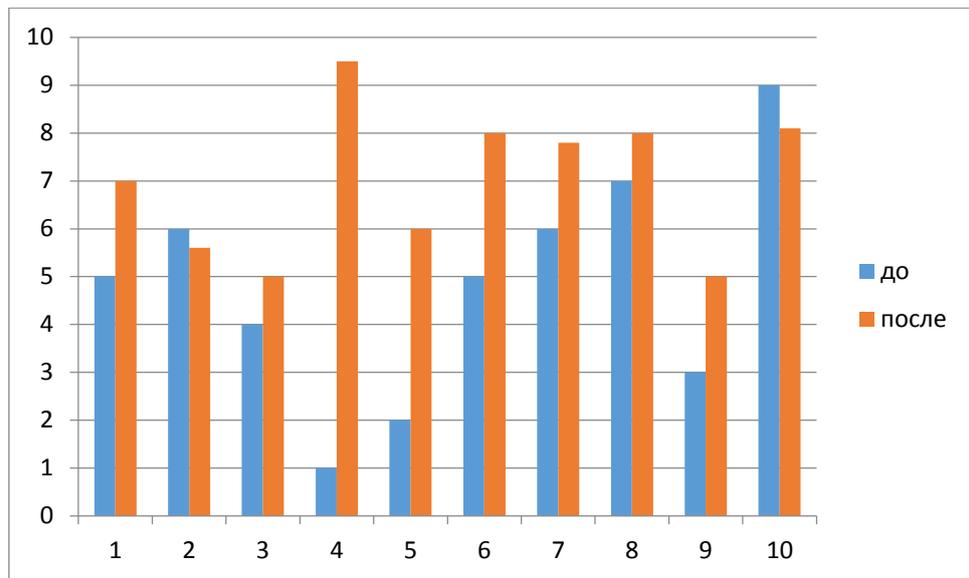


Рисунок 18 – Результаты исследования при использовании справочника

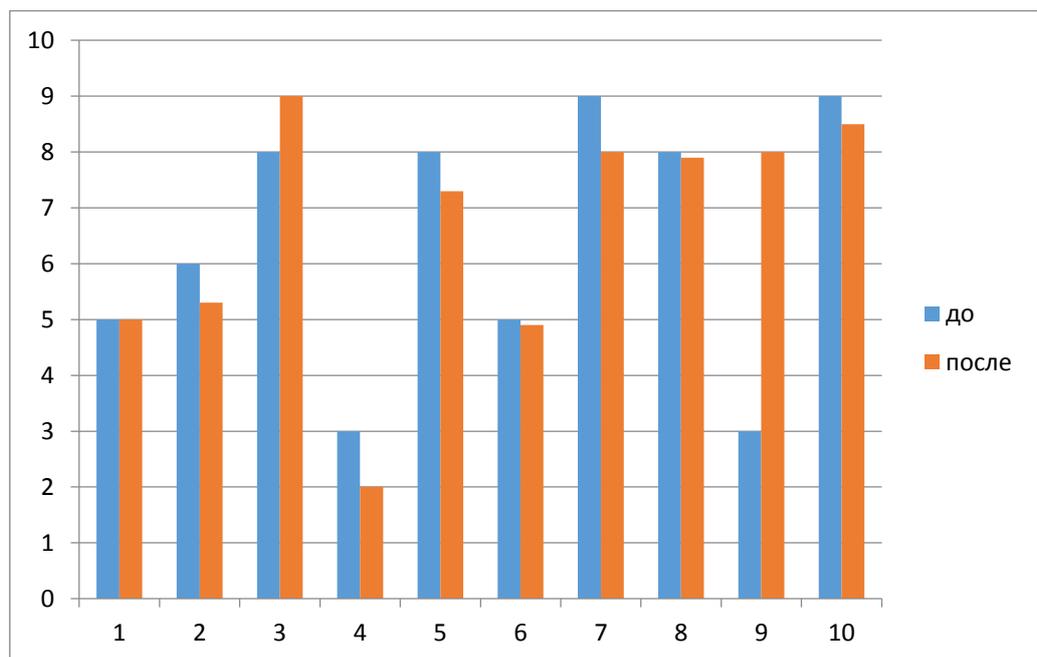


Рисунок 19 – Результаты исследования без использования справочника

3.3.2. Меры защиты.

При использовании системы были использованы следующие методы защиты информации:

Антивирусная политика – пособие не содержит вирусов.

Политика защиты персональных данных – пособие не содержит и не собирает сведения о персональных данных.

Политика соблюдения авторских прав – пособие не является плагиатом, не требует дополнительной лицензии правообладателя, предоставляется по свободной лицензии.

Политика свободного доступа – пособие представлено в свободном доступе в электронной библиотеке, а так же на информационном портале колледжа.

Выводы по третьей главе.

Изложены основные понятия защиты информации, методы защиты, а так же представлена политика безопасности колледжа ГБПОУ "ЮУГК". Рассмотрены основные методы защиты созданной мультимедийной системы.

Заключение

Анализ литературы показал, что использование мультимедийных технологий в процессе обучения и защита их от несанкционированного копирования в настоящее время имеют огромное значение.

Выявление преимуществ и недостатков при работе с мультимедийными системами дало возможность создать мультимедийный ресурс для изучения дисциплины «Информатика и программирование».

Создана техническая документация по данному мультимедийному ресурсу, внедрена система защиты от его несанкционированного копирования.

Экспериментальные исследования на базе ГБПОУ "ЮУГК" подтвердили эффективность использования созданной системы в учебном процессе.

Библиографический список

1. Агапонов С.В., Джалиашвили З.О., Кречман Д.Л. и др. Средства дистанционного обучения. Методика, технология, инструментарий/ Под ред. Джалиашвили З.О. – СПб.: БХВ – Петербург. – 2003.
2. Агеев В.Н., Древис Ю.Г. Электронные издания учебного назначения: концепции, создание, использование. – М.: МГУП. – 2003.
3. Алексеева, М. Б. Технология использования систем мультимедиа [Текст] : учеб. пособие / М. Б. Алексеева, С. Н. Балан. – СПб. : Изд. дом «Бизнес-пресса», 2002. – 176 с.
4. Аминов И. Б., Суяров А. М. Применение информационных технологий для организации учебного процесса в колледже // Молодой ученый. — 2016. — №3.— С.768-769
5. Андерсен, Б. Б. Мультимедиа в образовании [Текст] : специализированный учебный курс / Бент Б. Андерсен, Катя ван ден Бринк. — Москва : Дрофа, 2007.

6. Андреев А.А. Дидактические основы дистанционного обучения. – М.: РАО. – 1999.
7. Аудит информационной безопасности: учебное пособие для вузов. Аверченков В. И. Флинта 2016г. 269 с
8. Башмаков, М. И., Информационная среда обучения [Текст] / М. И. Башмаков, С. И. Поздняков, Н. А. Резник. – СПб. : Свет, 1997. – 400 с.
9. Большой толковый словарь русского языка [Текст] / гл. ред. С. А. Кузнецов. — СПб.: Норинт, 1998. 5. Борзенко, А. Программное обеспечение для мультимедиа [Текст] / Андрей Борзенко // Компьютер-Пресс. — 1995. — № 2.
10. Борзенко, А. Е. Мультимедиа для всех [Текст] / А. Е. Борзенко, А. Г. Федоров. – М. : Компьютер Пресс, 1995. – 222 с. : ил
11. Бурятский Государственный Университет – Понятие технологии мультимедиа [Электронный ресурс]: [справочный листок] – Бурятский Государственный Университет, 2008. – Режим доступа: www.bsu.ru/content/hec/dambieva/powerpoint.doc
12. Вихман, В. В. Мультимедиа технологии [Текст] : электроннометодический комплекс : учебное пособие / В. В. Вихман. — Новосибирск : НГТУ, 2008.
13. Все для учителя –LCDS – приложение для создания электронных учебников [Электронный ресурс]: [справочный листок] – Все для учителя, 2013. – Режим доступа: http://it-t-a.ucoz.ru/index/lcds_prilozhenie_dlja_sozdaniya_ehlektronnykh_uchebnikov/0-45
14. Галатенко В.А. Основы информационной безопасности. Интернет-университет информационных технологий – ИНТУИТ.ру, 2008.
15. Галатенко В.А. Стандарты информационной безопасности. Интернет-университет информационных технологий – ИНТУИТ. ру, 2005.
16. Гусева, Е. Н. Информатика [Электронный ресурс] : учеб. пособие / Е. Н. Гусева ; Университетская библиотека онлайн (ЭБС). — Москва : Флинта, 2011. — 260 с.

17. Доклад «Информационная безопасность в образовательной организации». Бритикова Л. Г. Тамбов 2016г. [Электронный ресурс]. Режим доступа:- <http://mirznanii.com>

18. Единое окно доступа к образовательным ресурсам – Система REDCLASS Course [Электронный ресурс]: [справочный листок] – Единое окно доступа к образовательным ресурсам, 2012. – Режим доступа: http://window.edu.ru/resource/217/58217/files/redclass_course.pdf

19. Е.А.Коняева О.В.Смык. Применение мультимедийных технологий в образовании. Профессиональное образование: методология, технологии, практика. Сборник научных статей выпуск 10. Челябинск 2017

20. Защита конфиденциальной информации при электронном документообороте: учебное пособие. Минин И. В., Минин О. В. НГТУ. 2011 год. 20 с

21. Информатика под, ред. Черноскутовой И.А. Учебное пособие 2005-272 с.

22. Информатика под ред. Хубаева Г.Н. Учебное пособие 2010-288 с.

23. Информационная безопасность образовательного учреждения общего образования. М.И. Шубинский. Труды XV Всероссийской объединенной конференции «Интернет и современное общество» (IMS-2012), Санкт-Петербург, Россия, 2012.

24. Информационная безопасность образовательного учреждения. Использование компьютерных технологий и работа в сети Интернет. Баданов А.Г. 2010. Режим доступа:- <http://mirznanii.com>

25. Информационная безопасность образовательных учреждений в контексте противодействия угрозам терроризма и экстремизма. Каберник Виталий Владимирович. Начальник отдела перспективных научно-образовательных разработок МГИМО (У) МИД России. Москва 2012г. Режим доступа:- <http://mirznanii.com>

26. Информационная безопасность.[Электронный ресурс]. Режим доступа:- <https://dic.academic.ru/dic.nsf/ruwiki/8410>

27. Информационная безопасность.[Электронный ресурс]. Режим доступа:- <http://mirznanii.com/a/113170/informatsionnaya-bezopasnost>
28. Информационная безопасность и защита информации. Учебное пособие – М.: 2004 – 82 с.
29. Информационная безопасность: учебно-практическое пособие. Башлы П. Н., Баранова Е. К., Бабаш А. В. Евразийский открытый институт. 2011 г. 375 с
30. Информатика и ИКТ. Мультимедийные средства в образовании : учебник / В.В. Андреев, Н.В. Герова, А.А. Москвитина, О.М. Роговая ; РГУ им. С.А. Есенина. – Рязань, 2012. – 128 с.
31. Информационные технологии.[Электронный ресурс]. Режим доступа: - <http://mirznanii.com>
32. Колганов, А. Системы мультимедиа сегодня [Текст] / Александр Колганов // Компьютер-Пресс. — 1995. — № 4.
33. Компьютер-ИНФО – Средства разработки мультимедиа [Электронный ресурс]: [справочный листок] – Компьютер-ИНФО, 2010. – Режим доступа:- <http://inftech.webservis.ru/it/multimedia/ar10.htm>
34. ЛОКАЛЬНЫЙ НОРМАТИВНЫЙ АКТ. Правила информационной безопасности. Министерство образования и науки Пермского края ГБПОУ «Чайковский индустриальный колледж» . 2015г
35. Лопатин В.Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества. М.: 2000. – 428 с.
36. Мультимедиа в образовании.[Электронный ресурс]. Режим доступа:- <http://multiru.ru/solutions=18>
37. Мультимедийные средства обучения. [Электронный ресурс]. Режим доступа:- <http://pandia.ru/text/78/187/61976.php>
38. Методические основы проектирования электронных образовательных ресурсов, Соловое А.В., Меньшикова А.А., Клентак Л.С., 2013.
39. Обзор Help&Manual. [Электронный ресурс]. Режим доступа: - <http://www.ixbt.com/soft/help-and-manual.shtml>

40. Образование и XXI век: Информационные и коммуникационные технологии. – Отв. ред. Кинелев В.Г. – М.: Наука. – 1999.

41. Осин А.В. Предпосылки концепции образовательных электронных изданий //Материалы научно-практической конференции «Основные направления развития электронных образовательных изданий и ресурсов» – М.: РМЦ. – 2002.

42. Политика информационной безопасности областного государственного автономного профессионального образовательного учреждения «Старооскольский педагогический колледж»

43. Полат Е.С., Бухаркина М.Ю. Новые информационные технологии. - М.: Академия, 1999. - 220с.

44. Применение мультимедиа в педагогическом процессе.[Электронный ресурс]. Режим доступа: http://otherreferats.allbest.ru/pedagogics/00051348_0.html

45. Реферат.Тема: Методы защиты информации.[Электронный ресурс]. Режим доступа:- <http://mirznanii.com>

46. Руководство по качеству. ЮУрГТК 2015

47. Свободная энциклопедия «Википедия» (<http://ru.wikipedia.org/wiki/Мультимедиа>)

48. Смолянинова О.Г. Мультимедиа в образовании (теоретические основы и методика использования). – Красноярск: КрГУ. – 2002.

49. Терехов А.В, Чернышев А.В, Чернышев В.Н. Учебное пособие ТГТУ 2007-128 с.

50. Толково-словообразовательный словарь Ефремовой. Новый словарь русского языка [Текст] / Т. Ф. Ефремова. — Москва : Рус. яз., 2000.

51. Требования к архитектуре мультимедиа-систем[Электронный ресурс]. Режим доступа:- https://studopedia.su/6_56344_trebovaniya-k-arhitecture-multimedia-sistem.html

52. Тропченко, А. Ю. Методы сжатия изображений, аудиосигналов и видео [Текст] : учебное пособие по дисциплине «Теоретическая информатика» / А. Ю. Тропченко, А. А. Тропченко. — СПб. : СПбГУ ИТМО, 2009.

53. Тэй, В. Мультимедиа [Текст] : практическое руководство / Воган Тэй. — Минск : Попурри, 1997.
54. Тульский государственный университет. Кафедра технологии полиграфического производства и защиты информации. Контрольная работа по дисциплине «Теория информационной безопасности и методология защиты информации».[Электронный ресурс]. Режим доступа:- <http://mirznanii.com>
55. Угрозы информационным системам. Факторы, приводящие к информационным потерям. [Электронный ресурс]. Режим доступа:- http://andrey-2119163.narod.ru/protect_data/lecture_01.htm
56. Фролов А. В, Фролов Г. В Осторожно: компьютерные вирусы. М. 2003.
57. Чем открыть – Adobe Premiere [Электронный ресурс]: [справочный листок] – Чем открыть, 2012. – Режим доступа: http://chem-otkrit.ru/soft/Adobe_Premiere
58. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2008. – 544 с.
59. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. – М.: Книжный мир, 2009. – 352 с.
60. Этапы разработки мультимедийного проекта. [Электронный ресурс]. Режим доступа:- <http://megaobuchalka.ru/6/23483.html>
61. Якушин, А. В. Мультимедийные технологии [Электронный ресурс] : лекционный курс / А. В. Якушин. — Режим доступа: http://www.tula.net/tgpu/resouces/yakushin/html_doc/doc08/doc08index. — Загл. с экрана
62. Danger – Программные средства для создания и редактирования элементов мультимедиа [Электронный ресурс]: [справочный листок] – Danger, 2011. – Режим доступа: <http://dander.ru/gos/43.html>
63. Interface – Adobe Flash Professional [Электронный ресурс]: [справочный листок] – Interface, 2008. – Режим доступа: <http://www.interface.ru/home.asp?artId=6651>

64. SunRav Software – SunRav BookReader [Электронный ресурс]: [справочный листок] – SunRav Software, 2013. – Режим доступа: <http://www.sunrav.ru/docs/bookoffice/bookeditor/bookeditor.pdf>