Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

КОМПЛЕКС ЭЛЕКТРОННЫХ МАТЕРИАЛОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Информатика и вычислительная техника»
профилизации «Компьютерные технологии»

Идентификационный номер ВКР: 609

Екатеринбург 2018

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

К ЗАЩИТЕ ДОПУСКАЮ
Заведующая кафедрой ИС
_____ Н. С. Толстова
«____» _____ 2018 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

КОМПЛЕКС ЭЛЕКТРОННЫХ МАТЕРИАЛОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Исполнитель:
обучающаяся группы ЗКТ-401С О. В. Козырева
Руководитель:
канд. пед. наук, доцент И. А. Суслова
Нормоконтролер: Н. В. Хохлова

Екатеринбург 2018

АННОТАЦИЯ

Выпускная квалификационная работа состоит из комплекса электронных материалов и пояснительной записки на 54 страницах, содержащей 23 рисунка, 2 таблицы, 39 источников литературы и 1 приложение на 1 странице.

Ключевые слова: КОМПЛЕКС ЭЛЕКТРОННЫХ МАТЕРИАЛОВ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КОМПЬЮТЕРНЫЙ ВИРУС, СТАНДАРТ, WEBSITE X5.

Козырева, О. В. Комплекс электронных материалов «Информационная безопасность»: выпускная квалификационная работа / О. В. Козырева; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2018. — 54 с.

В работе рассмотрены вопросы обеспечения информационной безопасности.

Целью работы является разработка комплекса электронных материалов «Информационная безопасность». Для достижения цели было проанализировано федеральное законодательство и стандарты в области информационной безопасности; проанализирована литература и интернет-источники по теме: «Информационная безопасность»; проанализирована рабочая программа по дисциплине «Информатика и информационно-коммуникационные технологии» с целью выделения требований, предъявляемых к формированию знаний и умений при изучении раздела «Информационная безопасность», а также спроектирована структура, реализованы интерфейс, функционал и наполнение программного продукта «Комплекс электронных материалов “Информационная безопасность”».

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность выпускной квалификационной работы заключается в том, что информация, выступает основой всего процесса управления организации и заключается в её сборе, изучении, обработке.

От уровня организации сбора, обработки и передачи информации в целом зависит эффективность управления организации.

Обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле её состояния, выявлении её узких и слабых мест и противоправных действий.

Безопасность информации может быть обеспечена лишь при комплексном использовании всех имеющихся средств защиты, во всех структурных элементах производственной системы и на всех этапах технологического цикла обработки информации. Наибольший эффект достигается тогда, когда все используемые средства, методы и меры объединяются в единый целостный механизм — систему защиты информации (СЗИ). При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий.

Актуальность выбранной темы состоит в том, что для эффективной информационной безопасности нам необходимо составить комплекс электронных материалов.

Федеральный государственный образовательный стандарт (ФГОС) — совокупность обязательных требований к образованию определённого уровня и (или) к профессии, специальности и направлению подготовки, утверждённых федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в сфере образования. Настоящий Федеральный государ-

ственный образовательный стандарт представляет собой совокупность обязательных требований к среднему профессиональному образованию по специальности для профессиональной образовательной организации [21].

Объект работы является процесс обучения проблемам обеспечения информационной безопасности.

Предмет работы — учебные материалы по теме «Информационная безопасность и защита информации».

Цель работы: разработать комплекс электронных материалов «Информационная безопасность».

Задачи работы:

1. Проанализировать литературу и интернет-источники по теме «Информационная безопасность».

2. Проанализировать рабочую программу по дисциплине «Информатика и информационно-коммуникационные технологии» с целью выделения требований, предъявляемых к формированию знаний и умений при изучении раздела «Информационная безопасность».

3. Спроектировать структуру, реализовать интерфейс, функционал и наполнение программного продукта «Комплекс электронных материалов “Информационная безопасность”».

1 ОБЗОР ЛИТЕРАТУРЫ И ИНТЕРНЕТ-ИСТОЧНИКОВ ПО ТЕМЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

1.1 Обзор литературы и интернет-источников

1.1.1 Обзор литературы

Для разработки программного продукта «Комплекса электронных материалов», необходимо проанализировать литературу, что позволит понять теоретическую сторону и систематизировать материал.

В XXI веке проблема информационной безопасности стоит ребром. С совершенствованием существующих технологий хранения, передачи и обработки информации, а также с появлением новых, возникает всё больше потенциальных уязвимостей.

Подборка литературы содержит актуальные книги по информационной безопасности, которые позволяют оставаться в курсе последних тенденций развития данной области.

Книга Ю. А. Родичева «Нормативная база и стандарты в области информационной безопасности». Это учебное пособие, выпущенное в 2017 году, является одним из самых последних изданий по информационной безопасности. В нём рассмотрены наиболее важные нормативные документы Федеральной службы по техническому и экспортному контролю, а также международные и национальные стандарты Российской Федерации в области информационной безопасности. Издание предназначено дня студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности, слушателей курсов повышения квалификации по проблемам зашиты информации [27].

Книга А. В. Бабаш, Е. К. Барановой и Д. А. Ларина «Информационная безопасность. История защиты информации в России». Это учебное пособие,

выпущенное 2015 году, является ретроспективой в историю отечественной криптографии, начиная с её истоков в IX веке. В нём подробно разбираются вопросы рождения и становления российского криптоанализа, много внимания уделено виднейшим специалистам в этой сфере, а также личностям, связанным с криптографией: революционерам, разведчикам. Оно создано на основе множества исторических документов. Цель издания — популяризация криптографического подхода к защите информации и всестороннее ознакомление студентов с историческими предпосылками в данной области. Данная книга предназначена, как учебное пособие для студентов технических специальностей, но будет интересна всем, кто интересуется криптографией [3].

Книга Е. К. Барановой и А. В. Бабаш «Информационная безопасность и защита информации». Ещё одно учебное пособие от авторов «Истории защиты информации в России», посвящённое рассмотрению базовых вопросов информационной безопасности. Третье издание переработано и дополнено в соответствии с последними изменениями в сфере защиты информации, выпущено в 2016 году [2].

Книга В. В. Бондарева «Введение в информационную безопасность автоматизированных систем». В книге рассмотрена законодательная база информационной безопасности, приведён перечень основных возможных угроз, а также описываются подходы к созданию систем защиты информации. Здесь также приводится классификация предупредительных мер. Изучены вопросы программно-аппаратных механизмов обеспечения информационной безопасности. Книга выпущена в 2016 году [10].

Книга С. А. Нестерова «Основы информационной безопасности». В этой книге основательно и последовательно излагаются основы информационной безопасности, описываются практические аспекты её реализации. Читатель этой книги изучит: теоретические основы защиты информации; основы криптографии; защиту информации в IP-сетях; анализ и управление рисками в сфере информационной безопасности. Теоретический материал сопровождается лабораторными работами, выделенными в отдельный раздел.

Пособие может использоваться в системах повышения квалификации в рамках образовательной программы дополнительного профессионального образования «Информатика и вычислительная техника». Также может быть полезно широкому кругу специалистов в области информационных технологий. Книга выпущена в 2016 году [23].

Книга А. А. Бирюкова «Информационная безопасность: защита и нападение». Данная книга подойдёт системным администраторам, а также пользователям малых и средних сетей, осуществляющих защиту корпоративных ресурсов. В ней приводится как техническая информация об атаках и защите от них, так и рекомендации по организации процесса обеспечения информационной безопасности. Второе издание переработано в 2017 году в соответствии с последними тенденциями и содержит только самую актуальную информацию. Также оно обеспечивает более полное погружение в аспекты, связанные с проведением аудитов по безопасности и тестов на проникновение для различных систем. Подробно рассматриваются современные решения по маршрутизации, беспроводной связи и другим направлениям развития информационных технологий [8].

1.1.2 Обзор интернет-источников

Теоретическая информация по теме «Информационная безопасность» для разработки программного продукта. Для данной цели интернет-источники подходят намного лучше литературных источников, в силу своей актуальности.

Сайт «Хабрахабр» представляет собой электронный ресурс, посвящённый всевозможным областям индустрии информационных технологий. Он содержит много интересной для нас информации [31].

Электронная книга «Googling Security: How Much Does Google Know About You?» (Что Google знает о вас? И кто они говорят?) [34].

«Google наблюдает за вами» — такова главная идея данной книги. Авторы книги утверждают, что крупнейший в мире провайдер бесплатных веб-услуг на самом деле берёт со своих пользователей плату, только оплачивают они эти услуги не деньгами, а информацией о себе. Имея исчерпывающие данные о каждом пользователе, Google имеет огромный потенциал воздействия на социум. Авторы книги дают ряд советов, как оградить себя от всевидящего ока поискового гиганта.

Когда пользователь использует «бесплатные» услуги Google, он платит, большое время — с личной информацией о себе. Google зарабатывает состояние на том, что он знает о пользователе ... и каждый можете быть в шоке от того, насколько Google знает. Безопасность Google — первая книга, в которой рассказывается о том, как огромные информационные запасы Google могут использоваться против каждого человека или его бизнеса, и что пользователь может сделать, чтобы защитить себя.

В отличие от других книг по взлому Google, эта книга охватывает информацию, которую читатель раскрывает при использовании всех лучших приложений Google, а не только то, что опытные пользователи могут получить через результаты поиска Google. Профессор компьютерных наук Грег Конти West Point раскрывает последствия конфиденциальности Gmail, Google Maps, Google Talk, групп Google, Google Alerts, новых мобильных приложений Google и так далее. Опираясь на свои собственные исследования в области безопасности, Г. Конти показывает, как базы данных Google могут использоваться другими людьми с плохими намерениями, даже если Google преуспеет в своём обещании «не будь злым».

При прочтении данного издания исследователь раскроет след информационных «хлебных крошек», которые каждый из нас оставляет при использовании поиска Google как:

- Gmail можно использовать для отслеживания личной сети друзей, родственников и знакомых;

- инструменты карты и местоположения Google могут раскрывать местоположение дома каждого человека, имя его работодателя, семьи и друзей, планы поездок и намерения;
- информационные запасы Google и других онлайн-компаний могут быть разлиты, потеряны, приняты, переданы или вызваны в суд, а затем использованы для кражи личных данных или даже шантажа;
- рекламные услуги Google AdSense и DoubleClick могут отслеживать пользователя по всему Интернету;
- систематически уменьшить личную информацию, которую каждый раскрывает или отдаёт.

Эта книга представляет собой пробуждающий звонок и руководство по самообороне. Является незаменимым ресурсом для всех, от частных граждан до профессионалов в области безопасности, которые полагаются на Google.

Электронная книга «Unmasking the Social Engineer: The Human Element of Security». (Развязывание социального инженера: «Человеческий элемент безопасности») [37]. Социальная инженерия, а проще говоря — мошенничество с использованием социальных сетей и современных технологий, — одна из ключевых угроз безопасности нашего времени. Книга посвящена современным методам социальной инженерии и позволяет идентифицировать мошенников среди клиентов и контрагентов.

Развязывание социального инженера: «Человеческий элемент безопасности» фокусируется на объединении науки понимания невербальных коммуникаций с пониманием того, как социальные инженеры, мошенники используют эти навыки для создания чувства доверия и взаимопонимания в своих целях.

1.1.3 Обзор стандартов в области информационной безопасности

Дальше будет проведён анализ федерального законодательства и стандартов в области информационной безопасности.

Закон Российской Федерации от 21.07.1993г. N 5485-1 (ред. от 08.03.2015) «О государственной тайне» [19] регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности.

Положения настоящего Закона обязательны для исполнения на территории Российской Федерации и за её пределами органами законодательной, исполнительной и судебной власти, а также организациями, наделёнными в соответствии с федеральным законом полномочиями осуществлять от имени Российской Федерации государственное управление в установленной сфере деятельности (далее — органы государственной власти), органами местного самоуправления, предприятиями, учреждениями и организациями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне.

Федеральный закон «О коммерческой тайне» от 29.07.2004 г. N 98-ФЗ регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства. Положения настоящего Федерального закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

Положения настоящего Федерального закона не распространяются на сведения, отнесённые в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. N 149-ФЗ регулирует отношения при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;

- применении информационных технологий;
- обеспечении защиты информации.

Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

Федеральный закон от 27.07.2006 г. N 152-ФЗ «О персональных данных» регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее — государственные органы), органами местного самоуправления, иными муниципальными органами (далее — муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

Государственный стандарт Российской Федерации (ГОСТ) Р 50922–2006 г. «Защита информации. Основные термины и определения» устанавливает основные термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации.

Термины, установленные настоящим стандартом, рекомендуется использовать в правовой, нормативной, технической и организационно-распорядительной документации, научной, учебной и справочной литературе: защита информации — деятельность, направленная на предотвращение

утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [19].

ГОСТ Р 51275–2006 г. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации, в целях обоснования угроз безопасности информации и требований по защите информации на объекте информатизации. Настоящий стандарт распространяется на объекты информатизации, создаваемые и эксплуатируемые в различных областях деятельности (обороны, экономики, науки и других областях).

ГОСТ Р ИСО/МЭК 17799–2005 г. «Информационная технология. Практические правила управления информационной безопасностью» устанавливает рекомендации по управлению информационной безопасностью лицам, ответственным за планирование, реализацию или поддержку решений безопасности в организации. Он предназначен для обеспечения общих основ для разработки стандартов безопасности и выбора практических мероприятий по управлению безопасностью в организации, а также в интересах обеспечения доверия в деловых отношениях между организациями. Рекомендации настоящего стандарта следует выбирать и использовать в соответствии с действующим законодательством.

ГОСТ Р ИСО/МЭК ТО 13335–4–2007 г. «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер» является руководством по выбору защитных мер с учётом потребностей и проблем безопасности организации. В настоящем стандарте описан процесс выбора защитных мер в соответствии с риском системы безопасности и с учётом особенностей окружающей среды. Настоящий стандарт устанавливает способы достижения соответствующей защиты на основе базового уровня безопасности. Приведённый в настоящем стандарте подход к выбору защитных мер согласован с методами управления безопасностью информационных технологий, приведёнными в ИСО/МЭК ТО 13335–3.

ГОСТ Р 51188–98 г. «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство» распространяется на испытания программных средств (ПС) и их компонентов, цели которых — обнаружить в этих ПС и устранить из них компьютерные вирусы (КВ) силами специальных предприятий (подразделений), и устанавливает общие требования к организации и проведению таких испытаний.

Требования, установленные настоящим стандартом, направлены на обеспечение специальной обработки ПС в целях выявления КВ, а также на устранение последствий, вызванных возможными воздействиями КВ на операционные системы, системные и пользовательские файлы с программами и данными, начальные секторы магнитных дисков, таблицы размещения файлов.

Настоящий стандарт устанавливает типовые требования, предъявляемые к испытаниям ПС на наличие КВ.

ГОСТ Р 51898–2002 г. «Аспекты безопасности. Правила включения в стандарты» устанавливает для разработчиков стандартов правила включения в стандарты аспектов безопасности. Стандарт может быть применён к любым аспектам безопасности, относящимся к людям или имуществу, или окружающей среде, или к сочетанию этих сторон.

Правила, устанавливаемые настоящим стандартом, основаны на уменьшении риска, возникающего при использовании продукции, процессов или услуг.

Стандарт рассматривает полный жизненный цикл продукции, процесса или услуги, включая как предназначенное использование, так и возможное предсказуемое неправильное использование.

ГОСТ Р 52069.0–2003 г. «Защита информации. Система стандартов. Основные положения». Настоящий стандарт устанавливает цель и задачи системы стандартов по защите информации, объекты стандартизации, структуру, состав и классификацию входящих в неё стандартов и правила их обозначения.

Положения настоящего стандарта являются рекомендуемыми при разработке нормативных документов по стандартизации в области защиты информации, независимо от организационно-правовой формы и формы собственности предприятия, учреждения, организации-разработчика стандарта, а также при организации работ по стандартизации в области защиты информации органами управления Российской Федерации.

Стандарт является основополагающим государственным стандартом Российской Федерации в области защиты информации.

ГОСТ Р 53114–2008 г. «Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» (утверждён и введён в действие Приказом Ростехрегулирования от 18.12.2008 г. N 532-ст) из информационного банка «Отраслевые технические нормы». Настоящий стандарт устанавливает основные термины, применяемые при проведении работ по стандартизации в области обеспечения информационной безопасности в организации [19]. Термины, установленные настоящим стандартом, рекомендуется использовать в нормативных документах, правовой, технической и организационно-распорядительной документации, научной, учебной и справочной литературе.

1.2 Обзор рабочей программы

Рабочая программа учебной дисциплины «Информатика и информационно-коммуникационные технологии» является частью программы подготовки специалистов среднего звена по специальностям среднего профессионального обучения (СПО) технического профиля 13.02.01 Тепловые электрические станции, 13.02.03 Электрические станции, сети и системы и 13.02.06 Релейная защита и автоматизация электроэнергетических систем, реализуемых в Государственном автономном профессиональном образовательном

учреждении Свердловской области «Екатеринбургский энергетический техникум».

Дисциплина является профильной дисциплиной общеобразовательного цикла учебных планов по специальностям СПО с учётом профиля получаемого профессионального образования. В результате освоения учебной дисциплины обучающийся должен уметь:

- применять знания основ правовых аспектов использования компьютерных программ и работы в Интернете;
- применять навыки логического и алгоритмического мышления, формально описывать алгоритм;
- понимать программы, написанные на выбранном для изучения универсальном алгоритмическом языке высокого уровня, анализировать алгоритмы с использованием таблиц;
- записывать на алгоритмическом языке программы для решения стандартной задачи с использованием основных конструкций программирования и отладки таких программ;
- использовать готовые прикладные компьютерные программы по выбранной специализации;
- использовать готовые компьютерные программы при решении задач;
- анализировать соответствие модели моделируемому объекту (процессу);
- работать с базами данных;
- использовать компьютерные средства представления и анализа данных;
- соблюдать требования техники безопасности, гигиены и ресурсосбережения при работе со средствами информатизации;
- использовать компьютерные средства представления и анализа данных;

- строить математические объекты информатики, в том числе логические формулы;
- применять основные алгоритмы обработки числовой и текстовой информации, алгоритмы поиска и сортировки;
- применять полученные знания при решении различных задач.

В результате освоения учебной дисциплины обучающийся должен знать:

- роль информации и связанных с ней процессов в окружающем мире;
- основы правовых аспектов использования компьютерных программ и работы в Интернете;
- роль информатики и информационных технологий в современном обществе, специфику социального, экономического, политического, культурного, юридического, природного, эргономического, медицинского и физиологического контекстов информационных технологий;
- социальные, культурные и исторические факторы становления информатики;
- вклад информатики в формирование современной научной картины мира;
- этические аспекты информационных технологий;
- стандартные приёмы написания на алгоритмическом языке программы для решения стандартной задачи с использованием основных конструкций программирования и отладки таких программ;
- компьютерно-математические модели и способы анализа соответствия модели и моделируемого объекта (процесса);
- приёмы алгоритмического мышления и способы формального описания алгоритмов;
- основные конструкции языка программирования;
- способы хранения и простейшей обработки данных;

- компьютерные средства представления и анализа данных;
- требования техники безопасности, гигиены и ресурсосбережения при работе со средствами информатизации;
- важнейшие виды дискретных объектов, их простейшие свойства, алгоритмы анализа этих объектов, кодировании и декодировании данных и причины искажения данных при передаче;
- устройство современных компьютеров, тенденции развития компьютерных технологий;
- понятие «операционная система» и основных функциях операционных систем;
- роль компьютерных сетей в современном мире; базовые принципы организации и функционирования компьютерных сетей, нормы информационной этики и права, принципы обеспечения информационной безопасности, способов и средств обеспечения надёжного функционирования средств информационных технологий;
- основные алгоритмы обработки числовой и текстовой информации, алгоритмы поиска и сортировки.

Целью освоения раздела «Информационная безопасность и защита информации» является формирование у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

Задачи освоения раздела: формирование умения обеспечить защиту информации и объектов информатизации; формирование умения составлять заявительную документацию в надзорные государственные органы инфокоммуникационной отрасли; формирование навыков выполнения работ в области технического регулирования, сертификации технических средств, систем, процессов, оборудования и материалов; формирование навыков обеспечения защиты объектов интеллектуальной собственности и результатов исследований и разработок, как коммерческой тайны предприятия; настройка и обслуживание аппаратно-программных средств.

Количество часов на освоение программы учебной дисциплины: максимальной учебной нагрузки обучающегося 143 часа, в том числе: обязательной аудиторной учебной нагрузки обучающегося 95 часов; самостоятельной работы обучающегося 48 часов.

Тематический план, отражающий содержание раздела (перечень тем), структурированное по видам учебных занятий с указанием их объёмов в соответствии с учебным планом, приведён в таблице 1.

Таблица 1 — Структура раздела «Информационная безопасность»

№	Название темы	Вид занятия	Объём час	Кол-во часов в интерактивной и электронной форме	СРС
1	Введение в информационную безопасность	Лекция	2	2 ч. интерактивная форма	5
2	Правовое обеспечение информационной безопасности	Лекция	2	2 ч. интерактивная форма	5
3	Организационное обеспечение информационной безопасности	Лекция	2	2 ч. интерактивная форма	5
4	Технические средства и методы защиты информации	Лекция	2	2 ч. интерактивная форма	5
5	Программно-аппаратные средства и методы обеспечения информационной безопасности	Лекция	4	4 ч. интерактивная форма	5
6	Криптографические методы защиты информации	Лекция	2	2 ч. интерактивная форма	5

Окончание таблицы 1

7	Настройки учётных записей пользователей. Одноразовые блокноты	Лабораторная работа	2	1 ч. интерактивная форма / 1 ч. электронная форма	6
8	Антивирусные средства защиты информации	Лабораторная работа	2	1 ч. интерактивная форма / 1 ч. электронная форма	6
9	Защита ПК от несанкционированного доступа	Лабораторная работа	2	1 ч. интерактивная форма / 1 ч. электронная форма	6
10	Электронная цифровая подпись	Лабораторная работа	2	1 ч. интерактивная форма / 1 ч. электронная форма	6
11	Реализация дискреционной модели политики безопасности	Лабораторная работа	2	1 ч. интерактивная форма / 1 ч. электронная форма	6
12	Количественная оценка стойкости парольной защиты. Ассиметричные алгоритмы шифрования данных	Лабораторная работа	2	1 ч. интерактивная форма / 1 ч. электронная форма	6

Текущая самостоятельная работа по разделу «Информационная безопасность» направлена на углубление и закрепление знаний, на развитие практических умений и включает такие виды работ, как:

- работа с лекционным материалом;
- работа с рекомендованной литературой при подготовке к практическим занятиям;
- подготовка к зачёту.

Текущий контроль (ТК) — основная часть рейтинговой системы, основанная на беглом опросе раз в неделю или в две недели. Формы: оценка за сдачу теоретических мини зачётов, выполнение индивидуальных заданий и лабораторных работ. Важнейшей формой ТК, позволяющей опросить всех студентов на одном занятии являются теоретические модули, на которых студенты самостоятельно отвечают на вопросы для самостоятельной оценки.

2 ОПИСАНИЕ КОМПЛЕКСА ЭЛЕКТРОННЫХ МАТЕРИАЛОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

2.1 Педагогический адрес

Программный продукт «Комплекс электронных материалов “Информационная безопасность”» предназначен для студентов специальностей среднего профессионального образования технического профиля 13.02.01 Тепловые электрические станции, 13.02.03 Электрические станции, сети и системы и 13.02.06 Релейная защита и автоматизация электроэнергетических систем Государственного автономного профессионального образовательного учреждения Свердловской области «Екатеринбургский энергетический техникум» изучающих раздел «Информационная безопасность» дисциплины «Информатика и информационно-коммуникационные технологии».

2.2 Описание средства реализации и подходов к созданию комплекса электронных материалов

WebSite X5 — это компьютерная оффлайн программа для создания веб-сайтов.

Для многих пользователей онлайновые конструкторы сайтов стали привычными в использовании.

Для начала работы с WebSite X5 Evolution 10 необходимо скачать программное обеспечение и установить его себе на компьютер под Windows. Хостинг покупается отдельно. Порядок оплаты услуг системы также иной — едино разовая покупка движка обеспечит полноценное владение/распоряжение ими без ограничений и необходимости периодического внесения абонентской платы [38].

Программный продукт предназначен для быстрой и качественной подготовки пользователей к работе. При создании комплекса электронных материалов необходимо учитывать специфику этого продукта и руководствоваться требованиями к проектированию подобных средств. То есть, её содержание должно быть структурированным, информация тщательно подобрана, текст формулировок должен исключать двусмысленность, быть лаконичным и понятным; оформление должно быть эстетичным и соответствовать задаваемой тематике; контраст текста и общего фона не должен утомлять глаза, материал должен располагаться в центре окна; визуально должны выделяться зона заголовка, навигации и информационного блока; система навигации должна быть понятной.

Комплекс электронных материалов содержит:

- титульный лист;
- краткое изложение материала, сопровождающееся видеороликами, рисунками, схемами;
- удобную навигацию;
- инструкции по применению.

Основными функциональными возможностями программного продукта должны быть:

- информация об аудите информационной безопасности, их классификации, технологии работы;
- обеспечение доступности и понимания изложенного материала путём использования иллюстрированных примеров, с фрагментами мультимедиа;
- удобный интерфейс.

Состав программной документации должен включать следующие документы:

- описание программы, включающее общие сведения о программе, описание её логической структуры, используемые технические средства, этапы её реализации;

- инструкция пользователя, содержащая общие сведения о программе, о её структуре и необходимых параметрах установки.

Разработка программы должна выполняться по следующим этапам:

1) сбор и структурирование материала по теме «Информационная безопасность», выделение существенных моментов;

2) создание сценария взаимодействия разделов теоретического материала, логической последовательности;

3) обзор средств мультимедиа с целью определения наиболее подходящих для создания комплекса электронных материалов;

4) создание видеоматериалов;

5) разработка оформления;

6) оформление материала в виде комплекса электронных материалов;

7) проверка работоспособности продукта и внесение коррективов;

8) публикация комплекса электронных материалов.

Во время реализации этапов создания комплекса электронных материалов могут быть внесены корректировки.

Программный продукт представляет собой набор связанных между собой html-документов и был разработан при использовании программ:

- WebSite X5 Evolution 10;
- блокнот;
- iSpring QuizMaker.

Для начала работы с комплексом электронных материалов необходимо было открыть файл «index.html».

После запуска страницы, открывается меню программного продукта комплекса электронных материалов.

На главной странице находится меню навигации по всему комплексу электронных материалов. Из любого блока можно перейти в любой интересующий блок и выбрать соответствующий раздел.

Психологические особенности восприятия педагогического программного продукта предполагают соблюдение некоторых правил. Классическое

соотношение чёрного и белого не даёт эмоционального включения, а потому все творческие воплощения сопровождаются цветовым сопровождением. Есть три основных цвета: красный (# ff0000 в HTML или # F00 в CSS), жёлтый (# FFFF00 в HTML или # ff0 в CSS) и голубой (# 0000FF в HTML или # 00f в CSS). Нельзя их получить путём смешивания других цветов.

Дизайн и цвет. Возьмём за пример проекта — сайт, в процессе своего становления. На первом этапе, при разработке дизайна, цвета играют немаловажную роль при построении графических элементов, и насыщения концепции, вкладываемой заказчиком в продукт. На этом этапе цветовая гамма эмоционально подтверждает, либо идёт вразрез с содержательным графическим насыщением.

Например, красные фигуры кажутся меньше в сравнении с синими. Внутренний темп посетителя сайта замедляется с помощью синего и ускоряется красным, что обуславливает принятие, скорость принятия решения, на основе увиденного на странице.

Важным элементом является посыл заказчика: перспектива и рост (зелёный); стабильность и состоятельность (синий, серый, коричневый); агрессивность и власть (красный, чёрный); жизнерадостность, энергичность (жёлтый, оранжевый). На данном этапе за первые 20 секунд формируется первое отношение к самой странице сайте. Разработчики «угадывают» желания пользователей, и, по возможности их формируют. Грамотное использование цветов поможет отсеять целевую аудиторию, тем самым придав ощущение значимости избранным. Использование блеклости и смазанности, растягивает первое впечатление, смягчая его, незаметно переводя пользователя на четвёртый этап.

Второй и третий этап (вёрстка, программирование) в цветовом плане совершенствуют и окончательно интегрируют первый.

На четвёртом этапе, наполнение сайта, к эмоциональному восприятию добавляется содержательное. В данном случае, сам текст может либо контрастировать с первым этапом, либо дополнять его. Преимущества контраста в

общем удивлении пользователя, смешанности отношений, что может как заинтересовывать, так и разочаровывать, путать. Профессиональные разработчики способны формировать отношение потребителя с помощью комбинирования цветов, удерживая аудиторию.

Принцип пропорции. Данный принцип требует, чтобы различные объекты не были хаотично разбросаны по экрану.

Порядок. Объекты должны располагаться от верхнего левого угла экрана слева направо к нижнему правому углу экрана. Имеет смысл применять одни и те же цвета для различных блоков приложения.

Акцент. Выделение наиболее важного, которое должно быть воспринято в первую очередь.

Принцип равновесия. Равномерное расположение по экрану оптической тяжести изображения.

Принцип единства. Элементы изображения должны выглядеть взаимосвязано, правильно соотноситься по размеру, форме, цвету. Идентичные данные должны быть представлены однотипно. Для достижения единства в целом используются рамки, оси, поля.

Яркостные характеристики. Острота зрения при восприятии светлых объектов в 3–4 раза ниже, чем для тёмных. Светлые объекты на тёмном фоне обнаруживаются легче, чем тёмные на светлом.

Цветовые характеристики. Наиболее важными при выборе цветового решения можно считать следующие принципы: следует учитывать психофизиологическое воздействие на человека, а также глазу приятнее, если при оформлении используется нечётное число цветов 3 или 5 (1 уныло, 7 слишком пёстро).

При выборе гаммы для разрабатываемого сайта, необходимо принимать во внимание тот факт, что цвет может иметь всевозможные значения в различных культурах. Культурный аспект для цветной символики может

быть очень сильным, так что разработчик должен знать о том, какова аудитория сайта.

Существуют некоторые полезные советы, которые помогут разработчику в выборе правильной цветовой схемы для вашего сайта. Эти маленькие советы широко используют профессиональные веб-дизайнеры. Если хочется, чтобы текстовое содержимое было легко читаемым, выбирайте контрастные цвета. Используйте необходимое количество цветов. Минимальное количество цветов, может способствовать серости сайта. Если нужно привлечь пользователя, применяйте интенсивные цвета.

Можно найти дополнительные цветовые схемы приобщаясь чаще к природе. При использовании нескольких цветов большую роль играет их правильное сочетание.

2.3 Описание продукта и общая характеристика

«Комплекс электронных материалов» предназначен для изучения темы «Информационная безопасность». Программный продукт может использоваться при очной, заочной и (или) дистанционной формах обучения.

Наименование программного продукта: «Комплекс электронных материалов “Информационная безопасность”», в дальнейшем он будет именоваться «Комплекс».

В результате проведённой работы был создан комплекс в виде html-документов. Использование технологии разметки гипертекста позволяет использовать комплекс не только локально на персональном компьютере, но и разместить на веб-сервере.

Титульный лист комплекса приведён на рисунке 1.

Рисунок 1 — Внешний вид титульного листа комплекса

Внешний вид комплекса приведён на рисунке 2.

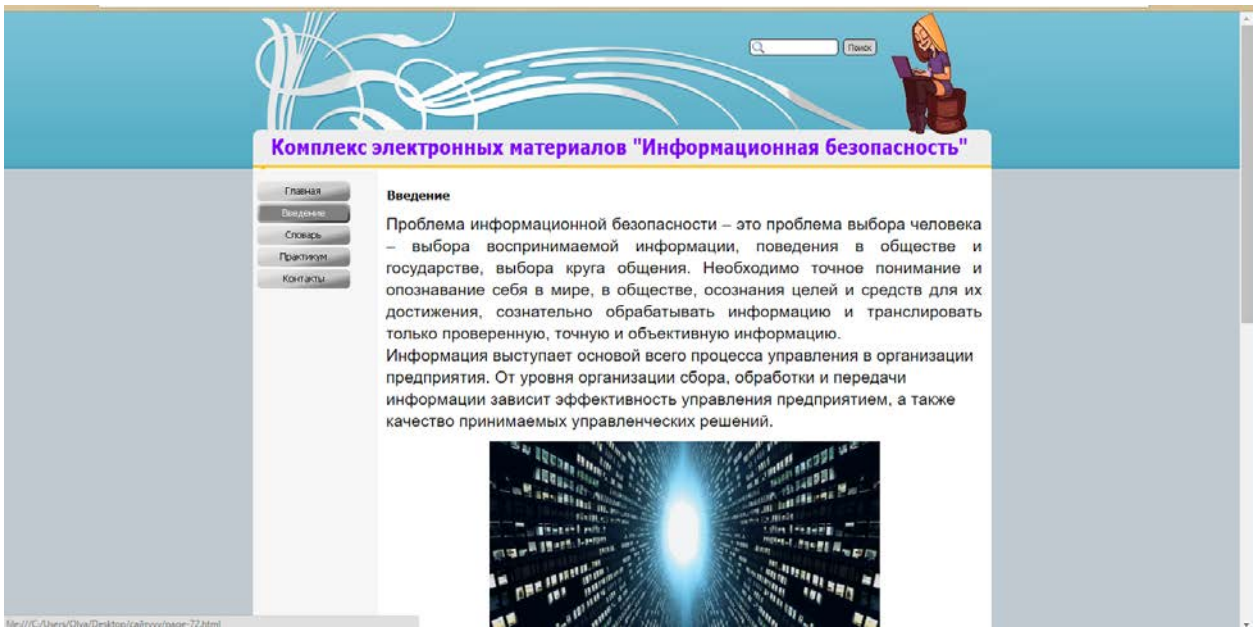


Рисунок 2 — Внешний вид комплекса

Комплекс включает следующие разделы:

- «Главная» — раздел содержит общую информацию о комплексе, информацию о разделах, минимальные требования к персональному компьютеру и программному обеспечению, а также указания по использованию комплекса для преподавателя и обучаемого;
- «Практикум» комплекса:

- «Лабораторные работы» — содержит базовые лабораторные работы по ознакомлению с основами информационной безопасности;
- «Контроль» — содержит набор тестовых заданий для самопроверки;
- «Словарь» — содержит теоретический материал, с возможностью представления в режиме по алфавиту; содержательное ядро комплекса;
- «Контакты» — раздел содержит указания общего характера.

В верхней части окна комплекса находится заголовок, в левой — панель навигации.

Также реализована возможность поиска страниц комплекса. Критерий — любое слово или сочетание букв каждой страницы. Для работы поиска необходимо разрешить заблокированное активное содержимое страницы в настройках браузера.

Комплекс содержит перекрёстные ссылки между страницами и всплывающие подсказки, рисунок 3.

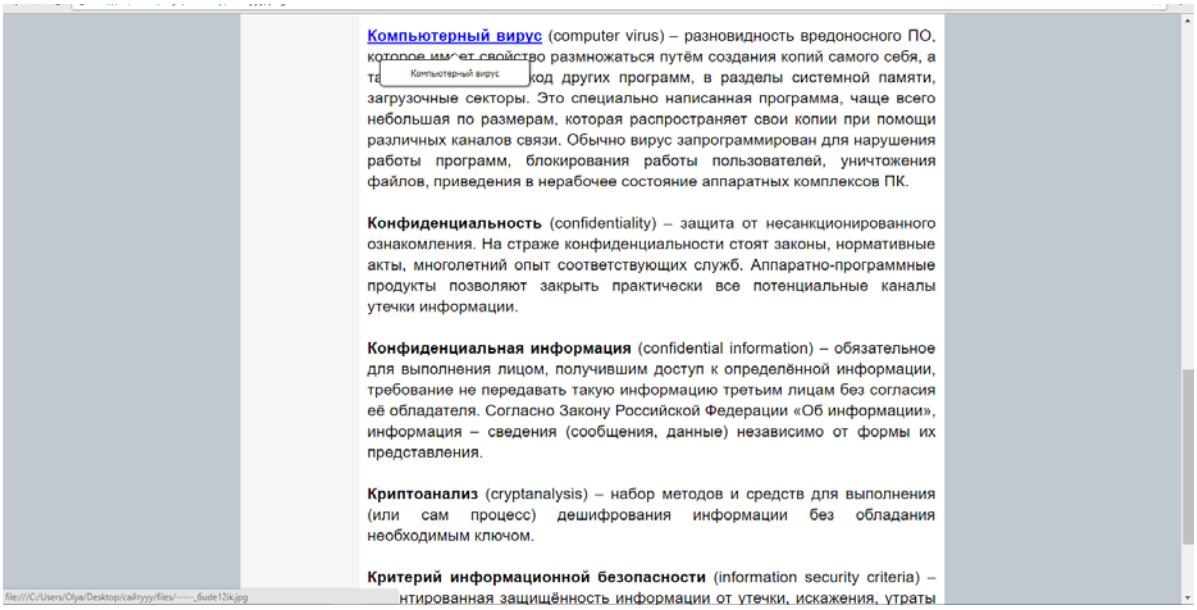


Рисунок 3 — Внешний вид всплывающей подсказки

Комплекс содержит презентацию, рисунок 4. Чтобы посмотреть пояснение к рисунку достаточно поднести курсор мыши к объекту на рисунке. В результате этого действия пользователя объект, над которым находится кур-

сор, поменяет цвет и появится пояснение. Документ прикреплённой презентации в формате .pdf.

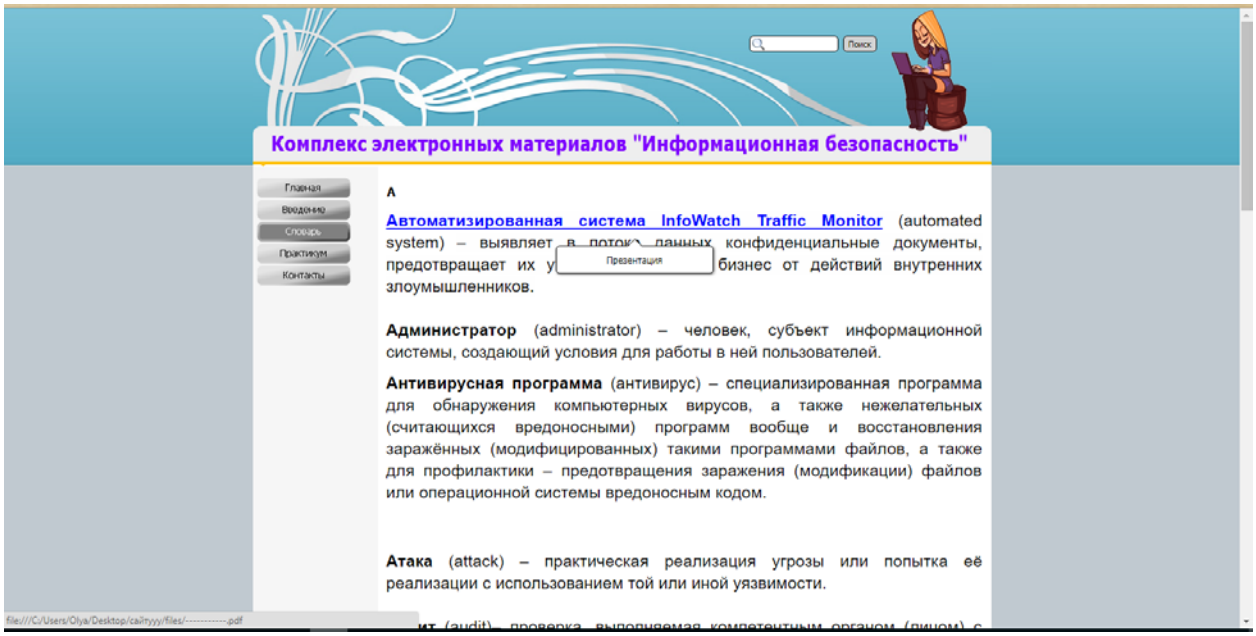


Рисунок 4 — Внешний вид страницы с демонстрацией прикреплённой презентации

Чтобы воспроизвести видео в комплексе, рисунок 5, достаточно поднести курсор мыши к объекту на тексте. В результате этого действия обучающегося студента, на экране монитора появится видео.

Рисунок 5 — Внешний вид страницы с запуском видео в комплексе

В комплексе представлены наглядные подсказки понятий в виде: изображений, схем, таблиц. Чтобы просмотреть картинку пользователю необхо-

димо поднести курсор мыши к объекту на тексте и перед ним откроется изображение, рисунок 6.

Рисунок 6 — Внешний вид страницы с примером картинки в комплексе

Пункт меню «Практикум» в комплексе является ссылкой на страницу с лабораторными работами. На рисунке 7 предусмотрена возможность контроля, которая заключается в прохождении лабораторных работ по изученной теме. После выполнения лабораторных работ отчёт необходимо выложить на сетевой диск.

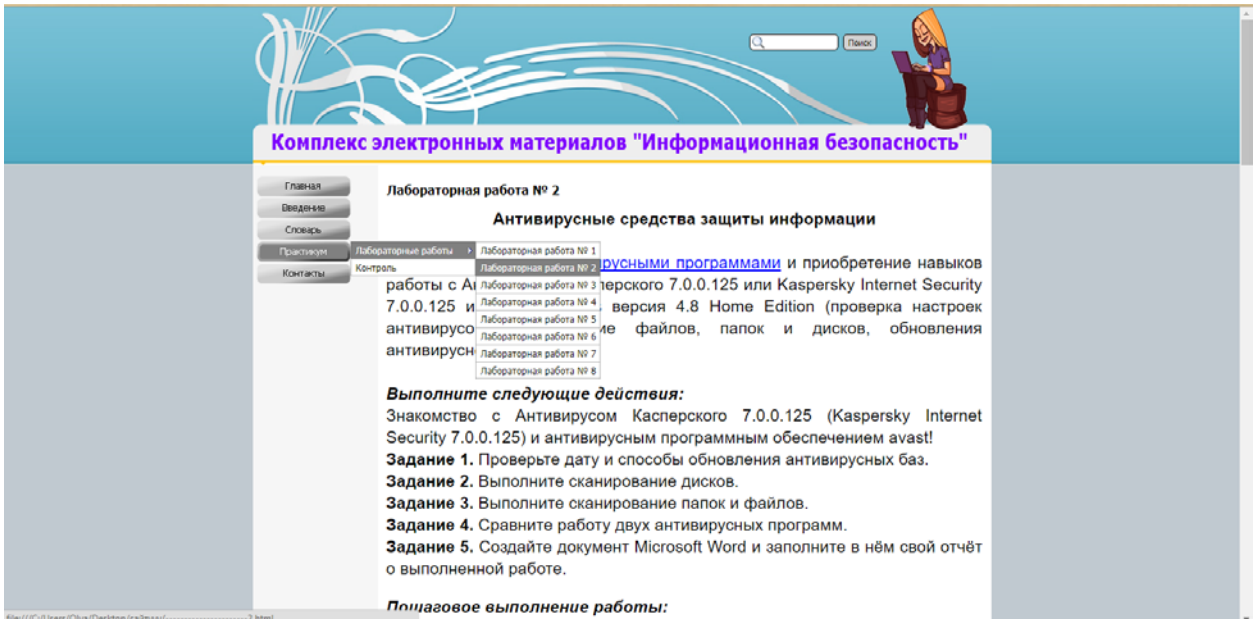


Рисунок 7 — Внешний вид страницы с лабораторной работой

2.4 Описание теоретического блока

Комплекс представляет собой отобранный и скомпонованный теоретический материал, представленный в удобной форме.

Содержание комплекса можно просматривать по алфавиту.

В режиме «Словарь» понятия разбиты по соответствующим им буквам русского алфавита. Для того чтобы перейти к требуемой статье необходимо выбрать букву, с которой начинается понятие, затем из представленного списка понятий, упорядоченных по алфавиту, выбрать необходимое.

Вид комплекса в режиме «Словарь» приведён на рисунке 8.

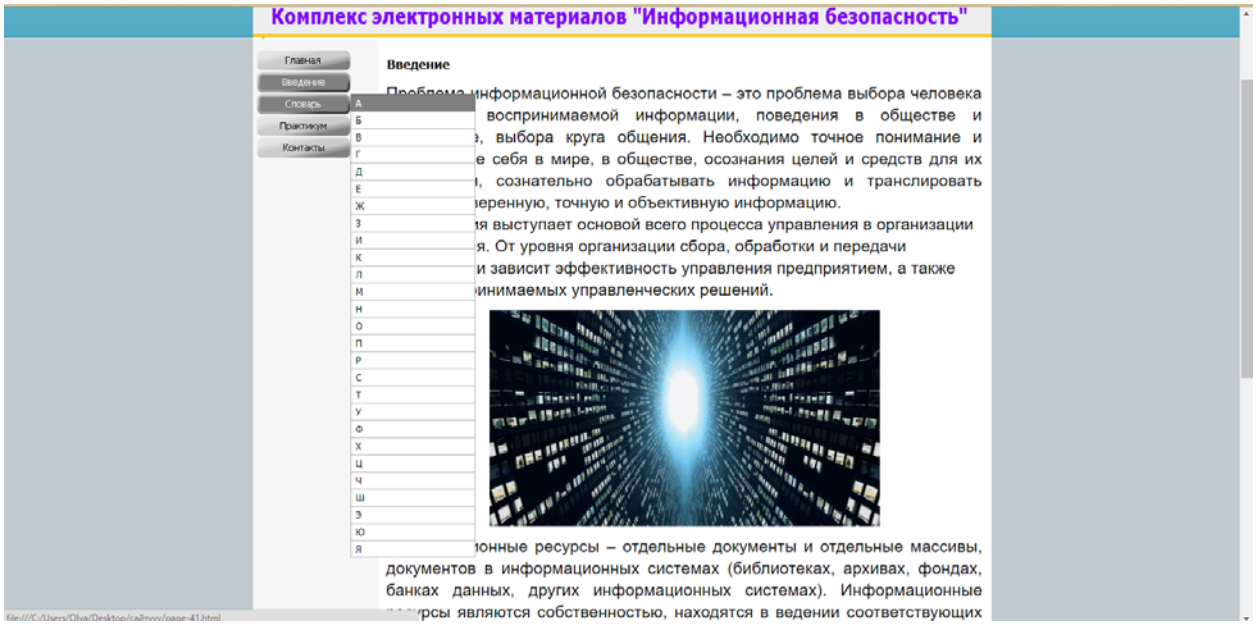


Рисунок 8 — Внешний вид комплекса в режиме «Словарь»

2.5 Описание контролирующего блока

В комплексе для возможности контроля представлен для прохождения тест по изученной теме. Контроль содержит вопросы с различными типами заданий. Тест состоит из 45 вопросов.

После прохождения теста сообщается его результат. Также после прохождения теста имеется возможность проанализировать допущенные ошибки, рисунок 9.

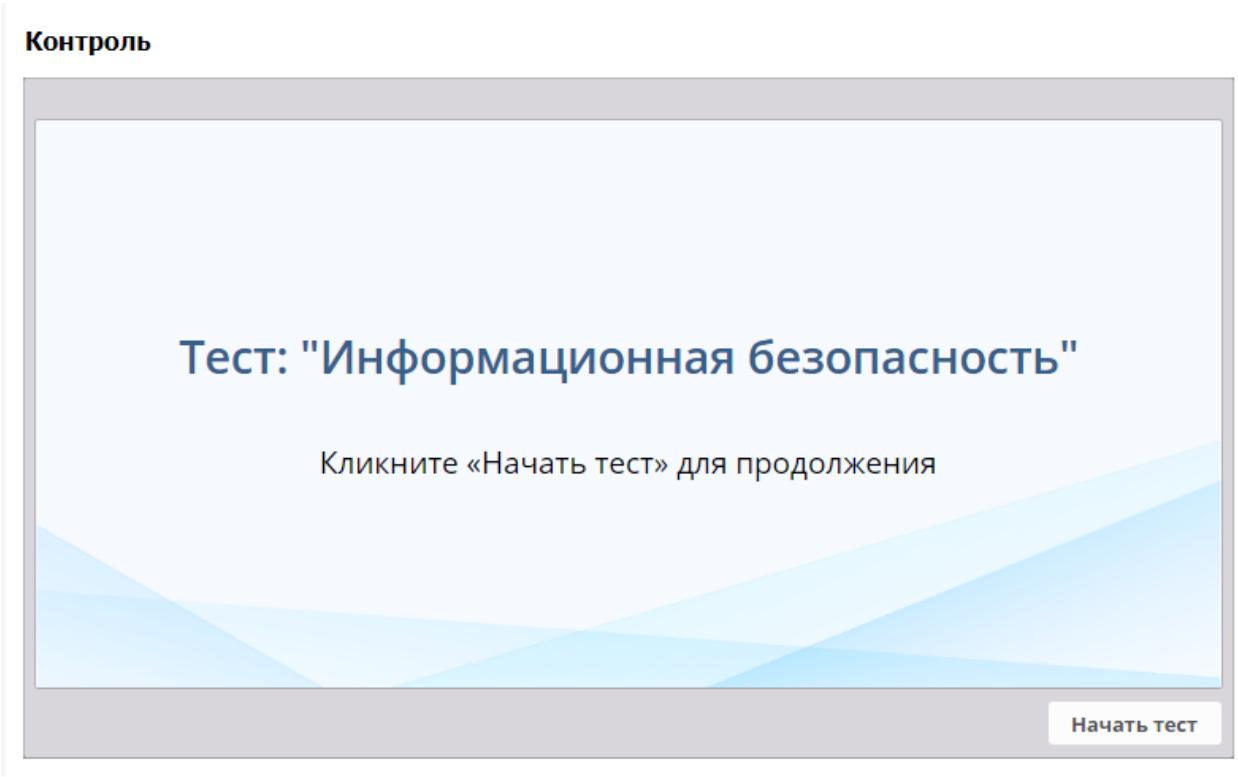


Рисунок 9 — Внешний вид страницы с размещённым тестовым заданием

2.6 Описание блока навигации

Навигация по комплексу осуществляется с помощью панели навигации. Главная панель навигации рисунок 10, находится в левой части окна, она предназначена для перемещения по основным структурным разделам комплекса.

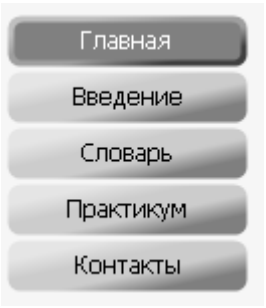


Рисунок 10 — Оформление главной панели навигации в комплексе

Ключевым фактором построения эффективного пользовательского интерфейса является понятная и грамотная навигация по сайту. Выпадающие меню идеально подходят для сайтов, в которых требуется реализовать мно-

гоуровневую иерархию разделов. Стандартная модель дизайна выпадающего меню заключается в наведении курсора мыши по основному разделу, после чего появляется вспомогательное меню, рисунок 11.

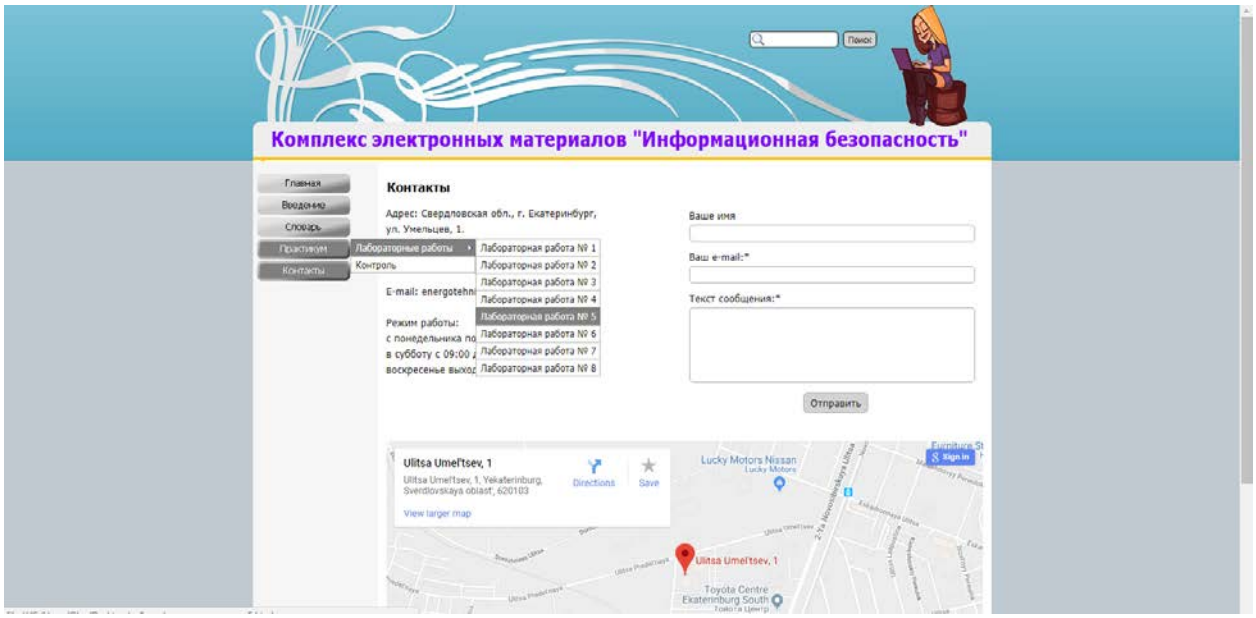
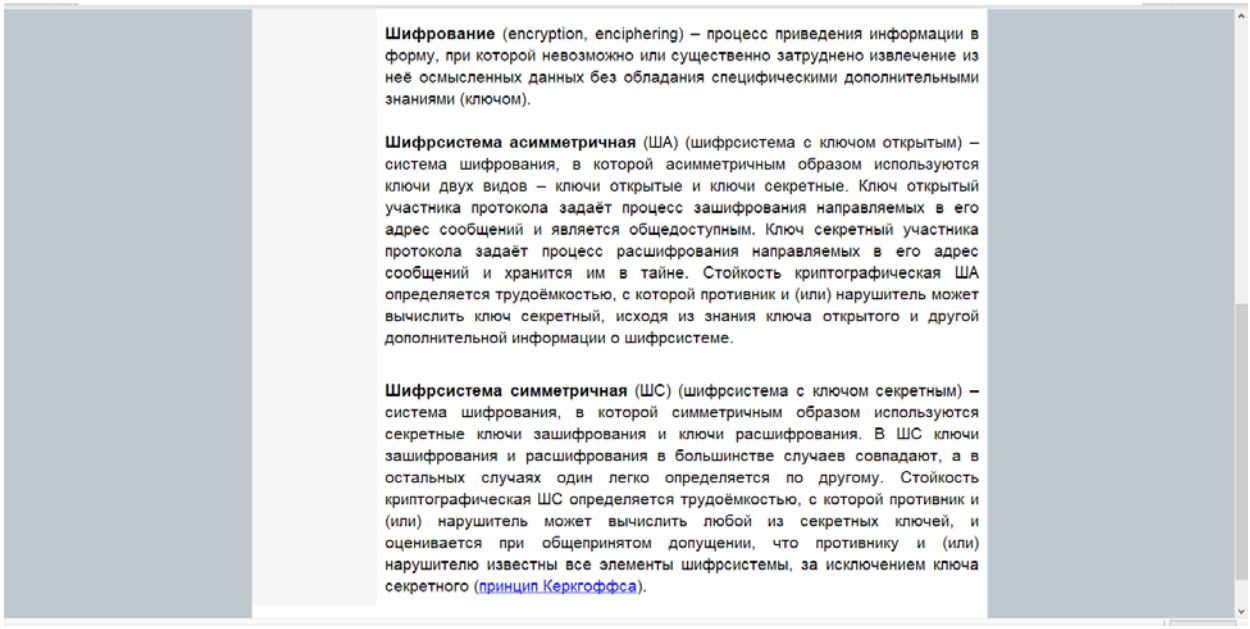


Рисунок 11 — Внешний вид всплывающего меню комплекса

В режиме «Словарь» по алфавиту после необходимых для работы определений содержатся ссылки на другие определения, связанные с данным понятием, рисунок 12.



Шифрование (encryption, enciphering) – процесс приведения информации в форму, при которой невозможно или существенно затруднено извлечение из неё осмысленных данных без обладания специфическими дополнительными знаниями (ключом).

Шифрсистема асимметричная (ША) (шифрсистема с ключом открытым) – система шифрования, в которой асимметричным образом используются ключи двух видов – ключи открытые и ключи секретные. Ключ открытый участника протокола задаёт процесс зашифрования направляемых в его адрес сообщений и является общедоступным. Ключ секретный участника протокола задаёт процесс расшифрования направляемых в его адрес сообщений и хранится им в тайне. Стойкость криптографическая ША определяется трудоёмкостью, с которой противник и (или) нарушитель может вычислить ключ секретный, исходя из знания ключа открытого и другой дополнительной информации о шифрсистеме.

Шифрсистема симметричная (ШС) (шифрсистема с ключом секретным) – система шифрования, в которой симметричным образом используются секретные ключи зашифрования и ключи расшифрования. В ШС ключи зашифрования и расшифрования в большинстве случаев совпадают, а в остальных случаях один легко определяется по другому. Стойкость криптографическая ШС определяется трудоёмкостью, с которой противник и (или) нарушитель может вычислить любой из секретных ключей, и оценивается при общепринятом допущении, что противнику и (или) нарушителю известны все элементы шифрсистемы, за исключением ключа секретного (принцип Керкгоффса).

Рисунок 12 — Внешний вид страницы с перекрёстными ссылками на другие понятия

Используя перекрёстные ссылки внутри страницы можно легко перемещаться по комплексу электронных материалов.

Если обучающийся студент, затрудняется в выборе необходимой страницы, к его услугам возможность поиска необходимой страницы по ключевым словам. Указав необходимую фразу в строку поиска (в правом верхнем углу экрана, под словом «Поиск»), пользователь, в результате выполнения алгоритма поиска, получит перечень страниц, наиболее подходящих для его запроса. Кнопка поиска по комплексу приведена на рисунке 13.

Рисунок 13 — Внешний вид страницы поиска по комплексу

2.7 Описание интерфейса и навигации

Продукт был разработан с помощью программы WebSite X5 Evolution 10 — это компьютерная оффлайн программа для создания веб-сайтов.

Многим пользователям онлайновые конструкторы сайтов стали привычны в использовании.

Для начала работы с WebSite X5 необходимо скачать программное обеспечение и установить его себе на компьютер под Windows [38].

В качестве платформы разработки комплекса была выбрана платформа WebSite X5 Evolution 10. Это обусловлено следующими факторами.

Над созданием WebSite X5 сплочённо работают 4 команды: поддержка, развитие, маркетинг и дизайн. Все, сотрудники Incomedia — компании, выросшей вокруг WebSite X5, — работают, чтобы создать продукт высокого качества. Реальные люди с реальными потребностями. Благодаря их советам и рекомендациям, появилась WebSite X5 10: быстрая и полноценная программа.

Программа позволяет активировать баннер с обязательной информацией о правовых нормах по защите конфиденциальности и файлах Cookie. В распоряжении функциональная онлайн-панель управления для доступа ко

всем данным веб-сайтов: статистике посещений, комментариям на страницах блога. С приложением WebSite X5 для iOS и Android можно следить за деятельностью сайтов даже со смартфона или планшета.

Полноценные адаптивные свойства, позволяющие пользователям просматривать сайт с мобильного устройства и выполнять простые действия со смартфона и планшета. Работая в визуальном режиме, можно настроить точки останова и определить размещение контента в зависимости от разрешения экрана с помощью адаптивной строки [38].

Представленный комплекс электронных материалов включает в себя теоретический материал, тестовые задания, лабораторные работы, презентации, фото и видеоматериалы. Для создания вышеперечисленного необходим комплекс специальных программ, позволяющий создавать HTML-страницы, из которых состоит данный продукт, а также программы для редактирования комплекса, создания объёмных изображений, видеоматериалов.

HTML-документы имеют ряд преимуществ:

- занимают меньший объём памяти, по сравнению с любыми текстовыми редакторами («сжимают» информацию в 2–10 раз);
- позволяют использовать фреймы — разграничители окна браузера, что облегчает работу с текстом;
- позволяют вставлять аудио и видео в документ;
- могут просматриваться различными типами веб-браузеров;
- предполагают возможность как автономной работы, так и работы в сети.

Таким образом, формат *.html* является наиболее подходящим для создания комплекса электронных материалов.

Наиболее простой способ создания html-документа — изменение расширения у любого текстового документа. Но этот способ не позволяет менять его структуру, вставлять аудио и видео.

Для редактирования документов можно использовать так называемые веб-эдиторы — программы для создания и редактирования сайтов в целом и

html-документов в частности. В данной работе использовалась программа «WebSite X5 Evolution 10». Главной её отличительной особенностью является удобный и понятный интерфейс с возможностью редактирования и внешнего вида, и содержания страниц, большой базой шаблонов, а также просмотра продукта без экспорта на носитель, рисунок 14.

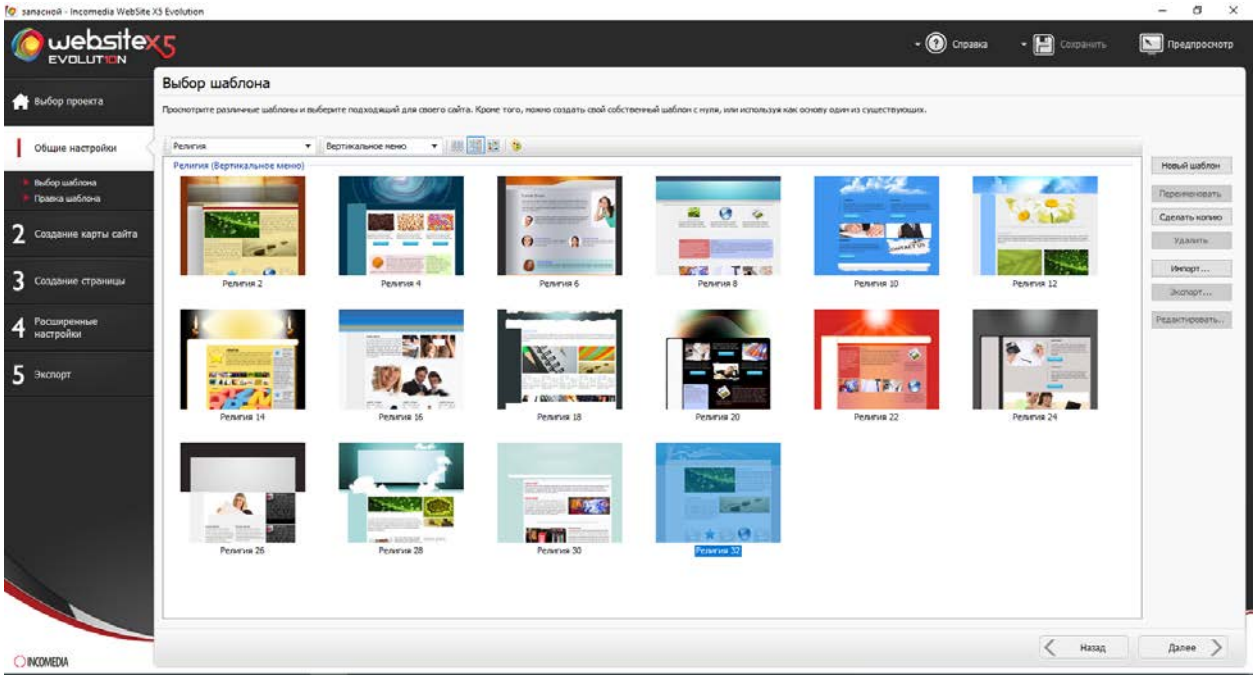


Рисунок 14 — Вид интерфейса WebSite X5 Evolution 10 для выбора шаблона

Выбор и правка графических шаблонов представлено на рисунке 15.

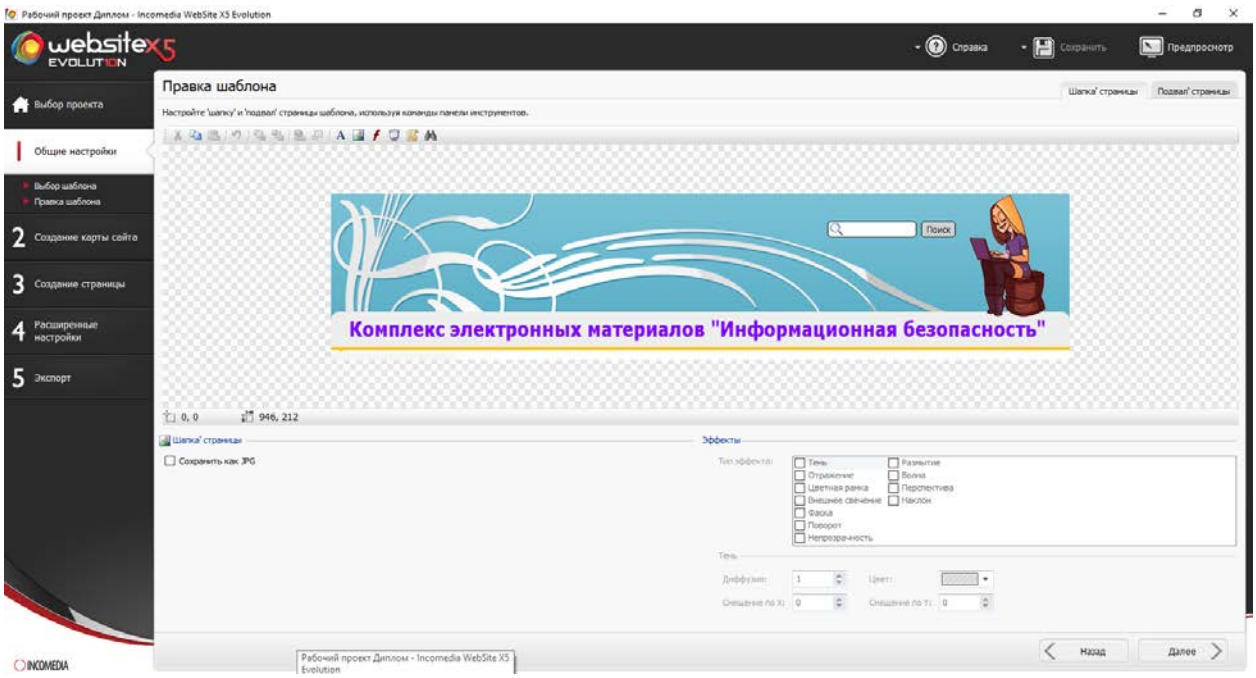


Рисунок 15 — Вид окна правка шаблона в комплексе

Создание карты сайта и интерфейса продукта представлено на рисунке 16.

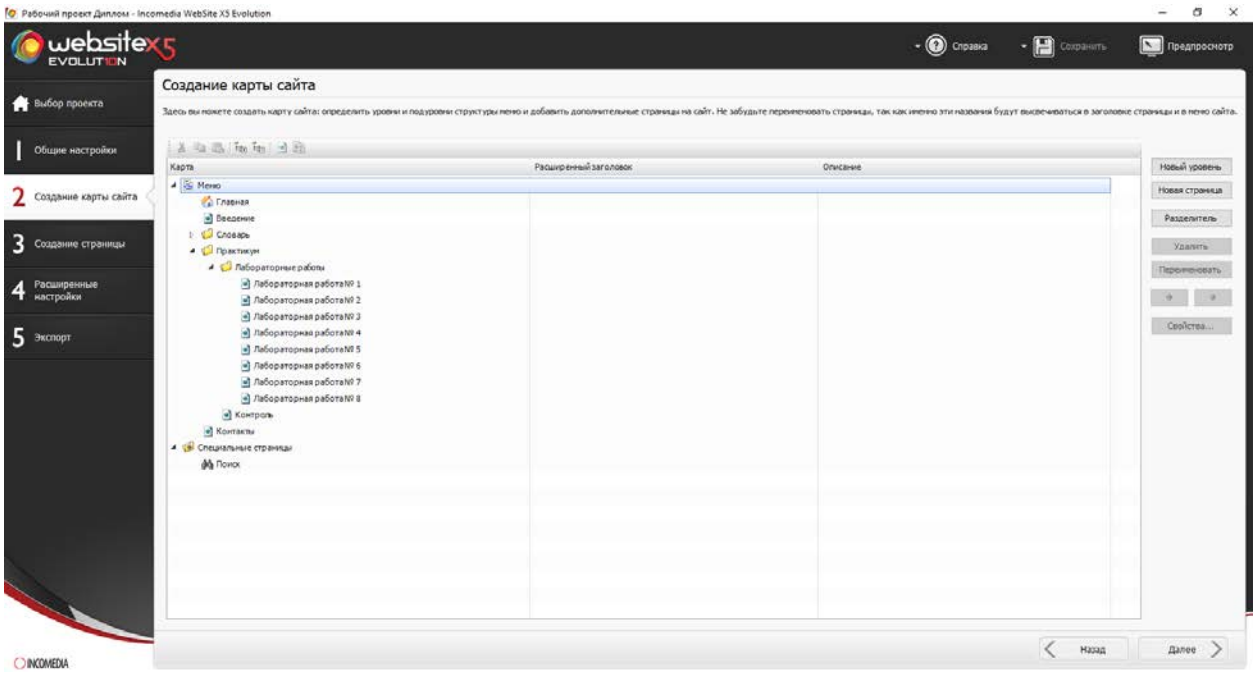


Рисунок 16 — Вид окна работы создания карты сайта с интерфейсом комплекса

Создание страниц представлено на рисунке 17, где можно вставить текст, картинки, таблицы, видео и аудио, почтовая форма, социальная сеть, гостевая книга, Flash-анимация.

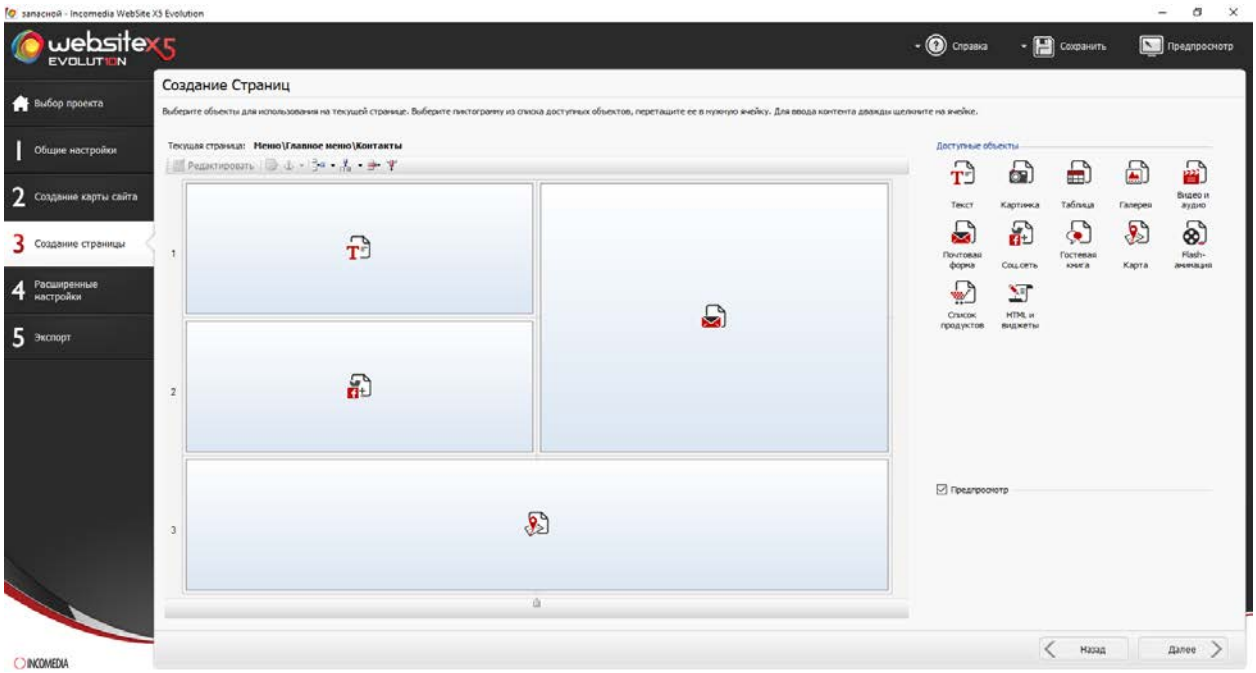


Рисунок 17 — Вид окна создания страниц для наполнения комплекса

Расширенные настройки продукта представлены на рисунке 18.

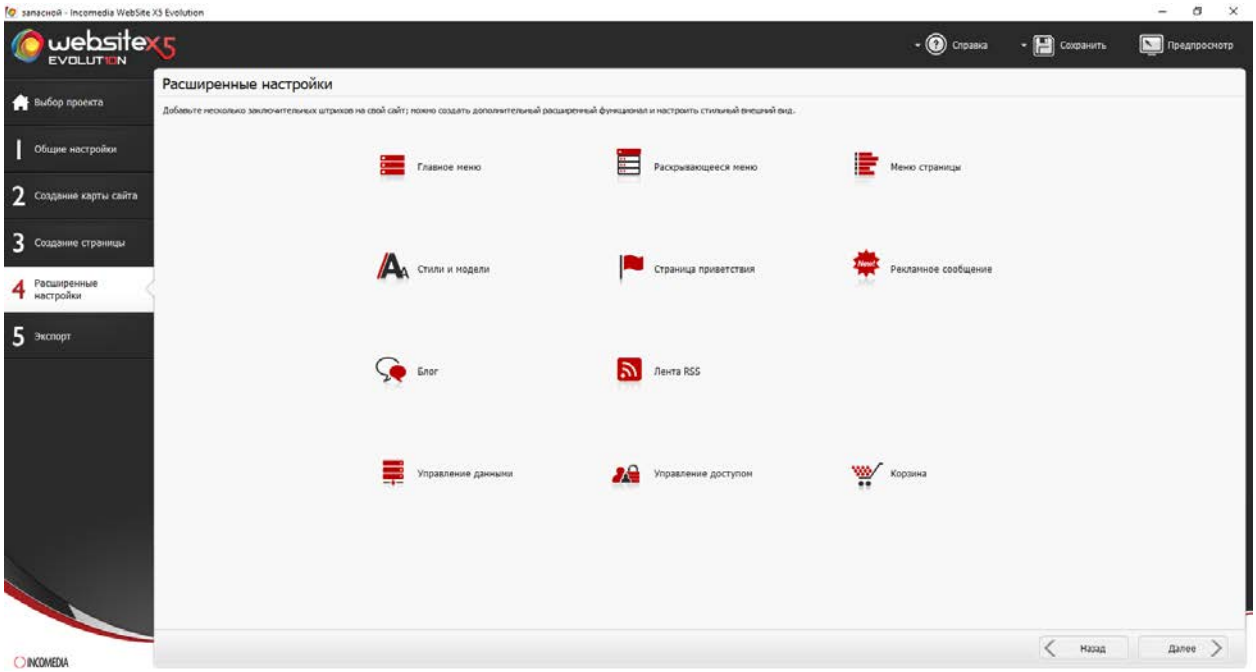


Рисунок 18 — Вид окна расширенных настроек продукта

Экспорт сайта продукта представлено на рисунке 19.

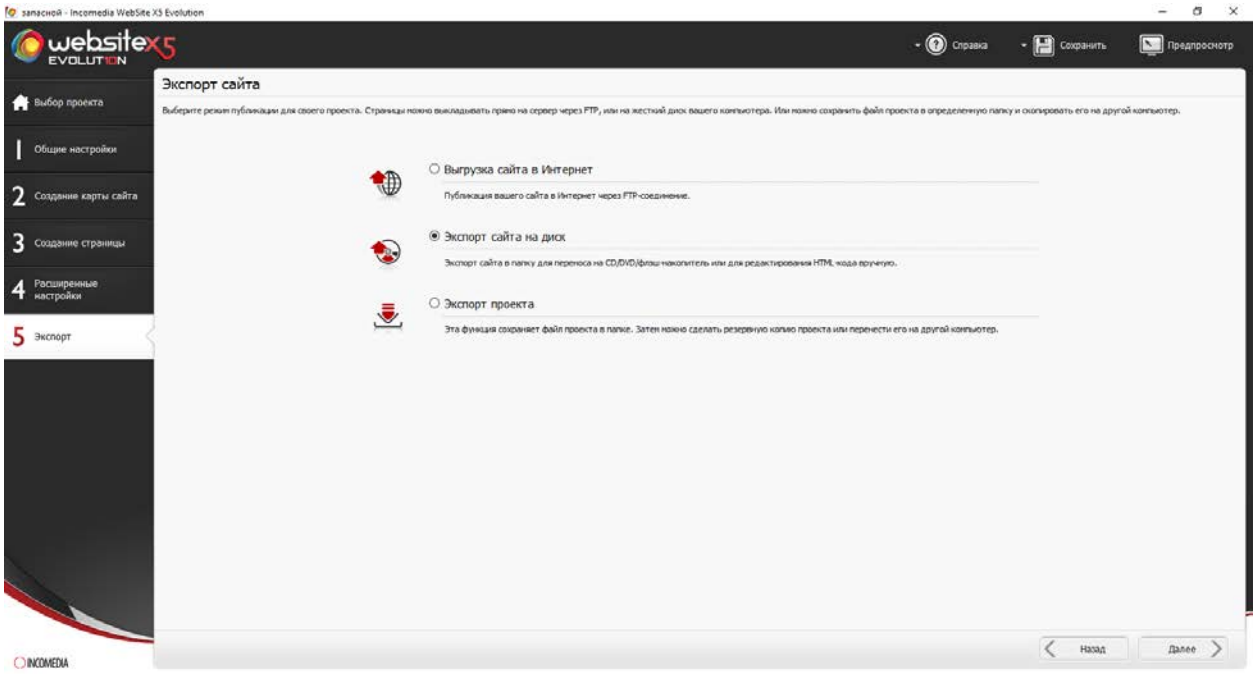


Рисунок 19 — Вид окна экспорт сайта комплекса

2.8 Инструкции по использованию комплекса электронных материалов для преподавателя и обучаемого

2.8.1 Инструкции по использованию комплекса электронных материалов для преподавателя

Возможность использования комплекса в процессе обучения схематично представлена на рисунках 20, 21.

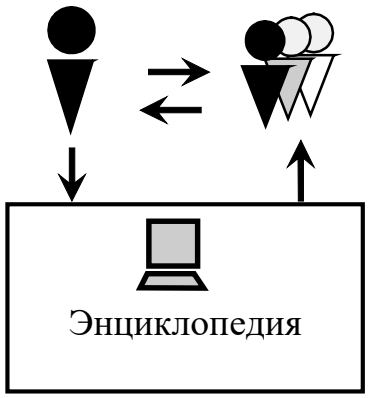


Рисунок 20 — Использование комплекса в учебном процессе для очной формы обучения

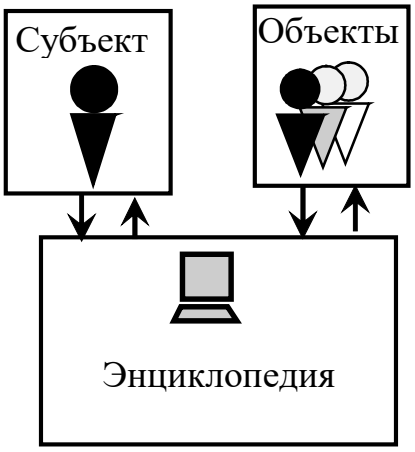


Рисунок 21 — Использование комплекса в учебном процессе для дистанционной и заочной формы обучения

Теоретические сведения, представленные в комплексе, можно использовать при проведении лекционных занятий. Изучение материала, представленного в комплексе, рекомендуется выносить на внеаудиторное время в ка-

честве домашнего задания. Комплекс можно использовать в процессе обучения для дистанционной и заочной форм обучения.

Инструкции по использованию комплекса для организации самостоятельной работы обучающихся представлены ниже.

Если обучающиеся изучают раздел самостоятельно вне учебного заведения, то необходимо предоставить данный комплекс на лазерных дисках, либо разместить его на веб-сайте.

Деятельность преподавателя носит консультирующий характер (обучающиеся консультируются с преподавателем по вызвавшим затруднения вопросам).

Разработанный комплекс является открытым, то есть преподаватель имеет возможность вносить изменения в его содержание.

Возможность использования комплекса в процессе самообучения представлена на рисунке 22.

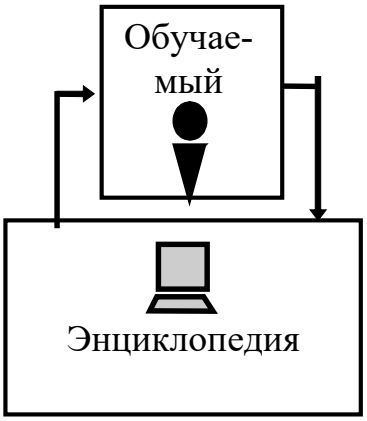


Рисунок 22 — Использование комплекса электронных материалов для самообучения

Для работы с данным комплексом нужен отдельный компьютер, со следующим установленным программным обеспечением:

- операционная система Windows Server 2008 R2/Vista/7 и более современные версии;
- один из браузеров (Internet Explorer не позднее версии 7.0; Opera; Firefox или Chrome);
- одно из средств виртуализации (Microsoft VirtualPC, VMware);

- любой PDF редактор;
- винчестер или жесткий диск (Seagate Barracuda емкостью 80 Гб);
- оперативная память (DDR 1024 Мбайт, частота которой 200 МГц);
- multi-привод (NEC DVD-RW), порты USB;
- дисплей (19” с разрешением 1024 x 768 пикселей);
- клавиатура (Logitech); манипуляторы: оптическая мышь (Genius Optical PS/2.

2.8.2 Инструкции по использованию комплекса электронных материалов для обучаемого

При работе с комплексом руководствуйтесь следующими инструкциями:

- расположитесь перед включенным компьютером;
- откройте ярлык «Комплекс электронных материалов»;
- в открывшемся комплексе выберите режим представления информации «Словарь» по алфавиту;
- дальнейшую работу осуществляйте по гиперссылкам, содержащимся в тексте страниц;
- при возникновении затруднений при поиске нужного определения воспользуйтесь возможностью поиска. Для этого введите искомую фразу в поле поиска и нажмите кнопку «Найти». В результате Вам будет предложена страница, содержащая перечень гиперссылок на страницы, удовлетворяющие Вашему запросу.

Для того чтобы вернуться на предыдущую станицу комплекса, можно воспользоваться стандартными кнопками браузера «Назад» и «Вперёд».

Использование комплекса предъявляет минимальные требования к компьютерам, установленным в компьютерных аудиториях.

На компьютерах должно быть установлено:

- операционная система Windows XPSP3/Vista/7 и более современные версии с эмуляторами операционных систем Linux;
- один из браузеров (Internet Explorer не позднее версии 7.0; Opera; Firefox или Chrome);
- микропроцессор (Intel Pentium 4, 2400 MHz (18 x 133);
- винчестер или жесткий диск (Seagate Barracuda емкостью 80 Гб);
- оперативная память (DDR 1024 Мбайт, частота которой 200 МГц);
- multi-привод (NEC DVD-RW);
- дисплей (19” с разрешением 1024 x 768 пикселей);
- клавиатура (Logitech); манипуляторы: оптическая мышь, порты USB.

2.8.3 Инструкции для установки и запуска комплекса

Для установки и запуска комплекса необходимо выполнить следующее:

- очистить или создать каталог C:\Temp;
- разархивировать файлы из архива «Комплекс электронных материалов.rar» в каталог C:\Temp;
- дождаться окончания копирования файлов;
- для более удобной работы разместить на рабочем столе (или в главном меню, или другом удобном Вам месте) ярлык «Комплекс электронных материалов»;
- для запуска комплекса открыть созданный Вами ярлык «Комплекс электронных материалов»;
- в случае необходимости установить программное обеспечение, указанное в разделе минимальных требований для работы с комплексом.

2.9 Результаты апробации

Апробация «Комплекса электронных материалов» проводилась со студентами энергетического техникума, которые обучаются на очной форме обучения. Апробация преследовала следующую цель: проверить результативность применения разработанной методики обучения студентов с использованием комплекса электронных материалов «Информационная безопасность».

Для апробации выбраны две группы: контрольная (КГ) и экспериментальная (ЭГ). Основанием для выделения КГ и ЭГ являются два фактора, с одной стороны, все группы обучались по одному и тому же государственному образовательному стандарту (что обеспечивало единство содержания обучения и требований к подготовке), но, с другой стороны, подготовка студентов КГ проводилась традиционным образом (без использования предложенной в работе методики с использованием комплекса «Информационная безопасность»).

Содержание контроля, проводимого после изучения темы «Информационная безопасность» в форме тестирования, регламентировалось рабочими программами соответствующих дисциплин. Полученные результаты проверки и оценивания доли усвоения (сформированности) теоретического материала планируется сопоставить с уровнем 0,7 соответствующим критерию В. П. Беспалько в модели полного усвоения знаний [6, с. 59].

Представленные критерии позволяют провести анализ результативности применения в учебном процессе разработанной методики обучения студентов с использование комплекса «Информационная безопасность».

Результаты исследования успешности сдачи темы на срезе знаний в контрольной и экспериментальных выборках представлены в таблице 2.

Таким образом, ориентируясь на критерий В. П. Беспалько [6] в модели полного усвоения знаний и умений, имеются все основания вести речь о вы-

соком уровне результативности обучения студентов в условиях использования интеллектуальных информационных систем.

Таблица 2 — Распределение студентов по группам успешности сдачи темы на срезе знаний в контрольной и экспериментальной группах

Градации усвоения	КГ		ЭГ	
	Количество человек	%	Количество человек	%
Недостаточное (<50%)	14	32,5	11	16
Посредственное (50%–70%)	22	51,2	23	33,3
Достаточное (> 70%)	7	16,3	35	50,7
Всего	43	100	69	100

Пример распределения студентов по группам успешности сдачи темы на срезе знаний иллюстрируется на рисунке 23.

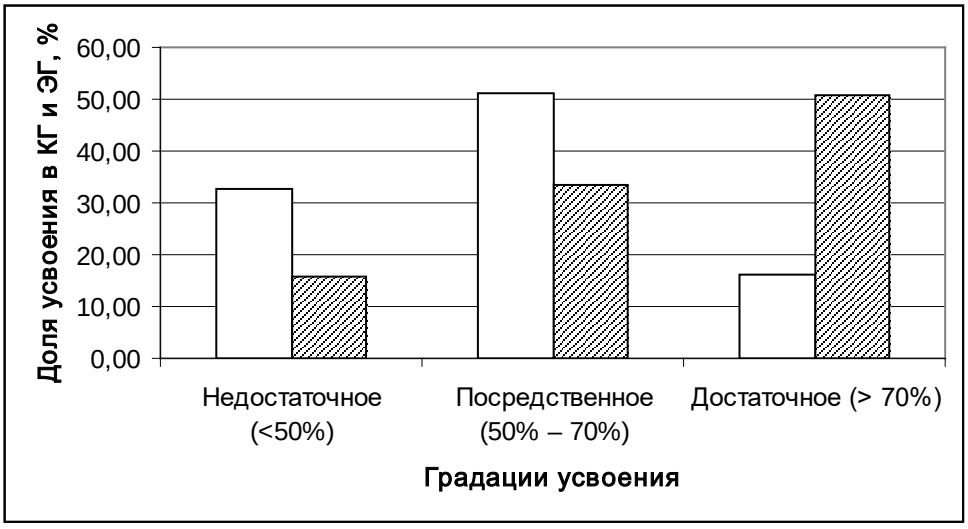


Рисунок 23 — Распределение студентов по группам успешности:

☐ — КГ; ▨ — ЭГ

Апробация показала, что представление информации в виде «Комплекса», стимулирует студентов к изучению материала, то есть способствует достижению учебной цели, повышению мотивации обучения.

Таким образом, можно сделать вывод, что комплекс электронных материалов формирует необходимые знания и представления об информационной безопасности и способствует достижению лучших результатов в обучении студентов.

ЗАКЛЮЧЕНИЕ

Проблема информационной безопасности — это проблема выбора человека — выбора воспринимаемой информации, поведения в обществе и государстве, выбора круга общения. Необходимо точное понимание и опознавание себя в мире, в обществе, осознания целей и средств для их достижения, сознательно обрабатывать информацию и транслировать только проверенную, точную и объективную информацию.

Информация выступает основой всего процесса управления в организации, труд руководителя заключается в её сборе, изучении, обработке. От уровня организации сбора, обработки и передачи информации зависит эффективность управления, а также качество принимаемых управленческих решений.

Информационные ресурсы — отдельные документы и отдельные массивы, документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). Информационные ресурсы являются собственностью, находятся в ведении соответствующих органов и организаций, подлежат учёту и защите, так как информацию можно использовать не только для товаров и услуг, но и превратить её в наличность, продав кому-нибудь, или уничтожить.

В условиях постоянного роста количества известных и появления новых видов информационных угроз перед предприятиями всё чаще встаёт задача обеспечения надёжной защиты от вредоносных программ и сетевых атак.

Информационная безопасность предприятия — это состояние защищённости корпоративных данных, при которой обеспечивается их конфиденциальность, целостность, аутентичность и доступность. Обеспечение информационной безопасности предприятия возможно только при системном и

комплексном подходе к защите. В системе информационной безопасности должны учитываться все актуальные компьютерные угрозы и уязвимости.

Полноценная информационная безопасность организаций подразумевает непрерывный контроль в реальном времени всех важных событий и состояний, влияющих на безопасность данных. Защита должна осуществляться круглосуточно и круглогодично и охватывать весь жизненный цикл информации — от её поступления или создания до уничтожения или потери актуальности.

В первой главе выпускной квалификационной работы нами проанализирована литература и интернет-источники по теме: «Информационная безопасность». Были рассмотрены базовые принципы, без реализации которых невозможно построение эффективной и безопасной деловой обстановки. Особое внимание уделено концептуальным положениям системы защиты информации, угрозам «конфиденциальной информации», а также действиям и причинам, приводящим к неправомерному получению «конфиденциальной информации». Приведены базовые понятия «информационной безопасности», аудита информационной безопасности предприятия. Показаны действия, направленные на реализацию политики безопасности, преимущества и функции, как реализуется комплексная защита и оптимизируется производительность, а также показаны предпринимаемые действия для центрального администрирования. Обеспечение информационной безопасности — это непрерывный процесс, требующий постоянного контроля.

Наши рекомендации на предприятии дадут возможность для наиболее рационального и эффективного использования, обработки, хранения информации и для повышения качества обеспечения информационной безопасности.

В нашей работе была изучена проблема обеспечения информационной безопасности и процесс проведения аудита по информационной безопасности предприятия.

Во второй главе создано информационное обеспечение для проведения аудита по информационной безопасности и предложены меры по повышению информационной безопасности предприятия.

Цель написания выпускной квалификационной работы, как разработка «Комплекса электронных материалов по “Информационной безопасности”», выполнена. Структура комплекса составлена. Изучена проблема обеспечения информационной безопасности предприятия. Проведён процесс аудита по информационной безопасности. Для проведения аудита по информационной безопасности создано информационное обеспечение. Организованы и предложены меры по повышению информационной безопасности. Разработана политика информационной безопасности. Изучены проблемы обеспечения информационной безопасности предприятия.

Разработан «Комплекс электронных материалов “Информационная безопасность”».

В ходе выполнения данной работы были изучены общие требования, предъявляемые к созданию комплекса и с учётом этих требований, были произведены анализ и разработка:

- структура комплекса;
- элементы графического интерфейса: кнопки, меню;
- вид главного окна комплекса.

Разработан комплекс с понятным меню для навигации по программному продукту, содержащему — словарь по алфавиту, лабораторный практикум, контроль, рекомендации, почтовая форма, карта.

Практическая часть включает в себя 8 лабораторных работ. По завершению работы студент может узнать свои результаты. Также можно поработать над своими ошибками и эффективно устранить их.

Контроль содержит 45 вопросов с различными типами заданий. Контроль предусмотрен после прохождения лабораторных работ для проверки качества усвоения материала студентами. Правильные ответы и оценку студент видит сразу после прохождения теста.

Вся информация строго структурирована, и весь программный продукт выполнен в соответствии с рекомендациями по психологическому цветовосприятию, что помогает в будущем придать узнаваемость бренду программы и проще ориентироваться при поиске в интернете более детальных настроек.

Программный продукт содержит блок полезной информации: полезные ссылки и рекомендации. Нижняя часть меню программного продукта содержит информацию об авторе, что все права защищены. Доступ к программному продукту может быть сделан как на локальном хостинге, так и на внешнем — это не повлияет на работу программного продукта.

Информация также структурирована и внутри блоков, то есть при нажатии на лабораторные — выводится список всех доступных лабораторных работ. На главной странице доступны ссылки ко всем практическим занятиям, что дополняет основное навигационное меню.

Все материалы на сайте доступны для индексации поисковым системам, и на каждой странице прописаны заголовки, описание и ключевые слова, что несомненно скажется на выдаче сайта при запросе студента, при учёте размещения в сети Интернет на определённом домене.

«Комплекс электронных материалов» подразумевает свободный доступ, все материалы сайта защищены законом об авторском праве. Любое копирование должно быть согласовано с администрацией сайта.

В результате поставленные задачи были решены, цель — достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Актив [Электронный ресурс]. — Режим доступа: http://www.nwaktiv.ru (дата обращения: 01.10.2017).

2. Бабаш А. В. Информационная безопасность и защита информации [Текст] / А. В. Бабаш, Е. К. Баранова. — Москва: Инфра-М, 2017. — 324 с.

3. Бабаш А. В. Информационная безопасность. История защиты информации в России [Текст] / А. В. Бабаш, Е. К. Баранова, Д. А. Ларин. — Москва: КДУ, 2015. — 736 с.

4. Бабаш А. В. Моделирование системы защиты информации. Практикум [Текст]: учебное пособие / А. В. Бабаш, Е. К. Баранова. — Москва: Просвещение, 2016. — 224 с.

5. Балыкина Е. Н. Сущностные характеристики электронных учебных изданий [Электронный ресурс]. — Режим доступа: http://goo.gl/BhdF63 (дата обращения: 05.12.2017).

6. Беспалько В. П. Программированное обучение. Дидактические основы [Текст] / В. П. Беспалько. — Москва: Высшая школа, 1970. — 300 с.

7. Библиотека программиста [Электронный ресурс]. — Режим доступа: https://proglib.io/ (дата обращения: 01.12.2017).

8. Бирюков А. А. Информационная безопасность: защита и нападение [Текст] / А. А. Бирюков. — Москва: ДМК Пресс, 2017. — 434 с.

9. Богомазова Г. Н. Обеспечение информационной безопасности компьютерных сетей [Текст] / Г. Н. Богомазова. — Москва: Академия, 2017. — 224 с.

10. Бондарев В. В. Введение в информационную безопасность автоматизированных систем [Текст]: учебное пособие / В. В. Бондарев. — Москва: МГТУ им. Н. Э. Баумана, 2016. — 252 с.

11. Бубнов А. А. Основы информационной безопасности [Текст]: Учебник / А. А. Бубнов, В. Н. Пржегорлинский, О. А. Савинкин. — Москва: Академия, 2018. — 256 с.

12. Википедия — свободная энциклопедия [Электронный ресурс]. — Режим доступа: http://ru.wikipedia.org/ (дата обращения: 01.10.2017).

13. Гуманитарная электронная библиотека [Электронный ресурс]. — Режим доступа: http://www.lib.ua-ru.net/katalog/41.html (дата обращения: 11.10.2017).

14. Зеер Э. Ф. Прогнозирование профессионального будущего личности: теория и практика [Текст] / Э. Ф. Зеер // Инновации в профессиональном и профессионально-педагогическом образовании: материалы 21-й Всерос. науч.-практ. конф., 25–26 мая 2016 г., г. Екатеринбург / Рос. гос. проф.-пед. ун-т. — Екатеринбург: Рос. гос. проф.-пед. ун-т, 2016. — С. 264–271.

15. Зеер Э. Ф. Самоопределение учащейся молодежи в современных конфликтующих реальностях: учебное пособие [Гриф Российской академии образования] [Текст] / Э. Ф. Зеер, М. В. Кормильцева, Э. Э. Сыманюк. — Рос. акад. Образования. — Моск. психолог.-соц. ун-т. — Москва: МПСУ, 2015. — 95 с.

16. Интернет библиотека электронных книг Elibrus [Электронный ресурс]. — Режим доступа: http://elibrus.1gb.ru/psi.shtml (дата обращения: 11.10.2017).

17. Информационная безопасность [Электронный ресурс]. — Режим доступа: http://bezopasnik.org/ (дата обращения: 01.10.2017).

18. Камский В. А. Защита личной информации в Интернете, смартфоне и компьютере [Текст] / В. А. Камский. — Москва: Наука и Техника СПб, 2017. — 272 с.

19. КонсультантПлюс [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/ (дата обращения: 01.10.2017).

20. Краковский Ю. М. Защита информации [Текст] / Ю. М. Краковский. — Москва: Феникс, 2017. — 347 с.

21. Министерство образования и науки Российской Федерации [Электронный ресурс]. — Режим доступа: http://www.минобрнауки.рф/ (дата обращения: 15.12.2017).

22. Научная онлайн-библиотека Порталус [Электронный ресурс]. — Режим доступа: http://www.portalus.ru/ (дата обращения: 02.01.2018).

23. Нестеров С. А. Основы информационной безопасности [Текст]: учебное пособие / С. А. Нестеров. — Москва: Лань, 2016. — 324 с.

24. Новые информационные коммуникационные технологии в образовании [Текст] / В. А. Трайнев, В. Ю. Теплышев, И. В. Трайнев. — 2-е изд. — Москва: «Дашков и К°», 2014. — 320 с.

25. Рабочая программа дисциплины «Информатика и ИКТ» [Электронный ресурс]. — Режим доступа: http://www.ekbenergo.ru/summaries/informatika.pdf (дата обращения: 01.12.2017).

26. Рогозин В. Ю. Основы информационной безопасности [Текст]: учебник / В. Ю. Рогозмн. — Москва: Юнити-Дана, 2016. — 287 с.

27. Родичев Ю. А. Нормативная база и стандарты в области информационной безопасности [Текст]: учебник для вузов. — Санкт-Петербург: Питер, 2017. — 256 с.

28. Российское образование. Федеральный образовательный портал. [Электронный ресурс]. — Режим доступа: http://www.edu.ru (дата обращения: 12.12.2017).

29. Управление персоналом организации [Текст]/ Под ред. А. Я. Кибанова. — Москва: ИНФРА-М, 2014. — 238 с.

30. Управление персоналом современной организации [Текст] / Под ред. С. В. Шекшня. — Москва: Интел-Синтез, 2013 — 368 с.

31. Хабрахабр [Электронный ресурс]. — Режим доступа: http://habrahabr.ru (дата обращения: 01.10.2017).

32. Эрганова Н. Е. Практикум по методике профессионального обучения [Текст]: учебное пособие / Н. Е. Эрганова, М. Г. Шалунова, Л. В. Коляс-

никова. — 2-е изд., пересмотр. и доп. — Екатеринбург. Рос. гос. проф.- пед. ун-т, 2011. — 89 с.

33. CodeProject — алгоритм сортировочной станции [Электронный ресурс]. — Режим доступа: http://www.codeproject.com/Tips/351042/Shunting-Yard-algorithm-in-Csharp (дата обращения: 21.12.2017).

34. Greg Conti Googling Security: How Much Does Google Know About You? [Электронный ресурс]. — Режим доступа: https://books.google.ru/ (дата обращения: 01.12.2017).

35. ICC Russia (International Chamber of Commerce) — Международная торговая палата [Электронный ресурс]. — Режим доступа: http://www.iccwbo.ru/ (дата обращения: 01.10.2017).

36. Stackoverflow [Электронный ресурс]. — Режим доступа: http://stackoverflow.com/ (дата обращения: 21.12.2017).

37. Unmasking the Social Engineer. The Human Element of Security. [Электронный ресурс]. — Режим доступа: https://www.litres.ru/ (дата обращения: 11.12.2017).

38. WebSite X5 [Электронный ресурс]. — Режим доступа: http://www.websitex5.com/ru/ (дата обращения: 01.10.2017).

39. YouTube [Электронный ресурс]. — Режим доступа: https://www.youtube.com/ (дата обращения: 02.01.2018).

ПРИЛОЖЕНИЕ

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

Институт инженерно-педагогического образования
Кафедра информационных систем и технологий
направление 44.03.04 Профессиональное обучение (по отраслям)
профиль «Информатика и вычислительная техника»
профилизация «Компьютерные технологии»

УТВЕРЖДАЮ
Заведующий кафедрой
_____Н. С. Толстова
«_____»_____2017 г.

ЗАДАНИЕ
на выполнение выпускной квалификационной работы бакалавра

студентки 4 курса, группы ЗКТ-401С Козыревой Ольги Викторовны.

1. Тема «Комплекс электронных материалов ”Информационная безопасность”»
утверждена распоряжением по институту от г. №

2. Руководитель Суслова Ирина Александровна, канд.пед.наук, доцент, доцент кафедры ИС ФГАОУ ВО «Российский государственный профессионально-педагогический университет»

3. Место преддипломной практики Государственное автономное профессиональное образовательное учреждение Свердловской области «Екатеринбургский экономико-технологический колледж»

4. Исходные данные к ВКР рабочая программа дисциплины «Информатика и ИКТ»

5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов)
Проанализировать литературу и интернет-источники по теме «Информационная безопасность».
Проанализировать рабочую программу по дисциплине «Информатика и информационно-коммуникационные технологии» с целью выделения требований, предъявляемых к формированию знаний и умений при изучении раздела «Информационная безопасность».
Спроектировать структуру, реализовать интерфейс, функционал и наполнение программного продукта ««Комплекс электронных материалов “Информационная безопасность”».

6. Перечень демонстрационных материалов
презентация
комплекс электронных материалов

7. Календарный план выполнения выпускной квалификационной работы

№ п/п	Наименование этапа ВКР	Срок выполнения этапа	Процент выполнения ВКР	Отметка руководителя о выполнении
1	Сбор информации по выпускной работе и сдача зачета по преддипломной практике	02.12.2016	15	
2	Выполнение работ по разрабатываемым вопросам их изложение в выпускной работе:			
	Разработать лабораторные работы	15.12.2017	15	
	Скомпоновать понятия по алфавиту и провести обработку видеоматериалов	25.12.2017	15	
	Реализовать комплекс электронных материалов	30.12.2017	15	
	Обеспечить навигационные переходы между понятиями	02.01.2018	10	
	Разработать инструкции	05.01.2018	10	
3	Оформление текстовой части ВКР	08.01.2018	5	
4	Выполнение демонстрационных материалов к ВКР	10.01.2018	5	
5	Нормоконтроль	12.01.2018	5	
6	Подготовка доклада к защите в ГЭК	13.01.2018	5	

8. Консультанты по разделам выпускной квалификационной работы

Наименование раздела	Консультант	Задание выдал		Задание принял	
		подпись	дата	подпись	дата

Руководитель _____ 10.11.17 *Задание получил* _____ 10.11.17
подпись дата подпись студента дата

9. Выпускная квалификационная работа и все материалы проанализированы.
Считаю возможным допустить Козыреву О.В. к защите выпускной квалификационной работы в государственной экзаменационной комиссии.

Руководитель _____ 17.01.2018
подпись дата

10. Допустить Козыреву О.В. к защите выпускной квалификационной работы в государственной экзаменационной комиссии (протокол заседания кафедры от __.__.2018 №____)

Заведующий кафедрой _____ _____
подпись дата