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

ДОПОЛНИТЕЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА «ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ»

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

Идентификационный номер ВКР: 217

Екатеринбург 2019

Министерство науки и высшего образования 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
Заведующий кафедрой ИС
_____ И. А. Суслова
«____» _____ 2019 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ДОПОЛНИТЕЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА «ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ»

Исполнитель:
обучающаяся группы ИБ-402 М. А. Помогаева
Руководитель:
канд. пед. наук, доцент К. А. Федулова
Нормоконтролер:
ст. преподаватель каф. ИС Н. В. Хохлова

Екатеринбург 2019

АННОТАЦИЯ

Выпускная квалификационная работа состоит из электронного учебного пособия «Электронно-цифровая подпись» и пояснительной записки на 76 страницах, содержащей 60 рисунков, 30 источников литературы, а также 2 приложения на 15 страницах.

Ключевые слова: ДОПОЛНИТЕЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА, ЭЛЕКТРОННОЕ УЧЕБНОЕ ПОСОБИЕ, ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ, CAMTASIA, WORDPRESS, LEARNINGAPPS, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ДОКУМЕНТОВЕДЕНИЕ.

Помогаева М. А., Электронное учебное пособие «Электронно-цифровая подпись»: выпускная квалификационная работа / М. А. Помогаева; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2019. — 76 с.

В результате выполнения выпускной квалификационной работы разработана дополнительная образовательная программа «Электронно-цифровая подпись» и электронное учебное пособие для нее.

Цель работы — разработать дополнительную образовательную программу «Электронно-цифровая подпись» и электронное учебно-методическое обеспечение для ее реализации.

В данной работе проанализирован и изучен материал, связанный с организацией обучения по программам дополнительного профессионального образования. На основе анализа подготовки современных документоведов и педагогов профессионального образования в сфере информационных технологий выявлена необходимость в расширении изучения темы «Электронно-цифровая подпись» и дифференциация программы в зависимости от профиля подготовки. Была разработана дополнительная образовательная программа «Электронно-цифровая подпись» и электронное учебно-методическое обеспечение для ее реализации.

СОДЕРЖАНИЕ

Введение 5
1 Проектирование дополнительной образовательной программы 8
1.1 Цели и задачи дополнительной образовательной программы 8
1.2 Актуальность разработки дополнительной программы «Электронно-цифровая подпись» 11
1.3 Анализ литературы и интернет-источников по теме «Электронно-цифровая подпись» 12
1.3.1 Анализ литературных источников 12
1.3.2 Анализ интернет-источников 14
1.3.3 Анализ нормативной документации по теме «Электронно-цифровая подпись» 15
1.4 Основные требования, предъявляемые к электронному учебному пособию, и средства его реализации 17
1.4.1 Дидактические требования электронных учебных пособий 17
1.4.2 Психологические требования, предъявляемые к электронным учебным пособиям 19
1.4.3 Информационно-технические требования, предъявляемые к электронным учебным пособиям 19
1.4.4 Электронные учебные пособия в дистанционных технологиях обучения 20
1.5 Средства реализации электронного учебного пособия 20
2 Разработка электронного учебного пособия «Электронно-цифровая подпись» 23
2.1 Педагогический адрес 23
2.2 Структура электронного учебного пособия «Электронно-цифровая подпись» 23

2.3 Интерфейс и навигация по электронному учебному пособию «Электронно-цифровая подпись» 26
2.4 Разработка обучающих видеороликов 40
2.5 Разработка элементов контроля для электронного учебного пособия .. 42
2.6 Методические рекомендации по использованию электронного учебного пособия «Электронно-цифровая подпись» 54
2.7 Результат апробации и внедрения 56
Заключение 58
Список использованных источников 60
Приложение А 64
Приложение Б 67

ВВЕДЕНИЕ

Служба делопроизводства служит главным элементом любой организации, которая обеспечивает ее работу, и является мощным механизмом, отвечающим за руководство главными процессами в организации, направляя остальные подразделения через отдельных исполнителей на реализацию общей цели, стимулируя активизацию сотрудников и упростить процессы деловой коммуникации, а также изменяя организационное действия всех работников.

Делопроизводство в нынешних организациях становится новой сверхтехнологичной процедурой, включающей системы информационного, организационного, правового и аналитического обеспечения ее функционирования, и обеспечивающей управленческие функции в области документирования главной деятельности организации, в особенности электронного документооборота.

В век активного развития информационных технологий, многие предприятия переходят на электронных документооборот. В связи с этим актуальным становиться вопрос проверки подлинности документов. Самым эффективным способом проверки подлинности документа является электронно-цифровая подпись — далее ЭЦП.

Современные стандарты определяют смещение акцента на самостоятельное освоение учебного материала за счет уменьшения часов аудиторной нагрузки, что воздействует на изменении требований, предъявляемых к учебно-методического обеспечению образовательного процесса. Кроме того, в круг профессиональных задач документоведов входят вопросы обеспечения информационной безопасности документации, что ставит вопрос о необходимости интеграции информационных технологий как в содержание подготовки современных документоведов, так и изменение методического обеспечения данной подготовки.

Вопросы, связанные с обучением использованию технологии ЭЦП, встречаются в содержании подготовки как студентов направления подготовки 46.03.02 Документоведение и архивоведение профиля «Правовое и документационное обеспечение управления персоналом», так и 44.03.04 Профессиональное обучение (по отраслям) профиля «Информационные технологии» профилизации «Информационная безопасность». Различие составляет уровень детализации содержания подготовки, так у документоведов — это знание нормативно-правовой базы ЭЦП и современные системы идентификации документов и аутентификации пользователей с использованием ЭЦП, а у специалистов в области обеспечения информационной безопасности — это принципы работы и построения электронно-цифровой подписи на уровне программирования.

В связи с данными требованиями возникает необходимость в организации подготовки современных специалистов, готовых на разном уровне использовать средства подтверждения подлинности документов, которую наиболее эффективно осуществлять в рамках программ дополнительного профессионального образования. Учебно-методическое сопровождение подобных программ, как правило, в современных условиях осуществляется удаленно с использованием соответствующего электронного методического обеспечения, которым может выступать электронное учебное пособие, что и определило тему выпускной квалификационной работы.

Объект выпускной квалификационной работы — процесс обучения слушателей дополнительной образовательной программы «Электронно-цифровая подпись».

Предмет выпускной квалификационной работы — учебные материалы по теме «Электронно-цифровая подпись»

Цель выпускной квалификационной работы — разработать дополнительную образовательную программу «Электронно-цифровая подпись» и электронное учебно-методическое обеспечение для ее реализации.

В соответствии с поставленной целью в работе определены следующие **задачи**:

1. Проанализировать литературу и интернет-источники по теме «Электронно-цифровая подпись» с целью формирования круга печатных и электронных изданий, рассматривающих те или иные технологии, используемые в деятельности как документоведов, так и будущих специалистов в сфере информационной безопасности.

2. Спроектировать содержание дополнительной образовательной программы «Электронно-цифровая подпись».

3. Проанализировать литературу и интернет-источники с целью выделения требований, предъявляемых к электронному учебному пособию на современном этапе развития образования.

4. Осуществить выбор средств реализации учебно-методического обеспечения реализации дополнительной образовательной программы.

5. Создать дополнительную образовательную программу «Электронно-цифровая подпись» и провести апробацию электронного учебного пособия для ее реализации.

1 ПРОЕКТИРОВАНИЕ ДОПОЛНИТЕЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1 Цели и задачи дополнительной образовательной программы

В современном мире одну из главных ролей играет дополнительное образование в российском обществе. Это связанно с тем, что это наиболее актуально в данное время, для профессиональной переориентации трудоспособности населения, освоение гражданами новых специальностей и получение новых знаний.

Дополнительное образование — это вид образования, направленный на всестороннее удовлетворение образовательных потребностей человека в интеллектуальном, духовно-нравственном, физическом и профессиональном совершенствовании [2].

До недавнего времени дополнительно профессиональное образование пользовалось спросом у более зрелого поколения. Происходило это в связи с появлений новых технологий, расширение производства и получение дополнительно профессионального образования было оптимальным решением для получения новых знаний и умений, при этом не тратя на этого несколько лет. Однако сегодня дополнительное образование пользуется спросом у тех, кто недавно был студентом. Связанно это с тем, что при выборе профессии учитывалось то, как профессия «модная» или «доступная», а по завершению обучения студентам просто не нравилась выбранная ими профессия, или они не заканчивали ее и нашли отличный выход из ситуации — получить дополнительной профессиональное образование.

Дополнительное профессиональное образование включает в себя виды обучения:

- профессиональная переподготовка с выдачей государственного диплома «О профессиональной переподготовке»;

- повышение квалификации с выдачей удостоверения о краткосрочном повышении квалификации по программам от 72 до 100 ак. час. и свидетельства о повышении квалификации по программе от 100 до 500 ак. час.;
- семинары, курсы, тренинги;
- мастер-классы [16].

Профессиональная переподготовка — это получение дополнительных знаний, умений и навыков по образовательным программам, предусматривающим изучение отдельных дисциплин, разделов науки, техники и технологии, необходимых для выполнения нового вида профессиональной деятельности [15].

Повышение квалификации — это вид проф. обучения специалистов, с целью получение слушателями дополнительных знаний, приобретения или совершенствование профессиональных умений и владений для исполнения обязанностей по занимаемой должности. Повышение квалификации — это часть дополнительного профессионального образования, которое способствуют обновлению практических и теоретических познаний специалистов связанных с повышением требований к степени их квалификации и потребностью в изучении современных способов решения профессиональных задач. По успешному прохождению повышения квалификации, слушатели получают:

- удостоверение о повышении квалификации — прошедшие программу от 72 до 100 часов;
- свидетельство о повышении квалификации — прошедшее программу от 100 часов и более.

Тренинги и семинары — это очень активная форма обучения, нацеленная на практическое осваивание приёмов применения той либо другой технологии. Они различаются от других форм обучения большое активностью участников, при этом большое внимание уделяется в получении практических навыков, которые можно сразу же применять на практике. На тренингах и семинарах обучение проходит в режиме действий, рассмотрения приобре-

тенного опыта, обратной связи участников, что представляет возможность исследовать собственные успешные и нет методы работы взаимодействия с другими людьми, а также получить уроки и многому обучиться в безопасной ситуации во время обучения. Это отличная интеллектуальная подпитка знаний, которая дает стимул к различным идеям и повысит профессиональный уровень. На тренингах и семинарах познают новыми веяниями в профессиональных областях, совершается взаимообмен опытом, раскрываются внутренние ресурсы, что обеспечивает возможность быть профессионалом в собственной области.

Мастер-классы проводят специалисты, являющиеся экспертами в своей области, которые делятся своими навыками и методиками, указывают на ошибки и дают подсказку для пути их разрешения.

Сроки обучения зависят от программы этого либо другого тренинга, мастер-класса или семинара.

После окончания обучения участники получают сертификаты.

Программы дополнительного профессионального образования повышают конкурентоспособность на рынке труда.

Дополнительное профессиональное образование в высшем учебном заведении помогает в:

- приобретении дополнительной специальности;
- повышении уровня собственной квалификации;
- развитии собственных способностей;
- повышении шанса собственного трудоустройства;
- повышении уровня профессиональной мобильности к прогрессивным условиям развития техники, науки, образования и производства.

Дополнительное образование пред классическими формами профессионального образования обладает достоинствами, такими как:

- обучение — краткосрочное;
- график учебного процесса — гибкий;
- наполняемость групп — небольшая;

- изучение новых информационных технологий.

Целью осуществления университетом концепции дополнительного профессионального образования может являться осуществление устойчивой функциональной деятельности вуза по реализации потребностей предприятий, учреждений и организаций в повышении квалификации и переподготовке сотрудников, работников педагогов общего и профессионального — в профессиональной переподготовке и повышении квалификации учащихся, студентов и населения — в их развитии.

Из этого следуют, что задачами дополнительного профессионального образования будут являться:

1. Реализация и организация системы определения спроса и формирование предложений по оказанию образовательных услуг в соответствии с потребностями потенциальных заказчиков.
2. Организация работы подразделений вуза по подготовке и реализации образовательных услуг в соответствии с потребностями заказчиков.
3. Оптимизация дополнительных образовательных программ для обучающихся университета с целью увеличения их мотивации на дополнительное образование.

1.2 Актуальность разработки дополнительной программы «Электронно-цифровая подпись»

В настоящее время очень стремительно развиваются системы электронного документооборота, увеличивается объём документов, находящийся в электронном виде.

Одними из важным проблем, становятся проверка документов на подлинность, а также их защита.

Для обучающихся в сфере документооборота, важно знать, как проверять на подлинность документы в электронном документообороте, в то время

как обучающиеся в сфере информационной безопасности, должны знать способы защиты документов в электронном документообороте.

Поэтому, становиться актуальным создать дополнительную образовательную программу для студентов, чьи направления подготовки затрагивают данные проблемы, для обучения более компетентных и конкурентоспособных специалистов на рынке труда в будущем.

Подготовка специалистов различается, для специалистов с области информационных технологий важно не только владение системами электронного документооборота, а также понимание алгоритмов защиты — возможность изменения и корректирования этих алгоритмов или же, создание новых способов проверки подлинности. Для документоведов — это еще и правовой аспект защиты, и другие процедурные вопросы.

1.3 Анализ литературы и интернет-источников по теме «Электронно-цифровая подпись»

1.3.1 Анализ литературных источников

При разработке электронного учебного пособия список литературы позволяет подобрать и систематизировать материал.

Учебное пособие В. Ю. Коржов, Н. А. Захарова «Комментарий к федеральному закону от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи» [11] представляет собой постатейный комментарий к Федеральному закону от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи», в котором с учетом сложившейся практики и актуальных изменений в законодательстве анализируются отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами. Комментарий ориенти-

рован на широкий круг лиц. При подготовке настоящего издания использованы нормативные правовые акты по состоянию на 1 сентября 2016 года.

Учебное пособие А. Э. Смирнов, Ю. А. Пономарева «Практикум по выполнению лабораторных работ по дисциплине «Криптографические методы защиты информации» [24] содержит обширные сведения применении различных методов защиты текстовой информации, изучаются классические криптографические системы, их стойкости на основе подбора ключа и хранения конфиденциальности информации. Так же симметричные блочные алгоритмы шифрования и асимметричные алгоритмы шифрования, общие сведения об электронной цифровой подписи.

Учебное пособие В. В. Бондарев «Введение в информационную безопасность автоматизированных систем» [1] рассмотрена законодательная база информационной безопасности, приведен перечень возможных угроз, отражены основные подходы к созданию систем защиты информации, представлена классификация предупредительных мер, изучены вопросы, связанные с программно-аппаратными механизмами обеспечения информационной безопасности.

В учебном пособии А. Б. Левина «Моделирование криптосистем» [14] рассмотрены основные математические и криптографические понятия, необходимые для моделирования криптосистем. Книга состоит из таких разделов, как «Основные понятия, используемые в криптографии», «Математические основы, используемые для анализа и построения криптосистем», «Криптографические алгоритмы DES, AES, RSA, Keccak, DSA», «Вопросы, связанные с анализом ключей», «Криптоанализ».

В учебном пособим С. О. Крамаров, О. Ю. Митясова, С. В. Соколов, Е. Н. Тищенко, П. С. Шевчук «Криптографическая защита информации» [12] рассмотрены основные понятия и методы криптографии как прикладной науки, тесно связанной с развитием техники и технологии, средств связи и способов передачи информации. Приводятся методы преобразования информации, которые не позволяют извлекать ее из перехватываемых сообщений;

современные методы шифрования; вопросы истории криптографии; теория кодирования. Даются примеры зашиты информации в ситуациях, связанных с государственной, военной, коммерческой, юридической или врачебной тайной.

1.3.2 Анализ интернет-источников

Портал «Моя ЭЦП» [19] — это ресурс, который помогает разобраться, что такое электронная подпись, для чего она нужна и как ей пользоваться. Кроме информационной поддержки, так же на данном портале оказывают услуги по изготовлению электронных подписей, прохождению аккредитаций на торговых площадках и сопровождение электронных торгов.

Интернет-ресурс «Единый портал электронной подписи» [7] — это уникальный проект акционерное общество (АО) «Аналитический центр», на котором можно найти исчерпывающую информацию об электронной подписи, преимуществах и схеме работы с ней. На сайте также можно узнать об электронных торгах и участии в них, о системах электронного документооборота, защите информации и многом другом. Так же, можно подать заявку на получение электронной подписи и сопутствующих услуг.

Сайт компании «КриптоПро», которая в настоящее время занимает лидирующее положение по распространению средств криптографической защиты информации и электронно-цифровой подписи в России. Сайт компании «КриптоПро» позволяет получить подробную информацию о продуктах для создания электронной подписи, сделанные одноименной компанией, получить бесплатную пробную версию программ на период до одного месяца, узнать информацию об автоматизированных учебных центрах по криптографической защите информации и электронно-цифровой подписи, а также есть форум, где вы можете общаться с другими пользователями сайта «КриптоПро», на интересующие вас темы или обсуждать проблемы связанные с данным программным обеспечением [13].

1.3.3 Анализ нормативной документации по теме «Электронно-цифровая подпись»

Нормативная документация учебного процесса, как правило включает учебный план подготовки и рабочие программы всех дисциплин.

Учебный план — документ, который определяет перечень, трудоемкость, последовательность и распределение по периодам обучения учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности и, если иное не установлено настоящим Федеральным законом, формы промежуточной аттестации обучающихся [28].

Рабочая программа — это нормативно-правовой документ, определяющий организацию образовательного процесса в образовательном учреждении по определенному учебному курсу (дисциплине) [28].

Дополнительная образовательная программа «Электронно-цифровая подпись» включает в себя два модуля подготовки:

- модуль 1: всего — 86 часов, лекции — 20 часов, лабораторные(практические) работы — 14 часов, самостоятельная работа — 52 часа;
- модуль 2: всего — 74 часа, лекции — 18 часов, лабораторные(практические) работы — 12 часов, самостоятельная работа — 44 часа.

Целью освоения дополнительной образовательной программы «Электронно-цифровая подпись» является формирование у студентов четкого представления и понимания теоретических и прикладных знаний о современных методах обеспечения аутентификации электронных документов в информационных инфраструктурах предприятий и организаций, а также формирование знаний, умений и навыков, позволяющих студентам проводить анализ используемых электронно-цифровых подписей, понимать и использовать современные алгоритмы построения этих подписей, производить оценку возможностей, ограничений и областей применений данных электронно-цифровых подписей.

Задачи:

1. Изучение понятия «электронная подпись», его места в законодательстве Российской Федерации и практике его применения в органах государственной власти и организациях независимо от формы собственности;

2. Изучение показателей назначения электронной подписи (ЭП) и архитектур подсистем, ее реализующих в системах электронного документооборота; основных участников правоотношений в сфере организации работы с электронными документами;

3. Изучение принципов функционирования единого пространства доверия ЭП и технических условий признания ЭП аналогом собственноручной;

4. Изучение особенностей построения и эксплуатации комплекса средств автоматизации сервисов подсистем обеспечения юридической значимости информационно-коммуникационных систем, используемых для нужд электронного документооборота;

5. Изучение особенностей реализации сервисов удостоверяющих центров и средств ЭП в продукции ведущих отечественных производителей.

Дополнительная образовательная программа направлена на формирование следующих компетенций:

- способность обеспечивать защиту персональных данных работников и конфиденциальной информации, в том числе при организации, осуществлении и документировании процессов оценки, аттестации и развития персонала;
- способность анализировать и выбирать методы и средства обеспечения информационной безопасности.

Как видно из анализа рабочей программы, общим для двух направлений является рассмотрение ЭЦП, только для документоведов — знание нормативно-правовой базы ЭЦП и современные системы идентификации документов и аутентификации пользователей с использованием ЭЦП, в том как специалисты в области обеспечения информационной безопасности должны понимать еще и принцип работы и построения Электронно-

цифровой подписи на уровне программирования, так же все специалисты должны понимать математические модели, которые стоят за формированием и проверкой ЭЦП.

Разработанная дополнительная образовательная программа позволит повысить уровень формирования у студентов четкого представления и понимания теоретических и прикладных знаний о современных методах обеспечения аутентификации электронных документов в информационных инфраструктурах предприятий и организаций, а также формирование знаний, умений и навыков, позволяющих студентам проводить анализ используемых электронно-цифровых подписей, понимать и использовать современные алгоритмы построения этих подписей, производить оценку возможностей, ограничений и областей применений данных электронно-цифровых подписей.

1.4 Основные требования, предъявляемые к электронному учебному пособию, и средства его реализации

1.4.1 Дидактические требования электронных учебных пособий

Электронное учебное пособие (ЭУП) — это программно-методический обучающий комплекс, предназначенный для самостоятельного изучения студентом учебного материала по определенным дисциплинам [9].

Разработка электронных учебных пособий, невозможна без выполнения условий к их качеству.

В основном, все электронные учебные пособия строятся по модульному принципу, содержать в себе:

- анимацию;
- навигацию;
- текстовую часть;

- графические изображения (блок-схемы, графики, таблицы, чертежи и др.);
- интерактивный блок;
- видеоролики;
- поисковую систему в пределах электронного учебного пособия.

В большинстве случаев, электронные учебные пособия разрабатываются для самостоятельного изучения студентами определенной дисциплины. Немаловажные отличия электронных учебных пособий от печатного учебника, состоит в том, что учебник не может вместить в себя столько обширный объем информации, который понадобиться студенту для освоения дисциплины, всегда потребуется дополнительная литература. В данном случае преимуществом электронного учебного пособия является то, что студентам не приходиться тратить большую часть времени на поиск нужной им информации, а также они могут проверить свои знания если в электронном учебном пособие имеются тестовые задания или упражнения, после выполнения которых, студент может увидеть, на сколько качественно он освоил материал.

Дидактические требования к электронному учебному пособию включают в себя:

- научность;
- доступность;
- проблемность;
- наглядность.

Научность обучения подразумевает собой достаточную наполненность, корректность и логичность изложения материала. Содержание материалов должно соответствовать стандартам образования.

Доступность обучения, означает степень сложности материала с учетом уровня подготовки, индивидуальных и возрастных особенностей студентов.

Проблемность обучения обусловлено учебно-познавательной деятельностью. В ситуации, когда студент сталкивается со сложностями, его мысли-

тельная активность возрастает, что положительно влияет на результат освоения нового материала и решения вызванных проблем.

Наглядность обучения обозначает эмоциональное понимание изучаемых объектов. Наглядность обучения при применении электронного учебного пособия содержит определенные преимущества пред традиционным бумажным учебником.

1.4.2 Психологические требования, предъявляемые к электронным учебным пособиям

Психологические требования к электронным учебным пособия можно разделит на две группы.

Первая группа включает в себя восприятие информации студентом (зрительное, слуховое), память, мышление, внимание (концентрация, устойчивость, переключаемость, объем).

Вторая группа включает в себя обеспечение комфортного, безопасного для здоровья и производительного труда студентов.

1.4.3 Информационно-технические требования, предъявляемые к электронным учебным пособиям

Основными информационно-техническими требованиями модно выделить:

- использование различных типов мультимедиа для представления материала;
- адаптация к уровню подготовки обучаемого и набору изучаемых тем;
- обеспечение удобной системы навигации и поиска информации;
- возможность удаленно в получении консультации преподавателя;
- наличие развитой системы контроля знаний.

Выполнение указанных требований позволит использовать учебный комплекс для индивидуальных и групповых (лекционных) занятий во всех формах обучения — очной, заочной и дистанционной [27].

1.4.4 Электронные учебные пособия в дистанционных технологиях обучения

Дистанционное обучение — обучение на расстоянии с активным использованием возможностей сетевого информационного пространства. Это одна из самых перспективных образовательных технологий. В современной школе дистанционное обучение часто применяется в инклюзивном образовании и при работе с одаренными детьми [25].

Дистанционное обучение предполагает самостоятельное изучение материала в заданный промежуток времени. Педагог — составляет дистанционный курс, далее только мотивирует и консультирует обучающихся, в то время как студенты, сами выбирают темп работы, порядок изученных тем и время для обучения.

Возможность обучения дистанционно через сеть Интернет позволяет активизировать учебный процесс. Включение аудио- и видео-материалов, онлайн тестирований, компьютерных тренажеров, интерактивными упражнениями и др. делает процесс обучения более эффективным и интересным, что повышает уровень освоения учебного материала.

Таким образом, можно сделать вывод, что электронные учебные пособия могут входить в состав дистанционных курсов.

1.5 Средства реализации электронного учебного пособия

Электронное учебное пособие разработано на платформе для создания Web-сайтов WordPress и опубликовано на хостинге Beget.

WordPress — это система управления содержимым сайта с открытым исходным кодом, написанная на языке Personal Home Page (PHP), который в настоящее время поддерживается большинством хостинг-провайдеров [6]. Система WordPress имеет значительно много тем, плагинов и виджетов, при этом остается максимально простой и удобной.

Хостинг Beget — это один из крупнейших хостинг-провайдеров из Санкт-Петербурга. Компания основана в 2007 году и сегодня занимает лидирующие позиции по количеству клиентов и качеству предоставляемых услуг в России и ближнем зарубежье [21].

При создании электронного учебного пособия в WordPress была использована тема Twenty Eleven [30]. Данная тема является бесплатной с возможностью платных расширений. В бесплатной версии темы, есть оптимальный набор функций, которые без труда помогут создать сайт быстро и со вкусом.

Также, были использованы плагины в WordPress:

- elementor;
- jQuery Smooth Scroll;
- watu quiz.

Elementor — это визуальный конструктор страниц, позволяющий создать любой дизайн страниц не зависимо от выбранной темы, меню очень удобное и простое [10].

Плагин jQuery Smooth Scroll позволяет добавить прокрутку на верх страницы сайта с помощью кнопки вверх которая отображается в нижней правой части экрана [26].

Плагин watu quiz позволяет создать тесты с отображением результата прохождения [29]. После создания теста и размещения его на странице, в настройках теста показывает количество прохождений, дату и баллы за прохождение.

Так же, при создании электронного учебного пособия были использованы:

- Google Диск;
- Camtasia Studio;
- Microsoft Office word;
- LearningApps.

Google Диск — это файловый хостинг, созданный и поддерживаемый компанией Google. Его функции включают хранение файлов в Интернете, общий доступ к ним и совместное редактирование. В состав Google Диска входят Google Документы, Таблицы и Презентации — набор офисных приложений для совместной работы над текстовыми документами, электронными таблицами, презентациями, чертежами, Web-формами и другими файлами [5].

Camtasia Studio — это программное обеспечение для захвата видео с экрана, разработанное компанией TechSmith. Пользователь определяет область экрана, которое должно быть захваченным. Camtasia Studio позволяет пользователю записывать звук с микрофона или динамиков, а также разместить на экране видеоматериалы с Web-камеры [4].

Microsoft Office Word — это хорошо знакомое всем приложение, главным предназначением которого является создание и редактирование текстовых документов. Функциональное наполнение продукта позволяет создавать документы различных типов, применяя всевозможные способы оформления и структурирования текста [20].

LearningApps — это приложение для поддержки обучения и процесса преподавания с помощью интерактивных модулей. LearningApps.org позволяет удобно и легко создавать электронные интерактивные упражнения. При желании любой учитель, имеющий самые минимальные навыки работы с информационно-компьютерными технологиями (ИКТ), может создать свой ресурс — небольшое упражнение для объяснения нового материала, для закрепления, тренинга, контроля [17].

2 РАЗРАБОТКА ЭЛЕКТРОННОГО УЧЕБНОГО ПОСОБИЯ «ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ»

2.1 Педагогический адрес

Электронное учебное пособие «Электронно-цифровая подпись» предназначено для следующих категорий слушателей: для студентов направления подготовки 44.03.04 Профессиональное обучение (по отраслям) профиля «Информационные технологии», для студентов направления подготовки 46.03.02 Документоведение и архивоведение, а также для всех желающих, имеющих достаточный уровень компьютерной грамотности.

Электронное учебное пособие предназначено для формирования у студентов четкого представления и понимания теоретических и прикладных знаний о современных методах обеспечения аутентификации электронных документов в информационных инфраструктурах пред-приятий и организаций, а также формирования знаний, умений и навыков, позволяющих студентам проводить анализ используемых электронно-цифровых подписей, понимать и использовать современные алгоритмы построения этих подписей, производить оценку возможностей, ограничений и областей применений данных электронно-цифровых подписей.

2.2 Структура электронного учебного пособия «Электронно-цифровая подпись»

Разработка электронного учебного пособия начинается с проектирования его структуры, которая и определяет его содержание и способы взаимодействия с ним.

Структура электронного учебного пособия имеет три основных блока:

- 44.03.04 Профессиональное обучение (по отраслям);

- 46.03.02 Документоведение и архивоведение;
- справочная информация.

Структуру можно представить в виде иерархии элементов представленной на рисунке 1.

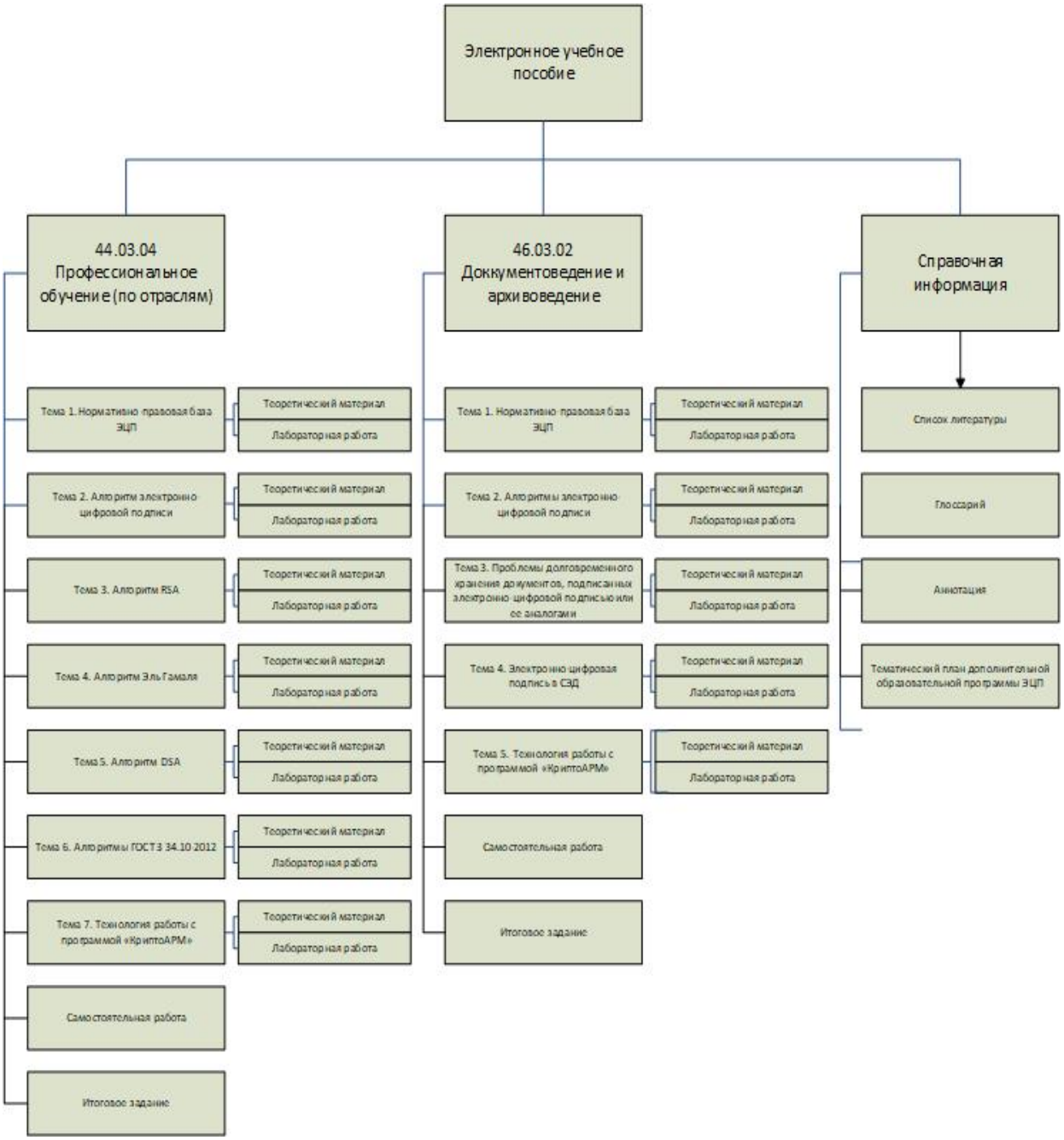


Рисунок 1 — Иерархия электронного учебного пособия

Блок «44.03.04 Профессиональное обучение (по отраслям)» содержит теоретический и практический материал по темам, соответствующим тематическому плану дополнительной образовательной программы для данного направления. Так же данный блок содержит материалы итогового задания по

окончанию прохождения данной дополнительной образовательной программы.

Блок «46.03.02 Документоведение и архивоведение» содержит теоретический и практический материал по темам, соответствующим тематическому плану дополнительной образовательной программы для данного направления. Так же данный блок содержит материалы самостоятельной работы и итогового задания по окончанию прохождения данной дополнительной образовательной программы.

Блок «Справочная информация» содержит следующие разделы:

- список литературы — содержит ссылки на литературные и интернет источники, а также названия учебной литературы;
- глоссарий — содержит список основных терминов и понятий, используемых в данном учебном пособии;
- о разработчике — в ней представлена информация о разработчиках дополнительной образовательной программы «Электронно-цифровая подпись» и о электронном учебно-методическом обеспечении для ее реализации;
- тематический план дополнительной образовательной программы «Электронно-цифровая подпись» — содержит список тем и часов, отводимых на их изучение.

На рисунке 2 представлен титульный лист электронного учебного пособия.

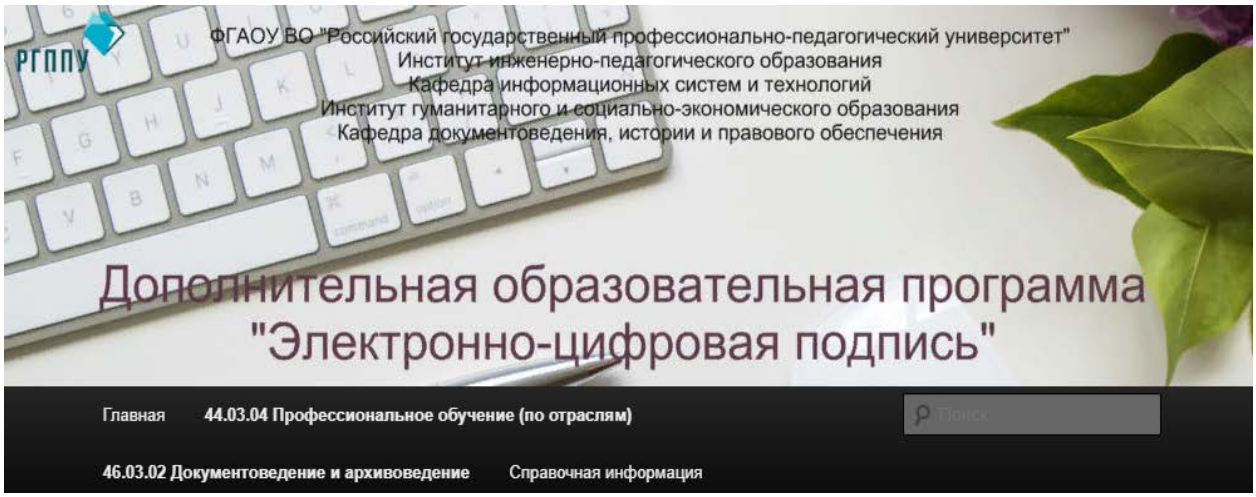


Рисунок 2 — Титульный лист электронного учебного пособия

Электронное учебное пособие, сделанное при помощи платформы, для создания Web-сайтов имеет немаловажные удобства в применении в учебном процессе, такие как:

- отсутствие требований установки или расширенных прав доступа для запуска;
- возможность запускать на компьютере, планшете или телефоне при наличии интернета;
- возможность передачи обучающемуся просто предоставить ссылку на сайт, где расположено электронное учебное пособие;
- наличие навигационного меню, для более быстрого перемещения;
- минимальные системные требования для работы с электронным учебным пособием;
- для их распространения не нужны деньги или бумага;
- не занимают много места [22].

2.3 Интерфейс и навигация по электронному учебному пособию «Электронно-цифровая подпись»

Данное электронное учебное пособие предназначено для студентов, желающих изучающие дополнительную образовательную программу «Электронно-цифровая подпись» и уровнем подготовки в области информационных технологий или документоведения.

Интерфейс — это совокупность средств, методов и правил взаимодействия (управления, контроля и т. д.) между элементами системы [3]

На главной странице находиться форма для записи на дополнительную образовательную программу «Электронно-цифровая подпись», информация о электронном учебном пособии и видеоролик-приветствие, продемонстрированный на рисунке 3, в котором представлена информация о структуре и содержании электронного учебного пособия.

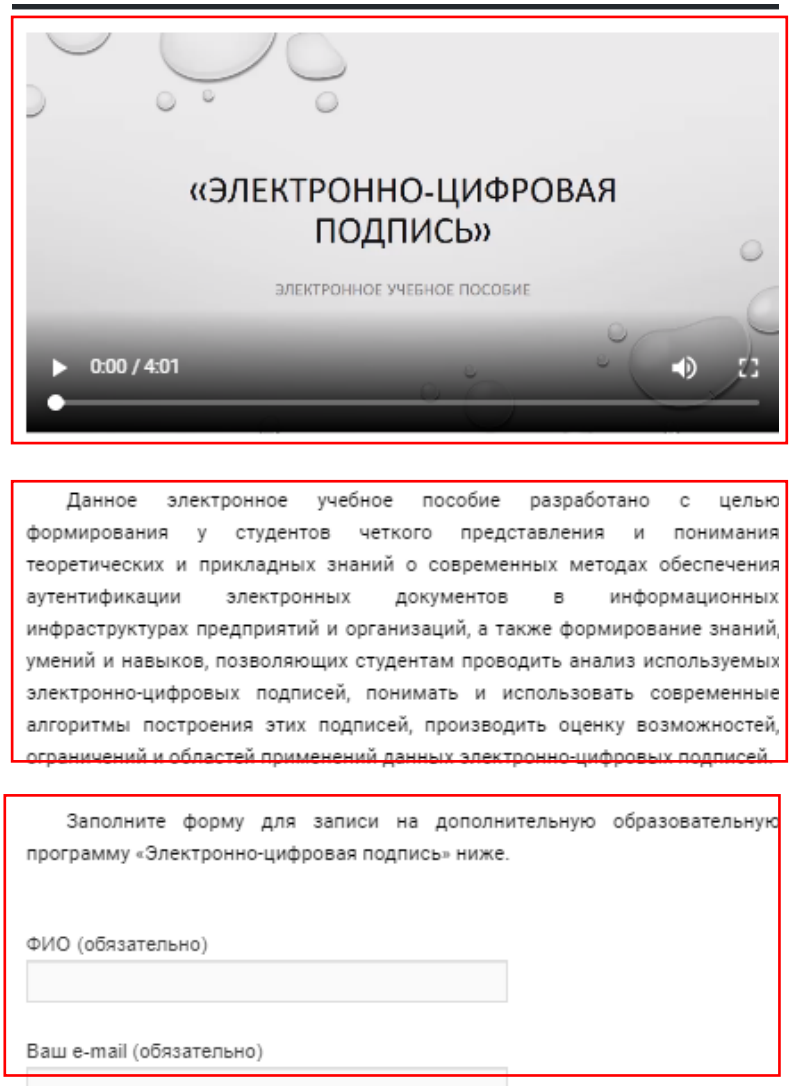


Рисунок 3 — Главная страница электронного учебного пособия

Поскольку электронное учебное пособие предназначено для обучения специалистов разного уровня, это было учтено при проектировании интерфейса — в частности, главного навигационного меню, что продемонстрировано на рисунке 4.

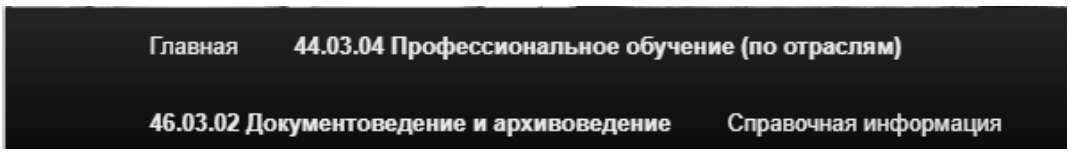


Рисунок 4 — Главное меню электронного учебного пособия

Данное меню было создано в настройках WordPress на боковой панели, во вкладке «Меню», как показано на рисунке 5.

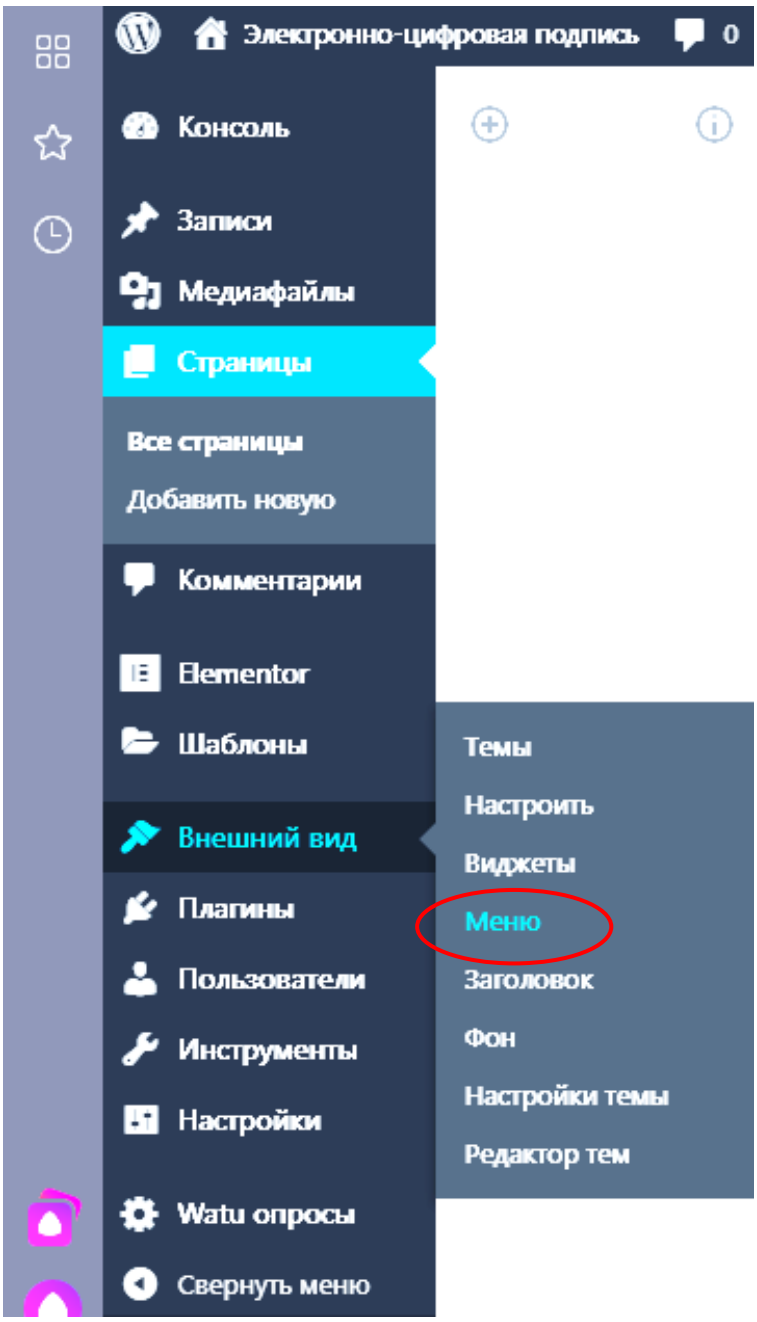


Рисунок 5 — Панель настроек WordPress

В настройке было выбрано название и тип меню, как показано на рисунке 6.

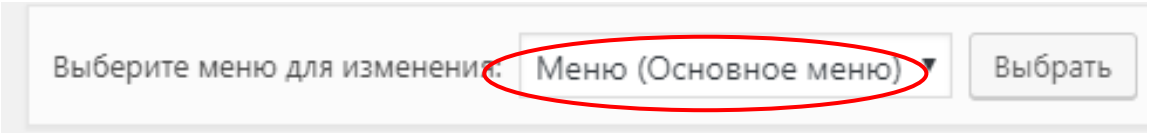


Рисунок 6 — Название и тип меню

Были добавлены страницы меню, как показано на рисунке 7.

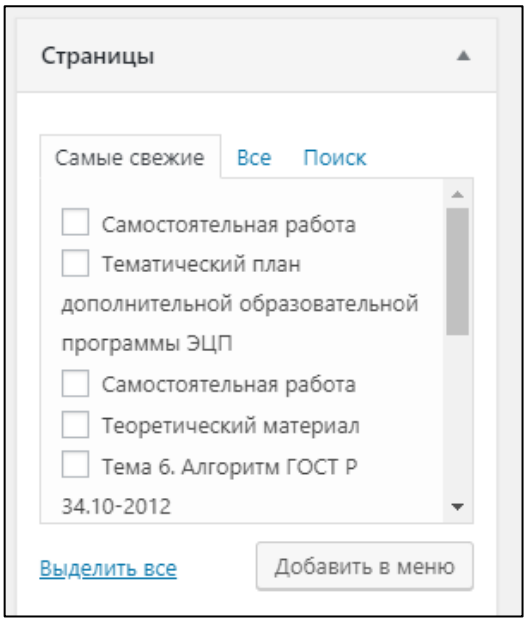


Рисунок 7 — Добавление страниц меню

Также была настроена структура меню, главные страницы и их дочерние элементы как показано на рисунке 8.

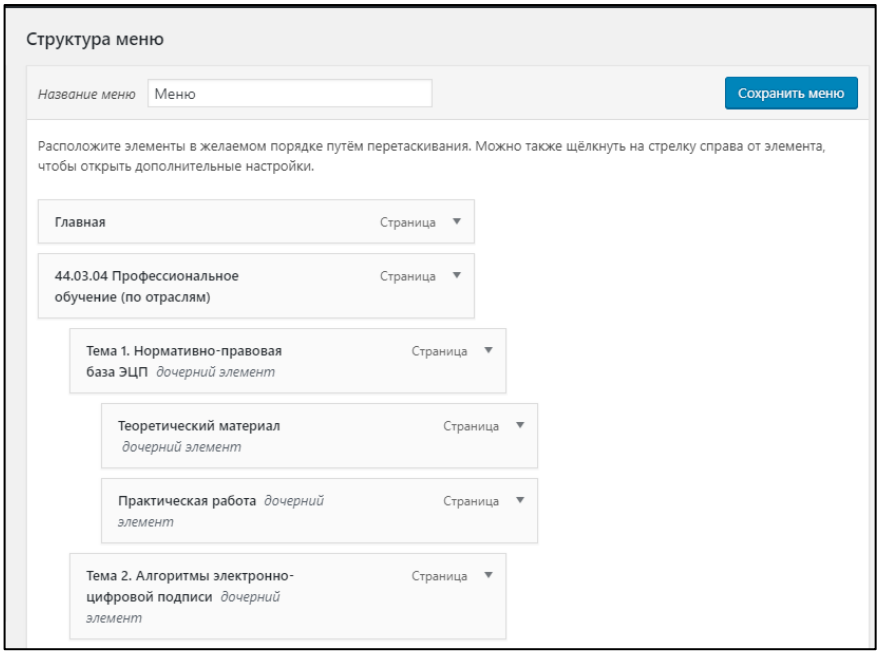


Рисунок 8 — Настройка структуры меню

Для облегчения работы с электронным учебным пособием студентам в поиске теоретического или практического занятия определенной темы, на которой они остановились, было сделано выпадающее меню, продемонстрированное на рисунке 9.

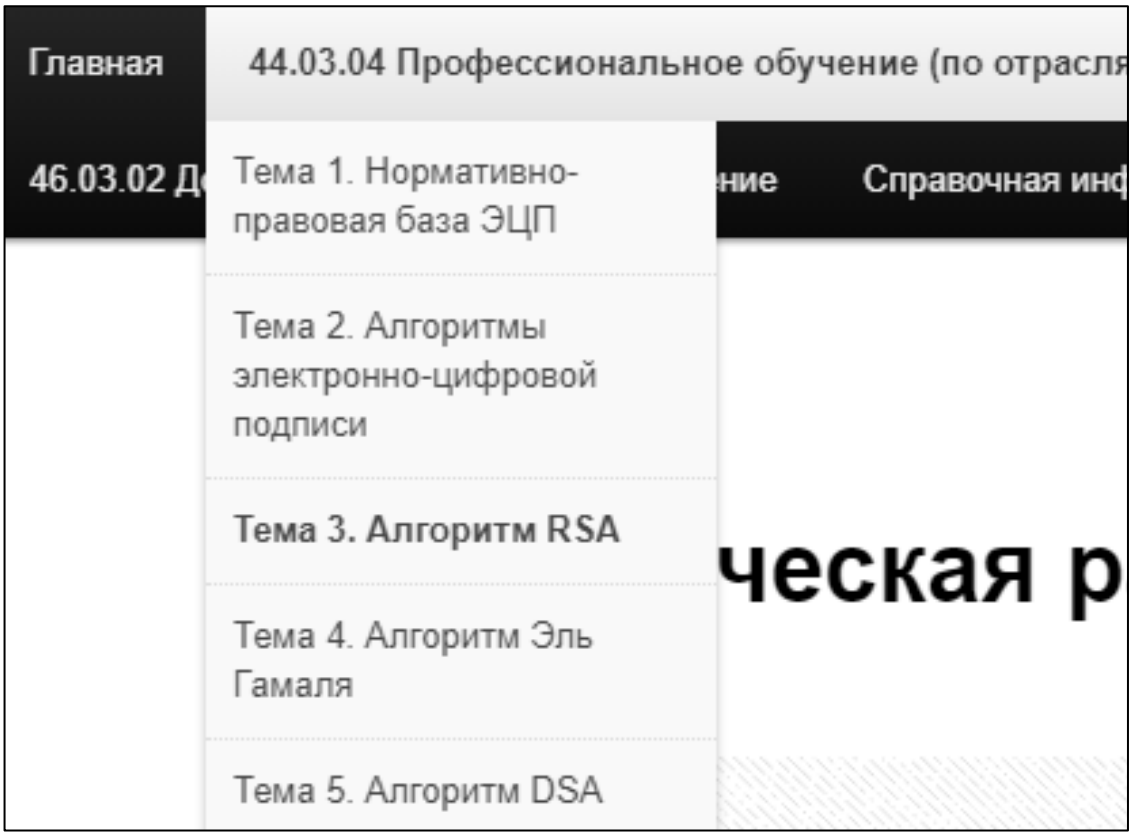


Рисунок 9 — Выпадающее меню в электронном учебном пособии

Выпадающее меню было сделано с помощью темы сайта, показанного на рисунке 10.

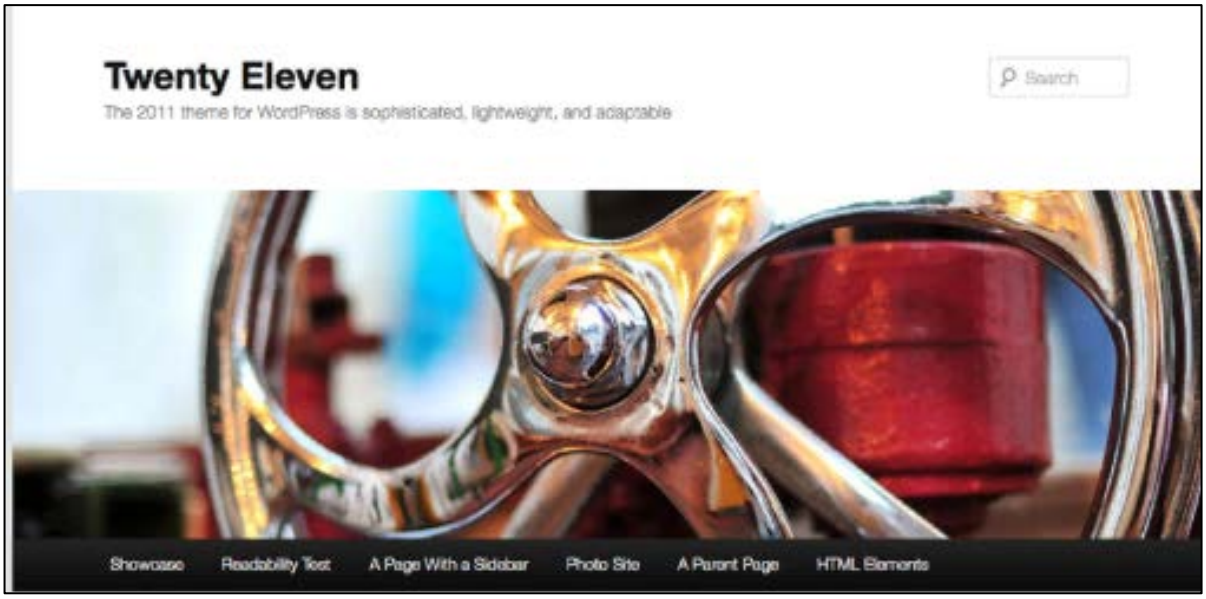


Рисунок 10 — Выбранная тема сайта

Изображение заголовка было скачено из сети интернет, продемонстрировано на рисунке 11.

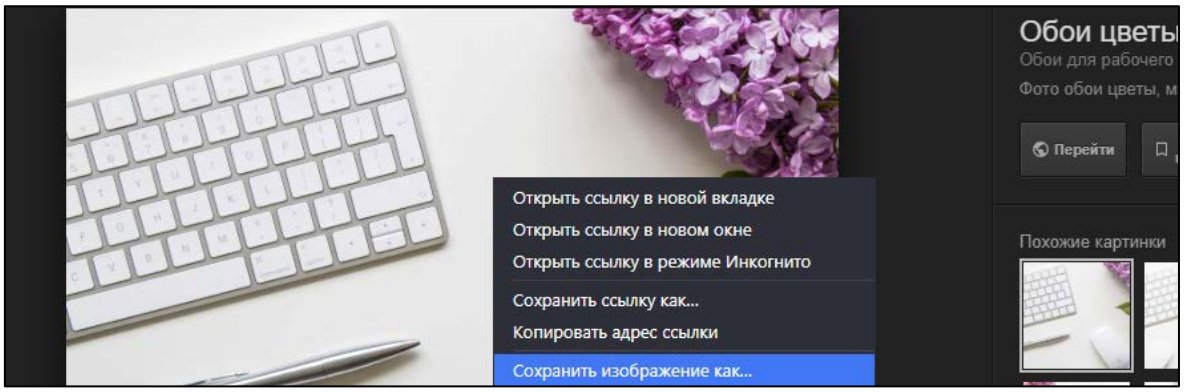


Рисунок 11 — Скачивание изображение для заголовка

На данное изображение была добавлена надпись «Электронно-цифровая подпись» и логотип в программе Paint, как показано на рисунке 12.

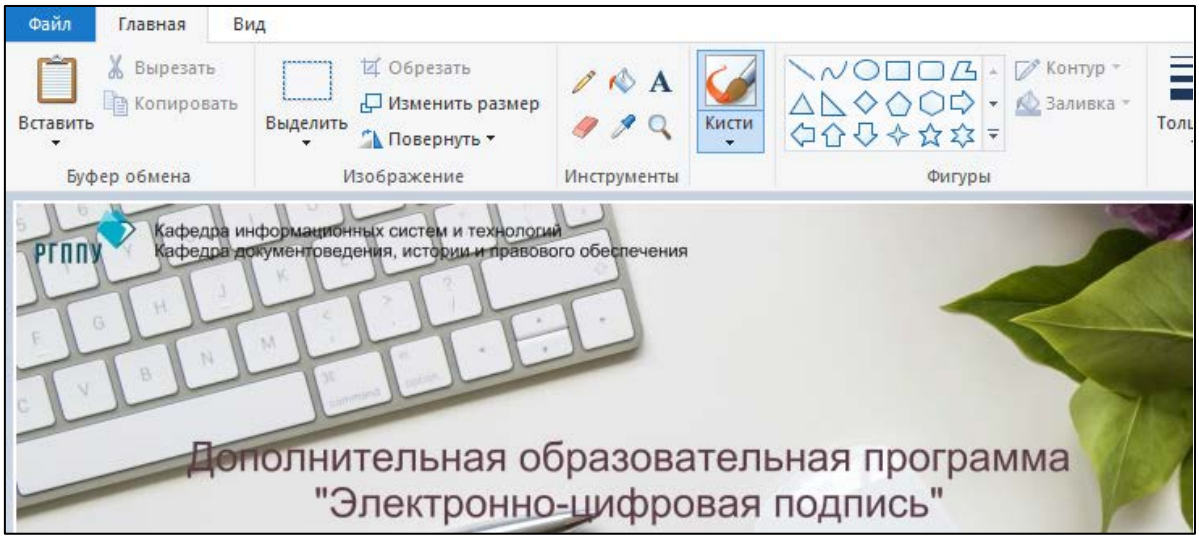


Рисунок 12 — Добавление надписи и логотипа на изображение в Paint

А также добавлено в изображение заголовка в основных настройках WordPress показано на рисунке 13.

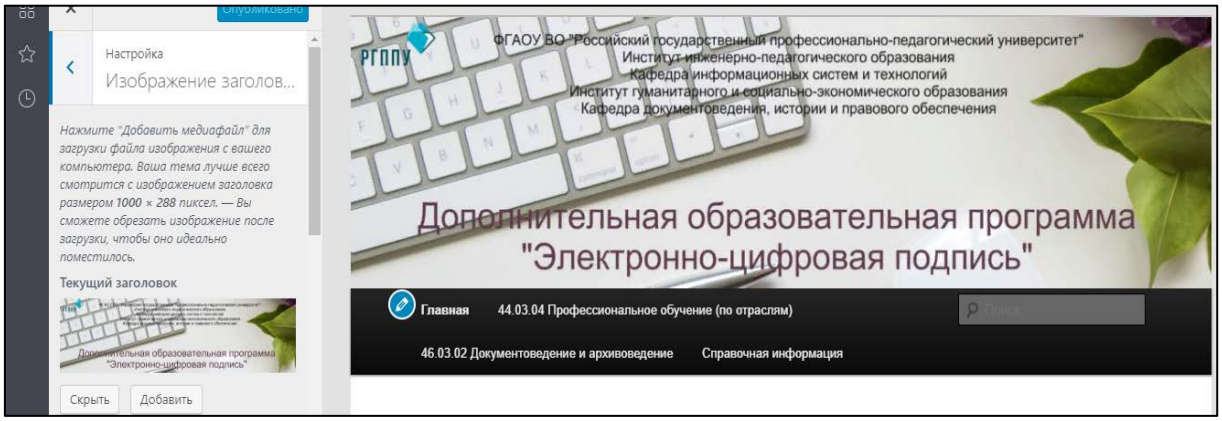


Рисунок 13 — Добавление изображения для заголовка в WordPress

В меню справа есть окно для поиска информации по электронному учебному пособию, которое показано на рисунке 14.

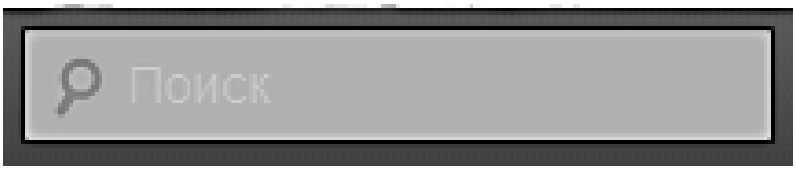


Рисунок 14 — Окно поиска информации в электронном учебном пособии

Окно для поиска информации было добавлено в настройке виджетов WordPress, что продемонстрировано на рисунке 15.

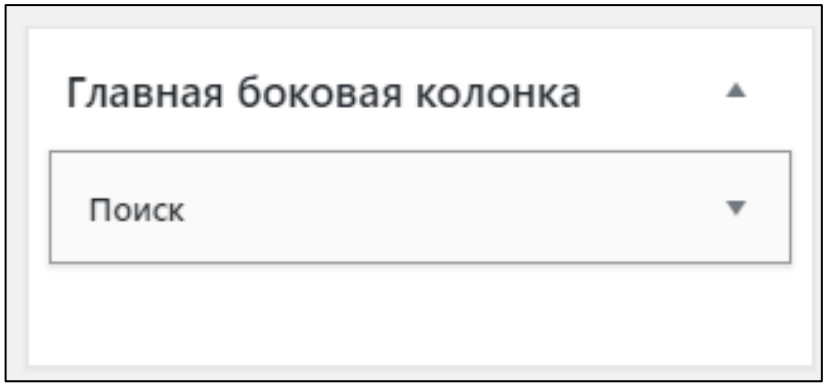


Рисунок 15 — Настройка виджета «Поиск»

Цветовая схема электронного учебного пособия была выбрана светлая, в настройках темы WordPress, представлено на рисунке 16.

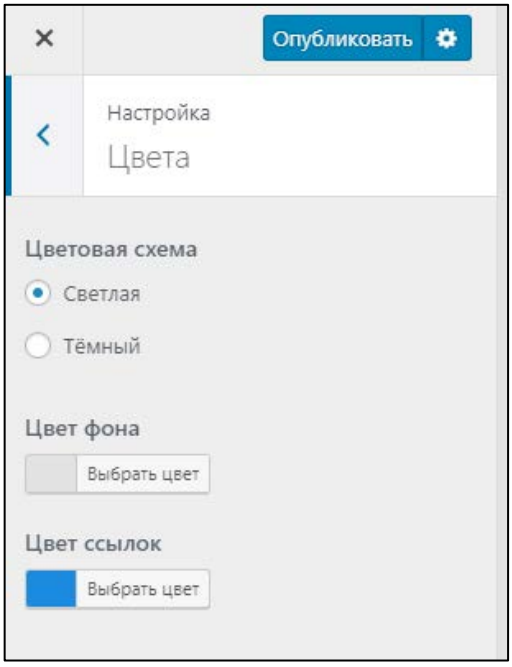


Рисунок 16 — Выбор цветовой схемы в электронном учебном пособии

В каждой рассматриваемой теме на основной странице написано, что будет в ней рассмотрено, как показано на рисунке 17.

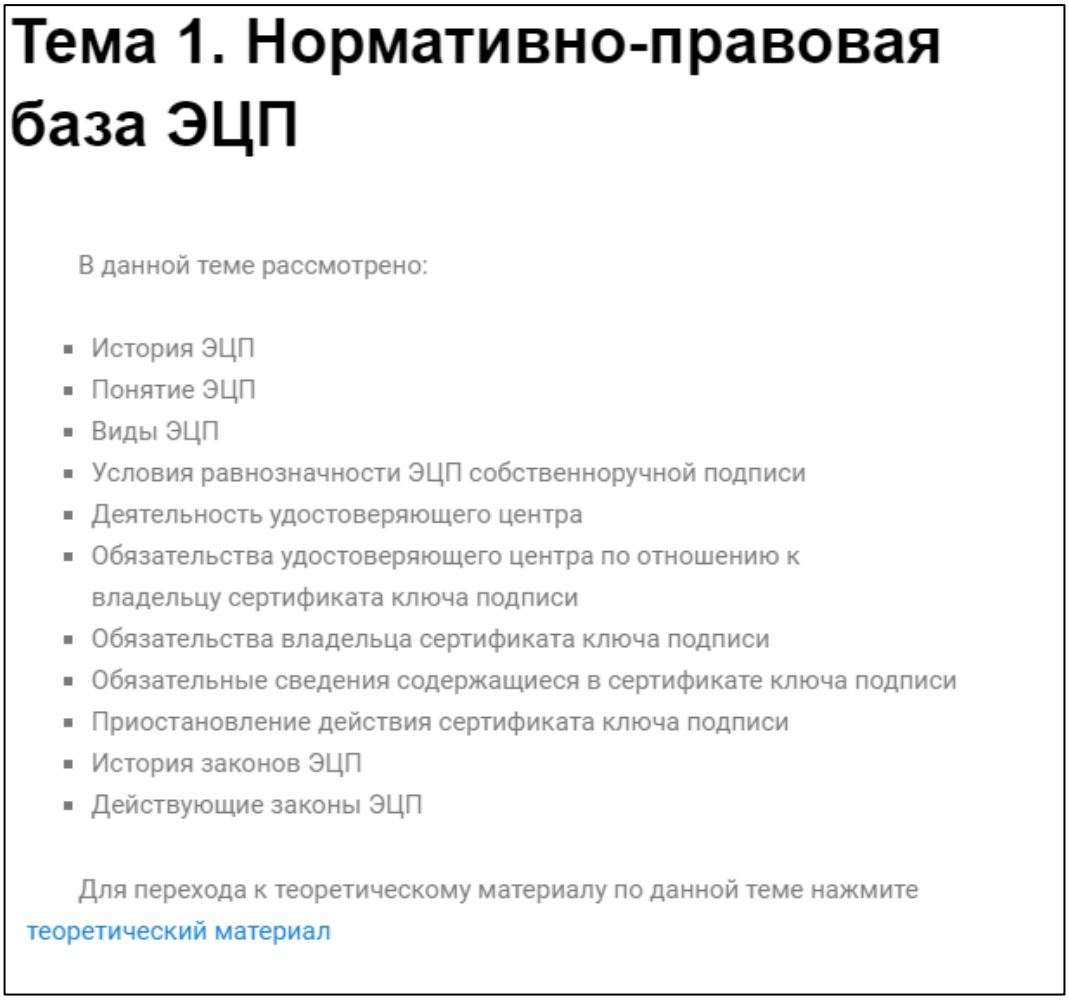


Рисунок 17 — Основная страница выбранной темы

На основных страницах тем, сделаны переходы при нажатии на текст синего цвета, синий цвет стоит по умолчанию, представлено на рисунке 18.

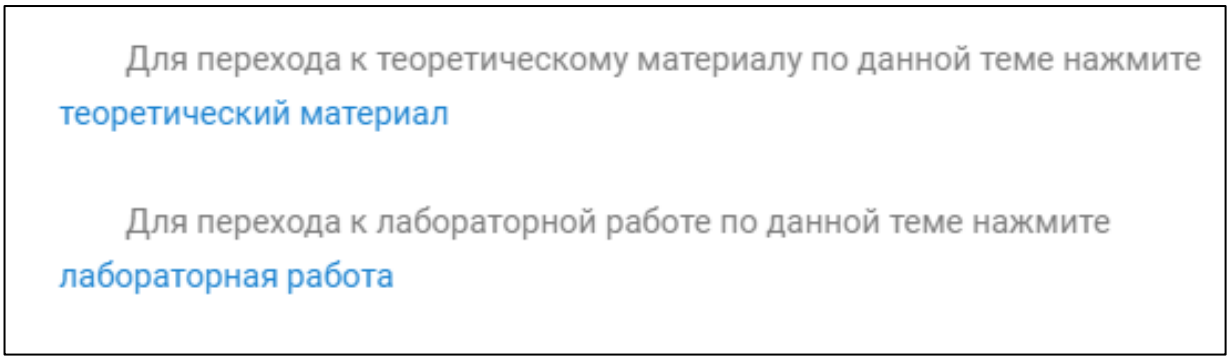


Рисунок 18 — Пример ссылок на теоретический и практический материал

Данные переходы на теоретический и практический материал сделаны с помощью плагина Elementor, представленного на рисунке 19.

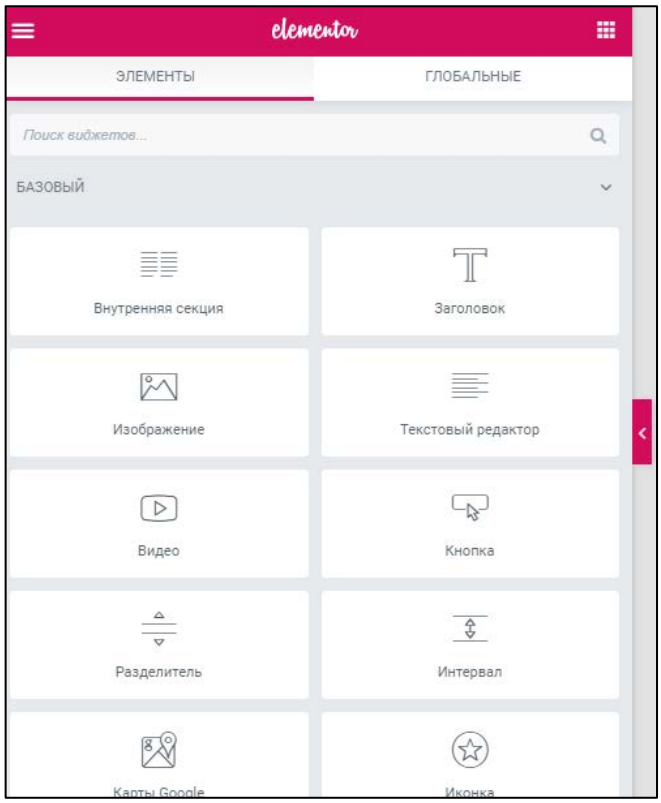


Рисунок 19 — Плагин Elementor

На теоретический и практический материал также возможно перейти через выпадающее меню, которое продемонстрированное на рисунке 20.

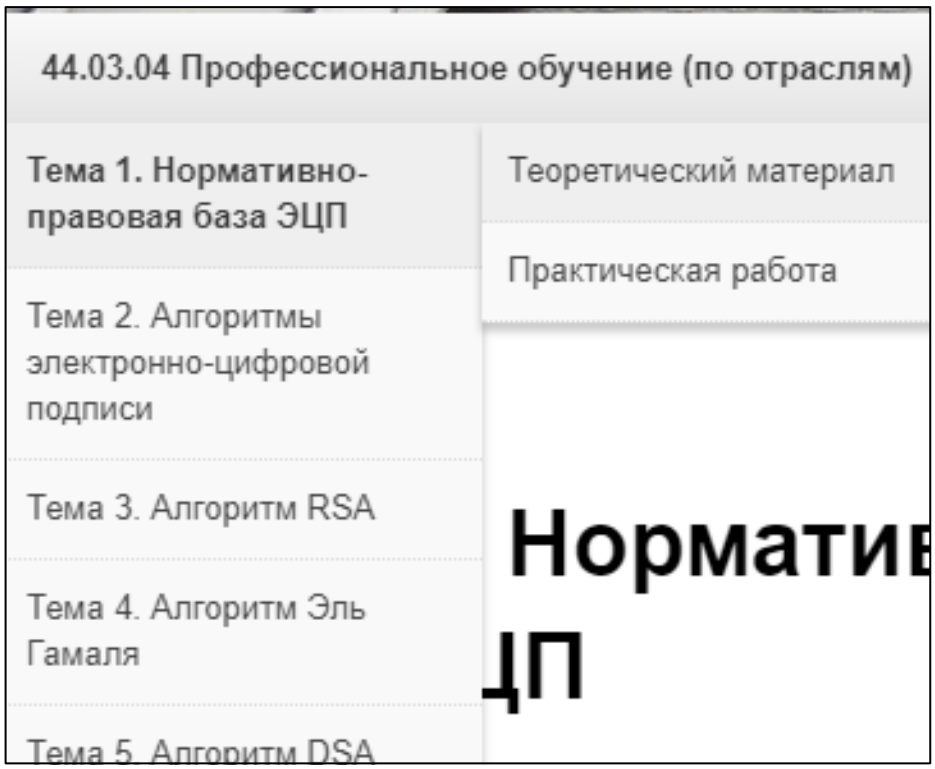


Рисунок 20 — Переход к лекционному или практическому материалу с помощью выпадающего меню

Для того чтобы начать редактировать страницу с помощью плагина Elementor, нужно нажать на кнопку вверху страницы «Редактировать в Elementor», как показано на рисунке 21.

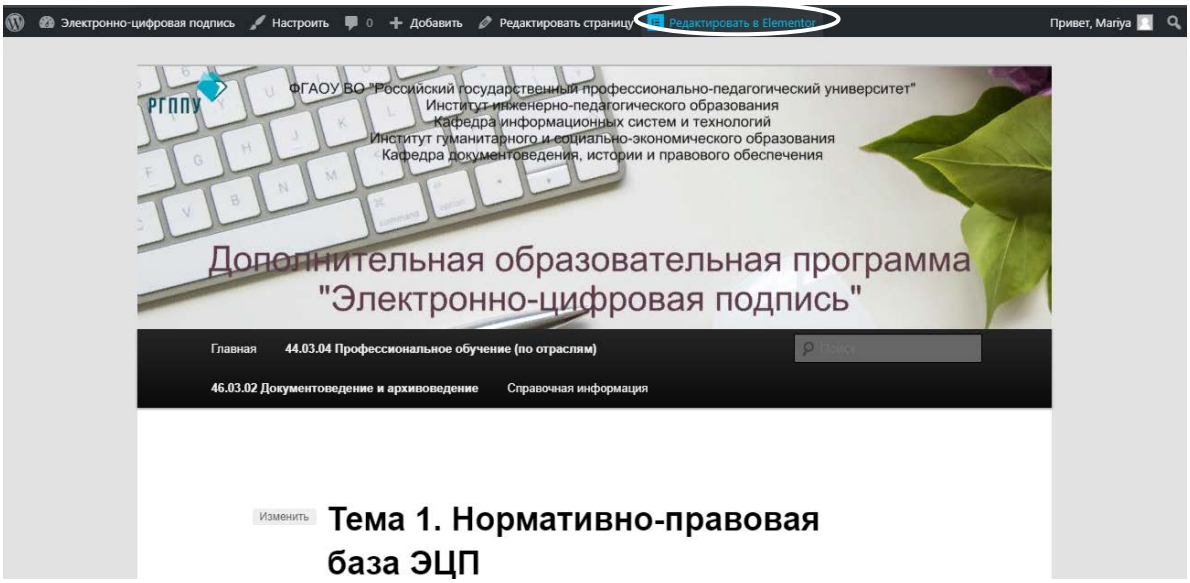


Рисунок 21 — Кнопка, предназначенная для редактирования страницы в Elementor

Чтобы написать текст на странице нужно выбрать блок «Текстовый редактор», показанный на рисунке 22.

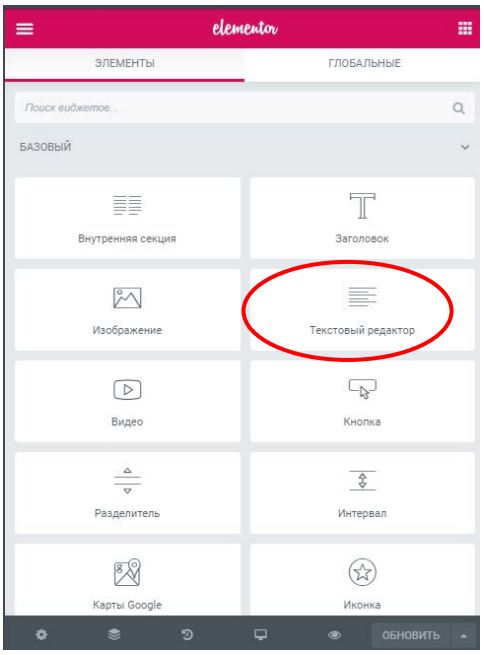


Рисунок 22 — Блок «Текстовый редактор»

Для работы с данным блоком нужно перенести его в область для размещения виджетов справа, как показано на рисунке 23.

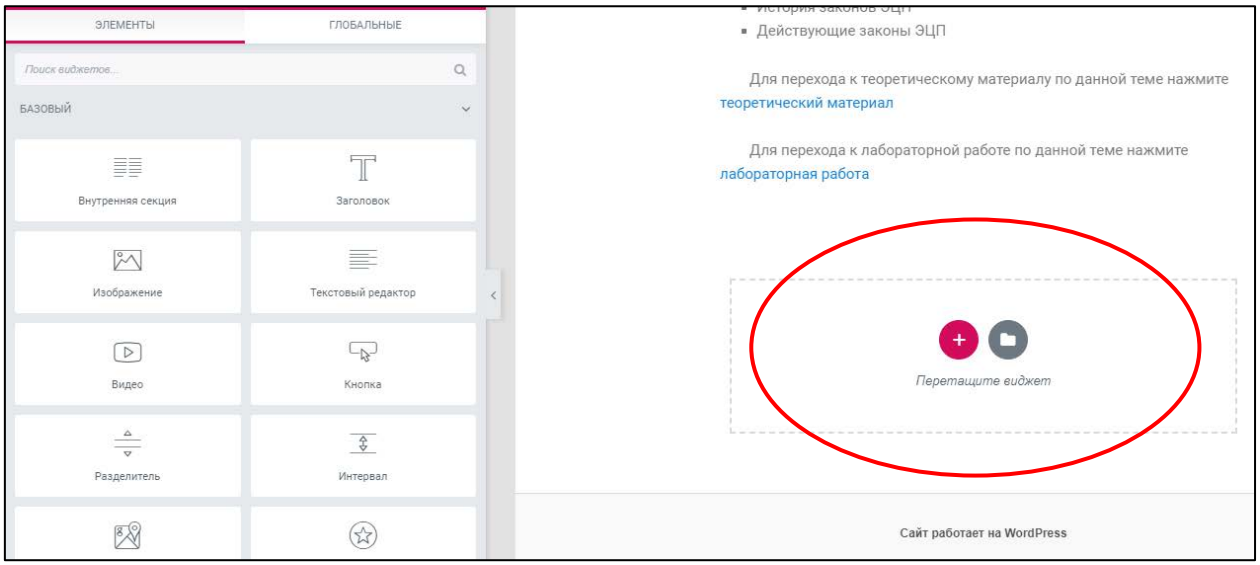


Рисунок 23 — Область для виджетов

Далее необходимый текст был набран, сделан маркированный список во вкладке «Содержимое» рисунок 24.

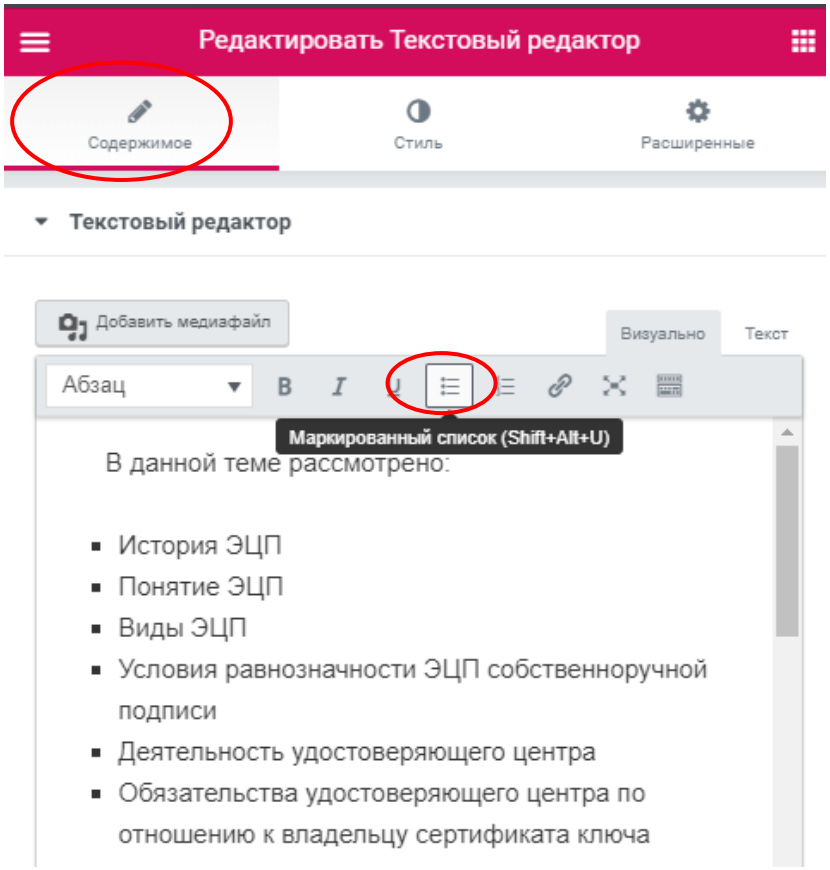


Рисунок 24 — Кнопка для работы с маркированным списком, во вкладке «Содержимое»

Чтобы сделать ссылки для перехода на другие страницы нужно нажать «Вставить/Изменить ссылку», показано на рисунке 25.

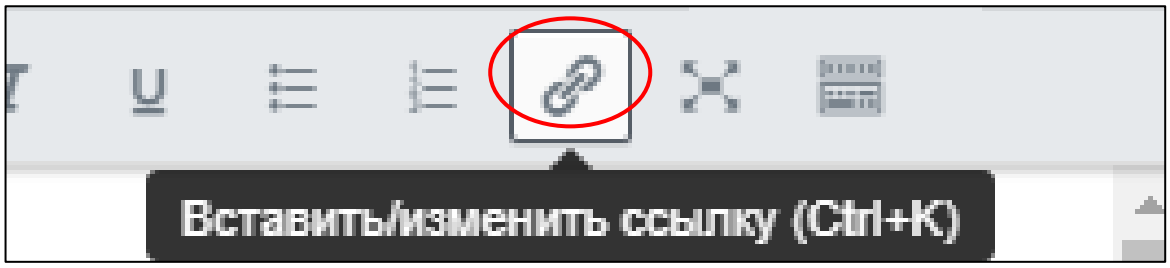


Рисунок 25 — Кнопка для вставки ссылки

Далее нужно выбрать нужную страницу для вставки и нажать «Добавить ссылку» продемонстрированно на рисунке 26.

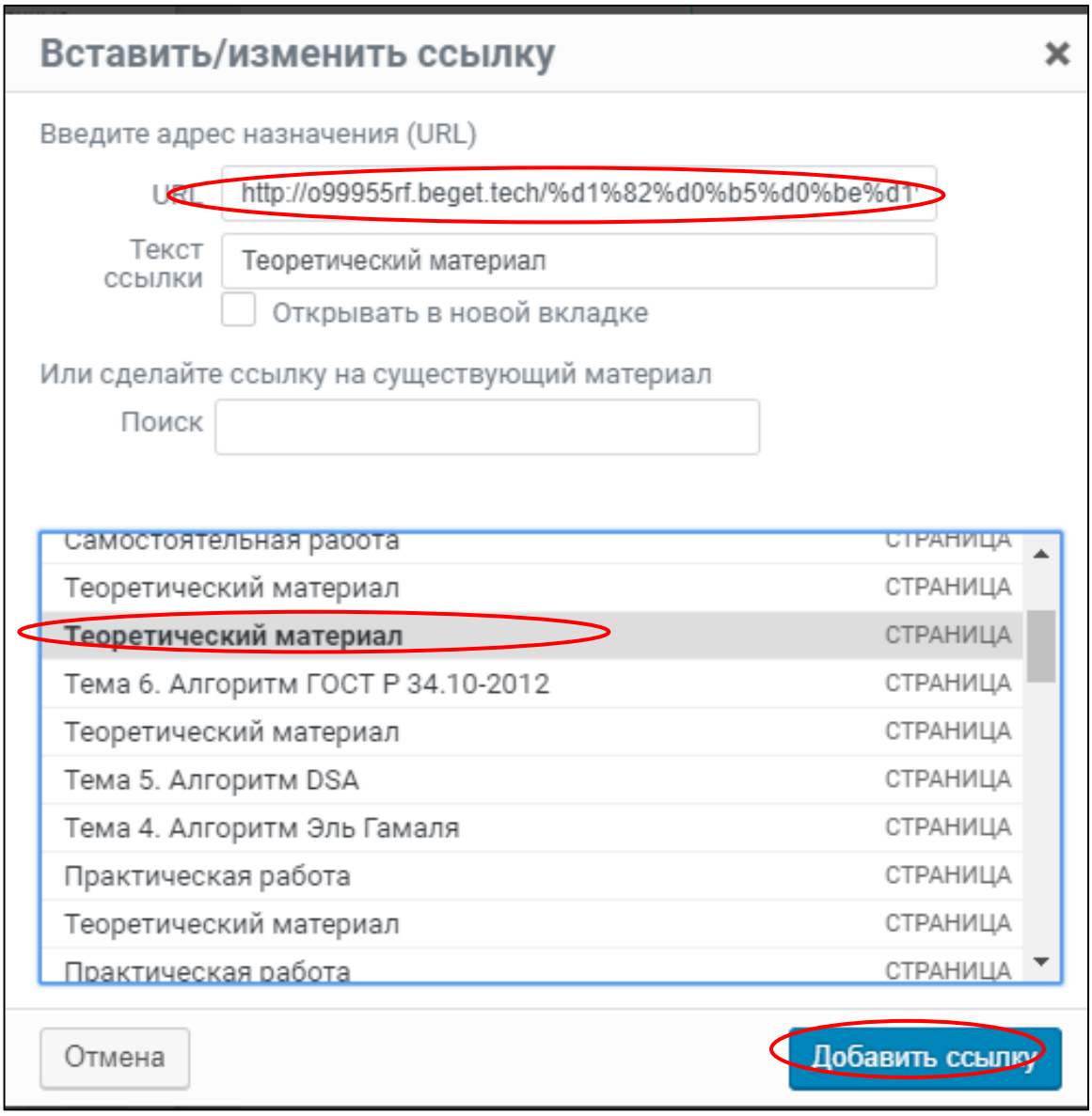


Рисунок 26 — Добавление ссылки на страницу

Отступы текста от края сделаны с помощью вкладки «Текст» кодом, показанным на рисунке 27.

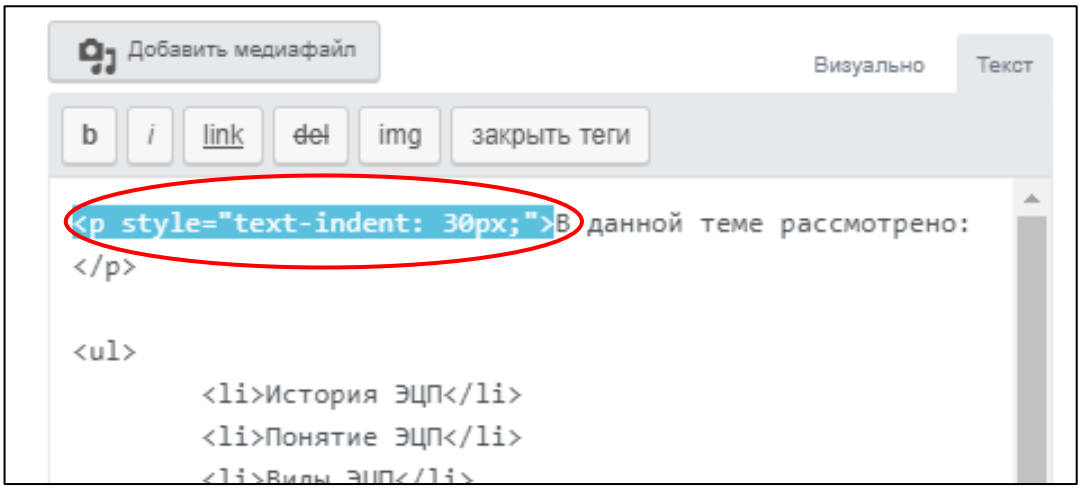


Рисунок 27 — Пример редактирования текста кодом

Для более продуктивной работы стоит придерживаться простой схемы работы с электронным учебным пособием «Теоретический материал — Практический материал», а также прохождения тем в заданном порядке.

В каждом теоретическом или практическом материале вначале есть содержание, которое является навигационным меню по странице, как показано на рисунке 28.

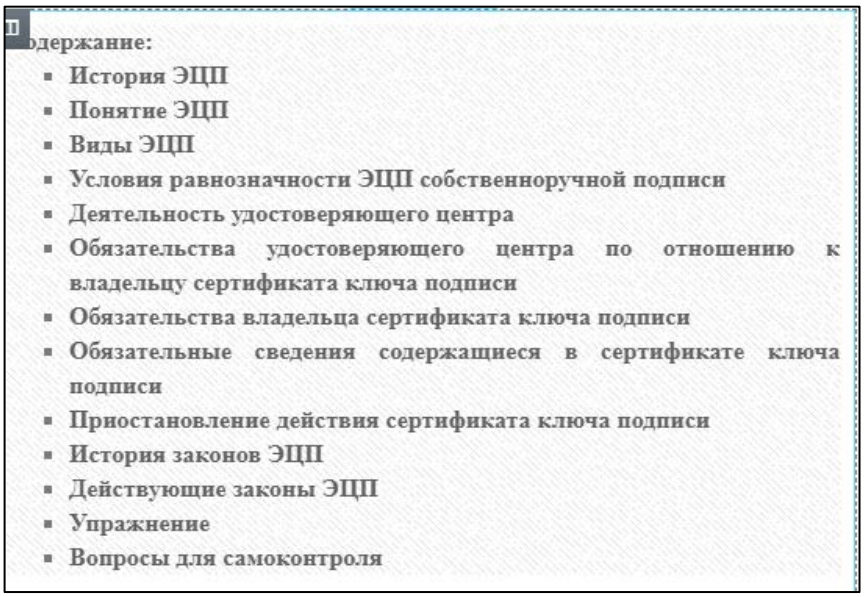


Рисунок 28 — Навигационное меню по странице

Навигационное меню на странице было сделано, через плагин Elementor в текстовом редакторе, просто написав код к тексту, на который будут нажимать для перехода, как показано на рисунке 29.

Рисунок 29 — Код текста, на который будут нажимать для перехода на основной

Также кодом нужно прописать, на какой текст при нажатии будут переходить, показано на рисунке 30.

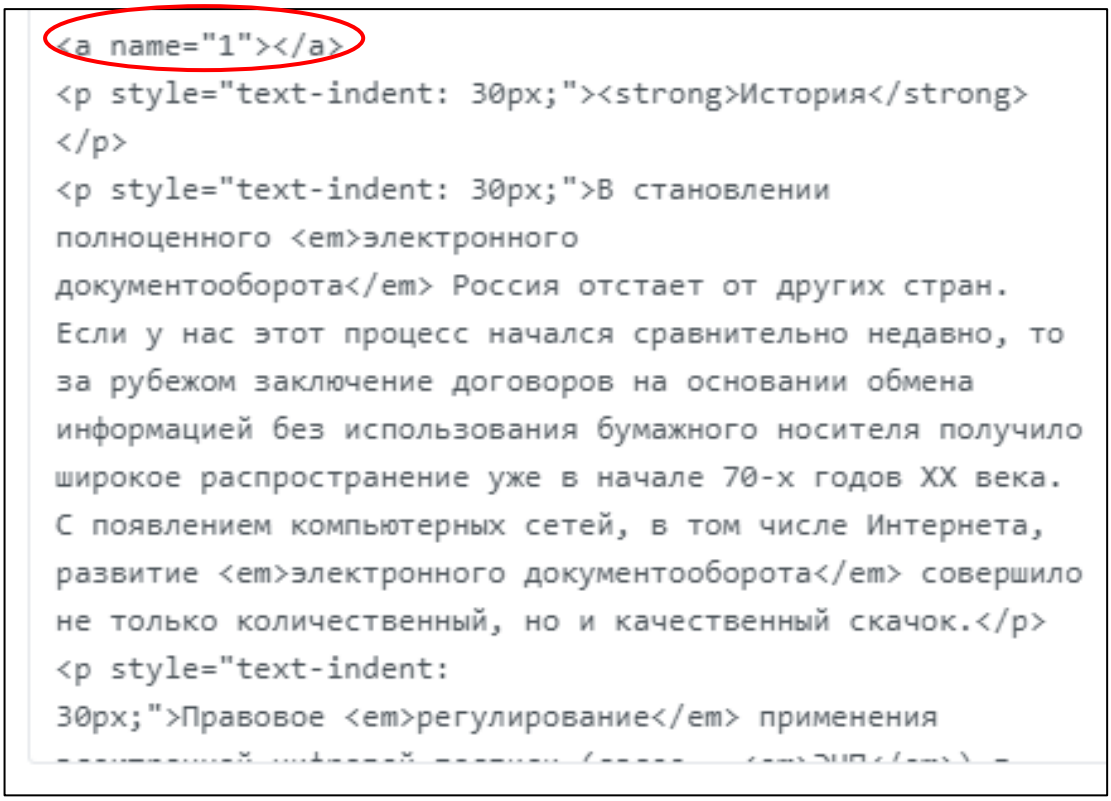


Рисунок 30 — Код текста, на который будут переходить

2.4 Разработка обучающих видеороликов

В электронном учебном пособии сделаны небольшие видеоролики на темы лекции в программе Camtasia. Чтобы запустить видеоролики, нужно нажать на стрелочку в левом нижнем углу или в центре изображения показано на рисунке 31.

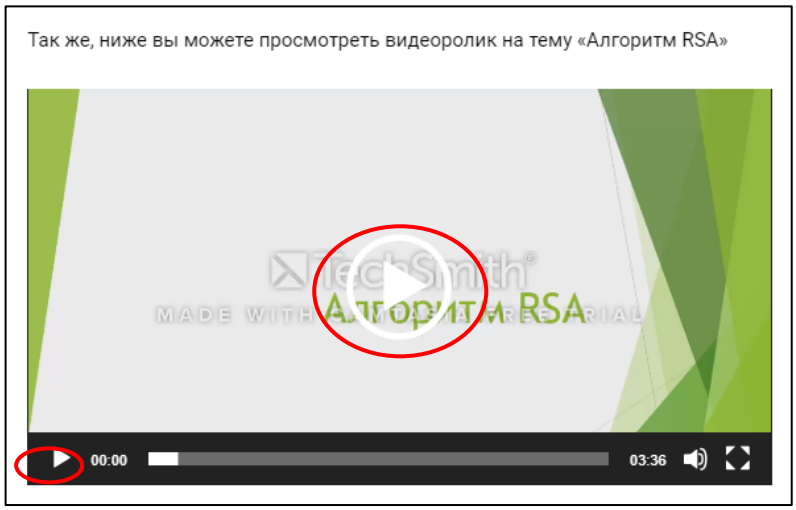
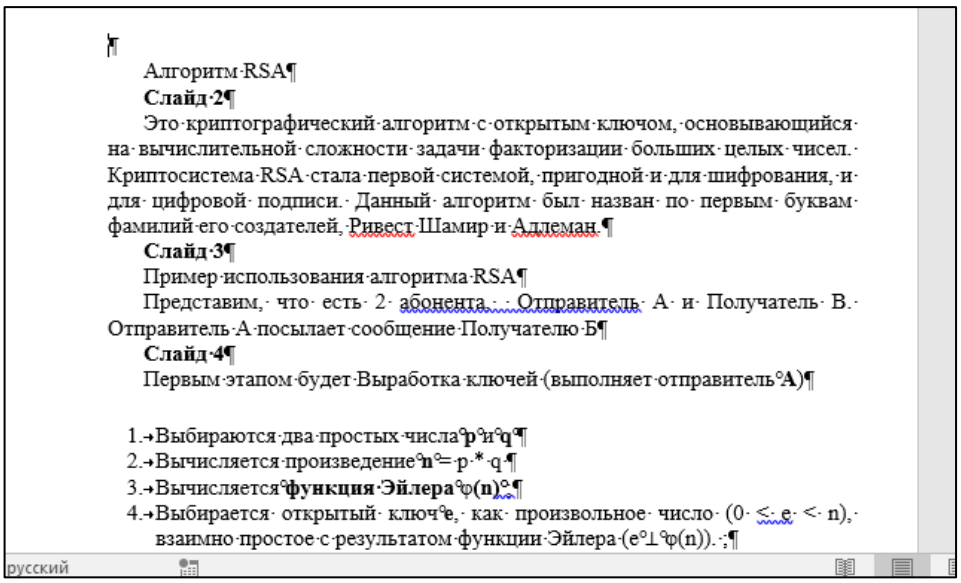


Рисунок 31 — Пример видеоролика в электронном учебном пособии

Для создания данного видеоролика был написан сценарий в Microsoft Word, представлено на рисунке 32.



Алгоритм RSA

Слайд 2

Это криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Данный алгоритм был назван по первым буквам фамилий его создателей, Ривест Шамир и Адлеман.

Слайд 3

Пример использования алгоритма RSA

Представим, что есть 2 абонента . . Отправитель А и Получатель В. Отправитель А посылает сообщение Получателю Б

Слайд 4

Первым этапом будет Выработка ключей (выполняет отправитель **A**)

1. Выбираются два простых числа **p** и **q**
2. Вычисляется произведение **n** = p * q
3. Вычисляется **функция Эйлера** **φ(n)**
4. Выбирается открытый ключ **e**, как произвольное число (0 < e < n), взаимно простое с результатом функции Эйлера (e ⊥ φ(n)).

русский

Рисунок 32 — Сценарий видеоролика

Далее, была сделанная презентация в Microsoft Power Point показано на рисунке 33.

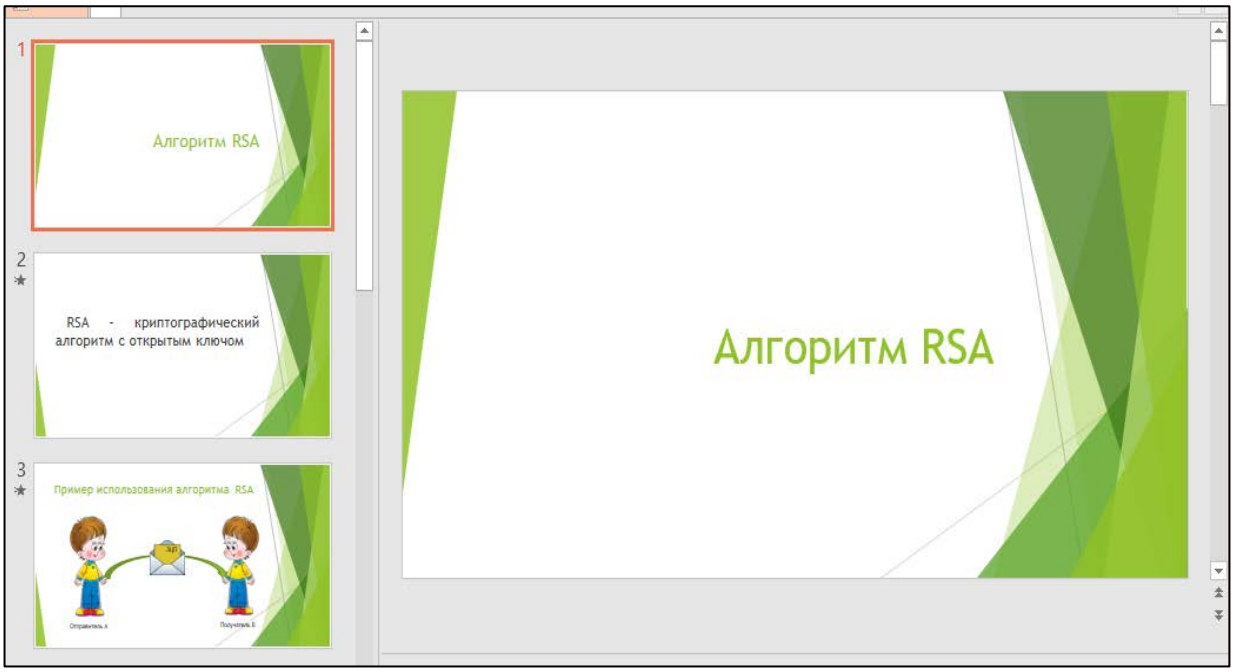


Рисунок 33 — Презентация для видеоролика

А также производилась запись и монтаж в программе Camtasia Studio, что представлено на рисунке 34.

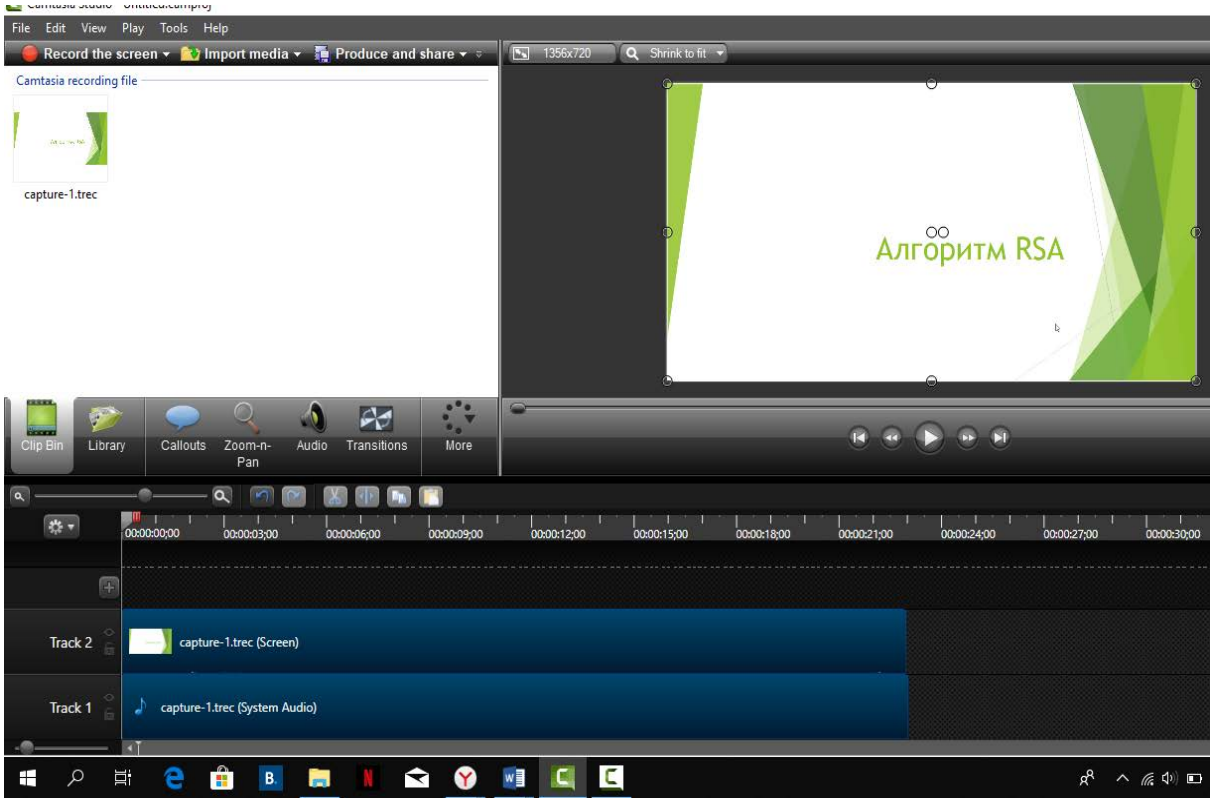


Рисунок 34 — Монтаж видеоролика и Camtasia

Camtasia Studio, как нельзя лучше, подходит для создания различных обучающих уроков и видео-курсов [8].

2.5 Разработка элементов контроля для электронного учебного пособия

Для текущего и итогового контроля знаний и умений слушателей в условиях дополнительного образования взрослых рекомендуется применять интерактивные методы, которые позволяют повысить активность обучающихся [23].

Интерактивные способы контроля качества знаний обучающихся, способствуют повышению их заинтересованности, обнаружению достижений, успехов обучающихся, а главное углублению знаний и умений [18].

В конце каждого теоретического материала сделан контроль, в виде интерактивных упражнений в LearningApps продемонстрировано на рисунке 35.

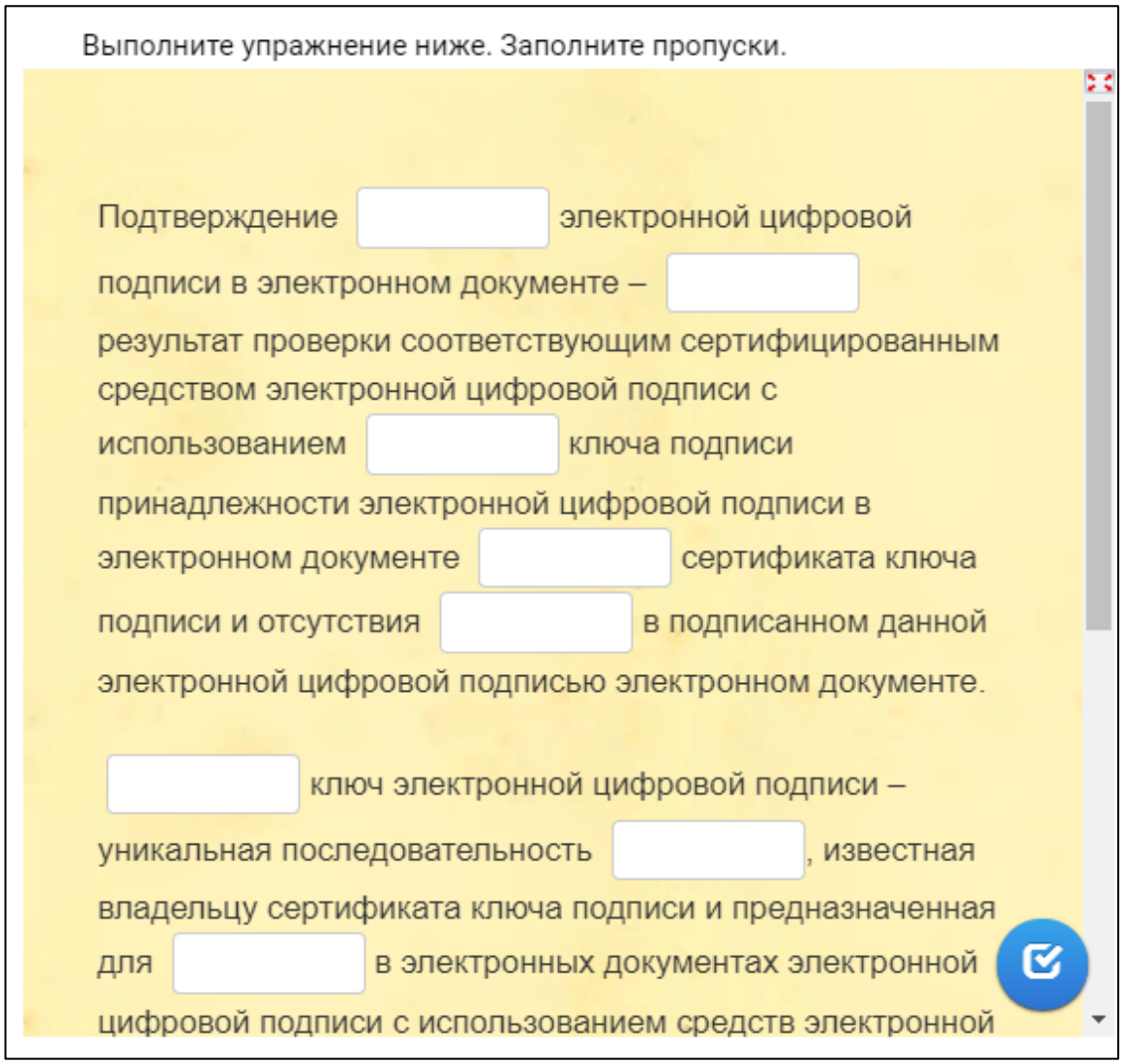


Рисунок 35 — Пример упражнения в LearningApps

Для того чтобы создать интерактивное упражнение, нужно зайти на сайт LearningApps.org и нажать на область меню «Новое упражнение» показано на рисунке 36.

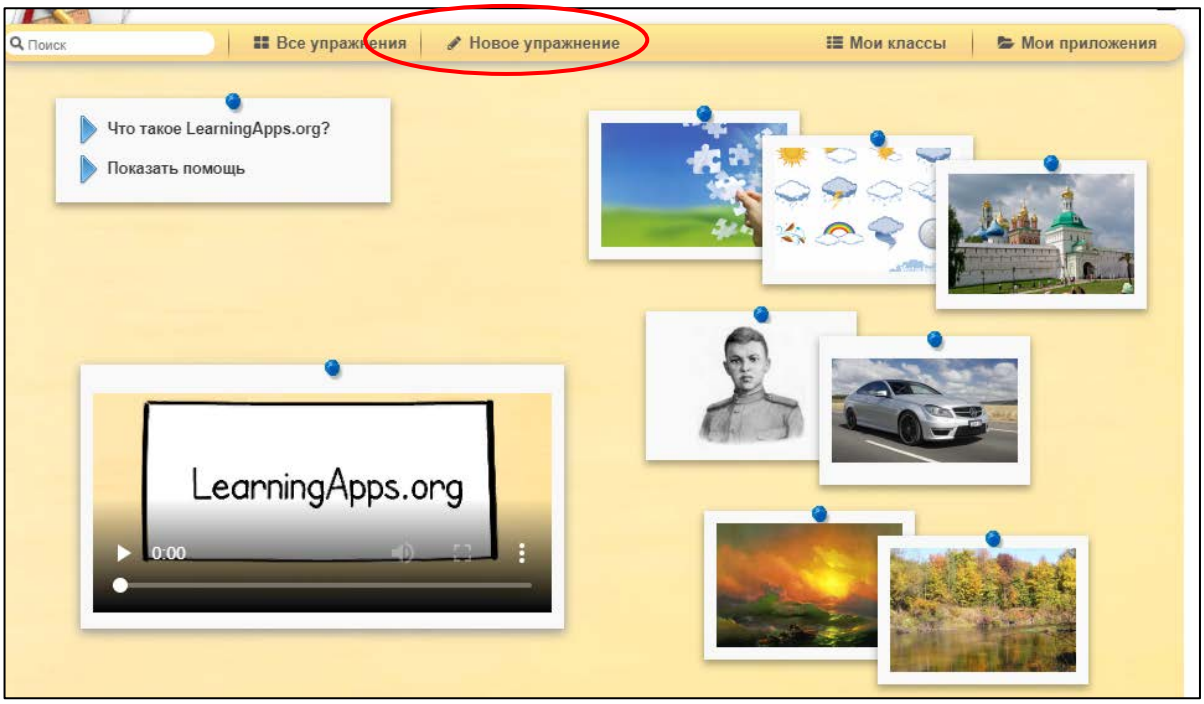


Рисунок 36 — Главная страница сайта LearningApps

Далее, выбираем упражнение «Заполнить пропуски», как показано на рисунке 37.

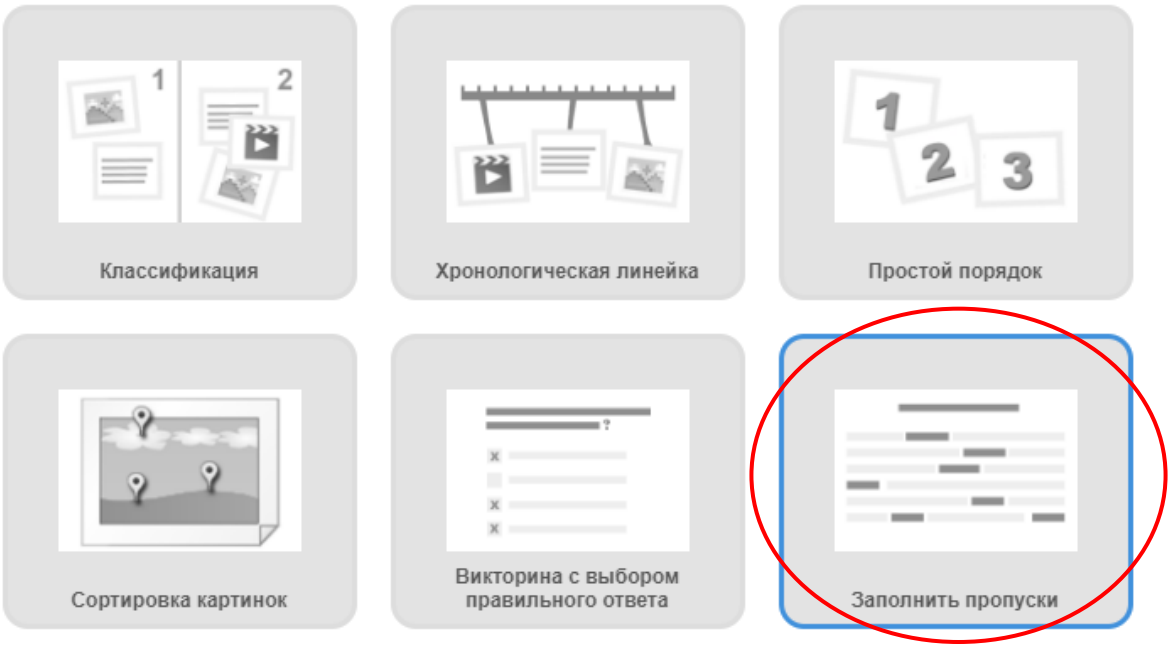


Рисунок 37 — Выбор упражнения «Заполнить пропуски»

В открывшемся окне нажимаем кнопку «Создать новое приложение» показано на рисунке 38.

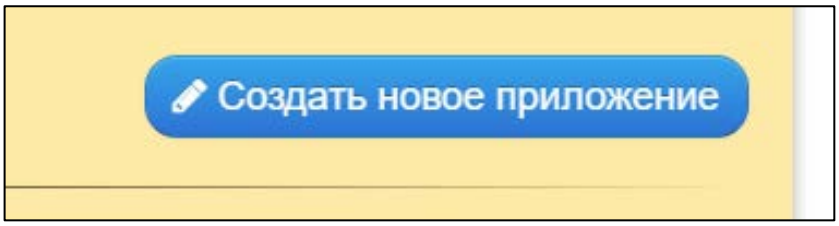


Рисунок 38 — Кнопка «Создать новое упражнение»

Пишем название упражнения, устанавливаем тип задания и при необходимости, можно написать задание для создаваемого упражнения, если это не требуется, можно оставить поле пустым, представлено на рисунке 39.

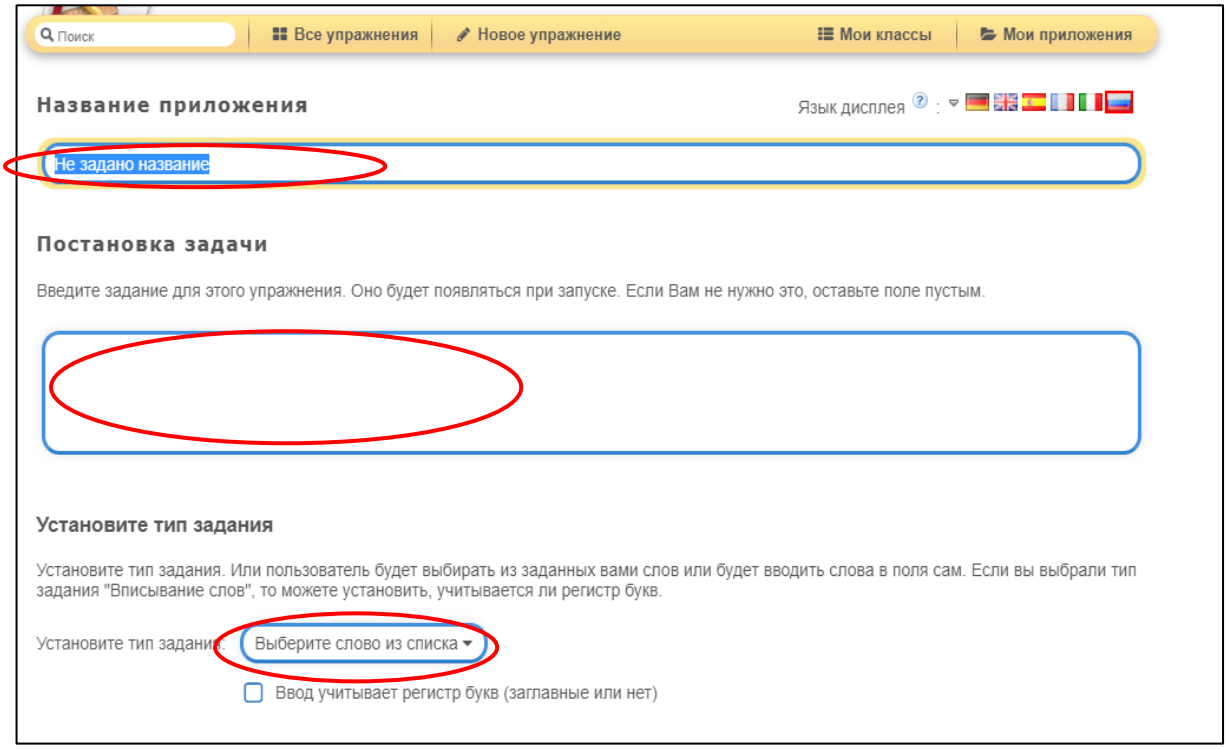


Рисунок 39 — Поле, для названия, постановки задачи и установки типа задания для упражнения

Вписываем текст задания, в котором будут пропуски и заменяем пропущены слова на «-1-», «-2-» и так далее, ниже, в местах обозначенных «-1-», «-2-» и так далее вписываем слова, которые пропущены в тексте, представлено на рисунке 40.

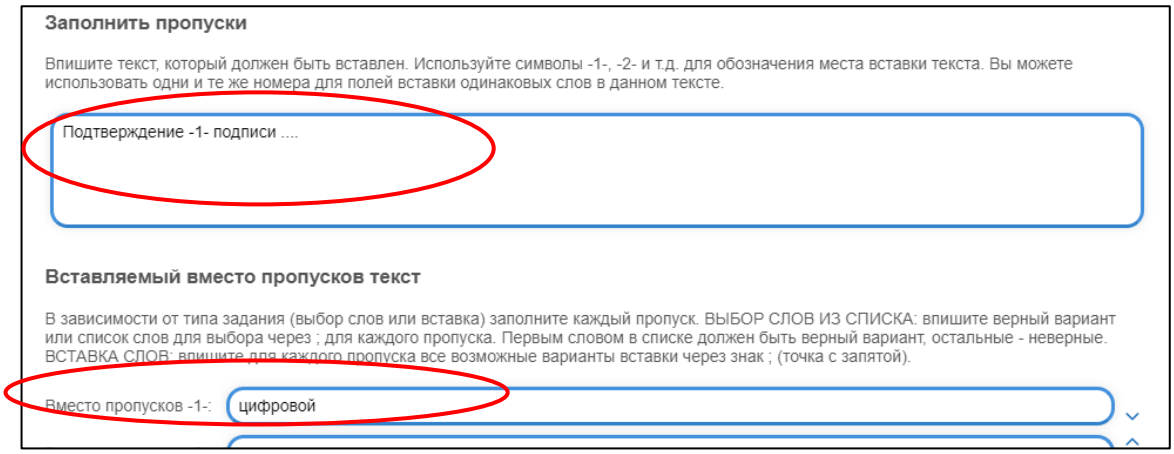


Рисунок 40 — Подготовка текста задания

По завершению создания упражнения, нажимаем кнопку «Установить и показать в предварительном просмотре» показано на рисунке 41.

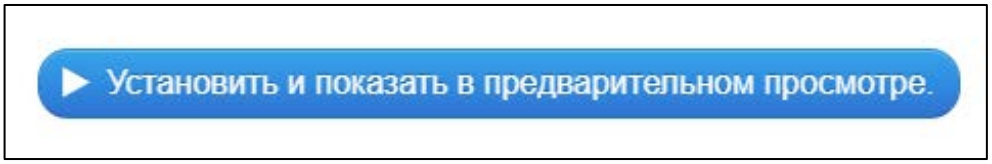


Рисунок 41 — Кнопка «Установить и показать в предварительном просмотре»

Далее сохраняем упражнение, нажимая кнопку «Сохранить приложение» представлено на рисунке 42.

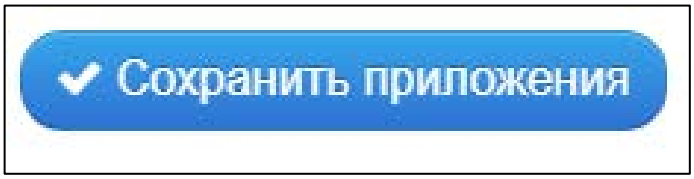


Рисунок 42 — Кнопка «Сохранить приложение»

Для того чтобы вставить интерактивное упражнение в электронное учебное пособие, скопируем строчку кода «Привязать» показано на рисунке 43.

Рисунок 43 — Код для привязки

Далее в электронном учебном пособии вставляем его в конец теоретического материала в Elementor, во вкладке «Текст» показано на рисунке 44.

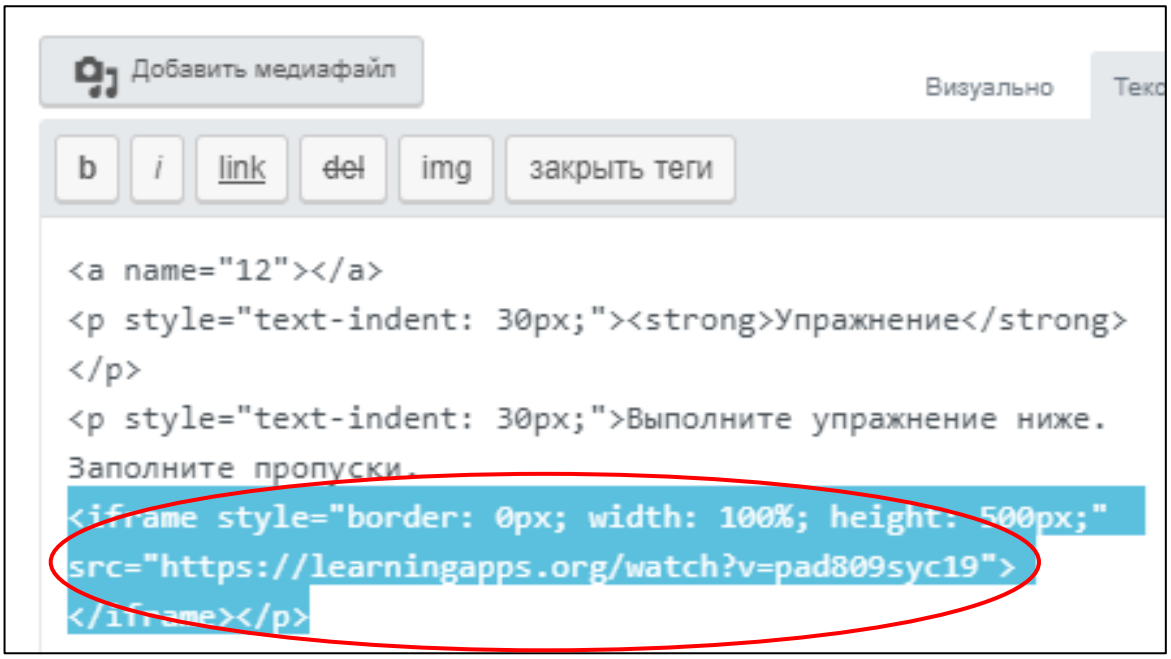


Рисунок 44 — вставка кода упражнения в Elementor

Для контроля усвоения материала, сделаны тесты с помощью плагина Watu Quiz. Чтобы начать тестирование, нужно начать отвечать на вопросы, выбрав правильный ответ и нажать кнопку «далее», так же, внизу отображается количество вопросов, показано на рисунке 45.

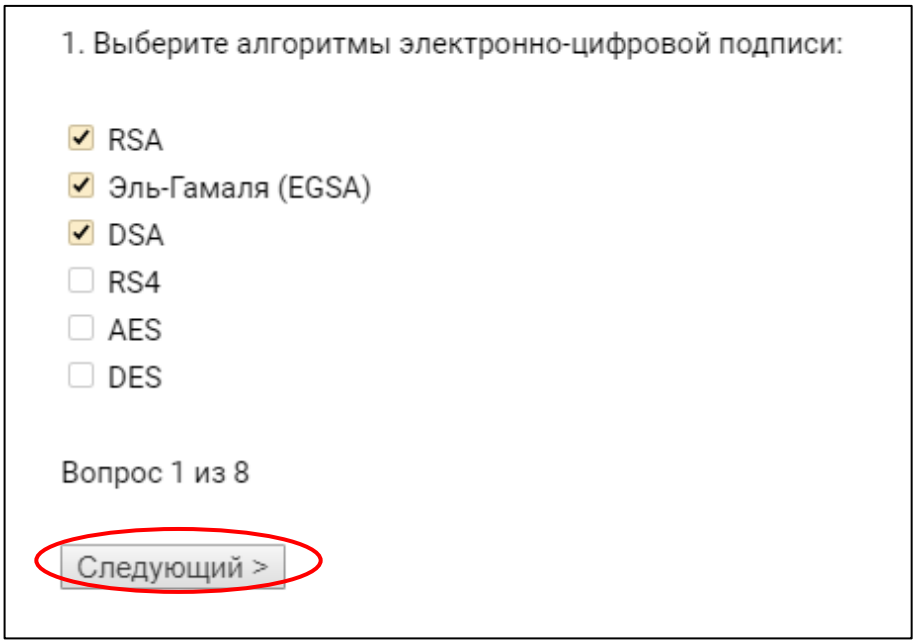


Рисунок 45 — Пример вопроса в тесте

Если студент, не ответил на вопрос с обязательным ответом, будет выведено уведомление, как продемонстрированно на рисунке 46.

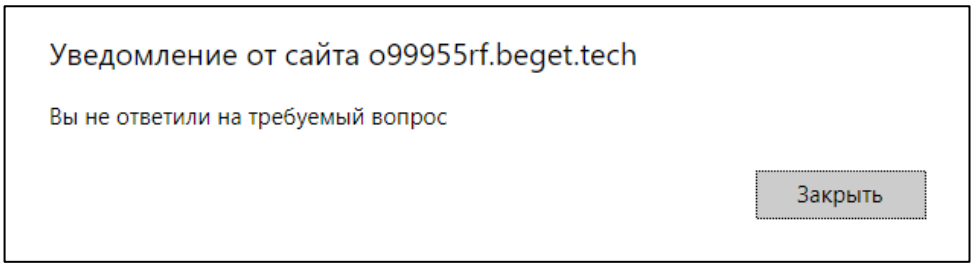


Рисунок 46 — Уведомление о том, что не студент не ответил на обязательный вопрос

По завершению прохождения теста, будут показаны баллы и оценка, представлено на рисунке 47.

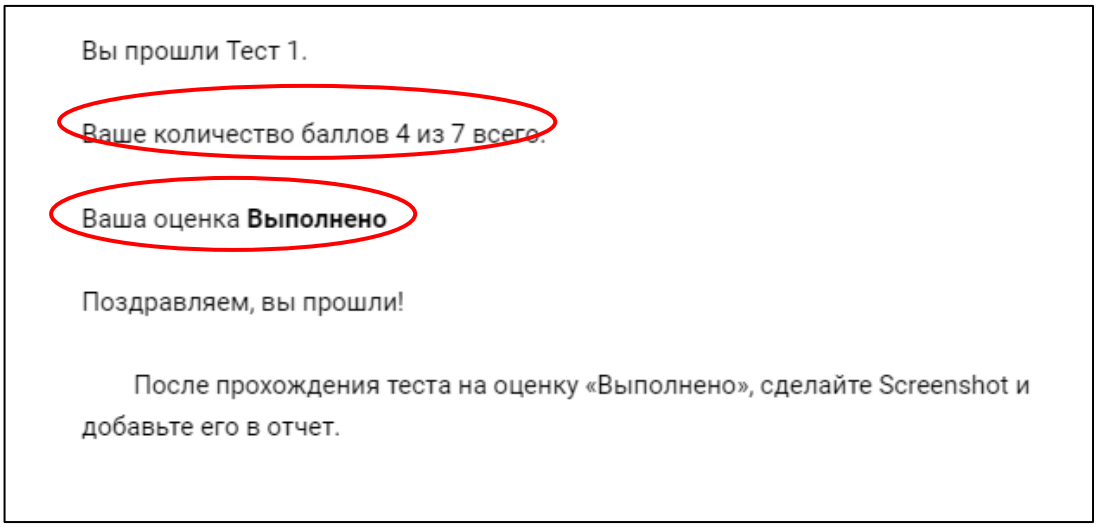


Рисунок 47 — Итог прохождения теста

Чтобы сделать данный тест, нужно зайти во вкладку «Watu опросы» в боковой панели, что представлено на рисунке 48.

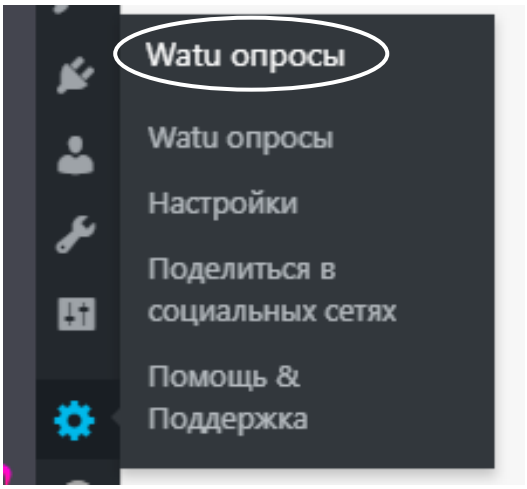


Рисунок 48 — Вкладка «Watu опросы»

Далее нажимаем «Создать новый опрос» показано на рисунке 49.

Рисунок 49 — Вкладка «Создание нового опроса»

Пишем имя опроса и выбираем нужные параметры, отмечая их галочкой, представлено на рисунке 50.

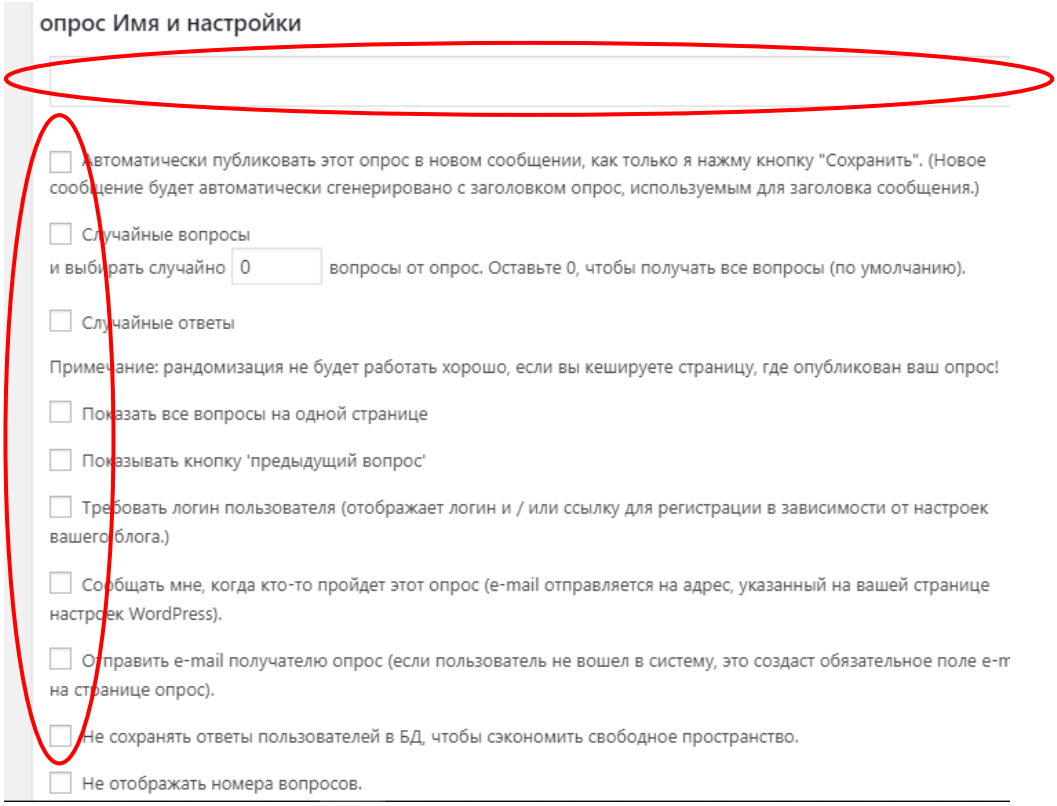


Рисунок 50 — Настройка опроса

Нажимаем сохранить, как показано на рисунке 51.

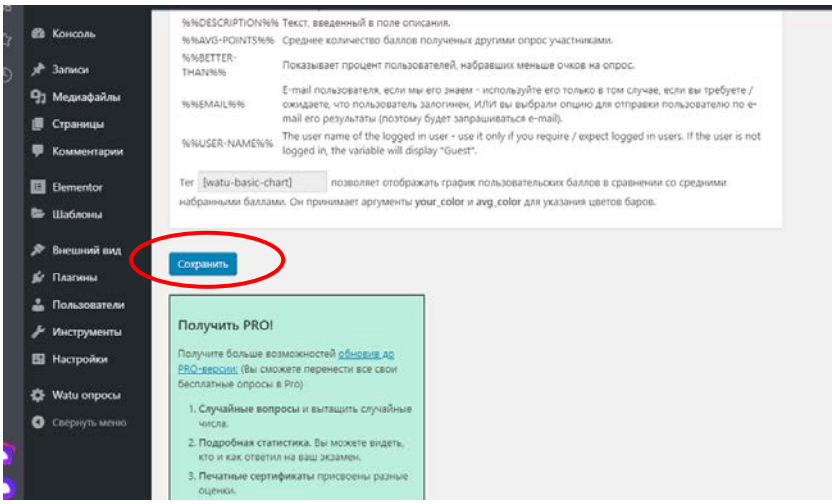


Рисунок 51 — Кнопка сохранения опроса

Далее нажимаем «Создать новый вопрос» показано на рисунке 52.

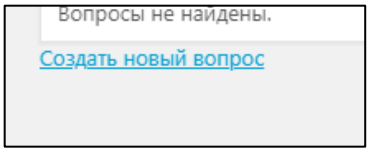


Рисунок 52 — Создание нового вопроса

Пишем тест вопроса и выбираем тип ответа, как показано на рисунке 53.

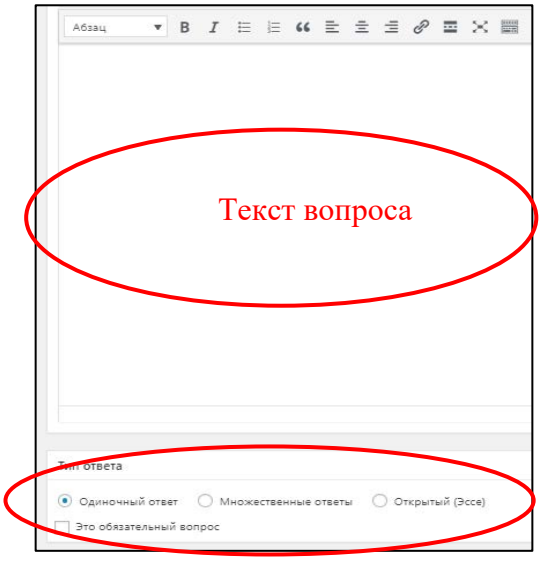


Рисунок 53 — Создание текста для вопроса и выбор типа ответа

Далее вписываем варианты ответа, помечаем правильные варианты ответов и ставим балы за правильно выбранные варианты ответов, продемонстрировано на рисунке 54.

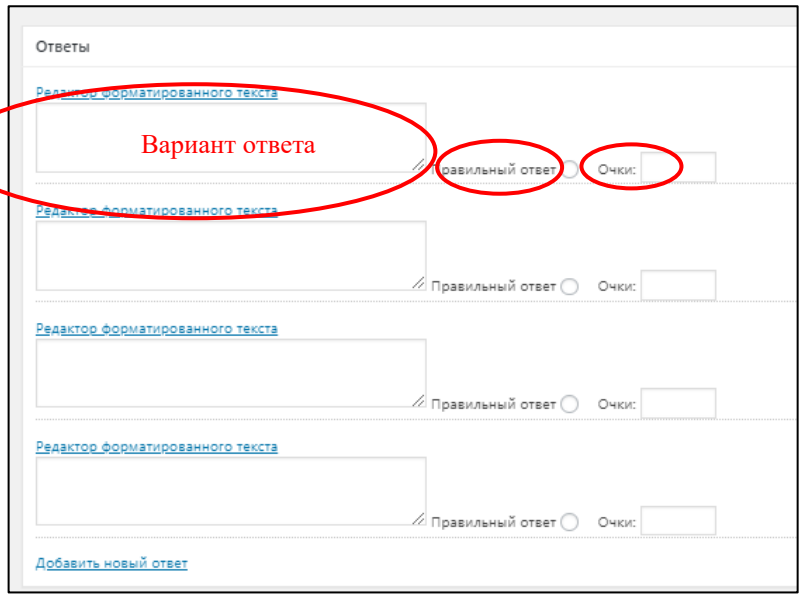


Рисунок 54 — Создание вариантов ответов

Нажимаем кнопку «Сохранить» и аналогично делаем следующие вопросы, показано на рисунке 55.

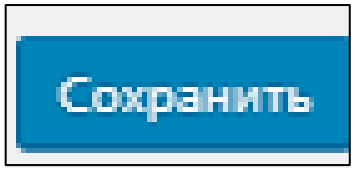


Рисунок 55 — Сохранения вопроса для теста

В каждом модуле, по прохождению теоретического и практического материала, есть самостоятельная работа студентов представлено на рисунке 56.

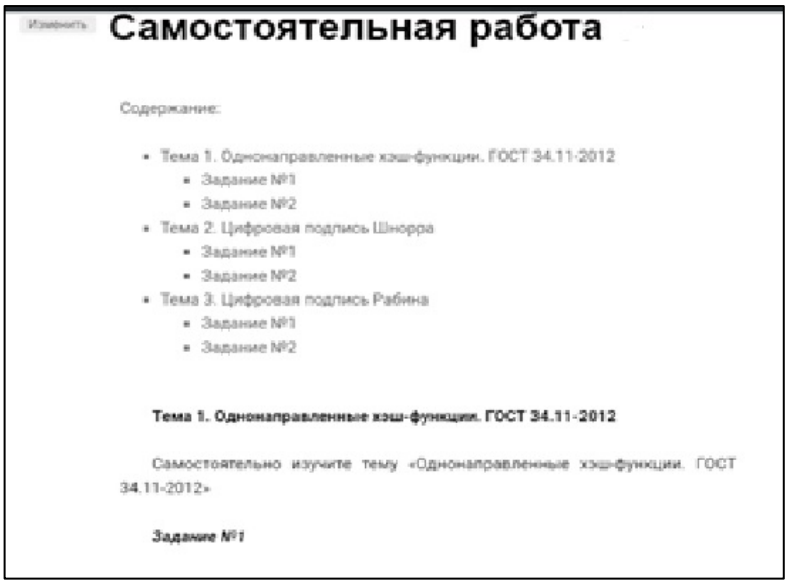


Рисунок 56 — Страница самостоятельной работы

Так же, по прохождению изучения тем выбранного модуля, есть итоговое задание, показано на рисунке 57.

Рисунок 57 — Итоговое задание

В вкладке меню «Справочная информация» студент может перейти в глоссарий, для поиска определений, использованных в электронном учебном пособии. При нажатии на нужную букву, страница перейдет на радел, где расположены слова, начинающиеся на букву, которую выбрали, продемонстрированно на рисунке 58.

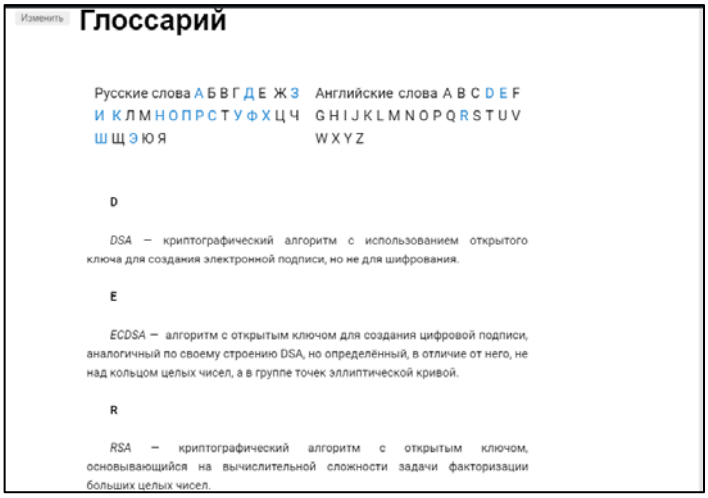
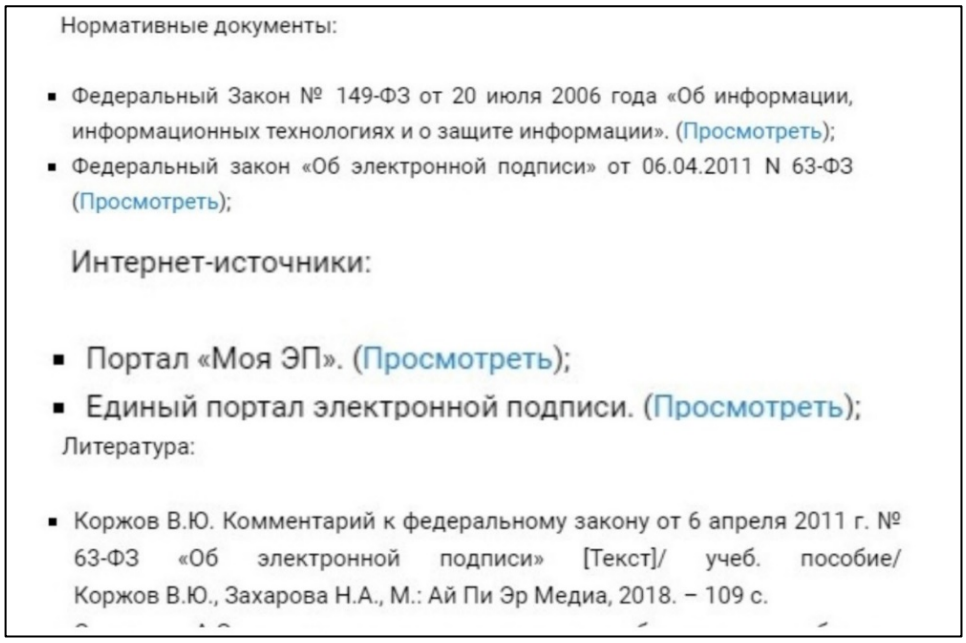


Рисунок 58 — Страница глоссария

При переходе на «Список литературы» будет выведен список «Нормативные документы», «Интернет источники» и «Литература» показано на рисунке 59. При нажатии на надпись «Просмотреть», студенту сразу же откроется литературный источник, который он выбрал.


Нормативные документы:

- Федеральный Закон № 149-ФЗ от 20 июля 2006 года «Об информации, информационных технологиях и о защите информации». (Просмотреть);
- Федеральный закон «Об электронной подписи» от 06.04.2011 N 63-ФЗ (Просмотреть);

Интернет-источники:

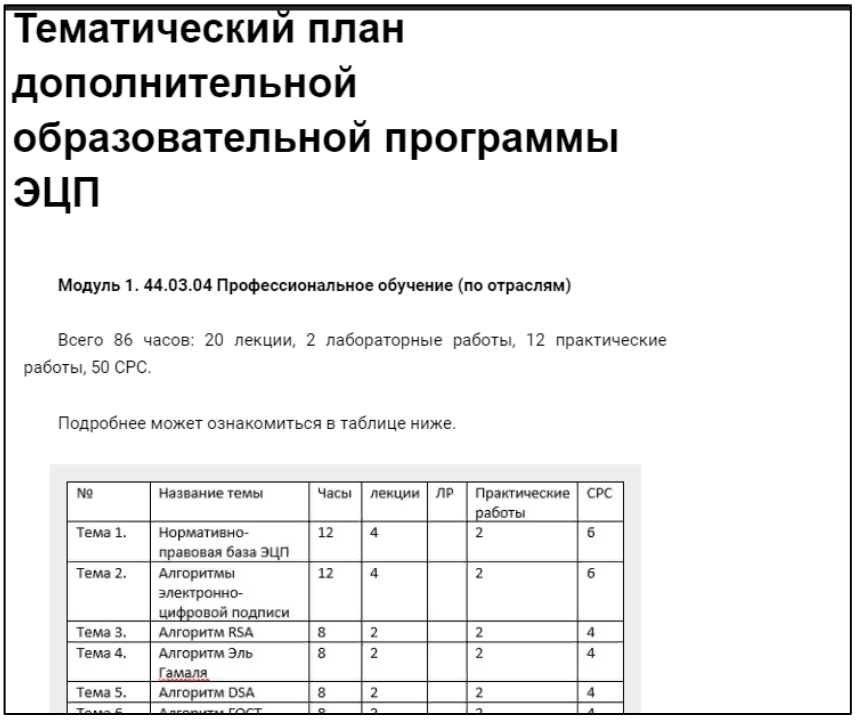
- Портал «Моя ЭП». (Просмотреть);
- Единый портал электронной подписи. (Просмотреть);

Литература:

- Коржов В.Ю. Комментарий к федеральному закону от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [Текст]/ учеб. пособие/ Коржов В.Ю., Захарова Н.А., М.: Ай Пи Эр Медиа, 2018. – 109 с.

Рисунок 59 — Нормативные документы, интернет-источники и литература

Вкладка «Тематический план дополнительной образовательной программы ЭЦП» в «Справочные материалы» написанны темы и часы для каждого модуля, что бы студенты могли посмотретьсписок тем, которые нужно изучить, для освоения дополнительной образовательной программы «Электронно-цифровая подпись», представленно на рисунке 60.


Тематический план дополнительной образовательной программы ЭЦП

Модуль 1. 44.03.04 Профессиональное обучение (по отраслям)

Всего 86 часов: 20 лекции, 2 лабораторные работы, 12 практические работы, 50 СРС.

Подробнее может ознакомиться в таблице ниже.

№	Название темы	Часы	лекции	ЛР	Практические работы	СРС
Тема 1.	Нормативно-правовая база ЭЦП	12	4		2	6
Тема 2.	Алгоритмы электронно-цифровой подписи	12	4		2	6
Тема 3.	Алгоритм RSA	8	2		2	4
Тема 4.	Алгоритм Эль Гамаля	8	2		2	4
Тема 5.	Алгоритм DSA	8	2		2	4

Рисунок 60 — Тематический план дополнительной образовательной программы «Электронно-цифровая подпись»

2.6 Методические рекомендации по использованию электронного учебного пособия «Электронно-цифровая подпись»

Электронное учебное пособие предполагается использовать слушателям дополнительной образовательной программы «Электронно-цифровая подпись».

ЭУП может быть использовано в качестве основного, дополнительного или дистанционного средства в обучении студентов.

Рекомендуется процесс обучения построить по следующе схеме: сначала изучение теоретического материала, потом переход к лабораторным (практическим) работам, далее студент проходит текущий контроль по каждой теме, но возможен и другой порядок, который устанавливается педагогом при осуществлении обучения по дополнительной образовательной программе. В процессе изучения студент может обратиться при необходимости к списку литературы и глоссарию.

В самом начале изучения дополнительной образовательной программы «Электронно-цифровая подпись» рекомендуется прочитать рабочую программу для ознакомления с содержанием теоретических, практических и лабораторных работ.

Далее идут разделы, которые нужно изучить в процессе освоения дополнительной образовательно программы «Электронно-цифровая подпись». Разделы рекомендуется изучать в установленном порядке, чтобы приобретенные знания были структурированы и систематизированы. Каждый раздел состоит из теоретического материала и практической (лабораторной) работы, согласно структуре и содержанию дополнительной образовательной программы, а также текущего контроля по каждой теме. Для того чтобы приступить к выполнению лабораторных (практических) работ, следует изучить теоретический материал, в котором излагается, то что пригодится вам для успешного выполнения лабораторных (практических) работ, которое следует осуществлять по порядку.

В лабораторных (практических) работах обязательны к выполнению все задания. В конце каждой лабораторной (практической) работы находятся контрольные вопросы и задания, результаты выполнения которых необходимо оформить в виде отчета.

Также в каждом разделе имеется текущий контроль по теме, это необходимо для закрепления изученного материала и выставления оценок, контроль сделан в виде теста и в виде контрольных заданий. Для того чтобы перейти к изучению следующего раздела необходимо успешно пройти контроль и правильно решить все контрольные задания, а также оформить результаты в ответ.

После изучения всех тем дополнительной образовательной программы «Электронно-цифровая подпись» необходимо выполнить итоговое задание и оформить отчет по нему.

Для того чтобы начать работу с электронным учебным пособием необходимо выполнить следующую действия:

1. Открыть сайт http://o99955rf.beget.tech в любом удобном для вас браузере.

2. Откроется главная страница электронного учебного пособия для перехода к работе нужно выбрать модуль дисциплины, подходящий именно вам.

3. Для навигации по различным разделам электронного учебного пособия воспользуйтесь главным меню, которое находится сверху.

4. Для быстрой прокрутки в начало страницы следует воспользоваться кнопкой «вверх», которая появляется в нижнем правом углу при прокручивании страницы вниз.

5. Переход от теории к лабораторным (практическим) работам осуществляется через выпадающее меню сверху.

6. Для прохождения тестового задания необходимо прочитать вопрос, выбрать правильный ответ и нажать кнопку «Далее».

В электронном учебном пособии имеются средства контроля, а именно:

- контрольные вопросы;
- тестовые задания;
- итоговые задания;
- интерактивный контроль.

Для успешного прохождения теста необходимо набрать больше 70 % правильных ответов.

- на оценку удовлетворительно — необходимо набрать не менее 70 %;
- на оценку хорошо — от 75 % до 85 %;
- на оценку отлично — более 85 %.

2.7 Результат апробации и внедрения

Апробация электронного учебного пособия проходила в Федеральном государственном автономном образовательном учреждении высшего образования «Российский государственный профессионально-педагогический университет» (РГППУ). В ней принимали участие студенты направления подготовки 44.03.04 Профессиональное обучение (по отраслям) профиль подготовки «Информационные технологии» профилизация «Информационная безопасность».

В результате апробации электронного учебного пособия были выявлены недостатки такие как, картинки не увеличивались, не было создано примеров отчетов по лабораторным (практическим) работам, отсутствие тем и задач в лабораторных (практических) работах, кроме того, были даны пожелания, содержащиеся в том, чтобы книги из рекомендованной литературы можно было просмотреть из самого электронного учебного пособия, чтобы не искать в сети Интернет. В основном, пожелания и замечания студентов были удовлетворены и исправлены.

Наряду с замечаниями были отмечены несомненными достоинства электронного учебного пособия, а именно наличие хорошо организованной и

продуманной навигации, полного содержания тем, находящегося в данном электронном учебном пособии, наличие простого и понятного навигационного меню, мультимедийного контента, направленного на улучшение понимания и визуализации информации.

ЗАКЛЮЧЕНИЕ

Проблема создания и внедрения в учебный процесс вузов электронных учебников и пособий активно разрабатывается в настоящее время. Примененные различных информационно-коммуникационных технологий требует объединения разные компоненты дидактической системы, и делает электронные учебные пособия не только средством учебного назначения, но и полноценным компонентом информационного образовательного пространства, в котором преподаватель и студент находятся как субъекты процесса обучения.

Преподаватель и студент, общаясь в этом пространстве, образовывают группу равноправных субъектов, которая решает общую задачу. С этой точки зрения электронный учебник можно рассматривать как среду обучения, среду профессиональной творческой деятельности, среду накопления знаний и источником познавательной информации.

Вопросы информационной безопасности и ее обеспечения сегодня стали актуальными не только для специалистов в области информационных технологий, но и в области обработки и представления документов. Возникает необходимость в разработке модульных программ, объединенных общей тематикой, но различным содержанием. Причем реализация данных программ ложиться на систему дополнительного образования и предполагает использование дистанционных технологий обучения, которые должны быть поддержаны соответствующими электронными учебно-методическими материалами.

В рамках выпускной квалификационной работы было разработано электронное учебное пособие «Электронно-цифровая подпись», которое предназначено для слушателей дополнительной образовательной программы.

На первом этапе выполнения работы было проанализировано понятие дополнительное образование и структура системы дополнительного образо-

вания. Далее были рассмотрены литература и Интернет-источники по теме «Электронно-цифровая подпись» с целью формирования круга печатных и электронных изданий, рассматривающих те или иные технологии, используемые в деятельности как документоведов, так и будущих специалистов в сфере информационной безопасности.

Нам основании анализа было спроектировано содержание дополнительной образовательной программы «Электронно-цифровая подпись», разделенное на два модуля в зависимости от категории слушателей.

На следующем этапе выполнения выпускной квалификационной работы были проанализированы требования, предъявляемые к электронному учебному пособию на современном этапе развития образования, которые были учтены при разработке пособия.

Были выбраны средства реализации электронного учебного пособия: WordPress, Camtasia Studio и LearningApps.

С помощью данных программных средств была спроектирована структура и реализовали интерфейс электронного учебного пособия по дисциплине «Электронно-цифровая подпись», а также электронное учебное пособие было наполнено содержанием, созданы видео-материалы и средства интерактивного контроля.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Бондарев В. В. Информационная безопасность автоматизированных систем [Текст]: учебное пособие / В. В. Бондарев, Москва: Московский государственный технический университет им. Н. Э. Баумана, 2016. — 252 с.

2. Википедия — свободная энциклопедия [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Дополнительное_образование (дата обращения: 24.05.2019).

3. Википедия — свободная энциклопедия [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Интерфейс (дата обращения: 16.04.2019).

4. Википедия — свободная энциклопедия [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Camtasia (дата обращения: 29.04.2019).

5. Википедия — свободная энциклопедия [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Google_Диск (дата обращения: 03.05.2019).

6. Википедия — свободная энциклопедия [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/WordPress (дата обращения: 06.05.2019).

7. Единый портал электронной подписи [Электронный ресурс]. — Режим доступа: https://iecp.ru (дата обращения: 02.05.2019).

8. Инфобизнес [Электронный ресурс]. — Режим доступа:https://biz-iskun.ru/programma-kamtaziya-studio-dlya-novichkov.html (дата обращения: 02.06.2019).

9. Инфоурок — ведущий образовательный портал России [Электронный ресурс]. — Режим доступа: https://infourok.ru/elektronnie-uchebnie-posobiya-v-sovremennom-obrazovatelnom-processe-969371.html (дата обращения: 14.04.2019).

10. Клуб WP — путеводитель в мире WordPress [Электронный ресурс]. — Режим доступа: https://clubwp.ru/blog/plugins-wordpress/best-plugins-wordpress/3-luchshih-konstruktora-stranits.html (дата обращения: 19.05.2019).

11. Коржов В. Ю. Комментарий к федеральному закону от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [Текст]: учебное пособие/ В. Ю. Коржов, Н. А. Захарова, Москва: Ай Пи Эр Медиа, 2018. — 109 с.

12. Крамаров С. О. Криптографическая защита информации [Текст]/ учебное пособие/ С. О. Крамаров, О. Ю. Митясова, С. В. Соколов, Е. Н. Тищенко, П. С. Шевчук, Москва: Издательский центр РИОР: ИНФРА-М, 2018. — 321 с.

13. КриптоПро [Электронный ресурс]. — Режим доступа: https://www.cryptopro.ru/about (дата обращения: 22.05.2019).

14. Левина А. Б. Моделирование криптосистем [Текст]: учебное пособие/ А. Б. Левина, Москва: Интермедия, 2017. — 144 с.

15. МБОУ Образовательный центр «Созвездие» [Электронный ресурс]. — Режим доступа: http://center-psi.ru/obrazovanie (дата обращения: 29.04.2019).

16. МБОУ Образовательный центр «Созвездие» [Электронный ресурс]. — Режим доступа:http://center-psi.ru/dopolnitelnoe-professionalnoe-obrazovanie (дата обращения: 15.04.2019).

17. МБОУ «Школа-гимназия» [Электронный ресурс]. — Режим доступа: https://www.yamg.ru/images/files/dot/metodicheskie-rekomendacii/learningappsorg.pdf (дата обращения: 21.05.2019).

18. Педагогическое сообщество урок.рф [Электронный ресурс]. — Режим доступа: https://урок.рф/library/interaktivnie_metodi_kontrolya_znanij_na_zanyatiyah_v_074848.html (дата обращения: 11.05.2019).

19. Портал «Моя ЭП» [Электронный ресурс]. — Режим доступа: http://my-ep.ru (дата обращения: 26.03.2019).

20. Приложения от Microsoft Corporation [Электронный ресурс]. — Режим доступа: https://officeapplications.net/microsoft-word/ (дата обращения: 02.06.2019).

21. Про хостинг и партнёрские программы хостингов [Электронный ресурс]. — Режим доступа: https://hosting-partners.ru/hosting/hosting-beget (дата обращения: 30.03.2019).

22. Разработка электронного учебника [Электронный ресурс]. — Режим доступа: http://ekrost.ru/poster/razrabotka-elektronnogo-uchebnika.html (дата обращения: 30.03.2019).

23. Репозиторий БГПУ [Электронный ресурс]. — Режим доступа: https://elib.bspu.by/bitstream/doc/7559/1/Интерактивные%20методы%20контроля%20знаний%20обучающихся%20в%20условиях%20дополнительного%20образования%20взрослых.pdf (дата обращения: 29.05.2019).

24. Смирнов А. Э. Практикум по выполнению лабораторных работ по дисциплине криптографические методы защиты информации» [Текст]: учеб. пособие/ А. Э. Смирнов, Ю. А. Пономарева, Москва: Московский технический университет связи и информатики, 2015. — 67 с.

25. Современный урок [Электронный ресурс]. — Режим доступа: https://aujc.ru/texnologiya-distancionnogo-obucheniya/ (дата обращения: 11.05.2019).

26. ТОП — Самый популярный Блог в России [Электронный ресурс]. — Режим доступа: https://info-effect.ru/jquery-smooth-scroll-plavnaya-prokrutka-i-knopka-vverx.html (дата обращения: 11.05.2019).

27. Файловые архив для студентов. StudFiles [Электронный ресурс]. — Режим доступа:https://studfiles.net/preview/909640/page:7/ (дата обращения: 30.05.2019).

28. Об образовании в Российской Федерации [Электронный ресурс]: Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 01.05.2019). — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_140174/ (дата обращения: 25.03.2019).

29. Ok2web — сайт web разработок [Электронный ресурс]. — Режим доступа: https://ok2web.ru/10-luchshih-plaginov-viktoriny-i-testov-dlja-wordpress-2019/ (дата обращения: 08.05.2019).

30. WordPress [Электронный ресурс]. — Режим доступа: https://ru.wordpress.org/themes/twentyeleven/ (дата обращения: 27.03.2019).

ПРИЛОЖЕНИЕ А

Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Российский государственный профессионально-педагогический университет»

Институт инженерно-педагогического образования

Кафедра информационных систем и технологий

Направление подготовки 44.03.04 Профессиональное обучение (по отраслям)

Профиль «Информатика и вычислительная техника»

Профилизация «Информационная безопасность»

УТВЕРЖДАЮ
Заведующий кафедрой

_____ И.А. Суслова
подпись и.о. фамилия

« ___ » _____ 2019 г.

ЗАДАНИЕ
на выполнение выпускной квалификационной работы бакалавра

студента (ки) *4* курса группы *ИБ-402*

Помогаевой Марии Андреевны
фамилия, имя, отчество полностью

1. Тема ***Электронное учебное пособие «Электронно-цифровая подпись»***
утверждена распоряжением по институту от «_____» _____ 20 г. № ___
2. Руководитель ***Федулова Ксения Анатольевна***
фамилия, имя, отчество полностью

доцент (ученая степень) *к.пед.н.* (ученое звание) *доцент кафедры ИС* (должность) *РГППУ* (место работы)

3. Место преддипломной практики Кафедра ИС ИИПО ФГАОУ ВО РГППУ
4. Исходные данные к ВКР
   1. Рабочая программа дисциплины «Защита персональных данных»
   2. Рабочая программа дисциплины «Защита сетевых информационных систем»
   3. Крамаров С.О. «Криптографическая защита информации»
5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов)
   1. Проанализировать литературу и интернет-источники по теме «Электронно-цифровая подпись»

2. Спроектировать содержание дополнительной образовательной программы «Электронно-цифровая подпись».
3. Проанализировать литературу и интернет-источники с целью выделения требований, предъявляемых к электронному учебному пособию на современном этапе развития образования.
4. Осуществить выбор средств реализации электронного учебного пособия.
5. Реализовать электронное учебное пособие по дисциплине «Электронно-цифровая подпись» и провести его апробацию.

6. Перечень демонстрационных материалов, презентация, выполненная в MS PowerPoint, электронное учебное пособие «Электронно-цифровая подпись»

7. Календарный план выполнения выпускной квалификационной работы

№ п/п	Наименование этапа дипломной работы	Срок выполнения этапа	Процент выполнения ВКР	Отметка руководителя о выполнении
1	Сбор информации по выпускной квалификационной работе		10%	подпись
2	Выполнение работ по разрабатываемым вопросам и их изложение в пояснительной записке:		60%	подпись
2.1	Анализ литературы и интернет-источники по теме «Электронно-цифровая подпись».		10%	подпись
2.2	Проектирование содержания дополнительной образовательной программы «Электронно-цифровая подпись».		20%	подпись
2.3	Реализация электронное учебное пособие по дисциплине «Электронно-цифровая подпись» и провести его апробацию.		30%	подпись
3	Оформление текстовой части ВКР		10%	подпись
4	Выполнение демонстрационных материалов к ВКР		10%	подпись
5	Нормоконтроль		5%	подпись
6	Подготовка доклада к защите в ГЭК		5%	подпись

8. Консультанты по разделам выпускной квалификационной работы

Наименование раздела	Консультант	Задание выдал		Задание принял	
		подпись	дата	подпись	дата

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

9. Дипломная работа и все материалы проанализированы.
Считаю возможным допустить ***Помогаеву М.А.*** к защите выпускной квалификационной работы в государственной экзаменационной комиссии.
Руководитель _____ _____
подпись дата

10. Допустить ***Помогаеву М.А.*** к защите выпускной квалификационной работы
фамилия и. о. студента

в государственной экзаменационной комиссии (протокол заседания кафедры от «___» _____ 20____г., № _____)

Заведующий кафедрой _____ _____
подпись дата

ПРИЛОЖЕНИЕ Б

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

Утверждаю
Проректор по образованию
_____Е.Ю. Щербина
«____»_____2019 г.

Дополнительная образовательная программа

«Электронно-цифровая подпись»

Екатеринбург 2019 г.

Дополнительная профессиональная образовательная программа «Электронно-цифровая подпись». Екатеринбург, ФГАОУ ВО «Российский государственный профессионально-педагогический университет», 2019. 8 с.

Составители: Федулова К.А., к.п.н., доцент, доцент кафедры информационных систем и технологий

Помогаева М.А., студент кафедры информационных систем и технологий

Рецензент: зав. кафедрой информационно-коммуникационных технологий в образовании УрГПУ, д.пед.н., проф. Стариченко Б.Е.

Программа одобрена на заседании кафедры информационных систем и технологий. Протокол от _____ № __.

Заведующая кафедрой ИС И.А. Суслова

Программа одобрена методической комиссией Института инженерно-педагогического образования. Протокол от _____ № __.

Председатель методической комиссии
Института ИПО А.О. Прокубовская

Программа одобрена учебно-методическим советом по дополнительному образованию РГППУ. Протокол от _____ № _____

Председатель УМС ДО О.Б. Акимова

Раздел 1. Характеристика программы

1.1. Цель – формирование у студентов четкое представление и понимание теоретических и прикладных знаний о современных методах обеспечения аутентификации электронных документов в информационных инфраструктурах государственных и частно-предпринимательских предприятий и организаций.

№	**Компетенции**
1	Способность обеспечивать защиту персональных данных работников и конфиденциальной информации, в том числе при организации, осуществлении и документировании процессов оценки, аттестации и развития персонала
2	Способность анализировать и выбирать методы и средства обеспечения информационной безопасности

1.2. Планируемые результаты обучения

В результате обучения слушатели должны:

№	**Знать**
1	Криптографические алгоритмы, используемые в современных криптосистемах аутентификации электронных документов. с открытым ключом;
2	Криптографические алгоритмы, используемые в стандартах аутентификации данных;
3	Методы выбора криптографических параметров, обеспечивающих необходимую стойкость криптосистемы к несанкционированному воздействию:
4	Ключевые системы современной криптографии и протоколы распределения ключей:
5	Приложения криптографии к решению задач аутентификации информации в компьютерных системах, в частности по проблемам информационной безопасности в банковских и торгово-экономических структурах;
№	**Уметь использовать**
1	Полученные знания в решении прикладных задач защиты информации в компьютерных технологиях банковских и торгово-экономических систем;
2	Строить и изучать математические модели криптографических алгоритмов;
3	Применять современные криптографические системы, системы управления контролем доступа, системы аутентификации и идентификации пользователей и документов в информационных технологиях банковских и торгово-экономических структурах;
№	**Владеть**
1	Навыками пользования библиотеками прикладных программ компьютерных систем для решения задач по защите информации в информационных технологиях;
2	Методами определения требований и состава средств, методов и мероприятий по организации комплекса средств аутентификации информации в компьютерных технологиях;
3	Способами использование методов организации, планирования и контроля функционирования комплекса средств аутентификации информации;
4	Навыками применения стандартов Федеральная служба по техническому и экспортному контролю Российской Федерации, Приказов и распоряжений ФСБ России по проблемам информационной безопасности в своей профессиональной деятельности;
5	Методами практического применения технических, программных и программно-аппаратных средств и методов аутентификации информации в компьютерных технологиях;

1.3. Категория обучающихся (слушателей):

Лица с высшим или средним профессиональным образованием.

1.4. Форма обучения

Очно-заочная.

1.5. Режим занятий, срок освоения программы

- Режим занятий – по согласованию со слушателем.
- Срок освоения программы: модуль 1 – 72 часа, модуль 2 – 72 часа.

Раздел 2. Содержание программы

2.1. Учебный (тематический) план

2.1.1 Модуль 1 – 44.03.04 Профессиональное обучение (По отраслям)

№ п/п	Название модулей (разделов) и тем	Всего часов	Формы контроля
1.	Нормативно-правовая база ЭЦП	12	Ответы на вопросы
2.	Алгоритмы электронно-цифровой подписи	8	Ответы на вопросы, компьютерное тестирование
3.	Алгоритм RSA	8	Ответы на вопросы, выполнение задания
4.	Алгоритм Эль Гамаля	6	Ответы на вопросы, выполнение задания
5.	Алгоритм DSA	6	Ответы на вопросы, выполнение задания
6.	Алгоритм ГОСТ 34.10-2012	8	Ответы на вопросы, выполнение задания
7.	Технологи работы в программе «КриптоАрм»	8	Ответы на вопросы, выполнение задания
8.	Однонаправленные хэш-функции. ГОСТ 34.11-2012	8	Ответы на вопросы, выполнение задания
9.	Цифровая подпись Шнорра	4	Ответы на вопросы
10.	Цифровая подпись Рабина	4	Ответы на вопросы
Итого:		72	
Итоговая аттестация			Аттестационная работа

2.1.1 Модуль 2 – 46.03.02 Документоведение и архивоведение

№ п/п	Название модулей (разделов) и тем	Всего часов	Формы контроля
1.	Нормативно-правовая база ЭЦП	12	Ответы на вопросы
2.	Алгоритмы электронно-цифровой подписи	12	Ответы на вопросы, компьютерное тестирование
3.	Проблемы долговременного хранения документов подписанных электронно-цифровой подписью или ее аналогами	8	Ответы на вопросы
4.	Электронно-цифровая подпись в СЭД	12	Ответы на вопросы
5.	Технология работы в программе «КриптоАрм»	10	Ответы на вопросы, выполнение задания
6.	Документирование использования электронно-цифровой подписи в организации	6	Ответы на вопросы
7.	Симуляторы электронно-цифровой подписи	8	Ответы на вопросы
8.	Организация хранения документов с электронно-цифровой подписью	4	Ответы на вопросы
Итого:		72	
Итоговая аттестация			Аттестационная работа

2.2. Распределение часов (трудоемкость) по темам и видам работ

2.2.1. Модуль 1 – 44.03.04 Профессиональное обучение (По отраслям)

№ п/п	Наименование разделов/модулей и тем	Общая трудоемкость	Аудиторные занятия		Заочная форма (часы)
		(часы)	Лекции (часы)	Семинары, практические занятия, лабораторные работы (часы)	
1.	Нормативно-праввоая база ЭЦП	12	4	2	6
2.	Алгоритмы электронно-цифровой	8	2	2	4

	подписи				
3.	Алгоритм RSA	8	2	2	4
4.	Алгоритм Эль Гамаля	6	2	2	2
5.	Алгоритм DSA	6	2	2	2
6.	Алгоритм ГОСТ 34.10-2012	8	2	2	4
7.	Технологи работы в программе «КриптоАрм»	8	2	2	4
8.	Однонаправленные хэш-функции. ГОСТ 34.11-2012	8			8
9.	Цифровая попись Шнорра	4			4
10.	Цифровая подпись Рабина	4			4
	Итого	72	16	14	42

2.2.2 Модуль 2 – 46.03.02 Документоведение и архивоведение

№ п/п	Наименование разделов/модулей и тем	Общая трудоемкость (часы)	Аудиторные занятия		Заочная форма (часы)
			Лекции (часы)	Семинары, практические занятия, лабораторные работы (часы)	
1.	Нормативно-правовая база ЭЦП	12	4	2	6
2.	Алгоритмы электронно-цифровой подписи	12	4	2	6
3.	Проблемы долговременного хранения документов подписанных электронно-цифровой подписью или ее аналогами	8	2	2	4
4.	Электронно-	12	4	4	6

	цифровая подпись в СЭД				
5.	Технология работы в программе «КриптоАРМ»	10	4	2	4
6.	Документирование использования электронно-цифровой подписи в организации	6			6
7.	Симуляторы электронно-цифровой подписи	8			8
8.	Организация хранения документов с электронно-цифровой подписью	4			4
	Итого	72	18	12	42

2.3. Календарный учебный график

Календарным учебным графиком является расписание учебных занятий, которое составляется и утверждается для каждой учебной группы.

2.4. Рабочие программы учебных модулей

2.4.1 Модуль 1 – 44.03.04 Профессиональное обучение (по отраслям)

Тема № 1. Нормативно-правовая база ЭЦП

Определение ЭЦП. Функции ЭЦП. Доктрина информационной безопасности Российской Федерации. Федеральный Закон Российской Федерации ФЗ №1 «Об электронной цифровой подписи». Приказ ФСБ РФ №66 от 9.02.2005 г. «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации». Указ Президента Российской Федерации № 000 от 01.01.01 года «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена

Тема № 2. Алгоритмы электронно-цифровой подписи

Виды алгоритмов. Генерация ключей. Симметричные и ассиметричные алгоритмы. Использование алгоритмов. Алгоритм DSA. Алгоритм RSA. Алгоритм Эль Гамаля..ГОСТ 34.10-2012.

Тема № 3. Алгоритм RSA

История создания алгоритма. Принцип работы алгоритма. Генерация ключей. Создание электронной подписи. Проверка электронной подписи. Криптостойкость. Плюсы и минусы алгоритма.

Тема № 4. Алгоритм Эль Гамаля

История создания алгоритма. Принцип работы алгоритма. Генерация ключей. Создание электронной подписи. Проверка электронной подписи. Криптостойкость. Плюсы и минусы алгоритма.

Тема № 5. Алгоритм DSA

История создания алгоритма. Принцип работы алгоритма. Генерация ключей. Создание электронной подписи. Проверка электронной подписи. Криптостойкость. Плюсы и минусы алгоритма.

Тема № 6. Алгоритм ГОСТ 34.10-2012

История создания алгоритма. Принцип работы алгоритма. Генерация ключей. Создание электронной подписи. Проверка электронной подписи. Криптостойкость. Плюсы и минусы алгоритма.

Тема № 7. Технология работы в программе «КриптоАРМ»

Программа «КриптоАРМ». Модули программы «КриптоАРМ». Версии программы «КриптоАРМ». Возможности программы «КриптоАРМ». Компания-разработчик программамы «КриптоАРМ».

Тема № 8. Однонаправленные хэш-функции. ГОСТ 34.11-2012

Назначение хэш-функций. Работа с хэш-функциями. Работа с ГОСТ 34.11-2012 Использование ГОСТ 34.11-2012. История создания хэш-функций.

Тема № 9. Цифровая подпись Шнорра

История создания алгоритма. Принцип работы алгоритма. Генерация ключей. Создание электронной подписи. Проверка электронной подписи. Криптостойкость. Плюсы и минусы алгоритма.

Тема № 10. Цифровая подпись Рабина

История создания алгоритма. Принцип работы алгоритма. Генерация ключей. Создание электронной подписи. Проверка электронной подписи. Криптостойкость. Плюсы и минусы алгоритма.

2.4.2 Модуль 2 – 46.03.02 Документоведение и архивоведение

Тема № 1. Нормативно-правовая база ЭЦП

Определение ЭЦП. Функции ЭЦП. Доктрина информационной безопасности Российской Федерации. Федеральный Закон Российской Федерации ФЗ №1 «Об электронной цифровой подписи». Приказ ФСБ РФ №66 от 9.02.2005 г. «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации». Указ Президента Российской Федерации № 000 от 01.01.01 года «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена

Тема № 2. Алгоритмы электронно-цифровой подписи

Виды алгоритмов. Генерация ключей. Симметричные и ассиметричные алгоритмы. Использование алгоритмов. Алгоритм DSA. Алгоритм RSA. Алгоритм Эль Гамаля. ГОСТ 34.10-2012.

Тема № 3. Проблемы долговременного хранения документов, подписанных электронно-цифровой подписью или ее аналогами

Обеспечение сохранности электронных документов. Обеспечение пригодности документов для использования. Обеспечение юридической значимости документов.

Тема № 4. Электронно-цифровая подпись в СЭД

Управление ключевой системой. Пакет документов. Центр удостоверения открытых ключей. Назначение ЭЦП в СЭД.

Тема № 5. Технология работы в программе «КриптоАРМ»

Программа «КриптоАРМ». Модули программы «КриптоАРМ». Версии программы «КриптоАРМ». Возможности программы «КриптоАРМ». Компания-разработчик программамы «КриптоАРМ».

Тема № 6. Документирование использования электронно-цифровой подписи в организации

Состав документов, регламентирующих применение ЭП (перечень документов, создание, хранение и использование которых должно осуществляться в форме электронных документов; инструкция по созданию и организации работы с электронными документами; номенклатура дел (с учетом использования электронных документов); правила определения лица, подписывающего электронный документ в СЭД, по его простой электронной подписи; инструкции о создании, выдаче и применении ключей простой электронной подписи; приказ о признании информации в электронной форме, подписанной простой электронной подписью, электронным документом)

Тема № 7. Симуляторы электронно-цифровой подписи»

Виды симуляторов ЭЦП. Назначение симуляторов ЭЦП. Преимущества

симуляторов ЭЦП. Характеристики симуляторов ЭЦП.

Тема № 8. Организация хранение документов с электронно-цифровой подписью

Сроки хранения документов с ЭЦП. Проверка юридической значимости. Доступ для чтения спустя много лет.

Раздел 3. Формы аттестации и оценочные материалы

Промежуточный контроль

Промежуточный контроль проводится в форме зачетов и экзаменов.

Итоговая аттестация

Итоговая аттестация проводится в форме выполнения аттестационной работы.

Итоговая аттестация осуществляется после освоения всех тем программы и успешного прохождения всех промежуточных форм контроля.

Оценочные материалы

Тесты и письменные задания.

Образцы тестовых заданий

Выберите правильный(е) вариант(ы).

1. Выберите алгоритмы электронно-цифровой подписи:
   а) RSA;
   б) Эль Гамаля;
   в) DSA;
   г) RS4;
   д) AES;
   е) DES.
2. Выберите, для чего предназначен алгоритм DSA:
   а) шифрование;
   б) электронно-цифровая подпись.
3. Выберите алгоритмы, основанные на схеме Эль Гамаля:
   а) DSA;
   б) ECDSA;
   в) RS4;
   г) RSA
4. Выберите, кем был предложен алгоритм DSA
   а) НИСТ (США);
   б) НИСТ (РФ);
   в) Тахером Эль-ГАмалем;
   г) Уитфилдом Диффи и Мартином Хеллманом

Образец практического задания

1. Для указанных открытых ключей пользователя RSA проверить подлинность подписанных сообщений (не менее 5):

Задание №1

Для указанных открытых ключей пользователя RSA проверить подлинность подписанных сообщений(не менее 5):

1. p=55, q=3: <7,28>, <22,15>,<16,36>
2. p=65, q=5: <6,42>, <10,30>,<6,41>
3. p=77, q=7: <13,41>, <11,28>,<5,26>
4. p=91, q=5: <15,71>, <11,46>,<16,74>
5. p=33, q=3: <10,14>, <24,18>,<17,8>
6. p=143, q=37: <46,85>, <16,74>,<129,116>
7. p=221, q=43: <59,19>, <79,164>,<58,20>
8. p=85, q=15: <24,39>, <39,51>,<83,42>
9. p=187, q=77: <139,90>, <62,163>,<95,57>
10. p=221, q=79: <207,142>, <112,9>,<82,147>
11. p=57, q=31: <25,28>, <12,42>,<48,15>
12. p=133, q=41: <52,89>, <82,120>,<67,128>
13. p=209, q=67: <49,125>, <105,17>,<136,97>
14. p=247, q=71: <249,124>, <95,214>,<173,10>
15. p=323, q=79: <312,122>, <142,29>,<229,134>

2. Найдите ответы на вопросы:
   1. Что является первым этапов любого асимметричного алгоритма?
   2. Кто был создателем алгоритма RSA?
   3. Как осуществляется подпись алгоритмом RSA?
   4. Какова криптостойкость алгоритма RSA?
   5. Минусы и плюсы использования ЭЦП на основе алгоритма RSA?

Раздел 4. Организационно-педагогические условия реализации программы

4.1. Учебно-методическое обеспечение и информационное обеспечение программы

Основная литература

1. Коржов В.Ю. Комментарий к федеральному закону от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [Текст]/ учеб. пособие/ Коржов В.Ю., Захарова Н.А., М.: Ай Пи Эр Медиа, 2018. – 109 с.

2. Смирнов А.Э. практикум по выполнению лабораторных работ по дисциплине криптографические методы защиты информации» [Текст]/ учеб. пособие/ Смирнов А.Э., Пономарева Ю.А., М.: Московский технический университет связи и информатики, 2015. – 67 с.

3. Бондарев В.В. Информационная безопасность автоматизированных систем [Текст]/ учеб. пособие/ Бондарев В.В., М.: Московский государственный технический университет им. Н.Э. Баумана, 2016. – 252 с.

4. Левина А.Б. Моделирование криптосистем [Текст]/ учеб. пособие/ Левина А.Б., М.: Интермедия, 2017. – 144 с.

Дополнительная литература

1. Борисов А.Н. Первичные документы: оформление, использование, хранение, выбытие [Текст]/ практикум бугалтера/ А.Н. Борисов., М.: Литагент «Юстицинформ», 2018. – 1687.

2. Крамаров С.О. Криптографическая защита информации [Текст]/ учеб. пособие/ Крамаров С.О., Митясова О.Ю., Соколов С.В., Тищенко Е.Н., Шевчук П.С., М.: Издательский центр РИОР: ИНФРА-М, 2018. – 321 с.

4.2. Материально-технические условия реализации программы

Электронная информационно-образовательная среда университета.

4.3. Кадровое обеспечение программы

Программа реализуется преподавателями кафедры информационных систем и технологий.

Дополнительная образовательная программа
«Электронно-цифровая подпись»

Подписано в печать _____. Формат 60×84/16. Бумага для множ. аппаратов.
Печать плоская. Усл. печ. л. ___. Уч.-изд. л.____. Тираж ____ экз. Заказ № ____.
ФГАОУ ВО «Российский государственный профессионально-педагогический университет». Екатеринбург, ул. Машиностроителей, 11.

Ризограф ФГАОУ ВО РГППУ. Екатеринбург, ул. Машиностроителей, 11.