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

ДИСТАНЦИОННЫЙ ОНЛАЙН-КУРС «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

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: 185

Екатеринбург 2018

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

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

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ДИСТАНЦИОННЫЙ ОНЛАЙН-КУРС «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Исполнитель:
обучающийся группы № ИБ-401 А.В. Тельминов
Руководитель:
канд. пед. наук, доцент К.А. Федулова
Нормоконтролер: Т. В. Рыжкова

АННОТАЦИЯ

Выпускная квалификационная работа состоит из дистанционного онлайн-курса «Криптографические методы защиты информации» и пояснительной записки на 55 страницах, содержащей 20 рисунков, 1 таблицу, 36 источников литературы, а также 1 приложение на 2 страницах.

Ключевые слова: ДИСТАНЦИОННЫЙ КУРС, КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ, ШИФРОВАНИЕ, MOODLE, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ.

Тельминов А.В. Дистанционный онлайн-курс «Криптографические методы защиты информации»**:** выпускная квалификационная работа / А.В. Тельминов; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. – Екатеринбург, 2018. – 61 с.

В работе рассмотрен процесс разработки дистанционного онлайн-курса средствами LMS Moodle.

Цель выпускной квалификационной работы: разработать дистанционный онлайн-курс «Криптографические методы защиты информации». Для достижения поставленной цели были проанализированы интернет-источники и учебно-методическая документация дополнительной образовательной программы «Криптографические методы защиты информации», также были рассмотрены вопросы, связанные с созданием дистанционного онлайн-курса и требованиями, предъявляемыми к нему, что позволило разработать структуру онлайн-курса по дополнительной образовательной программе «Криптографические методы защиты информации», а после реализовать дистанционный онлайн-курс по дополнительной образовательной программе «Криптографические методы защиты информации» средствами LMS Moodle.

СОДЕРЖАНИЕ

ВЕДЕНИЕ

Стремление защитить свои интересы было присуще человеку с давних пор. Еще в древности он использовал различные варианты кодирования информации, изобретал устройства, которые бы способствовали сохранению в тайне секретной информации и при этом обеспечивали легкость ее шифрования – расшифрования.

Из такой потребности выросла целая наука – криптография. Ранее криптография служила только интересам государства, но с появлением интернета ее методы стали интересовать и частных лиц. На сегодняшний день криптография широко используется хакерами, борцами за свободу информации и простыми пользователями, желающими защитить свои данные в сети.

С момента изобретения Интернета и его дальнейшего повсеместного распространения, а также превращения его в главное средство обмена информацией между людьми криптография стала актуальной для всех слоев населения. Актуальность криптографии в наше время объясняется тем, что доступ к Интернету и другим сетям обмена информацией есть у подавляющего большинства людей в развитых странах (при таких тенденциях доступ к сетям в скором времени будет и у всего человечества), однако далеко не вся информация, которой обмениваются люди, является защищенной. Так, например, за последнее время широкое распространение получили покупки онлайн, социальные сети, услуги государственных порталов, на которых сосредоточена важнейшая личная информация граждан. Кроме того, что информация сделалась более разнообразной и более конфиденциальной, увеличилось и общее количество информации.

Однако на современном этапе развития образования даже у специалистов в области информационной безопасности часто оказываются не сформированными компетенции в области использования методов криптографической защиты информации, и они нуждаются в повышении уровня сформированности данных компетенций.

В настоящее время все больше специалистов обращаются к краткосрочным и удаленным способам получения новых знаний, коими являются дистанционные курсы, которые уже успели завоевать лидирующие позиции в современных условиях реализации образовательной деятельности.

Именно необходимость организации соответствующей информационной подготовки педагогов профессионального обучения и обусловило тему выпускной квалификационной работы создание онлайн-курса по обучению криптографической защите данных.

Объект выпускной квалификационной работы: процесс обучения слушателей дистанционного онлайн-курса «Криптографические методы защиты информации».

Предмет выпускной квалификационной работы: учебные материалы для дистанционного онлайн-курса «Криптографические методы защиты информации».

Цель выпускной квалификационной работы: разработать дистанционный онлайн-курс «Криптографические методы защиты информации».

В связи с поставленной целью в работе необходимо решить следующие задачи:

- проанализировать интернет-источники и учебно-методическую документацию дополнительной образовательной программы «Криптографические методы защиты информации»;
- рассмотреть вопросы создания дистанционного онлайн-курса и требования, предъявляемые к нему;
- разработать структуру онлайн-курса по дополнительной образовательной программе «Криптографические методы защиты информации»;
- реализовать дистанционный онлайн-курс по дополнительной образовательной программе «Криптографические методы защиты информации».

1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРОЕКТИРОВАНИЯ ДИСТАНЦИОННЫХ КУРСОВ

1.1 Методические особенности дистанционного обучения

Дистанционное обучение, по мнению [20], необходимо рассматривать как особый вид обучения, для которого характерны определенные цели, функции, принципы, способы взаимодействия субъектов образовательного процесса.

Отличие дистанционного обучения от заочного заключается в том, что дистанционное обучение призвано обеспечивать максимальную интерактивность процесса образования, которая предполагает интерактивность между обучаемым и преподавателем, а также обратную связь между обучаемым и учебным материалом, а также возможность группового обучения. Наличие обратной связи позволяет обучаемому получать информацию о правильности его продвижения в процессе получения знаний, а также осуществлять самоконтроль, самооценку в этом процессе.

Основные цели дистанционного обучения сегодня – это:

- профессиональная подготовка и переподготовка кадров;
- повышение квалификации кадров по различным специальностям;
- подготовка школьников по отдельным учебным предметам к сдаче экзаменов экстерном;
- подготовка школьников к поступлению в учебные заведения определенного профиля;
- углубленное изучение тем, разделов из изучаемых дисциплин;
- ликвидация пробелов в знаниях, умениях, навыках обучаемых по определенным дисциплинам;
- базовый курс учебной программы для учащихся, не имеющих возможности по разным причинам посещать очные учебные занятия;
- дополнительное образование по интересам.

Планируемые результаты и содержание дистанционного обучения совпадают с результатами и содержанием очного обучения, отличие заключается в некоторых принципах обучения, а также формах подачи учебного материала и формах взаимодействия преподавателя и обучающихся между собой.

Безусловно, дистанционное обучение должно строиться в соответствии со всеми дидактическими принципами, которые имеют место в современной педагогике: объективности, научности; связи теории с практикой; последовательности, систематичности; доступности при необходимой степени трудности; наглядности и разнообразия методов; сознательности и активности обучаемых; прочности усвоения знаний, умений и навыков.

1.2 Использование методов дистанционного обучения в вузе

В настоящее время в отечественной и мировой практике существует несколько вариантов организации (модели) дистанционного образования:

- образование по типу экстерната – для учащихся, которые по разным причинам не могут посещать учебные заведения очно;
- университетское образование для учащихся, которые обучаются не стационарно, а на расстоянии, заочно (открытые формы) или дистанционно;
- образование на основе одновременного взаимодействия в сети нескольких учебных заведений – учебные заведения осуществляют совместную подготовку программ дистанционного обучения по различным дисциплинам;
- организация автономных образовательных учреждений, специализирующихся на различных формах дистанционного образования;
- локальное образование на основе автономных обучающих систем;
- дистанционное образование, интегрированное с традиционными способами, или, иначе, дистанционная поддержка образовательного процесса.

1.3 Виды взаимодействия и методы дистанционного обучения

Виды взаимодействия при дистанционном обучении:

- преподаватель-группа. Основной целью этого общения является постановка целей и анализ результатов деятельности студентов.
- преподаватель-студент. В данном случае преподаватель руководит действиями отдельного студента, дает советы, рекомендации, анализирует результаты деятельности.
- студент-преподаватель. Основной формой подобного общения является запрос учащегося, сообщающего преподавателю, в каком помощи он сейчас нуждается. При этом студент учится самостоятельно ставить проблему. Кроме того, при общении по данной схеме студент может представлять результаты своего труда.
- студент-студент. Подобные взаимодействия вначале возникают стихийно. Как правило, первыми вступают в контакт наиболее активные участники дистанционного курса.
- группа-студент и студент-группа. Сотрудничество с партнерами является необходимым условием активной деятельности студентов. У учащихся, участвовавших в групповой работе, рефлексивные способности формируются значительно более эффективно, чем у учащихся, осваивавших понятия самостоятельно или только в ходе общего обсуждения.

В зависимости от способа коммуникации преподавателей и обучаемых, выделяют методы дистанционного обучения.

Метод обучения посредством взаимодействия обучаемого, консультируемого либо репетируемого с образовательными ресурсами при минимальном участии преподавателей, репетиторов, консультантов, научных и технических руководителей (самообучение). Для осуществления этого метода преподавателями, репетиторами создаются и подбираются различные образовательные ресурсы: печатные, аудио и видеоматериалы, а также учебные пособия, доставляемые по телекомму-

никационным сетям (интерактивные базы данных, электронные издания и компьютерные обучающие системы).

Метод индивидуализированного преподавания и обучения, для которого характерны взаимоотношения одного учащегося, консультируемого студента или школьника, клиента, нуждающегося в научно-технических услугах, соискателя научной степени с одним преподавателем, репетитором, консультантом или научным и техническим руководителем (обучение «один к одному»). Этот метод может реализоваться в дистанционном обучении в основном посредством таких технологий, как телефон, голосовая почта, факс, электронная почта, система Скайп.

Метод, в основе которого лежит изложение учебного материала преподавателем, при этом обучаемые не играют активную роль в коммуникации (обучение «один к многим»). Данный метод используется педагогом, репетитором, консультантом, когда обучаемых и консультируемых целая группа, они примерно одинаково подготовлены и для всех одинаков конечный результат. Например, это происходит при подготовке школьников репетитором к ЕГЭ, или же при консультировании студентов по различным дисциплинам. Этот метод, свойственный традиционной образовательной системе, получает новое развитие на базе современных информационных технологий. Так, лекции, записанные на аудио или видеокассеты, читаемые по радио или телевидению, дополняются в современном дистанционном обучении так называемыми электронными лекциями, распространяемым по компьютерным сетям с помощью систем досок объявлений. Электронная лекция, которую готовят и подбирают преподаватели, репетиторы, консультанты может представлять собой подборку статей или выдержек из них, а также учебных материалов, подготавливающих обучаемых к будущим дискуссиям. На базе технологии электронной доски объявлений развивается также метод проведения учебных электронных симпозиумов, представляющих собой серию выступлений нескольких авторитетных ученых.

Метод, для которого характерно активное взаимодействие между всеми участниками учебного процесса (обучение «многие к многим»). Значение этого метода и интенсивность его использования существенно возрастает с развитием

обучающих телекоммуникационных технологий. Этот метод ориентирован на групповую работу студентов и представляет наибольший интерес для дистанционного обучения. Он предусматривает широкое использование исследовательских и проблемных способов обучения. Роль преподавателя при таком обучении сводится к тому, что он задает тему для студентов, школьников либо для соискателей научных степеней (ставит учебную задачу), а далее он должен создать и поддерживать такую благоприятную среду общения и психологический климат, при которых обучаемые могли бы работать в сотрудничестве. Преподаватель несет ответственность за координацию, управление ходом дискуссий, а также за подготовку материалов, разработку плана работы, обсуждаемых вопросов и тем.

Метод проектов предполагает комплексный процесс обучения, позволяющий обучаемому проявить самостоятельность в планировании, организации и контроле своей учебно-познавательной деятельности, результатом которой является создание какого-либо продукта или явления. В основе метода проектов лежит развитие познавательных, творческих интересов обучаемых, умений самостоятельно формировать свои знания.

Метод проблемного обучения основан на рассмотрении сложных познавательных задач, решение которых представляет существенный практический или теоретический интерес. В процессе проблемного обучения внимание учащихся фокусируется на важных проблемах, они стимулируют познавательную активность, способствуют развитию умений и навыков по решению этих проблем. Роль преподавателя сводится к наблюдению и поддержке, но не более.

Исследовательский метод обучения характерен наличием четко поставленных актуальных и значимых для участников целей, продуманной и обоснованной структуры, широкого использования арсенала методов исследования, использования научных методов обработки и оформления результатов.

Преимущества дистанционного обучения бесспорны, поэтому и возникает необходимость в подготовке онлайн курсов, в частности, по криптографии.

1.4 Значение криптографии и ее методов для подготовки педагогов профессионального обучения профилизации «Информационная безопасность»

Подготовка кадров в области информационной безопасности имеет существенные особенности, поскольку выступает не только как важная составляющая комплекса мероприятий государства по противодействию угрозам в информационной сфере, но и как реакция на спрос рынка, Кроме того, эта специальность возникла на стыке двух наиболее активно развивающихся направлений конца XX – начала XXI века: информационных технологий и технологий обеспечения безопасности. Этими особенностями, прежде всего, и определяются специфика профессиональной подготовки в области информационной безопасности и особые требования, предъявляемые к образовательным учреждениям при организации такого вида обучения.

Одной из важнейших составляющих информационной безопасности является криптография, которая понимается как наука о защите информации от прочтения ее посторонними. Защита достигается шифрованием, т.е. преобразованием, которые делают защищенные входные данные трудно-разыскиваемыми по входным данным без знания специальной ключевой информации ключа. Под ключом понимается легко изменяемая часть криптосистемы, хранящаяся в тайне и определяющая, какое шифрующие преобразование из возможных выполняется в данном случае. Криптосистема – семейство выбираемых с помощью ключа обратимых преобразований, которые образуют защищаемый открытый текст в шифрограмму и обратно.

Криптография сейчас касается самых разных сторон жизни. Любой человек сейчас сталкивался со словами «шифр», «криптограмма» и «ключ». Даже чтобы правильно действовать на просторах интернета необходимо иметь представление, хотя бы об основах криптографии. Главными задачами криптографии является сохранить конфиденциальность данных (сделав данные «нечитаемыми» для непосвященных), не потеряв их целостность (исключая возможность изменения дан-

ных неуполномоченными лицами). Современная криптография образует отдельное научное направление на стыке математики и информатики. Практическое применение криптографии стало неотъемлемой частью жизни современного общества ее используют в таких отраслях как электронная коммерция, электронный документооборот, телекоммуникации и других. Особенно развитию криптографии повлияли не только новые технические возможности, но и сравнительно широкое распространение криптографии для использования частными лицами.

Желательно, что бы методы шифрования обладали минимум двумя свойствами:

- законный получатель сможет выполнить обратное преобразование и расшифровать сообщение;
- криптоаналитик противника, перехвативший сообщение, не сможет восстановить по нему исходное сообщение без таких затрат времени и средств, которые сделают эту работу не целесообразной.

Подготовкой специалистов в области информационной безопасности занимаются педагоги профессионального обучения, которые также должны обладать готовностью в области обеспечения криптографической защиты информации.

Профессионально-педагогическому образованию долгое время не уделялось должного внимания. Продолжительное время в России мастера производственного обучения подготавливались в индустриально-педагогических техникумах, а преподаватели – на индустриально-педагогических факультетах вузов. Приоритетное развитие промышленной сферы в социалистический период обусловило подготовку в основном специалистов с рабочими профессиями, что в свою очередь определяло и структуру педагогических кадров профессиональной школы.

Изменение социально-экономических условий в обществе нарушило систему профессионального образования, в которой уже имелись сложные социальные, экономические и политические связи.

Переориентация на рыночные отношения нарушила эти связи и вскрыла следующие противоречия:

- между объективно необходимой потребностью в постоянно растущем уровне образования и профессиональной компетентности членов общества и ограниченными возможностями образовательных институтов;
- между потребностью общества в подготовке конкурентоспособных специалистов и низким профессиональным потенциалом педагогов;
- между необходимыми для развития профессионализма преподавателей и мастеров производственного обучения финансовыми и материальными средствами и реальной социально-экономической ситуацией, снижающей эффективность образования;
- между возросшей ролью прогрессивных педагогических технологий в интенсификации профессиональной подготовки специалистов и отсутствием специального педагогического образования у подавляющей части педагогов;
- между целесообразностью личностно-развивающего учебного процесса в системе дополнительного профессионального образования, требующего достаточно продолжительного времени, и краткосрочностью курсов обучения;
- между потребностью в кадрах, имеющих высокую профессиональную компетентность, и неразработанностью механизма управления профессиональным развитием специалистов;
- между необходимостью в интеграции и существующей разобщенностью различных звеньев системы подготовки и повышения квалификации профессионально-педагогических работников.

Выделенные противоречия определяют одну из главных приоритетных задач развития профессионально-педагогического образования: развитие системы подготовки, профессиональной переподготовки и повышения квалификации кадров для профессионального образования, включающей в себя, прежде всего, подготовку педагогических и управленческих кадров для системы профессионального образования.

Таким образом, делаем вывод о необходимости подготовки к криптографии педагогов профессионального обучения; повышении квалификации кадров для профессионального образования по профилизации «Информационная безопасность». С этой целью был разработан онлайн курс по дополнительной образовательной программе «Криптографические методы защиты информации».

1.5 Анализ литературы и интернет источников по теме «Криптографические методы защиты информации»

Для проектирования содержания онлайн курса следует изучить имеющуюся литературу и интернет источники по вопросам криптографической защиты информации.

Книга Михаил Адаменко «Основы классической криптологии. Секреты шифров и кодов» [1] предлагаемая вниманию читателей книга посвящена вопросам, касающимся истории появления и развития шифров и кодов, а также основам криптографии криптоанализа и криптологии. Особое внимание уделено особенностям использования кедов и шифров различной степени сложности, которые каждый человек при необходимости может применяла в повседневной жизни. В первой главе в простой и доступной форме разъясняется значение понятий «код» и «шифр», а также приводятся краткие сведения об основных терминах определениях, используемых при работе с кодами и шифрами. Во второй и третьей главах коротко изложены наиболее знаменательные и интересные события из истории появления различных кодов, а также из истории криптографии, Советы по использованию наиболее известных кодов даны в четвертой главе. Разделы пятой главы предлагаемой книги посвящены вопросам практического применения простых шифров в повседневной жизни.

Книга Бабаш А. В. «История криптографии. Часть I» [2] написана в форме пособия, направленного на изучение «классических» шифров, то есть шифров с симметричным ключом. После краткого исторического очерка в ней рассмотрены вопросы дешифрования простейших шифров, методы криптоанализа и синтеза

криптосхем, вопросы криптографиической стойкости, помехоустойчивости и имитостойкости шифрсистем. Архитектура пособия двухуровневая. Первый уровень предназначен для студентов, изучающих дисциплины криптографии и компьютерной безопасности, читателей, впервые знакомящихся с учебными материалами по криптографии. Второй уровень для аспирантов, преподавателей вузов соответствующего профиля, для круга специалистов, чьей задачей является использование криптографических средств защиты информации, для читателей, желающих познакомиться с теоретической криптографией.

Учебное пособие Бабенко Л. К. «Современные алгоритмы блочного шифрования и методы их анализа» [3] посвящено алгоритмам блочного шифрования: принципам их построения и анализа. Рассматриваются действующие стандарты, а также многие другие общеизвестные криптографические алгоритмы, в том числе и финалисты конкурса AES. Излагаются способы проведения атак на эти алгоритмы с помощью таких методов, как линейный и дифференциальный криптоанализ. Описан подход к применению нового метода криптоанализа линейно-дифференциального. Представлены виды криптоанализа на основе слайдовой атаки. В приложениях приведены таблицы с результатами анализа наиболее известных алгоритмов шифрования.

Доминик Байер «Microsoft ASP .NET. Обеспечение безопасности» [4]. Эта книга подробное руководство для программистов, которые используют Microsoft ASP .NET 2.0 и заинтересованы в обеспечении безопасности разрабатываемых приложений. В ней подробно рассказывается о способах внедрения в приложения превентивных мер защиты, в частности подтверждения ввода данных, аутентификации и авторизации. Рассмотрены методы обнаружения и обработки ошибок, ограничение функциональности с помощью частичного доверия, применение провайдеров защиты. Отдельная глава посвящена описанию инструментов, которые можно использовать для тестирования и улучшения защиты приложений.

Баричев С. Г. «Основы современной криптографии» [5] книга по основам криптографии. В первой главе рассказывается история криптографии, основные понятия и определения, требования к криптосистемам, а также краткие сведения о

криптоанализе. Далее рассматриваются традиционные симметричные и асимметричные криптосистемы, включая Криптосистемы Эль-Гамаля, Диффи-Хеллмана, Ривеста-Шамира-Адлемана, Меркля-Хеллмана и Хора-Ривеста, а также криптосистемы, основанные на эллиптических кривых. В последних главах рассматриваются электронные подписи и управление криптографическими ключами. В систематизированном виде рассмотрены вопросы создания симметричных и асимметричных криптографических систем защиты информации. Описаны алгоритмы электронных цифровых подписей, системы управления криптографическими ключами, имитозащита информации. Для специалистов в области защиты информации, может быть полезна студентам вузов.

Учебник Герман О.Н. «Теоретико-числовые методы в криптографии» [6] создан в соответствии с Федеральным государственным образовательным стандартом по направлениям подготовки «Информационная безопасность» и «Математика» (квалификация «бакалавр»). В учебнике описаны: элементы теории чисел, быстрые алгоритмы решения ряда важных задач с числами (возведение в степень, вычисление символов Лежандра, отсеивание составных чисел и др.) и многочленами над конечными полями (разложение на множители и нахождение корней); алгоритмы проверки чисел на простоту, разложения чисел на множители, дискретного логарифмирования, построения приведенного базиса решетки. Также даны криптографические приложения теоретико-числовых алгоритмов (криптосхема RSA, открытое распределение ключей, электронная цифровая подпись, криптосхемы, основанные на теории решеток).

Книга Горев А.И; Симаков А.А. «Обеспечение Информационной Безопасности» [7] рассматриваются вопросы, связанные с общими правилами применения технических (физических и аппаратных), программных, организационных (административных), правовых (законодательных) и морально-этических мер защиты информации.

Жданов О.Н. «Методика выбора ключевой информации для алгоритма блочного шифрования» [8]. Как известно, при использовании незащищенного канала актуарными являются задачи обеспечения конфиденциальности передавае-

мых данных и аутентификации источника сообщений. В настоящее время для решения этих задач используются итерированные симметричные алгоритмы блочного шифрования, такие как ГОСТ 28147-89. DES. IDEA, AES и т.п. Безопасность зашифрованных сведений обеспечивается не только алгебраической структурой алгоритма, но также и корректным выбором элементов ключевой информации (ключей таблиц замен). Автором на основе проведенного анализа существующих подходов к построению ключей и таблиц замен разработана методика генерации и тестирования ключевой информации для алгоритмов блочного шифрования. Автором совместно с В. А. Чалкиным эта методика программно-реализована. Представлены алгоритм и исходные тексты программ, приведены результаты экспериментов.

В книге Здор С.Е. «Кодированная информация. От первых природных кодов до искусственного интеллекта» [9] рассматриваются основные информационные понятия: код, элемент, система, пространство, среда, сеть. Коротко описываются действия, выполняемые над кодированной информацией, кодирование, перекодирование, декодирование, восприятие, переработка, реализация, передача, хранение, размножение. Анализируются свойства кодированной информации, такие как: количество, семантика, ценность, правдивость, понимание, востребованность, доступность, конфиденциальность, опасность, виртуальность. Прослеживается ход эволюционного информационного процесса, начиная от первых логических элементов и примитивных информационных кодов и заканчивая естественными разумными системами и настоящим искусственным интеллектом. Высказывается и обосновывается предположение, что такие феномены, как жизнь и разум, являются продуктами эволюции кодированной информации.

Земор Ж.Ж. «Курс криптографии» [10]. Понимание принципов криптографии стало для многих потребностью в связи с широким распространением криптографических средств обеспечения информационной безопасности. Данная монография написана на базе курса, читавшегося в Высшей национальной школе телекоммуникаций. Отличительной особенностью книги является то, что, помимо традиционной точки зрения на криптографию, в ней рассматриваются современ-

ные идеи и решения. Книга знакомит читателя с новейшими познаниями в области разложения на множители больших целых чисел, сложность которого стала причиной возникновения многих криптографических техник. Подробно описываются различные криптографические протоколы, выделяется понятие доказательства без переноса знания. Изучаются различные приложения к криптографии теории кодов с исправлением ошибок.

В книге Зубова А.Н. «Математика кодов аутентификации» [11] изложены известные из открытой печати конструкции, а также результаты исследований стойкости и эффективности реализации систем аутентификации информации, использующих криптографические методы.

В книге «Криптография: скоростные шифры» А. Молдовян и др. [12] рассматривается широкий круг вопросов, связанных с использованием криптографических методов защиты информации в компьютерных системах. Впервые излагается разработанная авторами концепция управляемых преобразований, являющаяся новым направлением прикладной криптографии. Представлены варианты построения управляемых операций и анализ их основных криптографических свойств. Дается описание ряда новых криптографических примитивов и скоростных криптосистем с оценкой их стойкости к дифференциальному, линейному и другим методам криптоанализа. Показана возможность построения операционных блоков, реализующих уникальные модификации операций для каждого значения управляющего кода. Отражены вопросы построения управляемых перестановок и управляемых подстановочных операций, в частности, управляемых сумматоров специального типа, а также представлены методы конструирования скоростных итеративных шифров на их основе.

В учебном пособии Литвинская О.С. «Основы теории передачи информации» [13] описаны основные положения теории связи, относящиеся к сигналам, модуляции и кодированию цифровой информации. В доступной форме изложены вопросы представления сигналов и способы их математической обработки. Отдельные формулы сопровождаются соответствующими пояснениями.

Книга Масленников М. «Практическая криптография» [14]. Книга посвящена прикладным проблемам современной криптографии. Наряду с основными теоретическими положениями рассматривается: создание криптографического ядра, встраивание криптографических алгоритмов в Microsoft Outlook и Lotus Notes, создание автоматизированной системы документооборота, технология отпечатков пальцев. Все программное обеспечение, описываемое в книге, создано в Borland C++ Builder. На прилагаемом к книге компакт диске находятся демонстрационные версии некоторых программ и документация. Для широкого круга IT-специалистов и специалистов, отвечающих за безопасность систем.

Пособие Черемушкина А. В. «Лекции по арифметическим алгоритмам» [15] представляет собой краткое введение в область современной вычислительной теории чисел и ее приложений к криптографическим задачам.

В книге Черчхаус Роберт «Коды и шифры. Юлий Цезарь» [16] рассказывается о системах шифрования от наиболее ранних и простых (в том числе о таких известных шифрмашинах времен Второй мировой войны, как Энигма и Хагелин) до самых современных и сложных. Рассматриваются вопросы стойкости систем шифрования и методы дешифрования. Издание снабжено приложением с множеством примеров и задач с решениями, которые будут интересны старшеклассникам, увлекающимся математическими головоломками.

1.6 Проектирование и разработка дополнительной образовательной программы «Криптографические методы защиты информации»

Анализ реализации требований по уровню подготовки выпускников средней школы в области информационной безопасности показывает, что в целом, кроме вопросов антивирусной защиты компьютеров и вопросов этических и правовых норм в отношении информации, средняя школа в настоящее время не дает достаточной начальной подготовки по вопросам информационной безопасности. Таким образом, обычный выпускник приступает к обучению по специальности «информационная безопасность» в колледже, имея достаточно низкую начальную подго-

товку. Задачей педагогов становится повышения уровня сформированности компетенций в области обеспечения информационной безопасности, однако в современных условиях появление все новых угроз ставит под сомнение актуальность подготовки самих педагогов, вынуждая последних постоянно повышать уровень своей квалификации через курсы и прохождения различных программ переподготовки.

Дополнительное образование в ВУЗе – это процесс воспитания и обучения с помощью различных дополнительных образовательных программ, оказания дополнительных образовательных услуг.

Дополнительное образование в ВУЗе позволяет студентам получить дополнительные знания, умения, практические навыки по образовательным программам, которые предусматривают дополнительное изучение отдельных дисциплин и разделов дисциплин, необходимых для профессиональной деятельности.

Получение дополнительного образования в высших учебных заведениях помогает повысить и расширить квалификацию специалистов, а также адаптировать их к современным экономическим и социальным условиям, и к ведению профессиональной деятельности. Дополнительное образование в ВУЗе регулярно сопровождается семинарами, тренингами, ролевыми играми, индивидуальной и групповой диагностикой, мастер-классами, консультированием.

Получая, дополнительное образование в ВУЗе, студенты имеют возможность получить диплом государственного образца или удостоверение о прохождении курсов того ВУЗа, в котором они проходят процесс обучения.

В учебный план направления подготовки 44.03.04 Профессиональное обучение (по отраслям) профиля Информационные технологии профилизации «Информационная безопасность» не включена дисциплина, посвященная вопросам рассмотрения криптографий и ее методов.

Главными задачами криптографии является сохранить конфиденциальность данных (сделав данные «нечитаемыми» для непосвященных), не потеряв их целостность (исключая возможность изменения данных неуполномоченными лицами).

Современная криптография образует отдельное научное направление на стыке математики и информатики. Практическое применение криптографии стало неотъемлемой частью жизни современного общества – ее используют в таких отраслях, как электронная коммерция, электронный документооборот, телекоммуникации и других.

Особенно развитию криптографии повлияли не только новые технические возможности, но и сравнительно широкое распространение криптографии для использования частными лицами. На основании вышеизложенного, можно сделать вывод о необходимости разработки дополнительной образовательной программы «Криптографические методы защиты информации».

Целями освоения дополнительной образовательной программы «Криптографические методы защиты информации» являются:

- изучить виды и типы шифрования, методы и средства обеспечения криптографической защиты информации;
- рассмотреть алгоритмы и стандарты шифрования;
- научить использовать методы криптографии в профессиональной деятельности для обеспечения информационной безопасности.

Дополнительная образовательная программа «Криптографические методы защиты информации» рассчитана на 72 часа, из которых 36 часов отводится на лекционные занятия, 8 часов на вопросы для самоконтроля, разработанные для проверки сформированности знаний, практические занятия и самостоятельная работа, которая представленная лабораторными работами и тестами, занимает 28 часов.

Процесс изучения дополнительной образовательной программы «Криптографические методы защиты информации» направлен на формирование элементов следующих профильно-специализированных компетенций:

- ПСК-6 (владение технологиями (алгоритмами) решения различных задач);
- ПСК-21 (способность применять криптографические протоколы для передачи и хранения данных в распределенных информационных системах).

На основании анализа содержания профильно-специализированных компетенций можно сделать вывод, что при изучении дополнительной образовательной программы «Криптографические методы защиты информации» необходимо ознакомится с основными понятия криптографии как науки, изучить методы шифрования, их актуальности, необходимости использования. Так же следует рассмотреть алгоритмы и стандарты криптографии, поточные шифрования, электронную цифровую подпись.

В соответствии с содержанием профильно-специализированных компетенций было спроектировано наполнение дополнительной образовательной программы «Криптографические методы защиты информации».

Тематический план дополнительной образовательной программы «Криптографические методы защиты информации» представлен в таблице 1.

Таблица 1 – Содержание и тематическое планирование дисциплины «Криптографические методы защиты информации»

№	Наименование разделов программы	Всего часов	Форма контроля
1.	Криптография и шифрование	8	Проверочный тест
2.	Базовые алгоритмы шифрования	10	Лабораторные работы
3.	Примеры использования базовых алгоритмов шифрования	10	Лабораторные работы
4.	Комбинированные методы шифрования	8	Проверочный тест
5.	Стандарты шифрования	10	Лабораторные работы
6.	Поточное шифрование	8	Лабораторные работы
7.	Электронная цифровая подпись	10	Проверочный тест
8.	Программные и аппаратные шифраторы	8	Проверочный тест
	Итого по всему курсу обучения	**72**	

В тематическом плане дополнительной образовательной программы указаны восемь темы, изучаемые в рамках данной программы, по каждой из которых предусмотрены: тесты, лабораторные работы или практические занятия, соответственно, в онлайн курс также должны быть включены заявленные темы и система должна обеспечить возможность разработки и представления в надлежащем виде лабораторных работ и тестового контроля.

2 РАЗРАБОТКА ОНЛАЙН-КУРСА ПО ДОПОЛНИТЕЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

2.1 Цель создания онлайн-курса по дополнительной образовательной программе «Криптографические методы защиты информации»

Информация приобрела самостоятельную коммерческую ценность не так давно и стала широко распространенным, почти обычным, товаром. Ее производят, хранят, транспортируют, продают и покупают, а значит воруют и подделывают и, следовательно, ее необходимо защищать.

Среди всего спектра методов защиты данных от нежелательного доступа особое место занимают криптографические методы. В отличие от других методов, они опираются лишь на свойства самой информации и не используют свойства ее материальных носителей, особенности узлов ее обработки, передачи и хранения.

Широкое применение компьютерных технологий и постоянное увеличение объема информационных потоков вызывает постоянный рост интереса к криптографии. В последнее время увеличивается роль программных средств защиты информации, просто модернизируемых не требующих крупных финансовых затрат в сравнении с аппаратными криптосистемами. Современные методы шифрования гарантируют практически абсолютную защиту данных, но всегда остается проблема надежности их реализации.

В настоящее время особо актуальной стала оценка уже используемых криптоалгоритмов. Задача определения эффективности средств защиты зачастую более трудоемкая, чем их разработка, требует наличия специальных знаний и, как правило, более высокой квалификации, чем задача разработки. Это обстоятельства приводят к тому, что на рынке появляется множество средств криптографической защиты информации, про которые никто не может сказать ничего определенного. При этом разработчики держат криптоалгоритм в секрете. Однако задача

точного определения данного криптоалгоритма не может быть гарантированно сложной хотя бы потому, что он известен разработчикам. Кроме того, если нарушитель нашел способ преодоления защиты, то не в его интересах об этом заявлять. Поэтому обществу должно быть выгодно открытое обсуждение безопасности систем защиты информации массового применения, а сокрытие разработчиками криптоалгоритма должно быть недопустимым.

Поскольку, как было замечено выше, данная тема не нашла свое отражение в учебном плане подготовки педагогов профессионального обучения профилизации «Информационная безопасность», было решено разработать дополнительную образовательную программу «Криптографические методы защиты информации» для студентов компьютерных специальностей и других категорий слушателей, обладающих компьютерной грамотностью и желающих повысить уровень информационной подготовки в области обеспечения криптографической защиты информации.

Целями создания дистанционного онлайн-курса «Криптографические методы защиты информации» стали:

- изучение видов и типов шифрования, методов и средств обеспечения криптографической защиты информации;
- рассмотрение алгоритмов и стандартов шифрования;
- изучение использования методов криптографии в профессиональной деятельности для обеспечения информационной безопасности.

2.2 Структура дистанционного онлайн-курса «Криптографические методы защиты информации»

Разработка онлайн курса начинается с определения его структуры, которая понимается как совокупность устойчивых связей частей объекта, обеспечивающих его целостность и тождественность самому себе, т.е. сохранение основных свойств при различных внешних и внутренних изменениях. Онлайн курса, согласно рабочей программе, рассчитан на 72 часа и будет занимать 8 недель обуче-

ния. Для каждой недели обучения предусмотрены лекционные занятия (36 часов), вопросы для самоконтроля, разработанные для проверки сформированности знаний (8 часов), практические занятия и самостоятельная работа, которая представленная лабораторными работами и тестами (28 часов).

Структура онлайн-курса представлена на рисунке 1 и состоит из 8 тем: «Криптография и шифрование», «Базовые алгоритмы шифрования», «Примеры использования базовых алгоритмов шифрования», «Комбинированные методы шифрования», «Стандарты шифрования», «Поточные шифрования», «Электронная цифровая подпись», «Программные и аппаратные шифраторы».

Первая неделя посвящена изучению понятий криптографии, шифрованию; ознакомлению с историей развитием технологий шифрования. Знакомству с основными методами шифрования: алгоритмами замены (подстановки), алгоритмами перестановки, алгоритмами гаммирования. Ознакомлением с симметричными и ассиметричными криптосистемами: их определениями, историей, особенностями, применением, преимуществами и недостатками

Вторая неделя онлайн-курса дает представление об основных, базовых алгоритмах шифрования: их описании и алгоритмов использования.

В третьей неделе представлены примеры использования базовых методов шифрования. Ознакомление с их историей, применением и алгоритмами использования.

На четвертой неделе рассматриваются комбинированные методы шифрования. Делаются выводы об актуальности их применения. Показаны методы и виды комбинированных методов шифрования, их примеры. Так же дается описание N-кратному шифрованию, его преимуществам и недостаткам.

Пятая неделя онлайн-курса посвящена стандартам шифрования. На этой неделе рассматриваются как Российские стандарты шифрования, так и зарубежные стандарты. Приводятся их примеры, описание и применение.

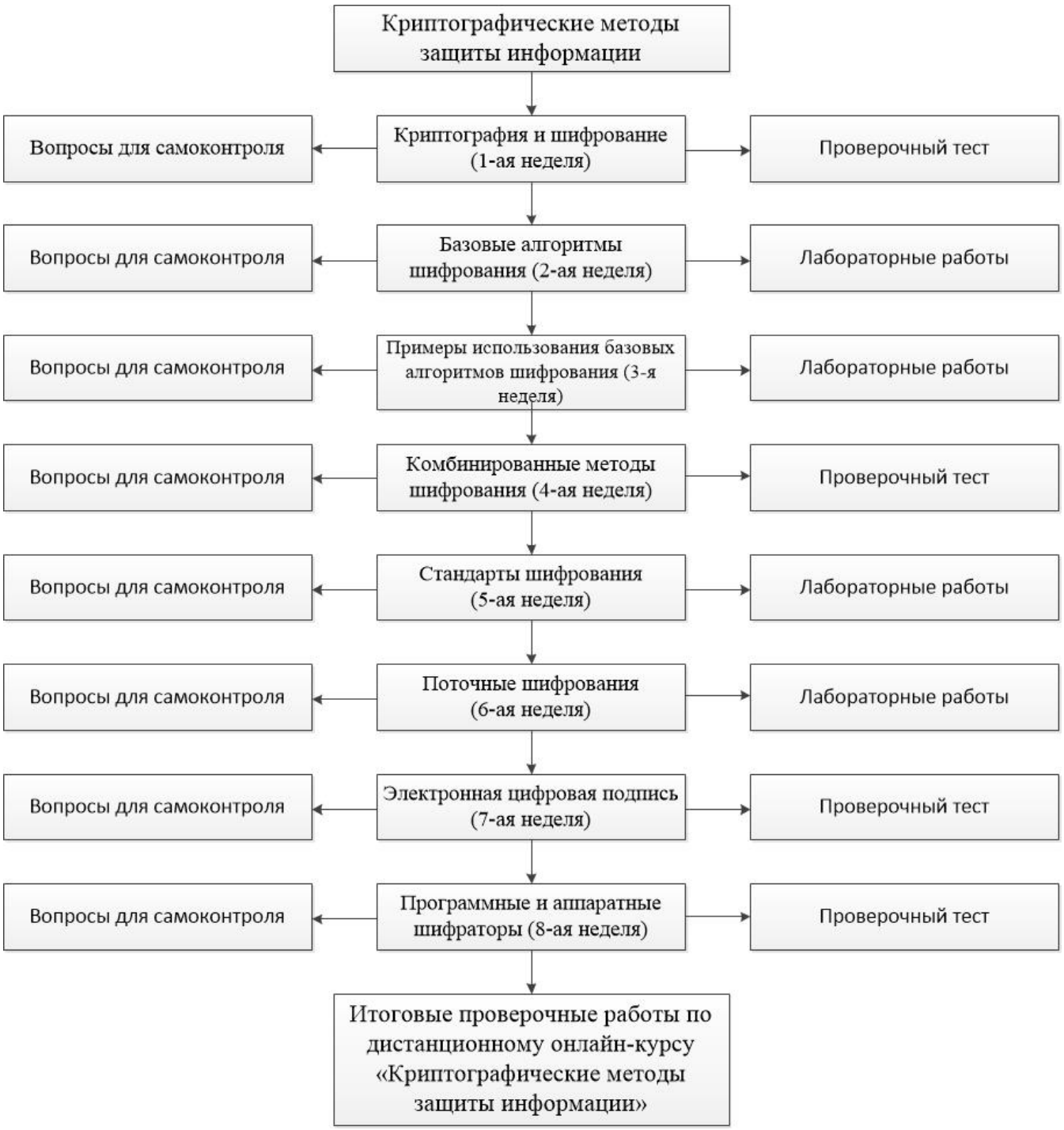


Рисунок 1 – Структура дистанционного онлайн-курса «Криптографические методы защиты информации»

На шестой неделе затронута такая тема как «Поточные шифрования». Идет ознакомление с их историей и принципами работы. Показаны виды поточных шифров, их примеры, описание, применение и отличие их от блочных шифров.

Электронная цифровая подпись это тема седьмой недели онлайн-курса. На этой неделе рассматриваются основные определение по данной теме, общая схема, функции вычисления и проверки и алгоритмы электронной цифровой подписи. Преподаватель дает представление обучающимся о видах угроз и перечне защиты, которые обеспечивает электронная цифровая подпись.

На восьмой неделе представлена тема «Программные и аппаратные шифраторы»: их описания, примеры, преимущества и недостатки.

2.3 Выбор средства для реализации онлайн-курса по дополнительной образовательной программе «Криптографические методы защиты информации»

Сегодня имеется большое количество платформ, позволяющих разрабатывать онлайн курсы: Eliademy, EduBrite, Versal, Basecamp, Edmodo, Udemy, Coursmos, Stepic и многие другие.

Однако система Moodle на сегодняшний день является одним из лидеров в области поддержки дистанционных курсов, в связи с ее уникальными достоинствами. Основные причины использования данной системы в том, что она бесплатна, имеет много различных возможностей, которые учителя и администраторы могут использовать для обучения и, в определенной степени, легка в использовании.

Широкие возможности LMS MOODLE обусловлены разнообразием форм подачи материала: ресурсы любых форматов (тексты, рисунки, видеофайлы, слайд-шоу, презентации) и деятельностные элементы (задание, лекция, тест). Благодаря этому «набору» преподаватель может организовать изучение материала в соответствии с программой дисциплины, учитывая при этом цели и задачи конкретной темы. Немаловажно, что LMS экономит время преподавателя, оценивая выполненные студентами задания и перемещая оценки в электронный журнал успеваемости.

LMS Moodle система управления курсами (электронное обучение), также известная как система управления обучением или виртуальная обучающая среда. Является аббревиатурой от англ. Modular Object-Oriented Dynamic Learning Environment (модульная объектно-ориентированная динамическая обучающая среда). Представляет собой свободное (распространяющееся по лицензии GNU GPL) веб-приложение, предоставляющее возможность создавать сайты для онлайн-обучения.

Организация учебного взаимодействия между участниками в онлайн и офлайн режимах. Формирование необходимого объема учебного материала в мультимедийной форме (графика, видео, аудио, презентации, мультипликация и т.д.). Обеспечение условий для индивидуального и группового обучения. Особенности проектирования электронных курсов в среде Moodle.

По уровню предоставляемых возможностей Moodle выдерживает сравнение с известными коммерческими LMS, в то же время выгодно отличается от них тем, что распространяется в открытом исходном коде это дает возможность «заточить» систему под особенности конкретного образовательного проекта, а при необходимости и встроить в нее новые модули.

Moodle ориентирована на коллаборативные технологии обучения – позволяет организовать обучение в процессе совместного решения учебных задач, осуществлять взаимообмен знаниями.

Широкие возможности для коммуникации – одна из самых сильных сторон Moodle. Система поддерживает обмен файлами любых форматов – как между преподавателем и студентом, так и между самими студентами. Сервис рассылки позволяет оперативно информировать всех участников курса или отдельные группы о текущих событиях. Форум дает возможность организовать учебное обсуждение проблем, при этом обсуждение можно проводить по группам. К сообщениям в форуме можно прикреплять файлы любых форматов.

Есть функция оценки сообщений как преподавателями, так и студентами. Чат позволяет организовать учебное обсуждение проблем в режиме реального времени. Сервисы «Обмен сообщениями», «Комментарий» предназначены для

индивидуальной коммуникации преподавателя и студента: рецензирования работ, обсуждения индивидуальных учебных проблем. Сервис «Учительский форум» дает педагогам возможность обсуждать профессиональные проблемы. Важной особенностью Moodle является то, что система создает и хранит портфолио каждого обучающегося: все сданные им работы, все оценки и комментарии преподавателя к работам, все сообщения в форуме. Преподаватель может создавать и использовать в рамках курса любую систему оценивания. Все отметки по каждому курсу хранятся в сводной ведомости. Moodle позволяет контролировать «посещаемость», активность студентов, время их учебной работы в сети.

В основу создания системы управления обучением Moodle были положены принципы, являющиеся обобщением большого количества работ таких ученых, как Лев Семенович Выготский, Джон Дьюи, Жан Пиаже, Эрнст фон Глазерфельд. Благодаря этим научным исследованиям получили развитие такие направления в области образования и психологии, как конструктивизм, конструкционизм, социальный конструктивизм.

2.4 Содержание дистанционного онлайн-курса «Криптографические методы защиты информации»

Разработанный дистанционный онлайн-курс рассчитан на 8 недель обучения. Каждая неделя состоит из лекционного материала по данной теме, вопросов для самоконтроля и задания на проверку знаний обучающегося. В конце всего курса так же так же предусмотрен ряд проверочных работ для закрепления материала обучающимся. Содержимое данного курса позволит как донести преподавателю в полном объеме материал до обучающегося, так и усвоить, и закрепить последнему знания по данной теме.

Содержание дистанционного онлайн курса по теме «Криптографические методы защиты информации»:

1. Криптография и шифрование.

1.2 Вопросы для самоконтроля.

1.3 Проверочный тест.

2. Базовые алгоритмы шифрование.

2.1 Вопросы для самоконтроля.

2.2 Лабораторные работы.

3. Примеры использования базовых алгоритмов шифрования.

3.1 Вопросы для самоконтроля.

3.2 Лабораторные работы.

4. Комбинированные методы шифрования.

4.1 Вопросы для самоконтроля.

4.2 Проверочный тест.

5. Стандарты шифрования.

5.1 Вопросы для самоконтроля.

5.2 Лабораторные работы.

6. Поточные шифрования.

6.1 Вопросы для самоконтроля.

6.2 Лабораторные работы.

7. Электронная цифровая подпись.

7.1 Вопросы для самоконтроля

7.2 Проверочный тест

8. Программные и аппаратные шифраторы.

8.1 Вопросы для самоконтроля.

8.2 Проверочный тест

Итоговая работа по всему изученному дистанционному онлайн-курсу.

К выполнению итогового теста слушатели будут допускаться, только в случае прохождения всех контрольных точек курса, а именно выполнения лабораторных работ, промежуточных тестов, ответов на вопросы для самоконтроля. Причем по итогам выполнения работа они должны набрать не менее 45 баллов. Итоговый тест дает возможность набрать еще максимум 30.

2.5 Разработка дистанционного онлайн-курса по дополнительной образовательной программе «Криптографические методы защиты информации»

Разработка дистанционного курса с использованием платформы Moodle начинается с определения названия курса и указания количества недель, отводимого на его изучение.

Сразу после регистрации платформа попросит определиться с техническими моментами задать настройки приватности; указать продолжительность курса; дать ему название, описание, определится с датами начала и конца курса; обеспечить доступность и многие другие. Перед началом работы над своим курсом необходимо проверить их, при необходимости, отредактировать. Пример показан на рисунке 2.

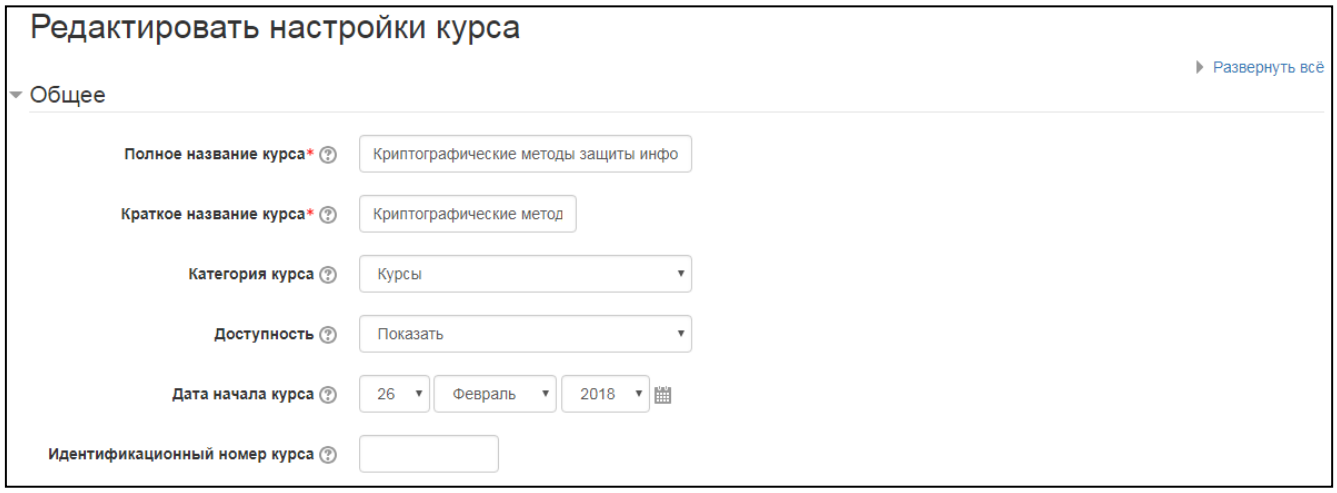


Рисунок 2 – Фрагмент основных настроек онлайн-курса в системе Moodle

Далее для входа в курс необходимо нажать на его название. В центральном блоке страницы представлено содержание курса, выделены тематические разделы курса, а по бокам – функциональные и информационные блоки. Все основные элементы управления курсом находятся слева в отдельном блоке – «Настройки». Чтобы внести какие-либо изменения на страницу курса необходимо включить. «Режим редактирования», который показан на рисунке 3. В этом случае на страницах вашего курса появятся маленькие значки (пиктограммы), пользуясь которыми Вы сможете изменять любой из элементов курса. Режим редактирования

может включаться двумя способами: через блок «Настройки» или кнопкой в правой верхней части страницы.

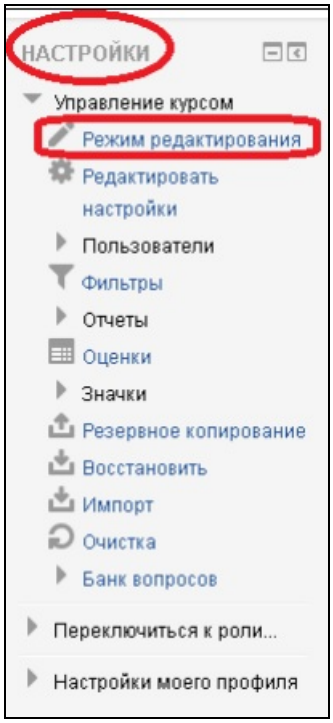


Рисунок 3 – Окно настроек

Обратите внимание, что режим редактирования доступен только тем пользователям, у которых есть права преподавателя курса. Интерфейс системы в режиме редактирования достаточно прост и представлен на рисунке 4. Здесь слева расположена навигационная панель, которая позволяет легко перемещаться внутри курса и увидеть все разделы, темы и методические материалы курса. Также для дистанционного онлайн-курса была написана аннотация, в которой описано содержание курса, а также круг лиц, для которых данный курс будет полезен и интересен. Именно грамотно написанная аннотация позволит привлечь слушателей на курс, а также даст им представление о данном курсе.

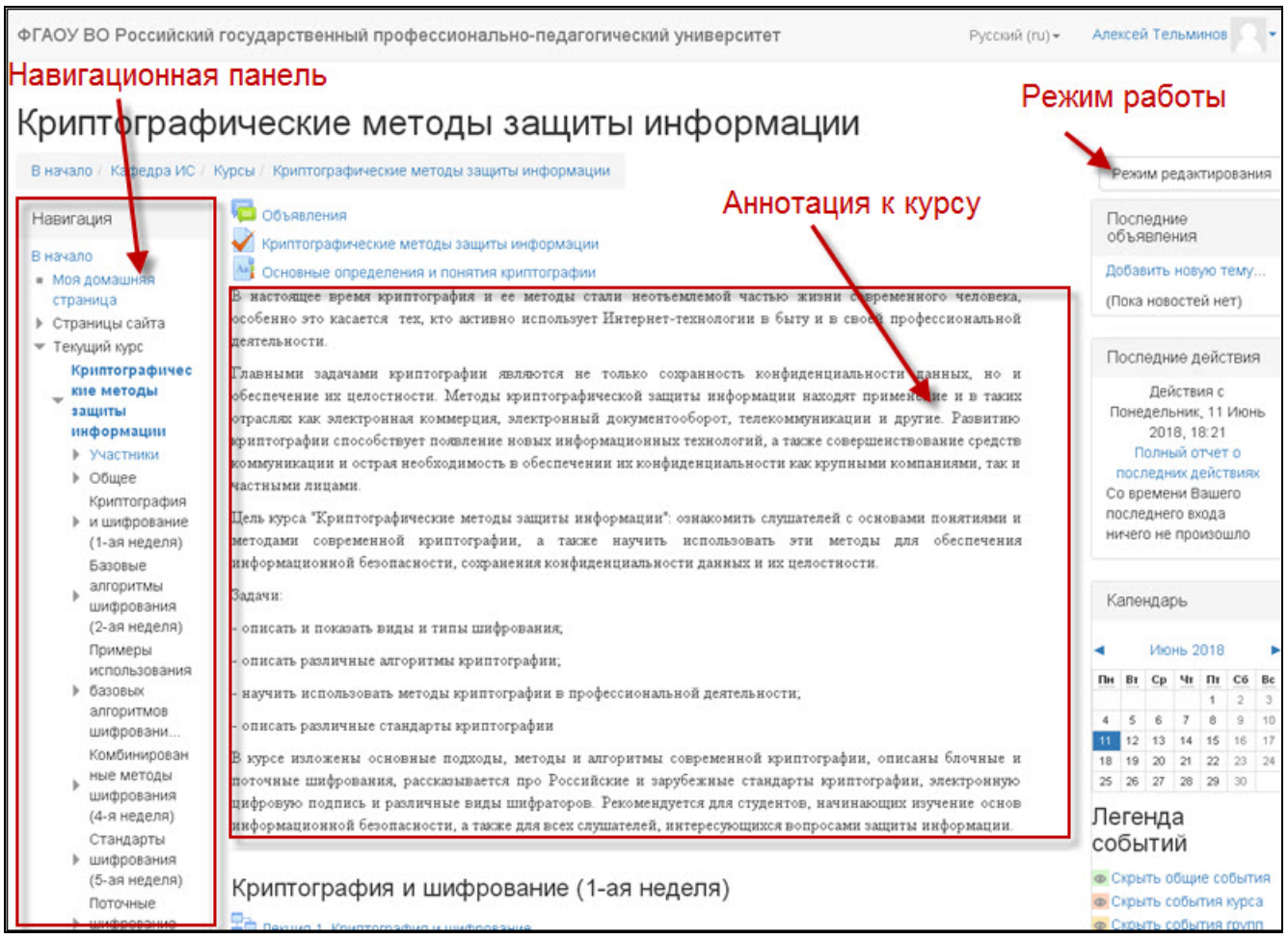


Рисунок 4 – Начальная страница курса с правами пользователя

В режиме редактирования страницы курса выглядит немного иначе, что можно заметить на рисунке 5. Системой Moodle для изменения контента курса предусмотрены различные кнопки и переключатели, как видно на рисунке у объявлений и других элементов курса появились значки, которые помогут в редактировании информации содержащейся в этих подпунктах, а также позволят скорректировать место их нахождения для более удобной и эффективной работы с курсом. Кроме того, в режиме редактирования можно добавить календарь, посмотреть и добавить объявления для слушателей дистанционного курса и посмотреть те изменения, которые были внесены в курс, что удобно при коллективной разработке курса. Однако в нашем случае, разработка курса велась от лица одного пользователя, и данный режим не был задействован.

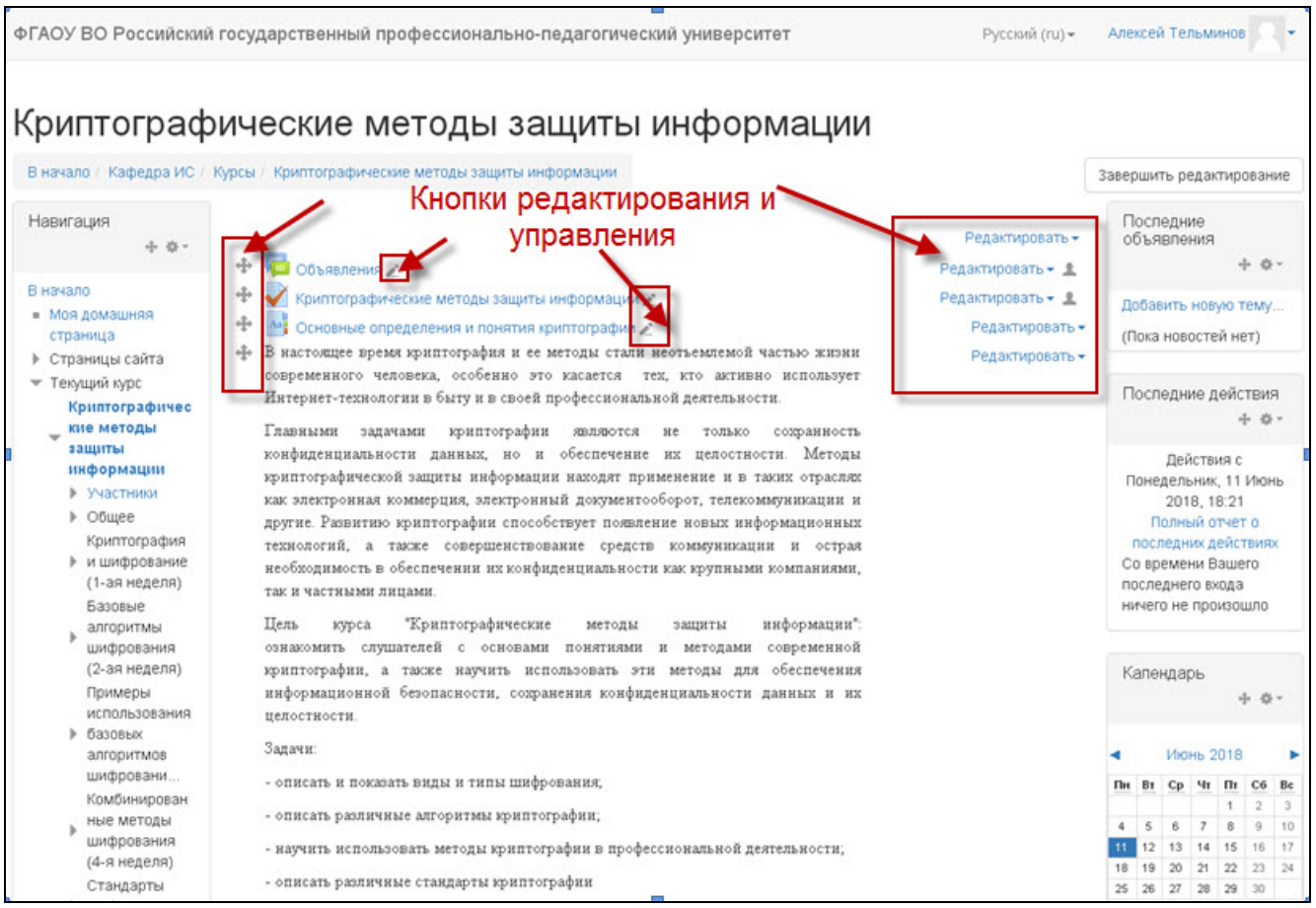


Рисунок 5 – Страницы курса в режиме редактирования

Запись студентов на курс осуществляется автоматически, после ввода кодового слова, которое при очной встрече выдается студентам любой формы обучения. Кодовое слово позволяет предоставить доступ к курсу только тем, кто знает пароль. Если поле оставить пустым, то любой пользователь сможет записаться на курс. Если задано кодовое слово, то любому пользователю при попытке записаться на курс потребуется его ввести. Для настройки этого способа записи на курс в блоке «Настройки» на левой панели курса необходимо было выбрать строку «Пользователи» и в раскрывшемся списке выбрать «Способы записи на курс», который показан на рисунке 6. Поскольку курс рассчитан как для студентов университета, так и для сторонних слушателей необходимо было определить различные вариации записи на курс.

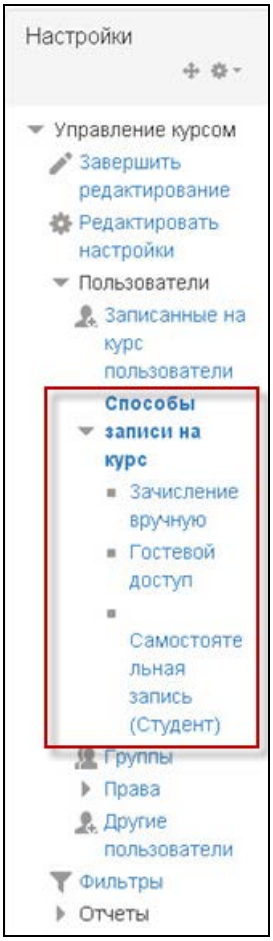


Рисунок 6 – Окно настроек для записи студентов на курс

На открывшейся странице и рисунке 7 представлены три способа записи на курс, кликнув на значок «шестеренки» (редактировать) напротив строки «Самостоятельная запись (Студент)» установим кодовое слово для записи на дистанционный курс «Криптографические методы защиты информации».

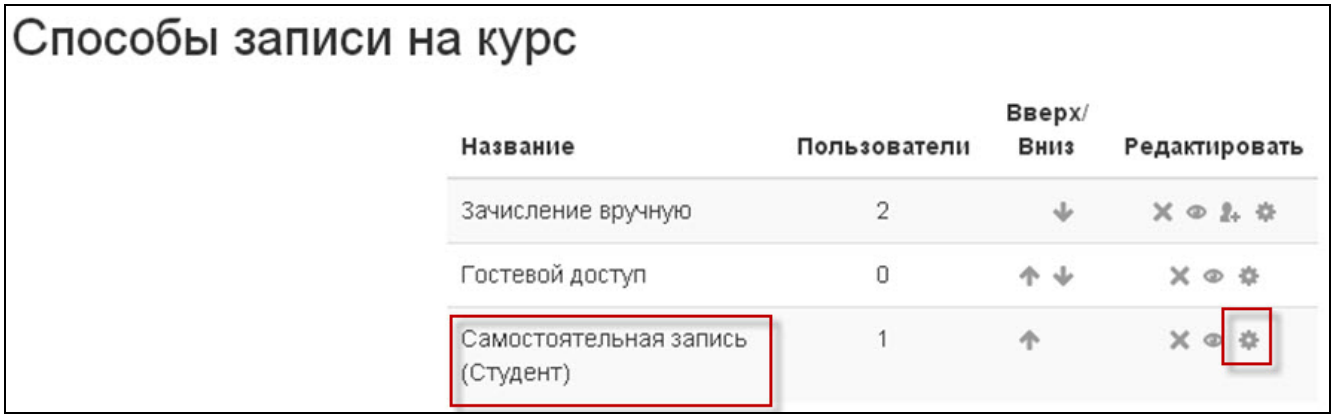


Рисунок 7 – Три способа записи на дистанционный онлайн-курс «Криптографические методы защиты информации»

Заполнили поля, как показано на рисунке 8, указав название способа, как ИБ-401, разрешили существующие записи на курс, разрешили новые зачисления, что необходимо для записи новых слушателей, кодовое слово задали «Екатеринбург». Кодовое слово может содержать: русские, английские буквы и цифры. Важно помнить, что не следует выбирать стандартные пароли, поскольку кодовое слово необходимо для того, чтобы доступ к дисциплине могли получить только те студенты и слушатели, которые проходят данный курс и имеют соответствующее разрешение на это.

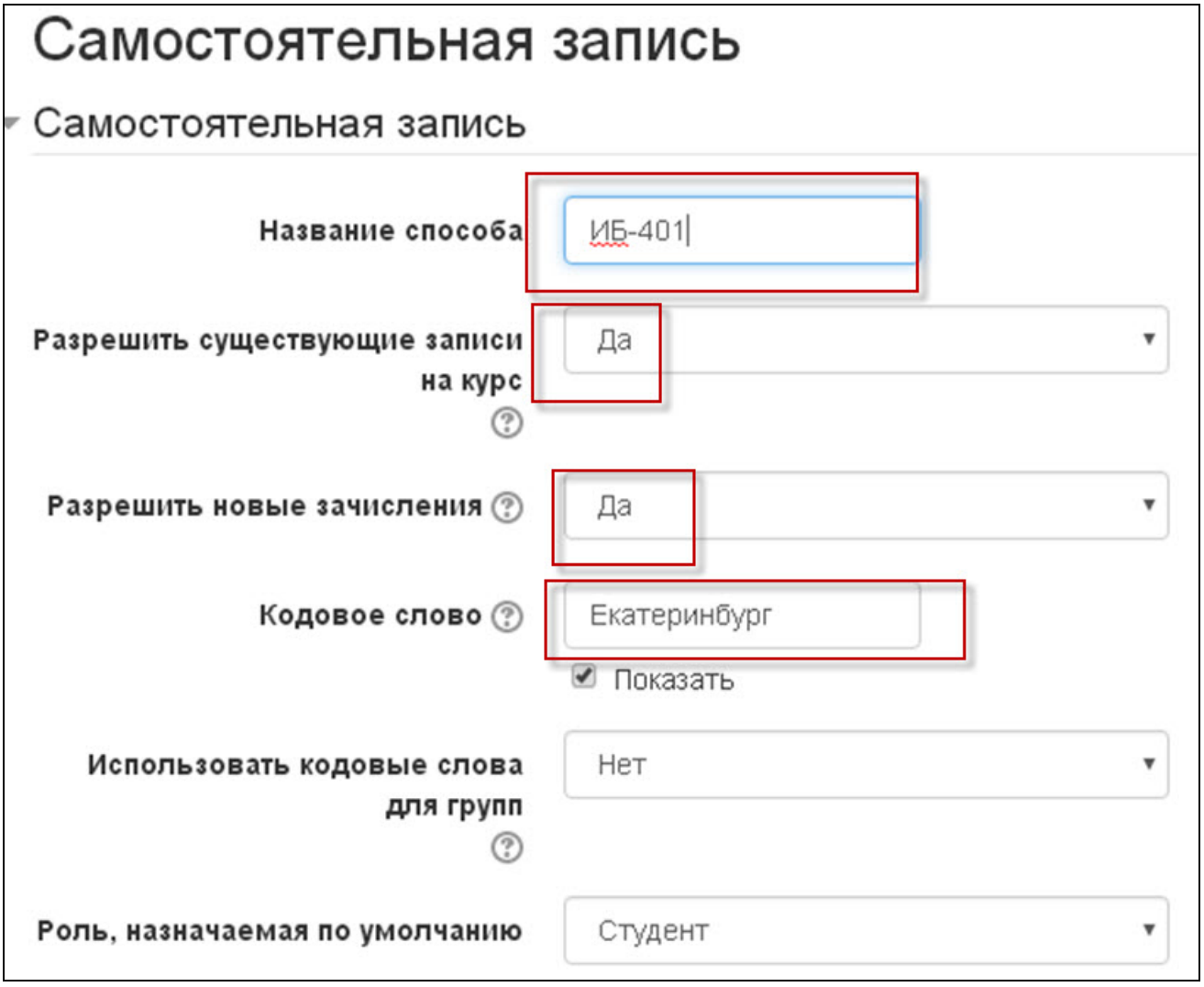


Рисунок 8 – Настройки самостоятельной записи слушателей на курс

Дополнительная образовательная программа «Криптографические методы защиты информации» составляет 72 часа. Согласно учебному плану данный курс разделен на 8 тем, в каждую из которых входят: лекционный материал, вопросы

для самоконтроля, проверочные тесты и лабораторные работы, пример фрагмента основной структуры курса приведен на рисунке 9.

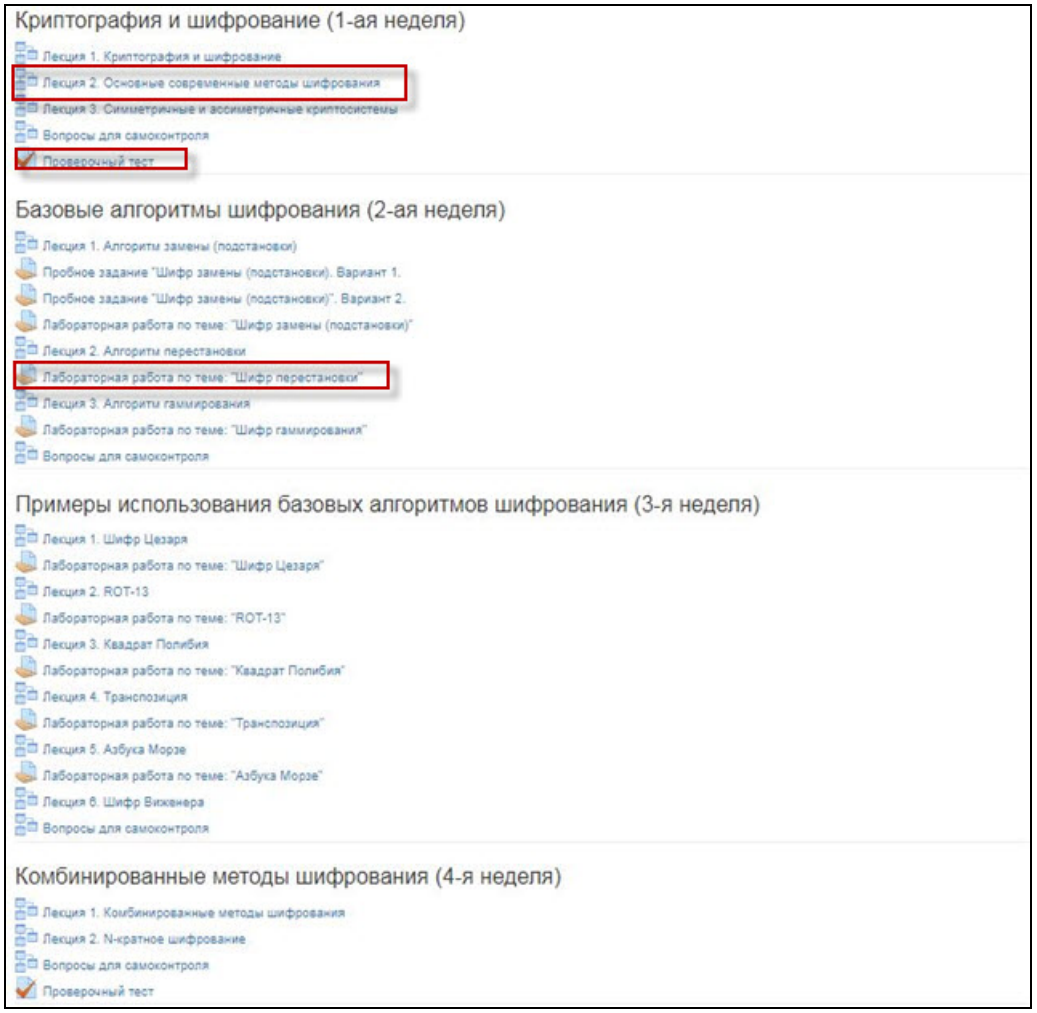
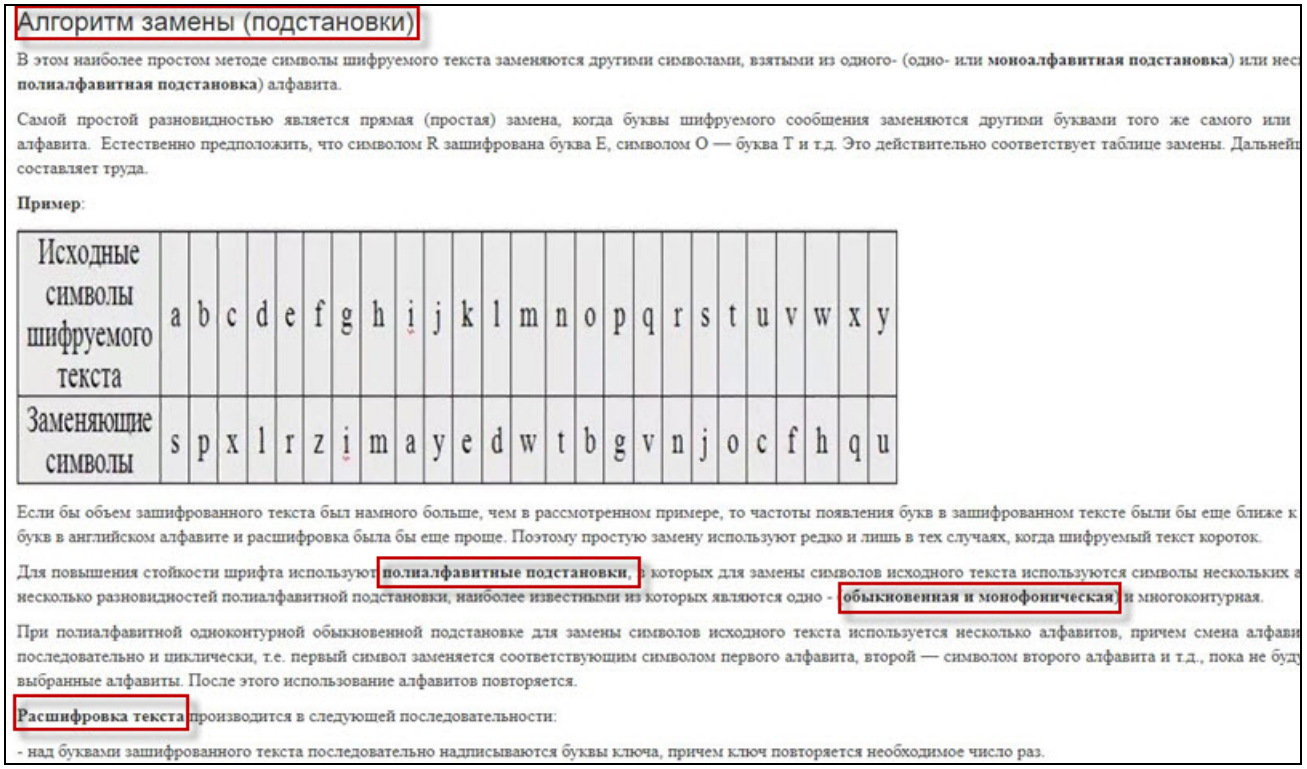


Рисунок 9 – Фрагмент основной структуры курса

Как видно из рисунка 9 в структуре курса имеются лекционные занятия, проверочные тесты, лабораторные работы, которые отмечены разными значками, все это позволяет сделать курс более удобным для использования даже для пользователя, не использовавшего системы дистанционного обучения, а также позволяет ему быстро сориентироваться в структуре курса и увидеть те, контрольные мероприятия, которые ему необходимо будет пройти.

На основании анализа литературы и интернет-источников по каждой теме был разработан учебный материал. Далее данный материал был структурирован и внесен в системы Moodle. Пример заполненного теоретического материала представлен на рисунке 10. LMS Moodle позволяет достаточно легко редактировать текстовые фрагменты, а также форматировать их по усмотрению преподавателя,

так в данной лекции был отформатирован заголовок, а также полужирным шрифтом выделены новые понятия, что позволит слушателю курса более внимательно отнестись к данной информации, а при необходимости найти то определение, которое используется далее в других лекциях.



Алгоритм замены (подстановки)

В этом наиболее простом методе символы шифруемого текста заменяются другими символами, взятыми из одного- (одно- или **моноалфавитная подстановка**) или нес **полиалфавитная подстановка**) алфавита.

Самой простой разновидностью является прямая (простая) замена, когда буквы шифруемого сообщения заменяются другими буквами того же самого или алфавита. Естественно предположить, что символом R зашифрована буква E, символом O — буква T и т.д. Это действительно соответствует таблице замены. Дальней составляет труда.

Пример:

Исходные символы шифруемого текста	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y
Заменяющие символы	s	p	x	l	r	z	i	m	a	y	e	d	w	t	b	g	v	n	j	o	c	f	h	q	u

Если бы объем зашифрованного текста был намного больше, чем в рассмотренном примере, то частоты появления букв в зашифрованном тексте были бы еще ближе к букв в английском алфавите и расшифровка была бы еще проще. Поэтому простую замену используют редко и лишь в тех случаях, когда шифруемый текст короток.

Для повышения стойкости шрифта используют **полиалфавитные подстановки**, в которых для замены символов исходного текста используются символы нескольких несколько разновидностей полиалфавитной подстановки, наиболее известными из которых являются одно - **обыкновенная и монофоническая**) и многоконтурная.

При полиалфавитной одноконтурной обыкновенной подстановке для замены символов исходного текста используется несколько алфавитов, причем смена алфави последовательно и циклически, т.е. первый символ заменяется соответствующим символом первого алфавита, второй — символом второго алфавита и т.д., пока не буду выбранные алфавиты. После этого использование алфавитов повторяется.

Расшифровка текста производится в следующей последовательности:

- над буквами зашифрованного текста последовательно надписываются буквы ключа, причем ключ повторяется необходимое число раз.

Рисунок 10 – Фрагмент лекции «Алгоритм замены (подстановки)»

Для упрощения перехода от одной страницы к другой была сделана удобная навигация в виде кнопок перехода, настройка навигационных элементов внутри лекции представлена на рисунке 11. Созданные кнопки навигации осуществляют переходы на содержательные элементы лекционного материала, при необходимости система Moodle позволяет сделать и более сложное навигационное меню, однако данный курс не предусматривает пересечения между темами и кнопки навигации были сделаны внутри каждой лекции.

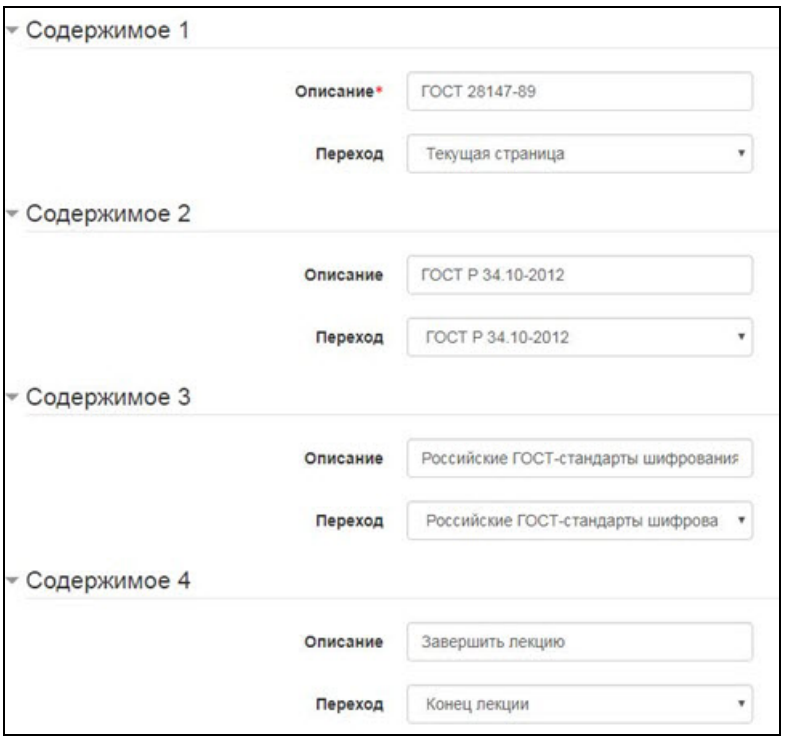


Рисунок 11 – Настройка кнопок перехода от одной страницы к другой

Использование такой дополнительной навигации позволяет пользователю не возвращаться в основное меню, а далее перемещаться по лекционному материалу, что не вызывает путаницы при прохождении материала, а позволяет запомнить его в правильно последовательности. Кроме того, в случае необходимости можно легко найти необходимую информацию, перемещаясь по информационным блокам, которые содержатся в страницах, на которые ссылаются кнопки навигации.

Кнопки навигации располагаются под лекционным материалом и, обращаясь к ним, можно перейти на другую страницу лекции, интерфейс дополнительного навигационного меню представлен на рисунке 12.

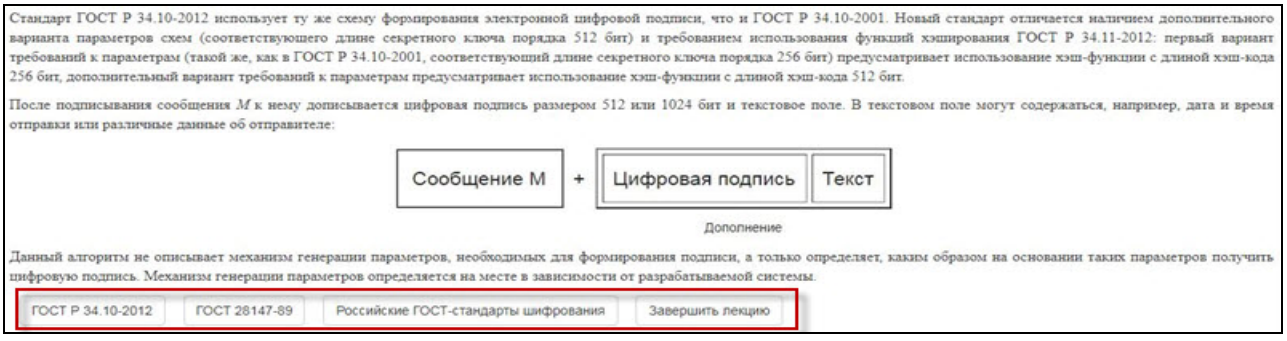


Рисунок 12 – Готовые кнопки перехода, расположенные под лекционным материалом

После того как был выбран и структурирован материал лекций создали блок вопросов для самоконтроля знаний, который показан на рисунке 13. Это было сделано для того, чтобы обучающийся, перед тем как приступать к проверочным работам и показывать свои знания и понимание тем лекций преподавателю, мог проверить себя сам: хорошо ли он усвоил материал и готов ли он к итоговым проверочным заданиям. После ответов на вопросы для контроля слушателей должен выбрать кнопку «Готов к контрольным заданиям» и система Moodle автоматически перейдет на страничку с ними.

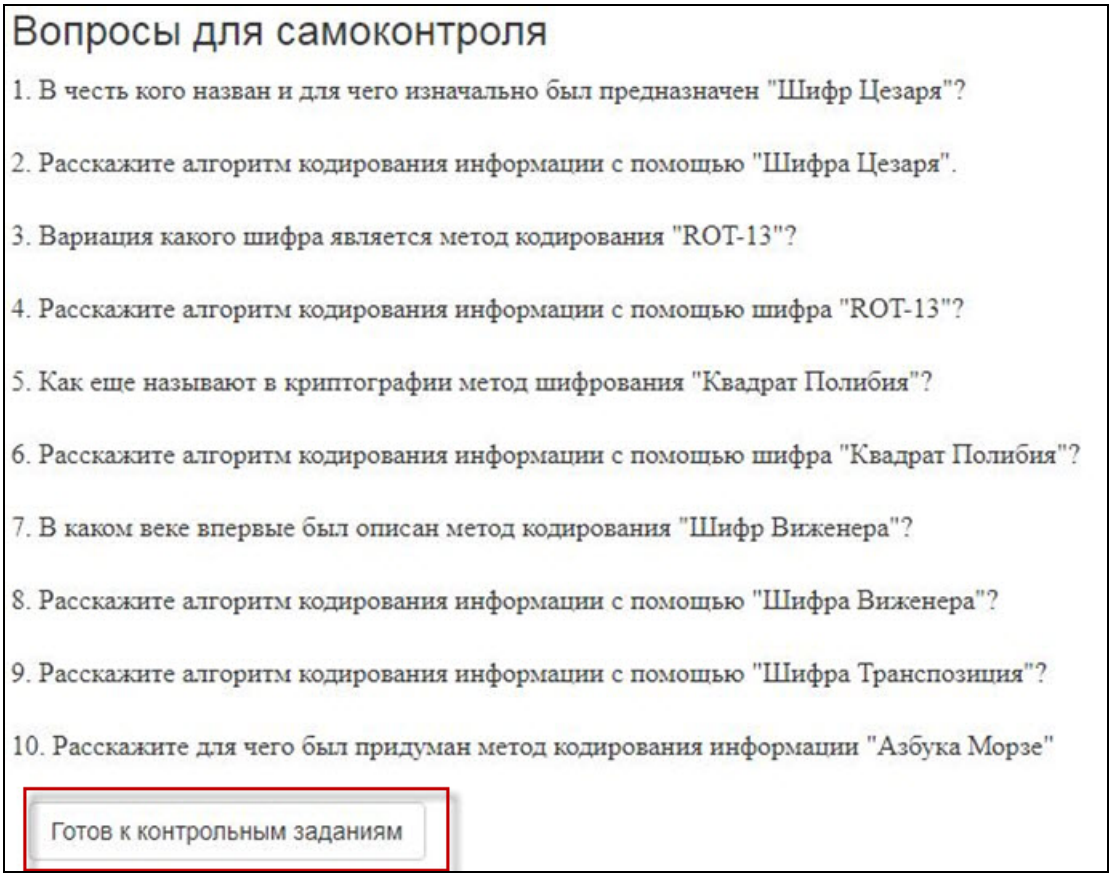


Рисунок 13 – Блок вопросов для самоконтроля «Неделя 3. Примеры использования базовых алгоритмов шифрования»

После того как обучающийся изучил лекционный материал и самостоятельно ответил на вопросы для самоконтроля, он переходит к выполнению лабораторной работы или проверочного теста, которые расположены ниже на этой же неделе, пример фрагмента курса представлен на рисунке 14.

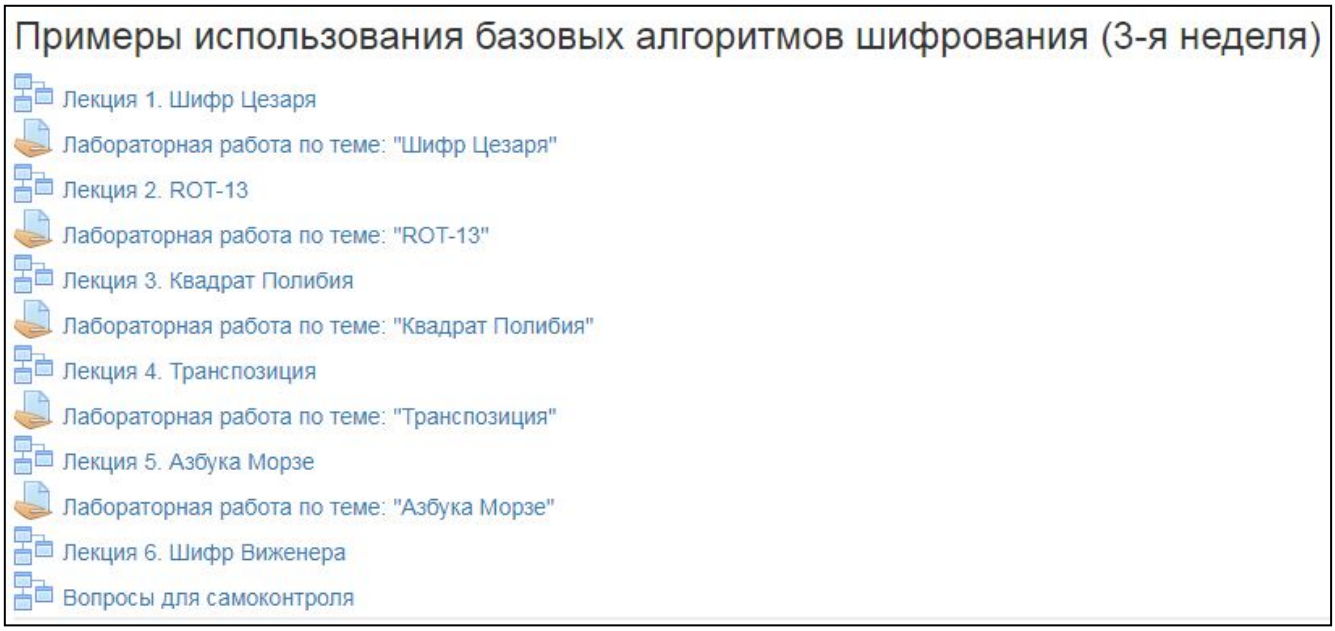


Рисунок 14 – Пример готовой тематической недели

Для разных тем дистанционного курса были разработаны различные средства контроля, где-то предложены только лабораторные работы, где-то только проверочные тесты, а для других тем эти средства были совмещены.

Интерфейс лабораторной работы показана на рисунке 15, где указаны тема работы, цель, результаты и ход самой работы, а также контрольное задание, которое необходимо выполнить по окончании работы и описать ход его решения в отчете, который направляется преподавателю.

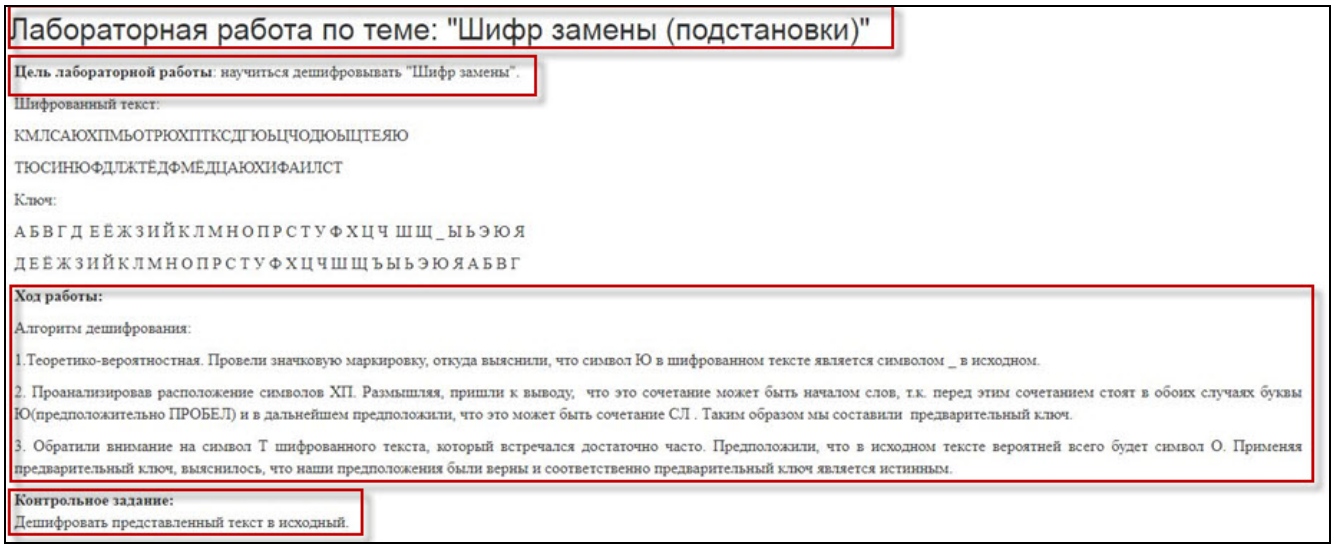


Рисунок 15 – Лабораторная работа «Шифр замены (перестановки)

Пример фрагмента проверочного теста, показанного на рисунке 16, также выполнен средствами системы Moodle. Как видно из рисунка система позволяет назначать количество полученных баллов за каждый вопрос, что позволяет сделать процесс контроля более точным и ранжировать вопросы теста.

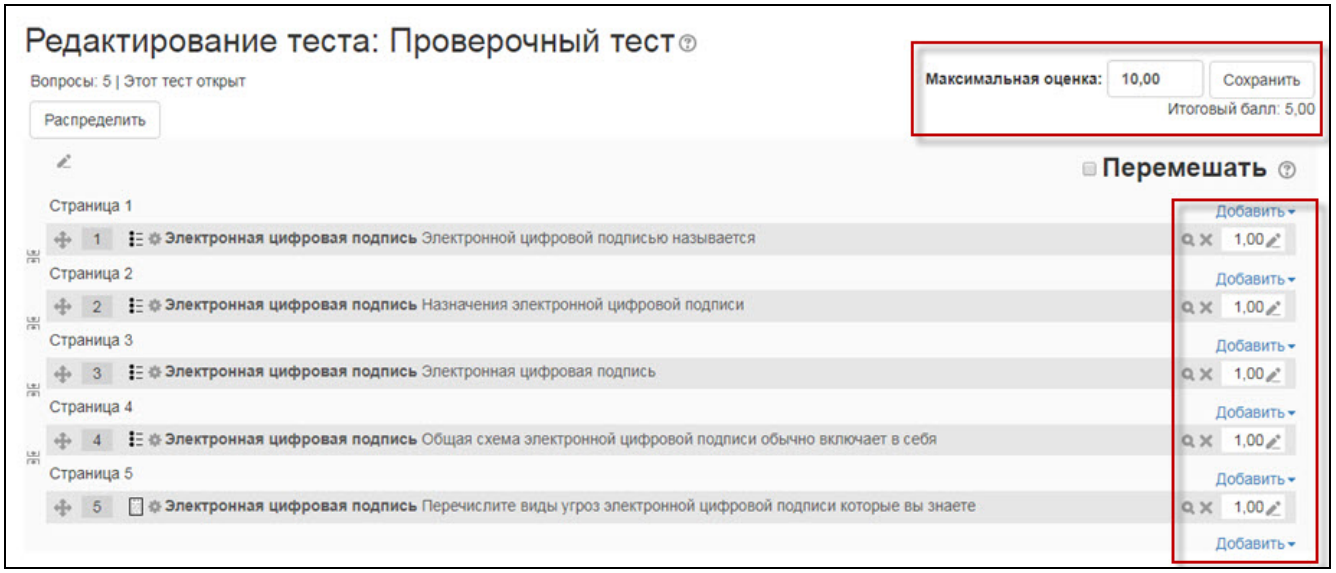


Рисунок 16 – Фрагмент проверочного теста

LMS Moodle позволять создавать тестовые задания различного типа: закрытой и открытой формы.

Так были разработаны тестовые задания с одним правильным вариантом ответа, интерфейс которого представлен на рисунке 17.

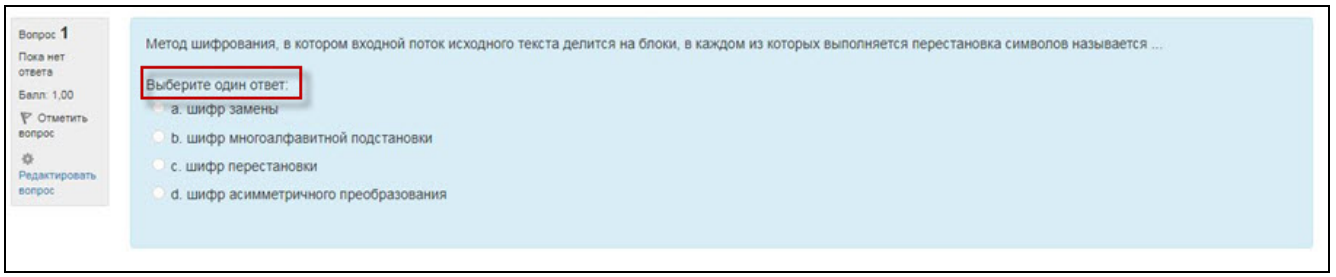


Рисунок 17 – Вопрос с одним правильным ответом

Интерфейс формы с примером вопроса с множественным выбором представлен на рисунке 18.

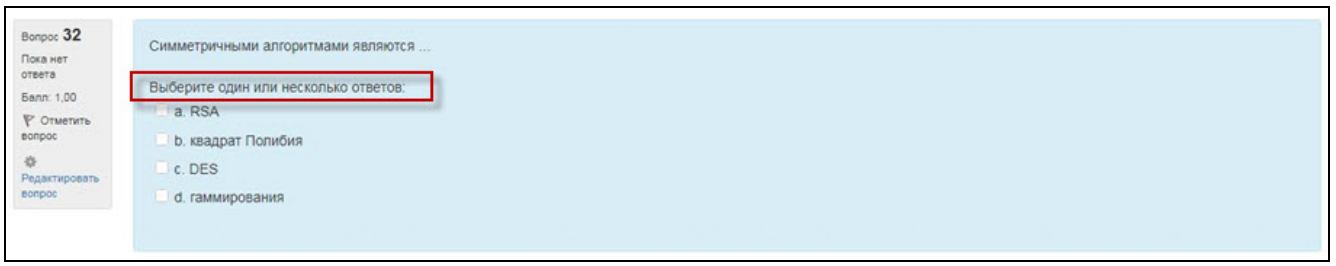


Рисунок 18 – Вопрос с множественным выбором

Использование тестовых заданий на соответствие позволяет отследить насколько усвоена логика связи понятий и определений курса, поэтому в тест были включены тестовые задания на соответствие, интерфейс которых представлен на рисунке 19.

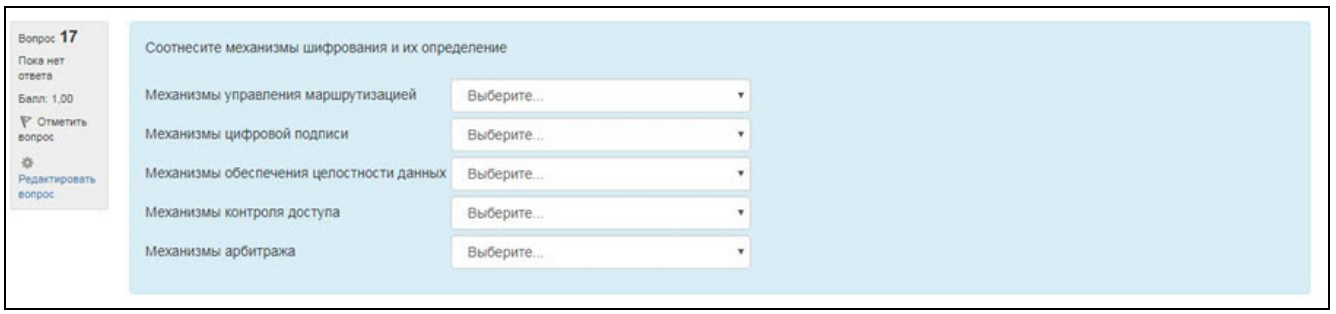


Рисунок 19 – Вопрос на соответствие

Включение тестовых заданий открытого типа позволит оценить не только насколько понятия и определения курса отложились в голове слушателей, но и оценить уровень словарного запаса слушателей, а также готовность использовать термины и определения, специфичные для криптографии как научной дисциплины. Кроме того, в нашем случае в качестве тестового задания на дополнение можно использовать ситуационную задачу, которая понимается как вид учебного задания, имитирующего ситуацию, которая могут возникнуть в реальной действительности. Пример такого тестового задания представлен на рисунке 20.

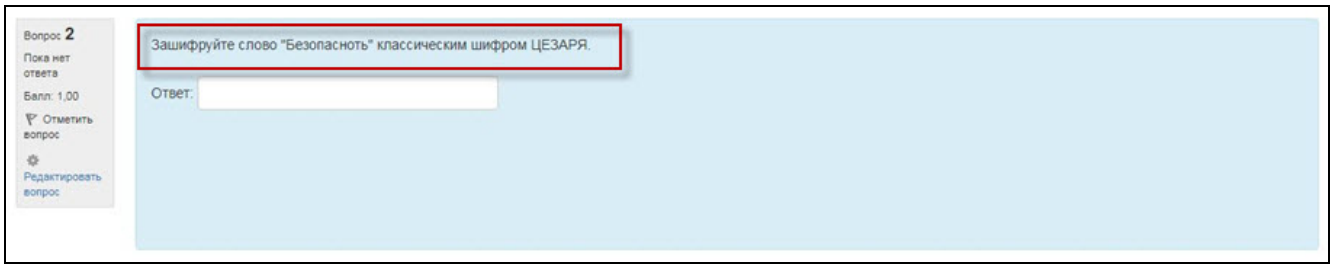


Рисунок 20 – Вопрос с кратким ответом

Таким образом, разработка дистанционного курса в LMS Moodle включает создание собственно курса, осуществление его настройки, а именно задание прав пользователей, назначение способов регистрации и записи на курс, определение структуры курса, наполнение его содержанием и разработку контролирующего инструментария.

2.6 Методические указания по использованию дистанционного онлайн-курса «Криптографические методы защиты информации» в учебном процессе

Дополнительная образовательная программа «Криптографические методы защиты информации» предназначена для студентов компьютерных специальностей и других категорий слушателей, обладающих компьютерной грамотностью и желающих повысить уровень информационной подготовки в области обеспечения криптографической защиты информации.

Целями создания дистанционного онлайн-курса «Криптографические методы защиты информации» стали:

- изучение видов и типов шифрования, методов и средств обеспечения криптографической защиты информации;
- рассмотрение алгоритмов и стандартов шифрования;
- изучение использования методов криптографии в профессиональной деятельности для обеспечения информационной безопасности.

Предполагается, что дистанционный онлайн курс будет изучаться по схеме сначала идет изучение теории, далее слушатель проходит текущий контроль по каждой теме, отвечая на вопросы для самоконтроля, потом переход к практическим и лабораторным работам, но возможен и другой порядок, который установит педагог-руководитель курса по ходу учебного процесса. В процессе изучения обучающийся может обратиться при необходимости к преподавателю или рассмотреть дополнительные материалы, которые имеются в курсе.

В курсе представлены разделы, которые надо изучить в процессе освоения дисциплины «Криптографические методы защиты информации». Разделы рекомендуется изучать в установленном порядке для того, чтобы полученные знания были структурированы и систематизированы. Каждый раздел состоит из теоретического материала, вопросов для самоконтроля, лабораторных работ и проверочных тестов, согласно структуре и содержанию учебного плана дополнительной образовательной программы, а также текущего контроля по каждой теме. Для того чтобы приступить к выполнению лабораторных работ и проверочных тестов, следует изучить теоретический материал, в котором излагается, то что может быть использовано для успешного прохождения лабораторных работ и проверочных тестов, которые следует выполнять по порядку, так как в процессе их последовательного выполнения решается одна сквозная задача и задания последующей лабораторной работы опираются на опыт, полученный в предыдущей лабораторной работе.

В лабораторных работах и проверочных тестах обязательны к выполнению все задания. В конце каждой лабораторной работы находятся тренировочные задания, которые необходимо выполнить, для того что бы было легче сделать контрольное задание, которое необходимо оформить в отчет и будет оценено преподавателем.

Так же в каждом разделе присутствует вопросы для самоконтроля по теме, это нужно для закрепления изученного материала, контроль сделан в виде блока вопросов, для того чтобы перейти к изучению следующего раздела необходимо успешно пройти их и выполнить все контрольные задания.

После изучения всех тем дисциплины «Криптографические методы защиты информации» необходимо пройти промежуточный контроль, в виде итогового теста. Так как в конце курса необходимо будет пройти итоговый тест, в котором вам можно будет добрать баллы для итоговой оценки.

Для того чтобы начать работу в дистанционном онлайн курсе по дополнительной образовательной программе «Криптографические методы защиты

информации» необходимо выполнить следующую последовательность действий:

1. В любом браузере перейти по ссылке lms-study.rsvpu.ru.
2. Откроется система Moodle, в которой нужно будет зарегистрироваться.
3. Далее нужно будет найти данный курс по названию. Для навигации по различным разделам системы Moodle воспользуйтесь главным меню, которое находится слева.
4. Переход на другую страницу лекции осуществляется кнопками навигации, которые находятся внизу каждой лекции.
5. Для прохождения тестового задания необходимо нажать на ссылку итоговый тест, которая находится вверху курса, и вы перейдете непосредственно к системе тестов.

В дистанционном онлайн-курсе имеются средства контроля, а именно:

- вопросы для самоконтроля;
- тестовые задания;
- лабораторные работы;
- итоговый тест.

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

- на оценку 3 необходимо набрать не менее 70%;
- на оценку 4 75%-85%;
- на оценку 5 85%-100%.

ЗАКЛЮЧЕНИЕ

Начало третьего тысячелетия ознаменовано рождением общества нового типа – информационного, в котором основным стратегическим ресурсом становится информация. Влияние, которое оказывают информационные процессы на все сферы жизни общества, актуализирует важнейшие вопросы социального бытия, в том числе вопросы информационных взаимодействий, включая борьбу за информационное пространство и противодействие различного рода информационным угрозам. В связи с этим не может не меняться ситуация в отношении исследования способов обеспечения информационной безопасности, а частности, методам и средствам обеспечения криптографической защиты данных.

Для этих целей в рамках выпускной квалификационной работы был разработан курс «Криптографические методы защиты информации».

На первом этапе работы был сделан обзор литературных и интернет-источников с целью определения содержания дистанционного курса и требований, предъявляемых к нему на современном этапе развития средств вычислительной и компьютерной техники.

Вторым этапом стало определение содержательного наполнения курса и проектирование дополнительной образовательной программы, что стало следствием отсутствия дисциплины «Криптографические методы защиты данных» в учебных планах специалистов в области информационной безопасности и защиты информации. Заявленное противоречие потребовало создание дистанционного курса по данной дисциплине.

Следующим этапом стало рассмотрение наиболее распространенных в настоящее время методов криптографической защиты информации и способов ее реализации. Выбор для конкретных систем должен быть основан на глубоком анализе слабых и сильных сторон тех или иных методов защиты. Обоснованный выбор той или иной системы защиты в общем-то должен опираться на какие-то критерии эффективности. К сожалению, до сих пор не разработаны подходящие

методики оценки эффективности криптографических систем. Поэтому в курс было решено включить те методы и средства обеспечения криптографической защиты, которые, по мнению ряда исследователей, сегодня являются наиболее эффективными и стабильными, а также рассмотреть основные стандарты на них как отечественные, так и зарубежные.

Далее была выбрана система дистанционного обучения, на платформе которой необходимо было реализовать данный курс. Ею стала LMS Moodle основным достоинством которой, кроме богатого функционала является ее бесплатность и постоянное обновление новыми готовыми решениями.

Заключительным этапом выполнения выпускной квалификационной работы стала разработка методический рекомендации по использованию созданного дистанционного онлайн-курса и рассмотрение возможностей его совершенствования и корректирования в зависимости от условий реализации и применения в учебном процессе.

Таким образом, задачи выпускной квалификационной работы выполнены, а цель достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Адаменко М. Основы классической криптологии. Секреты шифров и кодов [Текст] / М. Адаменко. – Москва: Машиностроение, 2014. – 256 с.

2. Бабаш А. В. История криптографии. Часть I [Текст] / А. В. Бабаш, Г. П. Шанкин. – Москва: Гелиос АРВ, 2002. – 240 с.

3. Бабенко Л. К. Современные алгоритмы блочного шифрования и методы их анализа [Текст] / Л. К. Бабенко, Е. А. Ищукова. – Москва: Гелиос АРВ, 2006. – 376 с.

4. Байер Д. Microsoft ASP .NET. Обеспечение безопасности [Текст] / Д. Байер. – Москва: Питер, Русская Редакция, 2008. – 430 с.

5. Баричев С. Г. Основы современной криптографии [Текст] / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. – Москва: СИНТЕГ, 2011. – 176 с.

6. Герман О. Н. Теоретико-числовые методы в криптографии [Текст] / О. Н. Герман, Ю. В. Нестеренко. – Москва: Академия, 2012. – 272 с.

7. Горев А. И. Обеспечение информационной безопасности [Текст] / А. И. Горев, А. И. Симаков. – Москва: Мир, 2005. – 844 с.

8. Жданов О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования [Текст] / О. Н. Жданов. – Москва: ИНФРА-М, 2015. – 607 с.

9. Здор С. Е. Кодированная информация. От первых природных кодов до искусственного интеллекта [Текст] / С. Е. Здор. – Москва: Либроком, 2012. – 168 с.

10. Земор Ж. Ж. Курс криптографии [Текст] / Ж. Ж. Земор. – Москва: Регулярная и хаотическая динамика, Институт компьютерных исследований, 2006. – 256 с.

11. Зубов А. Н. Математика кодов аутентификации [Текст] / А. Н. Зубов. Москва: Гелиос АРВ, 2007. – 288 с.

12. Молдовян А. А. Криптография: скоростные шифры [Текст] / А. А. Молдовян и др. – Москва: БХВ-Петербург, 2002. – 496 с.

13. Литвинская О. С. Основы теории передачи информации: учебное пособие. [Текст] / О. С. Литвинская, Н. И. Чернышев. – Москва: КноРус, 2015. – 168 с.

14. Масленников М. Практическая криптография: моногр. [Текст] / М. Масленников. – Москва: БХВ-Петербург, 2003. – 464 с.

15. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии [Текст] / А. В. Черемушкин. – Москва: МЦНМО, 2002. – 104 с.

16. Черчхаус Р. Коды и шифры. Юлий Цезарь [Текст] / Р. Черчхаус. – Москва: Огни, 2005. – 320 с.

17. Андреев А. В. Практика электронного обучения с использованием Moodle [Текст] / А. В. Андреев, С. В. Андреева, И. Б. Доценко. – Таганрог: Изд-во. ТТИ ЮФУ, 2008. – 146 с.

18. Мультимедиа-курсы: методология и технология разработки [Электронный ресурс] / Режим доступа http://ido.tsu.ru/ss/?unit=223 (дата обращения: 17.03.2018).

19. Гильмутдинов А. Х. Электронное образование на платформе Moodle [Текст] / А. Х. Гильмутдинов, Р. А. Ибрагимов, И. В. Цивильский. – Казань: КГУ, 2008. – 169 с.

20. Курмышев Н.В., Краснощеков К.Ю. Создание курсов в системе дистанционного обучения Moodle: учебно-методическое пособие для преподавателей [Электронный ресурс]. – Режим доступа: http://www.novsu.ru/file/1008712 (дата обращения: 17.03.2018).

21. Пастущак Т.Н., Соколов С.С., Рябова А.А. Создания электронного курса. Лекция в СДО Moodle: учебно-методическое пособие [Электронный ресурс]. – Режим доступа: http://sdo.gumrf.ru/pluginfile.php/3390/block_html/contentsozd_el_kursa_lec_Moodle.PDF (дата обращения: 20.03.2018).

22. Проекты федеральных государственных стандартов высшего профессионального образования [Электронный ресурс]. – Режим доступа: http://mon.gov.ru/pro/fgos (дата обращения: 20.03.2018).

23. Разработка электронных курсов [Электронный ресурс]. – Режим доступа: http://elearningcenter.ru/ (дата обращения: 27.03.2018).

24. Устюгова В. Н. Система дистанционного обучения Moodle: учебное пособие [Текст] / В. Н. Устюгова. – Казань: КГУ, 2010. – 280 с.

25. Анисимов А. М. Работа в системе дистанционного обучения Moodle: учебное пособие [Текст] / А. М. Анисимов. – Харьков: ХНАГХ, 2009. – 292 с.

26. Белозубов А. В. Система дистанционного обучения Moodle: учебно-методическое пособие [Текст] / А. В. Белозубов, Д. Г. Николаев. – Санкт-Петербург: Питер, 2007. – 108 с.

27. Групповая работа в системе Moodle [Электронный ресурс]. – Режим доступа: http://letopisi.ru/index.php (дата обращения: 28.03.2018).

28. Исследовательские организации в области информатизации и информационных технологий [Электронный ресурс]. – Режим доступа: http://www.it-journal.ru/ressursyshtml (дата обращения 04.04.2018).

29. Кузнецов А. А. Информационные и коммуникационные технологии в образовании: учебно-методическое пособие [Текст] / А. А. Кузнецов, С. В. Панюкова, И. В. Роберт. – Москва: Дрофа, 2008. – 216 с.

30. Мясникова Т. С. Система дистанционного обучения Moodle [Текст] / Т. С. Мясникова, С. А. Мясников. – Харьков: ХНАГХ, 2008, – 232 с.

31. Обучающая среда Moodle [Электронный ресурс]. – Режим доступа: http://docs.altlinux.org/current/school_server/moodle/index.html (дата обращения: 04.04.2018).

32. Портал «Информационно-коммуникационные технологии» [Электронный ресурс]. – Режим доступа: http://www.ict.edu.ru/ (дата обращения: 04.04.2018).

33. Портал электронного обучения [Электронный ресурс]. – Режим доступа: http://www.e-learning.by/ (дата обращения: 07.04.2018).

34. Просто о сложном: Moodle и не только [Электронный ресурс]. – Режим доступа: http://teacherdo.ru/ (дата обращения: 12.04.2018).

35. Дошина А. Д. Криптография. Основные методы и проблемы. Современные тенденции криптографии [Текст] / А. Д. Дошина, А. Е. Михайлова, В. В. Карлова // Современные тенденции технических наук: материалы IV Междунар. науч.-практ. конф. – Казань: Бук, 2015. – С. 10-13.

36. Логинова А. В. Модульная объектно-ориентированная среда обучения (Moodle): эффективная или несовершенная форма организации обучения? [Электронный ресурс]. – Режим доступа: https://moluch.ru/archive/89/17853/ (дата обращения: 07.06.2018).

ПРИЛОЖЕНИЕ