Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
Российский экономический университет имени Г.В. Плеханова
Ивановский филиал

Кафедра Математики, экономической информатики и вычислительной техники

Утверждено:
Зам. директора по УМР
_____
Гуськова И.В

Рабочая программа

Электронная цифровая подпись

Рекомендуется для направления: **080100.62 Экономика**

Профиль - **Бухгалтерский учет, анализ и аудит**

Квалификация (степень) выпускника - **бакалавр**

Одобрено:
МС Ивановского филиала
РЭУ имени Г.В. Плеханова
Протокол № 1 от 30.08.2014
Председатель Методического совета
_____Т.Ф.Аржаных

Рекомендовано кафедрой:
Протокол № *1*
От «*29*» *августа* 2014 г.

Зав. кафедрой _____Н.А.Капустин
(ФИО)

Иваново 2014

Автор-составитель: Ершов Б.Л.

должность доцент, к.т.н.

Общая образовательная программа **«Электронная цифровая подпись»** составлена в соответствии с требованиями Федерального Государственного образовательного стандарта высшего профессионального образования по специальности.

Дисциплина входит в федеральный (вузовский) компонент цикла общих математических и естественнонаучных дисциплин (Б.В.2.4) и является обязательной для изучения.

080100.62 (шифр)

«ЭКОНОМИКА» (наименование направления)

Утвержден на заседании Учебно-методического совета _____ института (филиала) «_____» _____ 201____г., протокол № _____.

Согласования со смежной кафедрой:

Зав. кафедрой Бухгалтерского учета, анализа и аудита
к.э.н., доцент _____ Л.И.Шарова
(подпись) *(ф. и. о)*

Зав. библиотекой _____ Хилинская И.Ю.
(подпись) *(ф. и. о)*

Содержание

1. Цели и задачи дисциплины.

Целью дисциплины является сформировать у студентов четкое представление и понимание теоретических и прикладных знаний о современных методах обеспечения аутентификации электронных документов в информационных инфраструктурах государственных и частнопредпринимательских предприятий и организаций.

В результате изучения дисциплины студенты должны овладеть методологическим инструментарием обеспечения целостности электронных документов и подтверждения их подлинности при обработке и передаче по каналам теледоступа в единых информационно-телекоммуникационных системах, методами, и средствами правового, организационно-административного, физического, технического, технологического, программного, программно-аппаратного и криптографического обеспечения формирования электронных документов и организации электронного документооборота.

Целью такой аутентификации физических и юридических лиц и электронных документов в информационной инфраструктуре коммерческой деятельности является защита информации от:

- активного перехвата;
- маскарада, когда абонент А посылает документ абоненту В от имени абонента С;
- ренегатства, когда абонент А заявляет, что не посылал документ абоненту В, хотя случай такой пересылки состоялся;
- подмены, когда абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А;
- повтора, когда абонент С повторяет ранее переданный документ, который абонент А посылал абоненту В.

В соответствии с Резолюцией Генеральной Ассамблеи ООН от 16.12.96 A/SI/628 «Типовой закон об электронной торговле», принятый Комиссией ООН по праву международной торговле (ЮНИСТРАЛ), «Руководству по принятию типового закона об электронной торговле», а также Федерального закона N63 от 06 апреля 2011 года «Об электронной подписи», Доктрины информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 9 сентября 2000 года, Приказа ФСБ РФ от 9 февраля 2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (не составляющих государственную тайну) целью электронной цифровой подписи является придание электронным документам юридической силы собственноручной подписи физического или юридического лица.

Овладеть международными стандартами информационного обмена, определить понятия угроз модификации и фальсификации электронных документов и особенности обеспечения и особенности обеспечения их устойчивости к несанкционированным воздействиям в условиях функционирования в России глобальных, региональных, корпоративных и локальных компьютерных сетей.

Важным условием в изучении дисциплины «Электронная цифровая подпись» является изучение методов формирования электронных документов и электронного документооборота, идентификации и аутентификации пользователей и документов в информационных инфраструктурах на основе электронной цифровой подписи, а также методов управления контролем доступа, необходимых для построения защищенных информационных систем локального, регионального, корпоративного и глобального назначений.

Предметом дисциплины является изложение основ правовой, организационно-административной, физической, технической, программной и программно-аппаратной защиты электронных документов от несанкционированных воздействий в современных информационных технологиях, средств и методов управления контролем доступа в компьютерных системах, методов идентификации и верификации пользователей и документов в открытых и специализированных современных информационных систем,

методов защиты авторских прав, защиты рекламной продукции в системах электронной коммерции.

Место дисциплины в области науки, техники и практики охватывает совокупность проблем, связанных с технологией организации электронного документооборота, аутентификацией пользователей и документов и защитой информации в информационной инфраструктуре предприятий и организаций, а также охватывает совокупность проблем, связанных с информационными технологиями, направленными на поддержку производственного и финансового менеджмента, организации предпринимательства, маркетинга, финансового и технико-экономического анализа, бухгалтерского учета и других сфер производственной и коммерческой деятельности.

Задачами изучения дисциплины являются:

1. Изучение организационно-административных и правовых средств и методов использования электронной цифровой подписи в виртуальном пространстве коммерческой деятельности.
2. Изучение роли и места электронной цифровой подписи в электронном документообороте информационной инфраструктуре государства.
3. Изучение теоретических основ построения системы электронной цифровой подписи.
4. Изучение состава, структуры и принципов работы программно-аппаратного комплекса электронной цифровой подписи.

4.1. Однонаправленные функции.

4.2. Алгоритм безопасного хэширования.

4.3. Алгоритмы электронной цифровой подписи.

4.4. Отечественный стандарт электронной цифровой подписи (ГОСТ Р34.10-94, ГОСТ Р 34.10-2001).

5. Изучение технологии работы с международными системами электронной цифровой подписи в составе программного комплекса PGP, рекомендованного Государственным образовательным стандартом, и отечественных программно-аппаратных комплексов «Русский офис», «Сигнал-«Ком», «Крипто-Банк», «Крипто-PRO», «Криптон-Подпись», ПКЗИ «ШИПКА».

Место дисциплины в области науки, техники и практики охватывает совокупность проблем, связанных с технологией и защитой информации в информационной инфраструктуре предприятий и организаций.

Содержание дисциплины: актуальность проблемы формирования электронных документов в информационных инфраструктурах торгово-экономической деятельности их передача по каналам теледоступа в Единой информационно-телекоммуникационной системе Российской Федерации, а также ведомственных и межведомственных телекоммуникационных сетях**,** международные стандарты информационного обмена, правовые основы защиты электронных документов от модификации и фальсификации в государственной, коммерческой, служебной, процессуальной, профессиональной деятельности. Федеральные Законы Российской Федерации по обеспечению информационной безопасности в информационных технологиях, Доктрина Информационной безопасности Российской Федерации, Концепция Национальной Безопасности Российской Федерации, нормативные и руководящие документы, Постановления Правительства Российской Федерации по проблемам обеспечения информационной безопасности, ведомственные Приказы и распоряжения.

Основные виды угроз электронному документообороту в компьютерных технологиях, локальных региональных, корпоративных и глобальных сетевых структурах информационного взаимодействия. Классификация средств и методов модификации и фальси-

фикации электронных документов со стороны несанкционированных пользователей. Классификация программных угроз сетевым компьютерным технологиям, краткая характеристика программных угроз в автоматизированных системах обработки данных.

Основные положения теории установления и подтверждения подлинности электронных документов и пользователей при взаимодействии в системе электронного документооборота. Методологические подходы к проблеме обеспечения достоверности и целостности электронных документов в сетевых компьютерных технологиях. Методы аутентификации электронных документов. Аппаратно-программные средства обеспечения подлинности информационных ресурсов. Физические и технические методы установления подлинности электронных документов и пользователей. Криптографические методы аутентификации информации в сетевых компьютерных технологиях. Программно-аппаратные средства и методы аутентификации информации в сетевых и локальных компьютерных технологиях. Программы аудита системы аутентификации компьютерных сетевых технологий.

Математические модели криптоалгоритмов (основы модульной арифметики и конечных полей), симметричные и асимметричные криптосистемы, понятие хэш-функции, методы построения хэш-функций, стандарты алгоритмов хэширования, стандарты шифрования, алгоритмы аутентификации и идентификации пользователей и документов в современных банковских и торгово-экономических технологиях (защита платежных систем с использованием интеллектуальных терминалов, полупроводниковых идентификационных карт и электронно-цифровой подписи, электронные деньги), проблемы распределения секретных ключей, протоколы распределения секретных ключей.

2. Место дисциплины в структуре ООП:

Дисциплина «Электронная подпись» относится к базовой части математического и естественнонаучного цикла (Б.2) ООП бакалавриата и преподается в 3 семестре.

Дисциплина «Электронная подпись» базируется на знаниях полученных студентами в процессе освоения школьной программы по предметам: Математика, Физика, Информатика и информационно-коммуникационные технологии. Из дисциплин профессионального цикла «Безопасность информационных технологий» имеет логическую и содержательно-методологическую взаимосвязи с дисциплинами: Экономика организации, Статистика, Бухгалтерский учет, Маркетинг, Коммерческая деятельность, Логистика, Менеджмент, Рекламная деятельность, Организация, технология и проектирование предприятий и Информационные технологии в профессиональной деятельности.

Содержание курса «Электронная подпись» в высшей школе базируется на сочетании в себе трех существующих сейчас основных направления в обучении информатике в школе и отражающих важнейшие аспекты ее общеобразовательной значимости:

- мировоззренческий аспект, связанный с формированием представлений о системно-информационном подходе к анализу окружающего мира, о роли информации в управлении, специфике самоуправляемых систем, общих закономерностях информационных процессов в системах различной природы;

- алгоритмический (программистский) аспект, связанный в настоящее время уже в большей мере с развитием мышления школьников.

- "пользовательский" аспект, связанный с формированием компьютерной грамотности, подготовкой школьников к практической деятельности в условиях широкого использования информационных технологий.

Освоение дисциплины «Электронная подпись» необходимо, как предшествующее для дисциплин профессионального цикла базовой части (Экономика организации, Статистика, Бухгалтерский учет, Маркетинг, Коммерческая деятельность, Логистика, Менеджмент, Рекламная деятельность, Организация, технология и проектирование предприятий и

Информационные технологии в профессиональной деятельности), а также учебной практики (Б.5.У).

3. Требования к результатам освоения дисциплины:

Процесс изучения дисциплины направлен на формирование следующих компетенций:

1. Владение культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения (ОК-1);
2. Осознание сущности и значения системы обеспечения информационной безопасности в развитии информационной инфраструктуры современного общества; владение основными методами и средствами получения, хранения, переработки информации и ее защиты от несанкционированной модификации и уничтожения; навыками работы с с программными и программно-аппаратными средствами обеспечения безопасности компьютерных технологий как средством управления информацией (ОК-8);
3. Способность применять основные законы социальных, гуманитарных, экономических и естественных наук в профессиональной деятельности, а также методы математического анализа и моделирования, теоретического и экспериментального исследования; методы восприятия и распознавания образов; методы криптографической защиты информации владением прикладного математического аппарата при решении профессиональных проблемных задач (ПК-1);
4. Способность осуществлять сбор, хранение, обработку, защиту, аутентификацию и оценку информации, необходимой для организации и управления профессиональной деятельностью (коммерческой, или маркетинговой, или рекламной, или логистической, или товароведной) (ПК-11);
5. Способность участвовать в разработке инновационных методов, средств и технологий в области профессиональной деятельности (коммерческой, или маркетинговой, или рекламной, или логистической, или товароведной) (ПК-17).

В результате изучения дисциплины студент должен:

- знать:

- криптоалгоритмы, используемые в современных криптосистемах аутентификации электронных документов. с открытым ключом;
- криптоалгоритмы, используемые в стандартах аутентификации данных;
- методы выбора криптографических параметров, обеспечивающих необходимую стойкость криптосистемы к несанкционированному воздействию:
- ключевые системы современной криптографии и протоколы распределения ключей:
- приложения криптографии к решению задач аутентификации информации в компьютерных системах, в частности по проблемам информационной безопасности в банковских и торгово-экономических структурах;
- средства и методы управления контролем доступа в компьютерных технологиях;
- средства и методы аутентификации и идентификации пользователей и документов в компьютерных технологиях;
- законодательную и нормативно-правовую базу обеспечения информационной безопасности;
- технологию построения защищенных компьютерных систем.

- уметь:

- применять полученные знания в решении прикладных задач защиты информации в компьютерных технологиях банковских и торгово-экономических систем;
- строить и изучать математические модели криптоалгоритмов;

- применять современные криптографические системы, системы управления контролем доступа, системы аутентификации и идентификации пользователей и документов в информационных технологиях банковских и торгово-экономических структурах.

***- владеть*:**

- способами определения требований и состава средств, методов и мероприятий по организации комплекса средств аутентификации информации в компьютерных технологиях;
- методами организации, планирования и контроля функционирования комплекса средств аутентификации информации;
- навыками пользования библиотеками прикладных программ компьютерных систем для решения задач по защите информации в информационных технологиях
- 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;
- способами практического применения технических, программных и программно-аппаратных средств и методов аутентификации информации в компьютерных технологиях;
- навыками использования специального математического аппарата в проведении прикладных исследований по проблемам защиты информации в компьютерных технологиях;
- методами организации системы управления контролем доступа в сетевых компьютерных технологиях и оценку их информационной безопасности.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов / зачетных единиц	Семестры			
		4			
Аудиторные занятия (всего)	54	54			
В том числе:	-	-	-	-	-
Лекции	20	20			
Практические занятия (ПЗ)	34	34			
Семинары (С)					
Лабораторные работы (ЛР)					
Самостоятельная работа (всего)	54	54			
В том числе:	-	-	-	-	-
Курсовой проект (работа)					
Расчетно-графические работы	54	54			
Реферат					
Другие виды самостоятельной работы					
Программная реализация проектов					
Вид промежуточной аттестации (зачет, экзамен)	зачет	зачет			
Общая трудоемкость часы	108	108			
зачетные единицы	3	3			

5. Содержание дисциплины

5.1. Содержание тем дисциплины.

Раздел 1. Организационные и правовые основы использования ЭЦП в торгово-экономической деятельности.

Предмет, содержание, задачи дисциплины. Организационные и правовые основы использования ЭЦП в торгово-экономической деятельности. Место дисциплины Электронная цифровая подпись в торгово-экономической деятельности» среди других дисциплин информационных технологий в торгово-экономической деятельности. Структура аутентификации электронных документов Российской Федерации: Федеральный Удостоверяющий центр, Удостоверяющие центры субъектов Российской Федерации, Удостоверяющие центры Уполномоченных органов субъектов Российской Федерации, Корпоративные Удостоверяющие центры. Их назначение и взаимодействие.

Тема 1. 1. Доктрина информационной безопасности Российской Федерации.

Основополагающее назначение Доктрины информационной безопасности Российской Федерации. Национальные интересы Российской Федерации
в информационной сфере и их обеспечение. Интересы личности в информационной сфере, интересы общества в информационной сфере, интересы государства в информационной сфере, четыре основные составляющие национальных интересов Российской Федерации в информационной сфере. Виды угроз информационной безопасности Российской Федерации применительно к структурам управления торгово-экономической деятельностью. Источники угроз информационной безопасности Российской Федерации применительно к торгово-экономической деятельности. Общие методы обеспечения информационной безопасности Российской Федерации в приложении к защите электронных документов от несанкционированной модификации и фальсификации. Обеспечение информационной безопасности Российской Федерации в сфере экономики: система государственной статистики: кредитно-финансовая система; информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики; системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности; системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

Тема 1. 2. Федеральный Закон Российской Федерации ФЗ №63 от 6 апреля 2011 года «Об электронной подписи».

Цель и сфера применения настоящего Федерального закона. Правовое регулирование отношений в области использования электронной цифровой подписи. Основные понятия, используемые в настоящем Федеральном законе: электронный документ, электронная цифровая подпись, владелец сертификата ключа подписи, средства электронной цифровой подписи, сертификат средств электронной цифровой подписи, закрытый ключ электронной цифровой подписи, открытый ключ электронной цифровой подписи, сертификат ключа подписи, подтверждение подлинности электронной цифровой подписи в электронном документе, пользователь сертификата ключа подписи, условия использования электронной цифровой подписи, статус удостоверяющего центра, обязательства удостоверяющего центра по отношению к владельцу сертификата ключа подписи.

Тема 1. 3. Приказ ФСБ РФ №66 от 9.02.2005 г. «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

Шифровальные (криптографические) средства защиты информации. Состав шифровальных криптографических средств защиты информации. Электронная цифровая подпись как элемент средств криптографической защиты информации (СКЗИ). Порядок разработки СКЗИ. Требования к СКЗИ и цель криптографической защиты информации с описанием предполагаемой модели нарушителя. Правила пользования создаваемым новым образцом СКЗИ. Состав аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи. Порядок реализации (распространения) и эксплуатации СКЗИ.

Тема 1. 4. Указ Президента Российской Федерации №351 от 17 марта 2008 года «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»

Постановляющая часть указа Президента Российской Федерации о возможности использования информационно-телекоммуникационных сетей международного информационного обмена. Размещение технических средств, подключаемых к информационно-телекоммуникационным сетям международного информационного обмена. Поддержание и развитие сегмента международной компьютерной сети "Интернет" для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

Раздел 2. Проблемы аутентификации пользователей и ЭЦП в информационных инфраструктурах торгово-экономической деятельности.

Организационные и правовые основы использования ЭЦП в торгово-экономической деятельности. Правовое регулирование отношений в области использования электронной цифровой подписи. Цель и сфера применения Федерального закона «Об электронной подписи». Понятийный аппарат по основным законодательным положениям Федерального закона «Об электронной подписи». Условия использования ЭП в торгово-экономической деятельности. Юридическое значение ЭП, сертификаты ключей ЭП, срок и порядок хранения сертификата ключа подписи в удостоверяющем центре. Удостоверяющие центры. Особенности использования ЭП в коммерческой деятельности.

Основные понятия и концепции идентификации пользователей и документов, проверка их подлинности. Идентификация и механизмы подтверждения подлинности пользователя в виртуальном пространстве. Взаимная проверка подлинности пользователей. Протоколы идентификации с нулевой передачей знаний. Проблемы аутентификации данных и электронная цифровая подпись.

Раздел 3. Однонаправленные хэш-функции. ГОСТ Р 34-11-94.

Назначение хэш-функции и требования предъявляемые к ней. Однонаправленные хэш-функции. Алгоритм безопасного хэширования SHA. Зарубежные однонаправленные хэш-функции MD2, MD4, MD5. Отечественный стандарт хэш-функции.

Раздел 4. Алгоритмы электронной цифровой подписи.

Тема 4. 1. Алгоритм цифровой подписи RSA (Райвест-Шамир-Адлеман) (факторизация больших чисел).

Методика построения алгоритма электронной цифровой подписи RSA. Математическая модель алгоритма RSA. Пример реализации алгоритма RSA.

Тема 4. 2. Алгоритм цифровой подписи Эль Гамаля (EGSA) (Методы дискретного логарифмирования).

Методика построения алгоритма электронной цифровой подписи Эль Гамаля (EGSA). Математическая модель алгоритма Эль Гамаля. Пример реализации алгоритма Эль Гамаля. Преимущества алгоритма Эль Гамаля по сравнению с алгоритмом ЭЦП RSA.

Тема 4. 3. Алгоритм цифровой подписи DSA (Методы дискретного логарифмирования).

Методика построения алгоритма электронной цифровой подписи DSA (Digital Signature Algoritm). Математическая модель алгоритма DSA. Пример реализации алгоритма DSA. Преимущества алгоритма DSA по сравнению с алгоритмом ЭЦП Эль Гамаля.

Тема 4.4. Алгоритмы ГОСТ Р 34-10-94 и ГОСТ Р 34-10-2001 (Методы дискретного логарифмирования).

Методика построения алгоритмов электронной цифровой подписи ГОСТ Р 34-10-94 и ГОСТ Р 34-10-2001. Математическая модель алгоритмов ГОСТ Р 34-10-94 и ГОСТ Р 34-10-2001. Примеры реализации алгоритмов ГОСТ Р 34-10-94 и ГОСТ Р 34-10-2001.

Раздел 5. Современные системы идентификации документов и аутентификации пользователей с использованием ЭЦП. «Слепая подпись».

Тема 5.1.Технология работы с программным комплексом PGP (шифрование и подписывание ЭЦП электронных документов).

Защиты передаваемых данных с помощью программного комплекса PGP. Функции, инсталляция и состав программной среды PGP. Генерация и распространение ключей. Криптографическая защита файлов и аутентификация электронных сообщений. Управление ключами и настройка общих параметров криптографической системы формирования и эксплуатации системы аутентификации электронных сообщений на основе электронной цифровой подписи. Методы математической формализации и прикладного математического обеспечения в системе PGP.

Тема 5.2. Технология работы с программным комплексом «Криптон-подпись» (ЭЦП и шифрование электронных документов).

Аппаратно-программный комплекс «Криптон» предназначен для защиты электронных документов (в том числе и с высокими грифами секретности). Программные средства криптографической защиты информации и аутентификации электронных документов обеспечивают безопасность информации в коммерческих, банковских, страховых, налоговых и т.д. автоматизированных информационных системах и имеют соответствующие сертификаты и лицензии ФСБ РФ и Федеральной службы по техническому и экспортному контролю. Защита и аутентификация информации осуществляется в соответствии с ГОСТ 28147-89 («Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»), ГОСТ Р34.10-2001 («Информационные технологии. Криптографическая защита. Процедура выработки и проверки электронной-цифровой подписи на базе асимметричного криптографического алгоритма»), ГОСТ Р34.11-94 («Информационные технологии. Криптографическая защита информации. Функция хэширования»). Правовой основой аутентификации электронных документов является Федеральный Закон Российской Федерации N1 от 10 января 2002 года «Об электронной цифровой подписи». Алгоритм формирования открытого и закрытого ключа электронной цифровой подписи на основе преобразований Эль Гамаля (методы дискретного логарифмирования) в метрике эллиптических кривых.

Тема 5.3. Технология работы с программным комплексом «Сигнал-Ком» (ЭЦП и шифрование электронных документов).

Пргораммно-аппаратный комплекс аутентификации электронных документов и криптографической защиты данных с сертификацией открытых ключей в Удостоверяю-

щих центрах «Сигнал-Ком», имеющий лицензии и сертификаты ФСБ и ФТСЭК. Технология работы рабочих станций, Удостоверяющего Центра, ведение реестров действующих, архивных и скомпроминтированных ключей. Формирования открытых и закрытых ключей электронной цифровой подписи на основе алгоритма RSA (факторизация больших простых чисел). Методика вычисления открытых и закрытых ключей на основе преобразований методом факторизации больших простых чисел, постановки и проверки электронной цифровой подписи при аутентификации электронных документов.

Тема 5.4. Технология работы с программным комплексом «Крипто-PRO» (ЭЦП и шифрование электронных документов).

Пргораммно-аппаратный комплекс аутентификации электронных документов и криптографической защиты данных с сертификацией открытых ключей в Удостоверяющих центрах «Крипто-PRO», имеющий лицензии и сертификаты ФСБ и ФТСЭК. Технология работы рабочих станций, Удостоверяющего Центра, ведение реестров действующих, архивных и скомпроминтированных ключей. Формирование открытых и закрытых ключей пользователей на основе методов дискретного логарифмирования в метрике эллиптических кривых. Формирование парных ключей конфиденциальной связи на основе преобразований Диффи-Хеллмана. Методика вычисления открытых и закрытых ключей на основе преобразований в метрике эллиптических кривых, постановки и проверки электронной цифровой подписи при аутентификации электронных документов.

Ведение реестра открытых ключей и их сертификатов на сервере Удостоверяющего центра, аннулирование сертификатов скомпроминтированных или просроченных открытых ключей пользователей в базе данных Удостоверяющего центра. Технология работы с ПКЗИ «ШИПКА».

Тема 5.5. Технология работы с программным комплексом защиты электронных товарных знаков и образцов готовой продукции в виртуальном пространстве (Методы стеганографии).

Технология работы с программным комплексом защиты электронных товарных знаков и образцов готовой продукции в виртуальном пространстве аутентификация рекламной продукции в системах электронной торговли и защита авторских прав электронных образцов готовой продукции , образцов товарных и фирменных знаков с использованием ЭЦП и методов цифровой стеганографии. Методика встраивание текстового файла в графические файлы, исключающая возможность распознавания его дестеганографирования.

Применение методов стеганографии при защите авторских прав в компьютерных технологиях.

Раздел 6. Комплексное использование программных средств в системах аутентификации пользователей в компьютерных технологиях.

Иерархия построения системы Удостоверяющих центров Российской Федерации, взаимосвязь Удостоверяющих центров различных уровней. Роль Федерального Удостоверяющего центра, Удостоверяющих центров субъектов Российской Федерации, корпоративных Удостоверяющих центров. Рекомендуемые носители ключевой и сертификационной информации (изделия «Шипка» и «Анкад»). Требования к формированию ключевой информации на сменных носителях отдельных пользователей, технология работы с ними, регламентная и внерегламентная замена ключевых носителей. Ведение баз данных сертификатов открытых ключей пользователей на серверах Удостоверяющих центров.

5.2 Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№ № разделов данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин							
		1	2	3	4	5	6	7	8
1.	Финансовая математика								
2.	Программные средства офисного назначения								
3.	Правовое обеспечение информационной деятельности								
4.	Математические методы и модели в коммерческой деятельности						13,18		
5.	Моделирование в маркетинговых исследованиях						13,18		
6.	Информационные сети и базы данных							9,10,11	
7.	Средства торговой инофрмации							9,10,11	
8.	Экономика организации								
9.	Статистика								
10.	Бухгалтерский учет								
11.	Маркетинг								
12.	Коммерческая деятельность								
13.	Стандартизация, метрология, подтверждение соответствия								
14.	Теоретические основы товароведения								
15	Менеджмент							2,3,13, 14,16	
16.	Логистика								
17	Правовое регулирование профессиональной деятельности								
18.	Рекламная деятельность								8-11
19.	Организация, технология и проектирование предприятий							5,6,8,9, 10,11,13	
21.	Организация и управление коммерческой деятельностью в оптовой торговле						2,4,7,10, 13,16,17, 18		
22.	Организация и управление коммерческой деятельностью в розничной торговле							2,4,7,10, 13,16,17, 18	
23.	Организация предпринимательской деятельности						2,4,7,10, 13,16,17, 18		
24.	Организация и управление коммерческой деятельностью в инфраструктуре рынка								2,4,7,10, 13,16,17, 18
25.	Электронная коммерция							9,10,11, 17	

26.	Организация и техника внешнеторговых операций						2,8,9,10, 11,17		
27.	Биржевое дело								
28.	Товароведение товаров однородных групп								
29.	Техническая оснащенность предприятий в сфере коммерции								
30.	Транспортное обеспечение коммерческой деятельности								8,9,10, 11,13, 16
32.	Организация и управление сервисом в торговле/ Управление продажей товаров и услуг								5-7, 9-11, 13-16
33.	Таможенное дело/ Управление поставками						1,2, 5-7, 9-11, 13-16		
34.	Безопасность предприятия в сфере коммерции/ Развитие сбытовой деятельности: дилеры, франчайзи, филиалы								
35.	Управление персоналом/ Организация труда персонала							7,12,13,14	
36.	Потребительское право/ Административная ответственность за правонарушения в сфере торговли						14,15,17		
37.	Международная торговля/ Международные торговые организации						11-14, 18		

5.3 Разделы дисциплин и виды занятий

№ п/п	Наименование раздела дисциплины	Лекц.	Практ. зан.	Лаб. зан.	Семин.	СРС	Всего
1.	**Раздел 1.** Организационные и правовые основы использования ЭЦП в торгово-экономической деятельности. Тема 1.1. Доктрина информационной безопасности Российской Федерации. Тема 1.2. Федеральный Закон Российской Федерации ФЗ №1 «Об электронной цифровой подписи» Тема 1.3. Приказ ФСБ РФ №66 от 9.02.2005 г. «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифро-	2				8	10

	вальных (криптографических) средств защиты информации». Тема 1.4. Указ Президента Российской Федерации №351 от 17 марта 2008 года «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»						
2.	**Раздел 2.** Проблемы аутентификации пользователей и ЭЦП в информационных инфраструктурах торгово-экономической деятельности	1				8	9
3.	**Раздел 3.** Однонаправленные хэш-функции. ГОСТ Р 34-11-94.	1				4	5
4.	**Раздел 4.** Алгоритмы электронной цифровой подписи.	8	10			26	44
5.	Тема 4.1. Алгоритм ЭЦП RSA (Райвест, Шамир, Адлеман – факторизация больших чисел).	2	2			6	10
6.	Тема 4.2. Алгоритм Эль Гамаля (дискретное логарифмирование). Метрика эллиптических кривых.	2	2			7	11
7.	Тема 4.3. Алгоритм DSA.	2	1			6	9
8.	Тема 4.4. Алгоритмы ГОСТ Р34.10-94 и ГОСТ Р 34-10-2001	2	4			7	13
9.	**Раздел 5.** Современные системы идентификации документов и аутентификации пользователей с использованием ЭЦП. «Слепая подпись».	7	24			12	43
10.	Тема 5.1.Технология работы с программным комплексом PGP (шифрование и подписывание ЭЦП электронных документов).	1	4			2	7
11.	Тема 5.2. Технология работы с программным комплексом «Криптон-подпись» (ЭЦП и шифрование электронных документов).	1	4			2	7
12.	Тема 5.3. Технология работы с программным комплексом «Сигнал-Ком» (ЭЦП и шифрование электронных документов).	1	4			2	7
13.	Тема 5.4. Технология с программно-аппаратным комплексом аутентификации электронных документов ПСКЗИ «ШИПКА»	1	4			2	7
14.	Тема 5.5. Технология работы с про-	1	4			2	7

	граммным комплексом «Крипто-PRO» (ЭЦП и шифрование электронных документов).						
15.	Тема 5.6. Технология работы с программным комплексом защиты электронных товарных знаков и образцов готовой продукции в виртуальном пространстве (Методы стеганографии).	1	4			2	7
16	**Раздел 6.** Комплексное использование программных средств в системах аутентификации пользователей в компьютерных технологиях	2	1			10	13
17	**ИТОГО**	20	34			54	108

6. Перечень практических или лабораторных занятий.

В дисциплине выполнение лабораторных практикумов не предусматривается.

Темы практических занятий:

Тема 4.1. Алгоритм ЭЦП RSA (Райвест, Шамир, Адлеман – факторизация больших чисел), (форма проведения – практическое занятие в компьютерном классе). Автоматизированная обучающая система.

Вопросы к теме:

1. Что такое модуль системы RSA?
2. Как вычисляется функция Эйлера, ее физико-математический смысл?
3. Как формируются открытые и закрытые ключи для формирования и проверки ЭЦП?
4. Что представляет собой ЭЦП в алгоритме RSA и как производится аутентификация электронного сообщения?
5. Какие множества параметров в системе аутентификации электронных сообщений в алгоритме RSA являются открыто распределяемыми, а какие секретными?

Тема 4.2. Алгоритм Эль Гамаля (дискретное логарифмирование), (форма проведения – практическое занятие в компьютерном классе). Автоматизированная обучающая система.

Вопросы к теме:

1. Математическое представления алгоритма дискретного логарифмирования в конечном поле (алгоритм Эль Гамаля).
2. Требования к выбору числового значения модуля дискретного логарифмирования «Р».
3. Требования к выбору основания степени «а».
4. Условия задания числового значения закрытого ключа $К_З$ и его функциональное назначения в алгоритме электронной подписи Эль Гаиаля?
5. Каким образом производится вычисление открытого ключа $К_О$ и его функциональное назначение в алгоритме Эль Гамаля?
6. Математическая модель процессов формирования электронной подписи и аутентификации электронного документа в алгоритме Эль Гамаля.

Тема 4.3. Алгоритм DSA (Digital signature algorithm), (форма проведения – практическое занятие в компьютерном классе). Автоматизированная обучающая система.

Вопросы к теме:

1. Математическое представления алгоритма дискретного логарифмирования DSA.
2. Требования к выбору числового значения модуля в алгоритме DSA «P».
3. Требования к выбору основания степени «a».
4. Условия задания числового значения закрытого ключа $К_З$ и его функциональное назначения в алгоритме электронной подписи DSA?
5. Каким образом производится вычисление открытого ключа $К_О$ и его функциональное назначение в алгоритме DSA?
6. Математическая модель процессов формирования электронной подписи и аутентификации электронного документа в алгоритме DSA.

Тема 4.4. Алгоритмы ГОСТ Р34.10-94 и ГОСТ Р 34-10-2001, (форма проведения – практическое занятие в компьютерном классе). Автоматизированная обучающая система.

Вопросы к теме:

1. Математическое представления алгоритма дискретного логарифмирования по указанным ГОСТам.
2. Требования к выбору числового значения модуля в алгоритмах ГОСТов «P».
3. Требования к выбору основания степени «a».
4. Условия задания числового значения закрытого ключа $К_З$ и его функциональное назначения в алгоритмах электронной подписи ГОСТов?
5. Каким образом производится вычисление открытого ключа $К_О$ и его функциональное назначение в алгоритмах ГОСТов?
6. Математическая модель процессов формирования электронной подписи и аутентификации электронного документа в алгоритмах ГОСТов.

Тема 5.1.Технология работы с программным комплексом PGP (шифрование и подписывание ЭЦП электронных документов).

Вопросы к теме.

1. Процесс инсталляции криптографической системы асимметричного преобразования данных и электронной цифровой подписи.
2. Формирование открытых и закрытых ключей шифрования данных и электронной цифровой подписи.
3. Обмен открытыми ключами шифрования данных и аутентификации электронной цифровой подписи в сетевых компьютерных корпоративных системах. Импортирование открытых ключей.
4. Формирование электронных цифровых подписей открытых электронных сообщений, передача электронного документа по системам теледоступа к вычислительным ресурсам, аутентификация принятого электронного документа..
5. Шифрование открытого электронного сообщения, передача по каналам теледоступа, дешифрование принятой криптограммы получателем.
6. Шифрование и подписывание электронной цифровой подписью электронного сообщения, передача по каналам теледоступа, дешифрование и аутентификация получаемого электронного документа.
7. Гарантированное уничтожение электронных документов и электронных сообщений. Формирование «невидимого диска».

Тема 5.2. Технология работы с программным комплексом «Криптон-подпись» (ЭЦП и шифрование электронных документов).

Вопросы к теме:

1. Инсталляция программного комплекса аутентификации электронных документов «Криптон-Попись».

2. Технология и алгоритм генерации открытых и закрытых ключей пользователей для аутентификации электронных документов.

3. Формирование конфигурации системы аутентификации, алгоритм действий пользователя.

4. Технология работы с файлом «Мастер ключей» при генерации ключей аутентификации электронных документов.

5. Ведение каталогов открытых и закрытых ключей на сменных машинных носителях.

6. Формирование и ведение «Баз данных» открытых ключей пользователей корпоративной системы.

7. Формирование ЭЦП и проверка подлинности электронных документов (аутентификация электронных документов).

Тема 5.3. Технология работы с программным комплексом «Сигнал-Ком» (ЭЦП и шифрование электронных документов).

Вопросы к теме:

1. Инсталляция программного комплекса защиты и аутентификации данных Signal-COM.

2. Алгоритм загрузки сертификационного центра на сервере криптографической защиты и аутентификации данных.

3. Алгоритм инсталляции программного комплекса криптографической защиты файлов «FILE-PRO» на персональных компьютерах, подключенных к корпоративной сети.

4. Алгоритм работы пользователя в системе криптографической защиты и аутентификации данных.

5. Формирование ключей шифрования данных их регистрация и получение сертификата в Сертификационном Центре.

6. Организация сетевого взаимодействия зарегистрированных пользователей.

7. Алгоритм организации сетевого обмена данными.

8. Установка электронной цифровой подписи в текстовый файл, передача подписанного файла по компьютерной сети, верификация принятого электронного документа.

9. Шифрование открытого электронного сообщения.

10. Режим одновременного шифрования и подписывания электронного сообщения.

11. Методы организации шифрования, формированию электронной цифрой подписи передачи, приема и аутентификации подписанных криптограмм в циркулярном режиме**.**

Тема 5.4. Технология работы с программным комплексом «Крипто-PRO» (ЭЦП и шифрование электронных документов).

Вопросы к теме:

1. Инсталляция программного комплекса защиты и аутентификации данных «Крипто PRO».

2. Алгоритм загрузки сертификационного центра на сервере криптографической защиты и аутентификации данных.

3. Алгоритм инсталляции программного комплекса криптографической защиты файлов на персональных компьютерах, подключенных к корпоративной сети.

4. Алгоритм работы пользователя в системе криптографической защиты и аутентификации данных.

5. Формирование ключей шифрования данных их регистрация и получение сертификата в Сертификационном Центре.

6. Организация сетевого взаимодействия зарегистрированных пользователей.

7. Алгоритм организации сетевого обмена данными.

8. Установка электронной цифровой подписи в текстовый файл, передача подписанного файла по компьютерной сети, верификация принятого электронного документа.

9. Шифрование открытого электронного сообщения.

10. Режим одновременного шифрования и подписывания электронного сообщения.

11. Методы организации шифрования, формированию электронной цифрой подписи передачи, приема и аутентификации подписанных криптограмм в циркулярном режиме.

Тема 5.5. Технология работы с программным комплексом защиты электронных товарных знаков и образцов готовой продукции в виртуальном пространстве (Методы стеганографии).

Вопросы к теме:

1. Формирование файла-контейнера как носителя стеганограммы.
2. Формирование исходного открытого текста.
3. Вычисление объемов файла-контейнера и исходного открытого текстза.
4. Алгоритм стеганографирования исходного открытого текста.
5. Передача заполненного файла-контейнера по канала теледоступа к вычислительным ресурсам.
6. Алгоритм дестаганографирования принимаемого файла-контейнера.

7. Примерная тематика курсовых проектов (работ).

В дисциплине выполнение курсовых проектов (работ) не предусматривается.

8. Учебно-методическое и информационное обеспечение дисциплины:

а) федеральные законы и нормативные документы:

1. Доктрина информационной безопасности Российской Федерации.
2. Федеральный закон Российской Федерации «Об информации, информационныч технологияч и защите информации» №149-ФЗ от 27 июля 2006 года.
3. Федеральный закон от 4 июля 1996 г. «Об участие в международном информационном обмене».
4. Федеральный закон от 06 апреля 2011 г. N 63-ФЗ "Об электронной подписи".
5. Концепция национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 17 декабря 1997 г. N1300. (В редакции Указа Президента Российской Федерации от 10 января 2000 г. N24.
6. Федеральный закон от 3 февраля 1996 г. N17-ФЗ «О банках и банковской деятельности».
7. Федеральный закон от 22 апреля 1996 г. N39-ФЗ «О рынке ценных бумаг».
8. Федеральный закон от 21 ноября 1996 г. N129-ФЗ «О бухгалтерском учете».
9. Окинавская хартия глобального информационного общества. Принята 22 июля 2000 года. Окинава.
10. Приказ ФСБ РФ №66 от 9 февраля 2005 года «Об утверждении Положения о разработке, производстве, реализации т эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)

11. Указ Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» №351 от 17 марта 2002 года.
12. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
13. ФСТК России. Руководящие документы. М., ФСТК, 2006 г.

б) основная литература:

1. Информатика для экономистов: Учебник / Российский университет дружбы народов; Под общ. ред. В.М. Матюшка. - М.: ИНФРА-М, 2006. - 880 с. - 3000 экз.-гриф МО РФ. [Режим доступа: ЭБС Znanium.com]
2. Информатика: учебник для бакалавров / под ред. В.В.Трофимова. - М.: ИД Юрайт, 2012. - 911 с. - (Бакалавр).-гриф УМО
3. Ершов, Б.Л. Основы экономической информатики и вычислительной техники [Текст]: учеб. пособие. Ч.3.: Основы создания программного продукта в среде Visual Basic / Б. Л. Ершов. - Иваново: ИГЭУ, 2006. - 180 с. - 2000 экз.-гриф УМО.
4. Ершов Б.Л. Информатика. Основы программирования: учеб. пособие. Ч. 2 / Б.Л. Ершов, Н.А. Капустин. - Иваново: Научная мысль, 2011. - 140 с.
5. Капустин Н.А. Основы информатики. Часть 1: учеб. пособие (практикум) / Н.А. Капустин, Б.Л. Ершов. - Иваново: Научная мысль, 2012. - 128 с.
6. Капустин Н.А. Основы информатики. Часть 2: учеб. пособие (практикум) / Н.А. Капустин, Б.Л. Ершов. - Иваново: Научная мысль, 2012. - 128 с.

б) Дополнительная литература

1. Журнал «АВТОМАТИКА. ИНФОРМАТИКА» 2000-2013 гг. [Доступ: НЭБ КиберЛенинка, http://cyberleninka.ru]
2. Журнал «ПРИКЛАДНАЯ ИНФОРМАТИКА» 2006-2011 гг. [Доступ: НЭБ КиберЛенинка, http://cyberleninka.ru]
3. Информатика: Учебное пособие / Под ред. Б.Е. Одинцова, А.Н. Романова. - 2-е изд., перераб. и доп. - М.: Вузовский учебник: НИЦ Инфра-М, 2012. - 410 с.
4. Информатика: Курс лекций. Учебное пособие / Е.Л. Федотова, А.А. Федотов. - М.: ИД ФОРУМ: ИНФРА-М, 2011. - 480 с.
5. Информатика: Учебник / В.А. Каймин; Министерство образования РФ. - 6-е изд. - М.: ИНФРА-М, 2010. - 285 с.
6. Информатика: аппаратные средства персонального компьютера: Учебное пособие / В.М. Яшин. - М.: ИНФРА-М, 2008. - 254 с.
7. Информатика в экономике: Учебное пособие / Под ред. Б.Е. Одинцова, А.Н. Романова. - М.: Вузовский учебник, 2008. - 478 с.
8. Word, Excel, PowerPoint - просто, кратко, быстро: Руководство пользователя / В.В. Мотов. - М.: ИНФРА-М, 2008. - 206 с.
9. Атли, К. Visual Basic. NET для программистов [Электронный ресурс] / К. Атли; Пер. с англ. - М.: ДМК Пресс, 2008. - 304 с.: ил.
10. Основы информатики: Учебное пособие / М.В. Жаров, А.Р. Палтиевич, А.В. Соколов. - 2-е изд., перераб. и доп. - М.: ФОРУМ, 2008. - 288 с.: ил.
11. Тесты, контрольные задания, вопросы для самопроверки на электронных носителях по информатике.
12. Научно-методичекие, руководящие, и нормативные материалы и документы «14 Пленума учебно-методического объединения ВУЗов по образованию в области информационной безопасности». М., 2011.

г) программное обеспечение:

1. Класс ПЭВМ не ниже Intel Pentium 64 Mb RAM, 2GB HDD с установленным программным обеспечением: Microsoft Windows XP, Microsoft Windows 2000 Professional, Microsoft Visual C^{++}.
2. Программно-аппаратный коплекс персональной криптографической защиты и аутентификации информации «ШИПКА» (шифрование-идентификация-подпись-кодирование-аутентификация (сертифицирован ФСБ и ФСТЭК РФ))
3. Автоматизированные обучающие системы (авторские разработки)
4. Программные и программно-аппаратные комплексы защиты и аутентификации информации, имеющие сертификаты ФСБ и ФСТЭК РФ. Программный комплекс международного обмена, защиты и аутентификации электронных сообщений PGP-9

9. Материально-техническое обеспечение дисциплины:

Технические средства обучения (средства ИКТ)

1. Экран (на штативе или настенный). Минимальный размер 1,25 х 1,25 м.
2. Мультимедиа-проектор. В комплекте: кабель питания, кабели для подключения к компьютеру, видео- и аудиоисточникам.
3. Персональный компьютер — рабочее место преподавателя. Основные технические требования: операционная система с графическим интерфейсом, привод для чтения и записи компакт-дисков, аудио- и видеовходы/выходы, возможность подключения к локальной сети и выхода в Интернет; в комплекте: клавиатура, мышь со скроллингом, коврик для мыши; оснащен акустическими системами, микрофоном и наушниками; может быть стационарным или переносным.
4. Персональный компьютер — рабочее место студента. Основные технические требования: Операционная система с графическим интерфейсом, привод для чтения компакт-дисков, аудио- и видеовходы/выходы, возможность подключения к локальной сети и выхода в Интернет; в комплекте: клавиатура, мышь со скроллингом, ковриkдля мыши; оснащен микрофоном и наушниками; может быть стационарным или переносным.
5. Принтер лазерный. Формат А4 Быстродействие не ниже 15 стр./мин., разрешение не ниже 600 х 600 dpi
6. Принтер цветной. Формат А4 Ч/б печать: 10 стр./мин. (А4), цветная печать: 6 стр./мин.
7. Принтер лазерный сетевой. Формат А4 Быстродействие не ниже 25 стр./мин., разрешение не ниже 600 х 600 dpi.
8. Сервер. Обеспечивает техническую составляющую формирования единого информационного пространства. Организацию доступа к ресурсам Интернета. Должен обладать дисковым пространством, достаточным для размещения цифровых образовательных ресурсов, необходимых для реализации образовательных стандартов по дисциплине Информатика и смежным дисциплинам, а также размещения работ учащихся.
9. Источник бесперебойного питания. Обеспечивает работоспособность в условиях кратковременного сбоя электроснабжения. Во всех образовательных учреждениях обеспечивает работу сервера, в местностях с неустойчивым электроснабжением необходимо обеспечить бесперебойным питанием все устройства.
10. Комплект сетевого оборудования. Должен обеспечивать соединение компьютеров в единую сеть с выделением отдельных групп, с подключением к серверу и выходом в Интернет.
11. Комплект оборудования для подключения к сети Интернет. Выбирается в зависимости от выбранного способа подключения конкретного ОУ.
12. Специальные модификации устройств для ручного ввода текстовой информации и манипулирования экранными объектами — клавиатура и мышь (и разнообразные устройства аналогичного назначения).

13. Копировальный аппарат.

Устройства для записи (ввода) визуальной и звуковой информации

1. Устройства создания графической информации (графический планшет). Рабочая зона — не менее формата А6; чувствительность на нажим; ручка без элементов питания.
2. Сканер. Оптическое разрешение не менее 1200 x 2400 dpi.
3. Цифровая фото/видеокамера.
4. Устройство для чтения информации с карты памяти (картридер).
5. Web-камера.
6. Устройства ввода/вывода звуковой информации — микрофон, наушники.
7. Устройства для создания музыкальной информации. Не менее четырех октав.
8. Внешний накопитель информации. Интерфейс USB.
9. Мобильное устройство для хранения информации (флеш).

10. Образовательные технологии:

10.1. При проведении практических занятий по дисциплине «Электронная подпись» могут использоваться следующие инновационно-педагогические технологии и инновационные методы в образовании:

1. доклады с презентациями на заданные темы или вопросы программы в условиях аудитории и Интернет, подготовленные лектором, студентом или группой студентов (по всем темам курса);
2. использование компьютерной визуализации учебной информации в различных формах, в том числе использование интерактивной доски как эффективного мультимедийного средства обучения приемам работы с офисными программными продуктами (по всем темам курса);
3. использование компьютерных обучающих программ (по всем темам курса);
4. интерактивное взаимодействие между преподавателем и студентами, реализованное в форме обмена офисными документами (по теме 2);
5. мастер-класс в области сетевых офисных технологий (по всем темам курса);
6. игровые технологии в форме деловых и ролевых игр (по темам 2, 8, 9, 10);
7. исследовательский метод обучения на основе поисковой, познавательной деятельности студентов путем постановки преподавателем практических офисных задач (по всем темам курса);
8. защита электронной почты (по теме 2);
9. персональные криптографические средства защиты электронных портфелей как формы документированных отчетов обучающихся о достижениях в усвоении курса (письменные работы, результаты выполнения творческих заданий, результаты тестирования) (по всем темам курса);
10. метод творческих заданий (по всем темам курса).
11. автоматизированные обучающие системы как метод активного процесса изучения теоретического и прикладного материала по дисциплине «Электронная подпись».

10.2. В системе инновационных технологий обеспечения учебного процесса автором были разработаны автоматизированные обучающие системы по следующим направлениям:

1. Автоматизированная обучающая система по изучению традиционных методов шифрования электронных сообщений и передачи ключей шифрования без ключей кодирования сеансовых ключей (трехпроходный метод Шамира).

2. Автоматизированная обучающая система по изучению методов возведения больших чисел в большие степени по модулю.
3. Автоматизированная обучающая система по асимметричным методам защиты и аутентификации электронных сообщений, а также открытого обмена ключами шифрования по открытым каналам теледоступа (метод Диффи-Хэллмана).
4. Автоматизированная обучающая система по формированию ключей защиты и аутентификации электронных сообщений, а также шифрованию и аутентификации открытых сообщений, составляющих банковскую и коммерческую тайны, на основе методов дискретного логарифмирования в метрике эллиптических кривых.
5. Автоматизированная обучающая система по методам обнаружения и исправления ошибок в компьютерных технологиях при работе в корпоративных сетевых системах передачи информации.

11. Оценочные средства (ОС):

11.1. Задания для самостоятельной работы студентов.

Разделы и темы для самостоятельного изучения	Виды и содержание самостоятельной работы
Раздел 1. Организационные и правовые основы использования ЭЦП в торгово-экономической деятельности	
Тема 1.1. Доктрина информационной безопасности Российской Федерации.	Изучить основные положения обеспечения информационной безопасности РФ в части защиты национальных интересов РФ, определить основные виды угроз информационной безопасности и источники таких угроз. Раскрыть сущность методов обеспечения информационной безопасности в различных сферах общественной жизни и в области международного сотрудничества. Дать характеристику основных положений государственной политики обеспечения информационной безопасности Российской Федерации и первоочередных мероприятий по ее реализации. Выделить структурные составляющие организационной основы системы обеспечения информационной безопасности Российской Федерации.
Тема 1.2. Федеральный Закон Российской Федерации ФЗ №1 «Об электронной цифровой подписи»	Определить цель и сферу применения Федерального Закона Российской Федерации «Об электронной цифровой подписи». Обосновать статус правового регулирования отношений в области использования электронной цифровой подписи. Изучить понятийный аппарат настоящего Федерального Закона . Определить условия использования электронной цифровой подписи: условия равнозначности; условия использование средств ЭЦП; условия соблюдения сроков и порядок выдачи и хранения сертификатов ключей подписи в Удостоверяющих центрах. Статус удостоверяющих центров, обязательства Удостоверяющего центра, обязательства владельца сертификата ключа подписи. Определить особенности использования электронной цифровой подписи.
Тема 1.3. Приказ ФСБ РФ №66 от 9.02.2005 г. «Об	Что относят к шифровальные (криптографические) средствам защиты информации конфиденциального характера (в

утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».	настоящем Положении именуются средствами криптографической защиты информации (далее - СКЗИ))? Дать определения понятиям: - средства шифрования; - средства имитозащиты; - средства электронной цифровой подписи; - средства кодирования; - средства изготовления ключевых документов (независимо от вида носителя ключевой информации); - ключевые документы (независимо от вида носителя ключевой информации). Определить назначение настоящего Положения в организации конфиденциального электронного документооборота и требования Положения ПКЗ-2005 носящие рекомендательный характер при разработке, производстве, реализации и эксплуатации средств аутентификации и шифрования. Определить Порядок производства СКЗИ, порядок реализации (распространения) СКЗИ и порядок эксплуатации СКЗИ.
Тема 1.4. Указ Президента Российской Федерации №351 от 17 марта 2008 года «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».	Дать интерпретацию цели и основных постановляющих положений Указа Президента Российской Федерации.
Раздел 2. Проблемы аутентификации пользователей и ЭЦП в информационных инфраструктурах торгово-экономической деятельности	Обосновать необходимость использования средств аутентификации в системах электронной коммерции на основе электронных цифровых подписей. Определить способы и приемы несанкционированного доступа и модификации электронных документов в электронной коммерции: перехват паролей, «маскарад», незаконное использование привилегий. Определить принцип безотказности электронного документооборота и методы его обеспечения. Определить цель аутентификации электронных документов. Дать классификационную структуру и определение возможных злоумышленных действий в системе электронной коммерции: активный перехват, маскарад, ренегатство, подмена, повтор.
Раздел 3. Однонаправленные хэш-функции. ГОСТ Р 34-11-94.	Определить назначение хэш-функции, условия необходимости и достаточности, принцип построения хэш-функции, алгоритмы безопасного хэширования. Определить принцип построения хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции.
Раздел 4. Алгоритмы электронной цифровой подписи.	

Тема 4.1. Алгоритм ЭЦП RSA (Райвест, Шамир, Адлеман – факторизация больших чисел).	1. Вычислить модуль, функцию Эйлера и закрытый ключи ЭЦП при следующих условиях: - число P = 23; число Q = 47; $К_о$ = 37. 2. На основании полученных данных вычислить значение ЭЦП для слова «финансирование», хэш-функция которого определиться как: 5; 13; 7; 3. 3. Аутентифицировать слово «финансирование».
Тема 4.2. Алгоритм Эль Гамаля (дискретное логарифмирование).	1. По заданным исходным данным P=23, G =7, $К_з$ = 2 вычислить значение открытого ключа $К_о$ и значение ЭЦП для слова «финансирование», хэш-функция которого определиться как: 5; 13; 7; 3. 3. Аутентифицировать слово «финансирование».
Тема 4.3. Алгоритм DSA.	1. По заданным исходным данным P=23, g =2, d =5, $К_з$ = 4 вычислить значение открытого ключа $К_о$ и значение ЭЦП для слова «финансирование», хэш-функция которого определиться как: 5; 13; 7; 3. 3. Аутентифицировать слово «финансирование».
Тема 4.4. Алгоритм ГОСТ Р 34-10-2001.	Задана эллиптическая кривая $E_7(2,6):Y^2=X^3+2X+6(mod7)$, задается случайная точка x=5. 1. Определить две точки (x_1,y_1), (x_2,y_2), затем еще две точки путем вычисления композиции первых двух. 2. Вычислить ЭЦП при хэш-значении h(m)=3.
Раздел 5. Современные системы идентификации документов и аутентификации пользователей с использованием ЭЦП. «Слепая подпись».	Дать характеристику и провести сравнительный анализ между отечественными криптографическими системами аутентификации электронных документов серии «КРИПТОН», «КРИПТО ПРО» и «Сигнал-Ком», а также их зарубежного аналога PGP-8. Определить функциональное назначение «Слепой подписи».
Тема 5.1.Технология работы с программным комплексом PGP (шифрование и подписывание ЭЦП электронных документов).	По учебно-методическим материалам изучить технологию формирования открытых и закрытых ключей аутентификации электронных документов, операции обмена открытыми ключами между пользователями корпоративной системы. Изучить технологию формирования и проверки ЭЦП и подлинности электронных документов.
Тема 5.2. Технология работы с программным комплексом «Криптон-подпись» (ЭЦП и шифрование электронных документов).	По учебно-методическим материалам изучить технологию формирования открытых и закрытых ключей аутентификации электронных документов, операции обмена открытыми ключами между пользователями корпоративной системы. Изучить технологию формирования и проверки ЭЦП и подлинности электронных документов.
Тема 5.3. Технология работы с программным комплексом «Сигнал-Ком» (ЭЦП и шифрование электронных документов).	По учебно-методическим материалам изучить технологию формирования открытых и закрытых ключей аутентификации электронных документов, операции обмена открытыми ключами между пользователями корпоративной системы. Изучить технологию формирования и проверки ЭЦП и подлинности электронных документов.
Тема 5.4. Технология работы с программным комплексом «Крипто-PRO»	По учебно-методическим материалам изучить технологию формирования открытых и закрытых ключей аутентификации электронных документов, операции обмена открытыми

(ЭЦП и шифрование электронных документов).	ключами между пользователями корпоративной системы. Изучить технологию формирования и проверки ЭЦП и подлинности электронных документов.
Тема 5.5. Технология работы с программным комплексом защиты электронных товарных знаков и образцов готовой продукции в виртуальном пространстве (Методы стеганографии).	По учебно-методическим материалам изучить технологию стеганографии и определить возможности ее применения в системе электронной коммерции для защиты авторских прав и рекламной продукции в компьютерных технологиях.
Раздел 6. Комплексное использование программных средств в системах аутентификации пользователей в компьютерных технологиях.	Самостоятельно изучить структуру иерархического построения системы Удостоверяющих центров Российской Федерации, взаимосвязь Удостоверяющих центров различных уровней. Роль Федерального Удостоверяющего центра, Удостоверяющих центров субъектов Российской Федерации, корпоративных Удостоверяющих центров. Рекомендуемые носители ключевой и сертификационной информации (изделия «Шипка» и «Анкад»). Требования к формированию ключевой информации на сменных носителях отдельных пользователей, технология работы с ними, регламентная и внерегламентная замена ключевых носителей. Ведение баз данных сертификатов открытых ключей пользователей на серверах Удостоверяющих центров.

11.2.Вопросы к зачету по дисциплине ЭЦП.

1. Возможные несанкционированные действия с электронными документами.
2. Назначение электронной цифровой подписи.
3. Технологические процедуры применения электронной цифровой подписи.
4. Назначение хеш-функции.
5. Требования к хэш-функции.
6. Структурный состав электронной цифровой подписи.
7. Алгоритм функционирования ЭЦП RSA.
8. Обобщенная схема функционирования ЭЦП RSA.
9. Технология функционирования ЭЦП в алгоритме RSA.
10. Математическая интерпретация алгоритма ЭЦП RSA.
11. Алгоритм ЭЦА Эль Гамаля.
12. Технология формирования ЭЦП в алгоритме Эль Гамаля.
13. Математическая интерпретация алгоритма ЭЦП Эль Гамаля.
14. Достоинства алгоритма ЭЦП Эль Гамаля.
15. Алгоритм ЭЦП DSA.
16. Математическая интерпретация ЭЦП DSA.
17. Отечественный стандарт ЭЦП.
18. Математическая интерпретация ЭЦП отечественного стандарта.
19. Общие положения Федерального Закона «Об Электронной цифровой подписи».
20. Условия применения ЭЦП в компьютерных технологиях и электронном документообороте.
21. Юридическое значение ЭЦП.
22. Сертификат ключа подписи.
23. Назначение Удостоверяющего Центра и требования, предъявляемые к нему.
24. Обязательства Удостоверяющего Центра.

25. Актуальность внедрения ЭЦП в торгово-экономическую деятельность.
26. Что такое «Электронная цифровая подпись»?

27. Что такое «Электронный документ»?

28. Кто является владельцем сертификатом ключа электронной цифровой подписи?

29. Что такое открытый и закрытый ключ электронной цифровой подписи, их функциональное назначение?

30. Дать определения понятиям «информационная система общего пользования» и «корпоративная информационная система».

31. Какие алгоритмы аутентификации электронных документов используются в современных компьютерных технологиях?

32. Как осуществляется аутентификация электронных документов по отечественному стандарту ГОСТ Р34.10-2001?

33. Определить функциональное назначение модуля «Конфигурация Криптон®Подпись», как производится его настройка.

34. Определить функциональное назначение модуля «Мастер ключей».

35. Как производится генерация открытого и закрытого ключа пользователя?

36. Как производится формирование «Базы данных открытых ключей», ее функциональное назначение в системе «Криптон®Подпись»?

37. Как осуществляется формирование ЭЦП и ее проверка в системе «Криптон®Подпись»?

38. Как осуществляется формирование нескольких подписей под одним электронным документом?

39. Как выполняется операция по вводу в «Базу данных открытых ключей» открытых ключей пользователей корпоративной системы?

40. Как выполняется проверка подлинности электронного документа подписанного несколькими пользователями***?***

Программа составлена в соответствии с требованиями ФГОС ВПО с учетом рекомендаций ПрООП ВПО по направлению 080100.62 Экономика

Автор-составитель:
Ершов Б.Л. к.т.н., профессор кафедры МЭИ и ВТ