РАБОЧАЯ ПРОГРАММА

Дисциплина:	Криптографические методы защиты информации
	_____
Наименование кафедры*(ПЦК, отделения и др.)*:	Экономико-математических методов и информационных технологий
	(ЭММиИТ) аббревиатура

Направление____38.04.01___ «Экономика»_____
(код специальности(направления), полное наименование)
Профиль Бизнес-аналитика

Сведения о разработчиках:

ФИО	Аббревиатура кафедры *(ПЦК, отделения и др.*	Ученая степень, звание
Сковиков Анатолий Геннадьевич	ЭММиИТ	К.т.н., доцент

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Криптографические методы защиты информации» принадлежит вариативной части дисциплин в структуре ОПОП магистратуры по направлению подготовки «Экономика» и является одной из дисциплин, в рамках которой изучаются основные направления обеспечения безопасности процессов хранения, передачи, обработки, распространения информации. Шифр дисциплины в рабочем учебном плане – Б1.В.ОД4. Дисциплина изучается студентами второго курса магистратуры.

Дисциплина занимает особое место в структуре ОПОП. Вместе с курсами по моделированию бизнес-процессов, курс «Криптографические методы защиты информации» составляет основу образования студента в части ОПОП, касающейся современных информационных технологий.

Дисциплина рассчитана на студентов магистратуры, имеющих подготовку по предшествующим курсам, касающихся основ программирования с использованием алгоритмических языков, алгебры и теории чисел, теории вероятности. Предполагается, что студенты магистратуры знакомы с основными понятиями алгебры, комбинаторики, теории вероятности, информатики, которые изучаются в рамках данной ОПОП перед изучением данной дисциплины.

Изучение курса «Криптографические методы защиты информации» базируется на компетенциях, сформированных у обучающихся в процессе изучения дисциплин ОПОП бакалавриата или специалитета. Кроме этого изучение курса «Криптографические методы защиты информации» базируется на компетенциях, сформированных у обучающихся в процессе изучения дисциплины «Проектирование информационных систем».

Знания, навыки и умения, приобретенные в результате прохождения курса «Криптографические методы защиты информации», будут востребованы в процессе подготовки и защиты выпускной квалификационной работы, проведении научных исследований, связанных с разработкой прикладного программного обеспечения, а так же информационных систем, ориентированных на многопользовательский режим работы, или же на работу в сети Интернет.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины формируются следующие компетенции:

- *способность самостоятельно осуществлять подготовку заданий и разрабатывать проектные решения с учетом фактора неопределенности, разрабатывать соответствующие методические и нормативные документы, а также предложения и мероприятия по реализации разработанных проектов и программ (ПК-5);*
- *способность оценивать эффективность проектов с учетом фактора неопределенности (ПК-6).*

В результате освоения дисциплины студент магистратуры должен:

Иметь представление:

- о критериях оценки защищенности систем;
- о проблемах и направлениях развития аппаратных и программных средств защиты информации;
- о современных криптографических системах.

Знать:

- понятие информации, способы ее представления, основные приемы получения, хранения, обработки информации;

- правовые акты в области защиты государственной тайны и информационной безопасности;
- правовые основы организации защиты государственной тайны и конфиденциальной информации;
- основные понятия криптографии;
- основные требования к системам криптографической защиты;
- основные алгоритмы криптографической защиты;
- основные алгоритмы электронной цифровой подписи;
- проблемы и направления развития криптографических систем.

Уметь:

- использовать программные и аппаратные средства персонального компьютера;
- ориентироваться в современной системе источников информации;
- использовать защищенные современные информационные технологии в своей профессиональной деятельности;
- применять средства антивирусной защиты;
- анализировать информационную безопасность многопользовательских систем;
- пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа;
- видеть и формулировать проблему защиты информации;
- видеть конкретную ситуацию;
- прогнозировать и предвидеть;
- ставить цели и задачи по обеспечению информационной безопасности.

Приобрести навыки:

- самостоятельнойисследовательскойработы;
- обеспечения безопасной работы на компьютере;
- организации эффективной защиты от вирусов;
- обеспечения защиты информации от внешних угроз.

Владеть, иметь опыт:

- использования инструментов криптографической защиты информации;
- использования современной терминологии в области информационной безопасности;
- применения методологии защиты в области информационной безопасности.

Дисциплина предполагает формирование у студентов магистратуры системных знаний по проблеме криптографической защиты информационных ресурсов и управлению информационными рисками, а также практических навыков безопасной работы в информационных системах.

3. ОБЪЕМ ДИСЦИПЛИНЫ

3.1 Объём дисциплины в зачетных единицах (всего): 4 зачетных единицы.

3.2 по видам учебной работы (в часах)

Вид учебной работы	Количество часов (форма обучения заочная)	
	Всего по плану	В т.ч. по семестрам
		№ семестра 4
1	2	3
Контактная работа обучающихся с преподавателем	31	31
Аудиторные занятия:	22	22
Лекции+/	8	8
практические и семинарские занятия		
лабораторные работы (лабораторный практикум)	14	14
Самостоятельная работа	113	113
Текущий контроль (количество и вид: конт.работа, коллоквиум,реферат)		
Курсовая работа		
Виды промежуточной аттестации (экзамен)	9	9
Всего часов по дисциплине	144	144

3.3 Содержание дисциплины. Распределение часов по темам и видам учебной работы

Форма обучения: заочная

Название разделов и тем	Всего	Виды учебной работы					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Компетенции
		лекции	Практические занятия, семинар	Лабораторная работа			
Раздел № 1. Предмет и задачи криптографии	15	1				14	ПК-5
Раздел № 2. Методы шифрования с закрытым ключом	31	1				30	ПК-6
Раздел № 3. Криптографические алгоритмы с открытым ключом	42	2		10	8	30	ПК-6
Раздел № 4. Электронная цифровая подпись	26	2		4	4	20	ПК-6
Раздел № 5. Совершенно секретные системы	21	2				19	ПК-6
Подготовка и сдача курсовой работы, экзамена	9						ПК-5, ПК-6
ИТОГО:	**144**	**8**		**14**	**12**	**113**	

4. СОДЕРЖАНИЕ КУРСА

№	Наименование раздела дисциплины	Содержание раздела дисциплины	Результат обучения, формируемые компетенции
1.	**Предмет и задачи криптографии**	Основные понятия: задачи, объект, предмет, методы криптографической безопасности. Политика в сфере обеспечения информационной безопасности России. Концептуальная модель информационной безопасности. Составляющие концептуальной модели информационной безопасности. Современная концепция информационной безопасности. Цели защиты информации. Носители защищаемой информации. Понятие информации. Сведения	Знает: основные понятия, изложенные в Доктрине информационной безопасности РФ и Федеральном Законе «Об информации, информационных технологиях и защите информации»;интересы личности, общества и государства в информационной области; понятие ценности информации, защиты информации, системы защиты

		и данные, отличие от информации. Информация по уровню доступа. Конфиденциальность информации. Понятие конфиденциальной информации. Требования к криптографическим системам защиты информации. Сведения из истории криптографии. Способы реализации криптографических методов. Понятие и виды криптографических атак. Криптографический протокол. Криптографические методы защиты информации. Методы стеганографии. Аппаратно-программные средства защиты информации: средства обеспечения конфиденциальности данных; средства аутентификации электронных данных и средства управления ключевой информацией. Классификация методов шифрования. Требования к современным шифрам.	информации; цели и концептуальные основы защиты информации; основные виды угроз безопасности информации и их классификацию; требования к криптографическим системам защиты информации; сведения из истории криптографии; понятие и виды криптографических атак. Умеет: производить анализ типов информации в зависимости от порядка ее предоставления; делать разбор методов обеспечения информационной безопасности; классифицировать в соответствии с уровнями обеспечения национальной безопасности группы субъектов; подразделять основные средства защиты по видам деятельности; пользоваться в своей профессиональной деятельности основными нормативными правовыми актами в сфере обеспечения информационной безопасности. Владеет: понятиями «информатизация», «информационные технологии», «информационная безопасность», «национальная безопасность», «доктрина информационной

			безопасности»; методами классификации конфиденциальной информации; навыками работы с документами в сфере обеспечения информационной безопасности.
2.	**Методы шифрования с закрытым ключом**	Простейшие методы шифрования с закрытым ключом. Общая схема симметричного шифрования. Методы замены. Пропорциональные шифры. Многоалфавитные подстановки. Методы гаммирования. Методы перестановки. Понятие композиционного шифра. Операции, используемые в блочных алгоритмах симметричного шифрования. Структура блочного алгоритма симметричного шифрования. Методы симметричного шифрования. Блочное и потоковое шифрование. Классическая сеть Фейстеля. Алгоритм шифрования DES и его модификации. Абсолютно надежный шифр. Основные свойства симметричных криптосистем. Режимы работы блочных алгоритмов. Алгоритм криптографического преобразования данных ГОСТ 28147-89. Основные свойства хэш-функций. Понятие хеш-функции. Использование блочных алгоритмов шифрования для формирования хеш-функции. Обзор алгоритмов формирования хеш-функций.	Знает: основные понятия и классификацию средств криптографической защиты информации; различия между стеганографией и криптографией; основные методы симметричного шифрования; классификацию методов симметричного шифрования; основные свойства симметричных криптосистем; понятие хеш-функции. Умеет: использовать блочные алгоритмы шифрования для формирования хеш-функции; использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем. Владеет: основными методами симметричного шифрования; алгоритмами формирования хеш-функций.
3.	**Криптографические алгоритмы с открытым ключом**	Основные понятия и классификация средств ассиметричной	Знает: понятия и классификацию ассиметричных методов

		криптографической защиты информации. Основные свойства асимметричных криптосистем. Предпосылки создания методов шифрования с открытым ключом и основные определения. Односторонние функции. Требования к алгоритмам шифрования с открытым ключом. Использование асимметричных алгоритмов для шифрования. Цифровая подпись на основе алгоритмов с открытым ключом. Генерация и хранение ключей. Формирование секретных ключей с использованием асимметричных алгоритмов. Распределение ключей. Управление ключами в системах с открытым ключом. Алгоритм Диффи-Хелмана. Алгоритм RSA. Алгоритм Эль-Гамаля. Криптографические системы на эллиптических кривых. Возможные атаки при использовании алгоритмов асимметричного шифрования.	шифрования; основные методы построения асимметричных криптосистем. Умеет: использовать односторонние функции в целях построения криптосистем; использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; использовать алгоритмы генерации, хранения и распределения ключей. Владеет: инструментами обеспечения безопасной работы в сети Интернет; методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом.
4.	**Электронная цифровая подпись**	История развития. Виды электронных подписей в Российской Федерации. Общая схема электронной цифровой подписи. Использование хеш-функций. Виды асимметричных алгоритмов цифровой подписи. Электронная подпись на основе алгоритма RSA. Цифровая подпись на основе алгоритма Эль-Гамаля. Стандарты на алгоритмы цифровой подписи. Стандарт цифровой подписи ГОСТ Р34.10-94. Новый отечественный стандарт ЭЦП. Управление открытыми ключами.	Знает: основные понятия, основные алгоритмы электронной цифровой подписи; основные стандарты на алгоритмы цифровой подписи; основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты. Умеет: проектировать и использовать системы электронной цифровой подписи; применять на практике алгоритмы управления открытыми ключами. Владеет: технологиями

		Протокол аутентификации Нидхэма-Шредера в случаях симметричной и асимметричной системы шифрования. Модели атак и их возможные результаты.	электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет.
5.	**Совершенно секретные системы**	Основные подходы к измерению информации. Энтропия и неопределенность. Норма языка и избыточность сообщений. Понятие совершенно секретной системы. Расстояние единственности.	Знает: основные подходы к измерению информации; основные понятия информатики – энтропия, неопределенность языка, норма языка, избыточность сообщений; понятие совершенно секретной системы. Умеет: строить теоретически совершенно секретную систему. Владеет: методами измерения информации и построения совершенно секретной системы.

5. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Практические и семинарские занятия не предусмотрены.

6. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Тема 3.КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ С ОТКРЫТЫМ КЛЮЧОМ.
Лабораторная работа №1.Программная реализация алгоритма RSA.
Трудоемкость – 5 часов, в том числе в интерактивной форме – 5 часов.
Цель работы:
Получение навыков использования ассиметричных криптографических алгоритмов.
Результаты лабораторной работы:учебный вариант криптографической системы с открытым ключом на алгоритме RSA, которая является первой изкриптосистем с открытым ключом.
Методические указания по выполнению работы смотреть в Приложении «Лабораторный практикум по дисциплине Криптографические методы защиты информации».
Тема 3.КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ С ОТКРЫТЫМ КЛЮЧОМ.
Лабораторная работа №2. Программная реализация криптографических протоколов.
Трудоемкость – 5 часов, в том числе в интерактивной форме – 5 часов.
Цель работы:
Ознакомиться с криптографическими протоколами,которые в настоящее время широко используются для обеспеченияинформационной безопасности. Освоить основные понятия, которые связаныс криптографическими протоколами.
Результаты лабораторной работы: учебные варианты протокола Диффи-Хелмана

формирования общего ключа и протокола подбрасывания монеты, которые моделируют работу с использованиемкриптографических протоколов.

Методические указания по выполнению работы смотреть в Приложении «Лабораторный практикум по дисциплине Криптографические методы защиты информации».

Тема 4.ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ.

Лабораторная работа №3.Программная реализация ЭЦП.

Трудоемкость – 4 часа, в том числе в интерактивной форме – 4 часа.

Цель работы:

Создать программу, которая реализует учебный вариант схем ЭЦП, используя алгоритмы с открытыми ключами.

Результаты лабораторной работы:учебные варианты ЭЦП на базе алгоритма Эль-Гамаля и алгоритма RSA.

Методические указания по выполнению работы смотреть в Приложении «Лабораторный практикум по дисциплине Криптографические методы защиты информации».

7. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

По дисциплине не предусмотрены курсовые работы, контрольные работы, рефераты.

8. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Виды самостоятельной работы студентов, обеспечивающие реализацию цели и решение задач данной рабочей программы:

- подготовка к практическим (лабораторным) занятиям;
- изучение тем дисциплины, выносимых для самостоятельного изучения студентам очной формы обучения;
- подготовка к сдаче экзамена.

В результате самостоятельной работы студент должен:

- **иметь представление** об информации, способах ее представления, о задачах объектах, предмете, методах информационной безопасности; об официальных органах, обеспечивающие информационную безопасность в Российской Федерации; о правовом обеспечении информационной безопасности; о концепции информационной безопасности Российской Федерации; различиях между стеганографией и криптографией.
- **знать** структуру информации, понятие «электронный документ» и «электронная подпись»; какие опасности и угрозы, возникают при использовании информации; основные понятия и классификацию средств криптографической защиты информации; основные методы симметричного шифрования; основные методы построения асимметричных криптосистем; классификацию компьютерных вирусов и вредоносных программ; методы и средства борьбы с вирусами и вредоносными программами.
- **уметь** использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; использовать алгоритмы генерации, хранения и распределения ключей; использовать антивирусное программное обеспечение.

Студенты выполняют задания, самостоятельно обращаясь к учебной литературе. Проверка выполнения заданий осуществляется путем электронного тестирования и устного опроса на практических занятиях. Для методического обеспечения самостоятельной работы

студентов разработан информационный комплекс, охватывающий все темы курса, вынесенные на самостоятельное изучение. Информационный комплекс выдается студентам в электронном виде. Кроме этого при подготовке следует использовать следующие ресурсы:

1. http://univertv.ru/video/matematika/ Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вас вопросу.
2. http://www.iqlib.ru/ Электронная библиотека IQlib образовательных и просветительских изданий. Образовательный ресурс, объединяющий в себе интернет-библиотеку и пользовательские сервисы для полноценной работы с библиотечными фондами. Свободный доступ к электронным учебникам, справочным и учебным пособиям. Аудитория электронной библиотеки IQlib – студенты, преподаватели учебных заведений, научные сотрудники и все те, кто хочет повысить свой уровень знаний.
3. http://eqworld.ipmnet.ru/ru/library.htm EqWorld – мир математических уравнений. Учебно-образовательная физико-математическая библиотека. Электронная библиотека содержит DjVu- и PDF-файлы учебников, учебных пособий, сборников задач и упражнений, конспектов лекций, монографий, справочников и диссертаций по математике, механике и физике. Все материалы присланы авторами и читателями или взяты из Интернета (из www архивов открытого доступа). Основной фонд библиотеки составляют книги, издававшиеся тридцать и более лет назад.
4. http://www.edu.ru/modules.php?op=modload&name=Web_Links&file=index&l_op=viewlink&cid=1314 Федеральный портал "Российское образование". Каталог образовательных ресурсов.

Материалы курса, выносимые студентам для самостоятельного изучения:

№ п/п	Наименование темы	Виды самостоятельной работы	Формы контроля
1	Политика в сфере обеспечения информационной безопасности России. Концептуальная модельинформационной безопасности. Официальные органы, обеспечивающие информационную безопасность в Российской Федерации. Обзор российского законодательства в сфереинформационных технологий.Федеральный закон «Об информации, информационных технологиях и о защитеинформации», законодательство РФ в сфере СМИ. Федеральный закон «О государственной тайне».	изучение	тестирование
2	Методы симметричного шифрования. Блочное и потоковое шифрование. Классическая сеть Фейстеля. Алгоритм шифрования DES и его модификации. Абсолютно надежный шифр. Основные свойства симметричных криптосистем.	изучение	тестирование
3	Основные свойства асимметричных криптосистем. Практические аспекты	изучение	тестирование

	использования криптосистем с открытым ключом. Алгоритм RSA. Алгоритм Эль-Гамаля. Криптографические системы на эллиптических кривых.		
4	Основные свойства цифровой подписи. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля. Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94. Схемы слепой подписи. Схемы неоспоримой подписи.	изучение	тестирование

Методические указания для обучающихся по освоению дисциплины

1. Планирование и организация времени, необходимого для изучения дисциплины.

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

- Изучение конспекта лекции в тот же день, после лекции – 10-15 минут.
- Изучение конспекта лекции за день перед следующей лекцией – 10-15 минут.
- Изучение теоретического материала по учебнику и конспекту – 1 час в неделю.
- Подготовка к лабораторному занятию – 30 мин.
- Всего в неделю – 2 часа 55 минут.

2. Описание последовательности действий студента («сценарий изучения дисциплины»).

При изучении дисциплины очень полезно самостоятельно изучать материал, который еще не прочитан на лекции. Тогда лекция будет гораздо понятнее. Однако легче при изучении курса следовать изложению материала на лекции. Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий:

- После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня (10-15 минут).
- При подготовке к лекции следующего дня, нужно просмотреть текст предыдущей лекции, подумать о том, какая может быть тема следующей лекции (10-15 минут).
- В течение недели выбрать время (1 час) для работы с литературой по криптографическим методам в библиотеке или изучить дополнительную литературу в электронной форме.

3. Методические рекомендации по подготовке практических (лабораторных) занятий.

По данному курсу предусмотрены лабораторные занятия. При подготовке к лабораторным занятиям следует изучить соответствующий теоретический материал по криптографическим методам и, если предусмотрено темой, изучить работу программ-калькуляторов. Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучаются и книги по криптоанализу.

Полезно использовать несколько учебников по курсу «Криптографические методы». Однако легче освоить курс придерживаясь одного учебника и конспекта. Рекомендуется, кроме «заучивания» материала, добиться состояния понимания изучаемой темы

дисциплины. С этой целью рекомендуется после изучения очередного параграфа выполнить несколько простых упражнений на данную тему. Кроме того, очень полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): о чем этот параграф?, какие новые понятия введены, каков их смысл?, какие математические принципы используются в этом параграфе и каков их смысл «своими словами»? Сами криптографические алгоритмы следует не заучивать, а «понять». С этой целью рекомендуется записать идею алгоритма, составить план преобразования открытого текста в шифртекст и обратно, сравнить используемые алгоритмы и теоремы в конспекте и в учебнике. При изучении теоретического материала всегда нужно рисовать схемы или графики.

Необходимо изучить лабораторную работу предыдущего занятия и выяснить те вопросы, которые показались непонятными. Полезно вначале освоить и провести «вручную» шифрование/ расшифрование небольшого текста (состоящего из одного–двух предложений), и только потом использовать программный код соответствующих программ-калькуляторов, которые рассматривались на предыдущем занятии. Такой подход позволяет студентам глубже, полнее понять современные алгоритмы шифрования.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Список рекомендуемой литературы
а)основная литература

№	Название, библиографическое описание	Кол-во экз. в библ. (на каф.)
1	Башлы П. Н.Информационная безопасность и защита информации [Электронный ресурс].- Москва : Евразийский открытый институт, 2012.	5
2	Партыка Т. Л.Информационная безопасность. - М. : Форум, 2011.	1
3	Чмора, А.Л.Современная прикладная криптография. - М.: Гелиос АРВ, 2001.	4

б)дополнительная литература

4. Ищейнов В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации. - М.: Форум : ИНФРА-М, 2014.
5. Мельников В. П.Информационная безопасность и защита информации. - М.: Академия, 2008.
6. Алферов А.П., Зубов А.Ю. и др. Основы криптографии: Учеб. пособие, 2-е изд.,испр. и доп. М.: Гелиос АРВ, 2002.- 480 с.: ил.

в)программное обеспечение

1. Стандартный пакет офисных программ корпорации Microsoft (Excel).
2. ОС Windows XP (или выше), браузер (InternetExplorer не ниже версии 8.0).
3. Программное средство PGP (PrettyGoodPrivacy) —программа для шифрования информации и создания электронных цифровых подписей, позволяющая выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде, в том числе прозрачное шифрование данных на запоминающих устройствах, например, на жёстком диске.

4. Научный калькулятор BCalc.
5. Любая среда программирования.

г)базы данных, информационно-справочные и поисковые системы

1. http://intuit.ru/
2. http://citforum.ru/
3. Электронный каталог научной библиотеки УлГУ.
4. КонсультантПлюс: справочная поисковая система (электронный ресурс).
5. Научная электронная библиотека eLibrary.ru
6. Электронная библиотечная система IPRbooks

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1. Аудитории для проведения лекционных и семинарских занятий, оснащенные проектором, ноутбуком (актовый зал, 703, 709 и др. аудитории).
2. Аудитории для проведения практических и лабораторных занятий (комп. классы – аудитории 1К, 49, 508, 711, 605, 407). Всего 63 рабочих места.
3. Аудитории, оборудованные интерактивными досками (603, 611).
4. Аудитории для проведения тестирования и самостоятельной работы студентов с выходом в интернет, комп.класс №806 (корпус по ул. Пушкинская, 4а), 1 сервер и 16 рабочих мест (MS Office)/
5. Читальный зал (803 аудитория) с компьютеризированными рабочими местами для работы с электронными библиотечными системами, каталогом и т.д.

Приложение

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Криптографические методы защиты информации»

1. Перечень компетенций, которые формируются в процессе изучения дисциплины

После изучения дисциплины «Криптографические методы защиты информации» обучающийся должен обладать следующими общекультурными и профессиональными компетенциями:

Профессиональные компетенции:

- способность самостоятельно осуществлять подготовку заданий и разрабатывать проектные решения с учетом фактора неопределенности, разрабатывать соответствующие методические и нормативные документы, а также предложения и мероприятия по реализации разработанных проектов и программ (ПК-5);
- способность оценивать эффективность проектов с учетом фактора неопределенности (ПК-6).

2. Показатели и критерии оценивания, шкала оценивания

При оценивании результатов освоения дисциплины (текущей и промежуточной аттестации) применяется балльная система. В качестве оценочных средств на протяжении семестра используются:

- общетеоретические вопросы и задания с открытой формой ответа;
- тестирование;
- лабораторные работы;
- итоговое испытание (экзамен).

При включении в проверочные задания общетеоретических вопросов студенту предоставляется возможность выбора и право ответа на определённое количество вопросов из списка. Общетеоретические вопросы соответствуют тематике лекционных занятий.

С помощью контрольных заданий тестового типа проверяются следующие элементы подготовки студентов по основам информационной безопасности в профессиональной деятельности:

1. основные положения курса «Криптографические методы защиты информации»;
2. важнейшие теоретические проблемы курса;
3. сущность и содержание основных дефиниций курса;
4. владение компьютерной и периферийной техникой, специализированными и прикладными программами;
5. знание основных принципов работы со специализированными программами;
6. знание специализированной терминологии курса;
7. навыки использования элементарных средств и методов защиты информации, знание основ построения криптосистем.

При составлении контрольных заданий все вопросы имеют одинаковое количество вариантов ответа. Вместе с тем задание формируется таким образом, чтобы правильный вариант ответа был только один из нескольких возможных ответов. В случае если используются различные типы заданий, то они группируются по отдельным рубрикам.

Оценка результатов освоения учебной дисциплины

Оценка результатов освоения учебной дисциплины включает в себя: текущий контроль знаний и промежуточную аттестацию студентов.

Текущий контроль знаний проводится в форме проведения лабораторных занятий, устного и письменного опроса, тестирования, оценки результатов самостоятельной

работы.

Работа по формированию профессиональных компетенций включает различные виды учебной и исследовательской работы, которые ориентированы на формирование у студента навыков работы. Указанные задачи решаются путем применения образовательных технологий обучающего (репродуктивного и продуктивного) характера и самообразования. В систему самостоятельной работы включены:

- работа с источниками информации и лекционным материалом;
- систематизация и интерпретация данных путем выполнения лабораторных работ, подготовки к семинарским занятиям;
- подготовка к контрольному тестированию;
- подготовка сообщений, выступлений по материалам самостоятельной работы.

Оценка качества подготовки на основании выполненных заданий ведется преподавателям (с обсуждением результатов) баллы начисляются в зависимости от сложности задания.

Оценка качества подготовки по результатам самостоятельной работы студента ведется:

- преподавателем – оценка глубины проработки материала, рациональность и содержательная ёмкость представленных интеллектуальных продуктов, наличие креативных элементов, подтверждающих самостоятельность суждений по теме;
- группой – в ходе обсуждения представленных материалов;
- студентом лично – путем самоанализа достигнутого уровня понимания темы.

Результаты работы по выполнению практических, самостоятельных и контрольных заданий являются ведущим компонентом в итоговой оценке компетенций по данному курсу.

При оценивании результатов освоения дисциплины (текущей и промежуточной аттестации) применяется балльная система. В качестве оценочных средств на протяжении семестра используются:

- общетеоретические вопросы и задания с открытой формой ответа;
- работа студентов на занятиях;
- выполнение индивидуальных заданий и лабораторных работ;
- тестирование;
- промежуточная аттестация.

При включении в проверочные задания общетеоретических вопросов обучающемуся предоставляется возможность выбора и право ответа на определённое количество вопросов из списка. Общетеоретические вопросы соответствуют тематике лекционных занятий.

Порядок проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

Текущий контроль успеваемости и промежуточная аттестация в рамках дисциплины проводятся с целью определения степени освоения обучающимися образовательной программы. Учебные достижения обучающихся по всем видам учебных заданий в ходе текущего контроля оцениваются по балльной системе в соответствии с Технологической картой. Текущий контроль успеваемости студентов проводится по каждой теме учебной дисциплины и включает контроль знаний на аудиторных и внеаудиторных занятиях, а также в ходе выполнения самостоятельной работы. Рубежный контроль по дисциплине проводится в рамках контрольных недель.

Технологическая карта

Оцениваемая аттестационная работа	**Виды текущей аттестации**	**Максимально е количество баллов**
ТЕКУЩАЯ АТТЕСТАЦИЯ		

Посещение практических занятий	Посещаемость (не менее 75% занятий)	10
Защита выполненной лабораторной работы	5 баллов за каждую выполненную и защищенную лабораторную работу	15
Тестирование	– 0 баллов при условии правильного ответа менее чем на 50% тестовых заданий; – 5 баллов при условии правильного ответа не менее чем на 50% тестовых заданий; – 7 баллов при условии правильного ответа не менее чем на 70% тестовых заданий; – 10 баллов при условии правильного ответа не менее чем на 90% тестовых заданий.	10
САМОСТОЯТЕЛЬНАЯ РАБОТА		
Подготовка доклада по тематике курса	Материал в электронном виде (предварительно пересылается преподавателю по электронной почте) представляется на практических занятиях и обсуждается в группе обучающихся	5

Необходимый минимум для допуска к промежуточной аттестации 25баллов (обязательным условием является выполнение в полном объеме предусмотренного программой комплекса лабораторных работ). Дополнительные требования для студентов, отсутствующих на занятиях по уважительной причине: выполненные лабораторные работы на собственном носителе, дополнительное практическое задание на экзамене.

Промежуточная аттестация по итогам освоения программы учебной дисциплины проводится в форме экзамена. Экзамен сдается согласно расписанию и служит формой проверки учебных достижений обучающихся по всей программе учебной дисциплины и преследуют цель - оценить учебные достижения за академический период.

Положительная аттестация предполагает:

- наличие системы знаний по предмету;
- умение излагать материал в логической последовательности, систематично, грамотным языком;
- владение специализированной терминологией;
- знание основных криптографических методов защиты информации, способы и механизмы их реализации;

- знание основных схем электронной цифровой подписи;
- умение применять на практике методы, средства и методы криптографической защиты информации.

Условием положительной аттестации (оценка «отлично») на экзамене является самостоятельное и уверенное применение студентом знаний в практической деятельности, полное изложение полученных знаний при ответе на вопросы билета, в соответствии с требованиями учебной программы, формулировка выводов и обобщений. Допускаются единичные несущественные ошибки, самостоятельно исправленные студентом.

Оценка «отлично» не ставится в случаях систематических пропусков студентом лабораторных занятиях по неуважительным причинам, отсутствия активного участия на практических и лабораторных занятиях.

Студент, получает оценку «хорошо», если при изложении полученных знаний возникают отдельные несущественные ошибки, исправляемые студентом по указанию преподавателя и выполнение заданий осуществляется с незначительной помощью преподавателя.

Студент, получает оценку «удовлетворительно», если его ответ является не полным (при этом принципиальными, существенными аспектами материала студент владеет свободно), что, в целом, не препятствует усвоению последующего программного материала, допускаются отдельные существенные ошибки, исправляемые с помощью преподавателя, возникают затруднения при выделении существенных признаков изученного и формулировке выводов.

Оценка «неудовлетворительно» ставится студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков

Список вопросов

1. Шифры одноалфавитной замены. Шифр Цезаря, квадрат «Полибия»
2. Ассиметричная криптография и электронная цифровая подпись. Понятия.
3. Аппаратное шифрование DES: структура, перестановки, сеть Файштеля, расширение ключа.
4. Шифры перестановки. Квадрат «Кардана».
5. TEA: структура, алгоритм, образующая функция, ключ.
6. Шифры многоалфавитной замены. Табло Виженера.
7. IDEA: структура, алгоритм, расширение ключа.
8. Шифровальный аппарат Вернама. Шифр Вернама (XOR).
9. Структура ГОСТ 28147-89: образующая функция, расширение ключа.
10. Шифр Плейфейера.
11. Классификация шифров по ключевой информации.
12. Конкурс AES: цели и условия конкурса, алгоритмы шифрования конкурса.
13. Шифр Хилла.
14. MARS структура: образующая функция, схемы входного и выходного перемешивания.
15. Типы криптоанализа шифрованных сообщений. Понятие защищенности шифрованных сообщений.
16. Основные принципы ассиметричной криптографии.
17. Нелинейные поточные шифры. Фильтрующие шифры. Линейный регистр сдвига.
18. Комбинирующие поточные шифры. Корреляционно-стойкий комбинирующий шифр.

19. Алгоритм Эль Гамаль (асимметричная криптография).
20. Комбинирующий поточный шифр с элементом памяти.
21. Код аутентификации сообщения (MAC). Способы построения MAC. HMAC.
22. Динамический поточный шифр.
24. Определение блочного шифрования. Блок информации. Ключ алгоритма. Абсолютно симметричный блочный шифр.
25. Аутентификация пользователя. Типы систем аутентификации (на симметричных и асимметричных криптосистемах, на сертификатах).
26. Обратимые операции в блочном шифровании.
27. Kerberos. Протокол распределения ключей.
28. Необратимые операции в блочном шифровании
29. Распространение ключей. Протоколы, основанные на использовании симметричной криптосистемы и случайных параметров.
30. Сети блочных шифров, ветви сети, раунд сети, образующая функция. SP-сеть, KASLT-сеть.
31. Распространение ключей. 3-х этапный протокол Шамира (Shamir).
32. Классическая структура сети Фейстеля. Ветви сети, материал ключа, раунд сети, образующая функция.
33. Распространение ключей. Протокол Needham-Schroeder.
34. Абсолютно симметричная сеть Фейстеля. Модификация сети Фейстеля для большего числа ветвей: тип 1 – размер блока, ветви сети, материал ключа, раунд сети, образующая функция.
35. Распространение ключей. Протоколы на основе асимметричных криптосистем.
36. Алгоритм RSA (асимметричная криптография).

Примеры тестовых заданий для самопроверки

1. Выберите правильный ответ.

Криптография – это:

а) наука, изучающая развитие компьютерных технологий;

б) наука, занимающаяся изучением методов и средств защиты информации;

в) наука, занимающаяся изучением методов и средств распределения информации;

г) наука, занимающаяся изучением информации.

2. Выберите правильный ответ.

Идентификатор – это:

а) уникальный признак данной информации, на основе которого можно доказательно установить ее подлинность;

б) уникальный признак данной информации, на основе которого можно доказательно установить ее существование;

в) уникальный признак нескольких видов информации, на основе которого можно доказательно установить их взаимосвязь;

г) уникальный признак информации, на основе которого можно установить ее целостность.

3. Выберите правильный ответ.

Современная криптография включает в себя:

а) симметричные криптосистемы, криптосистемы с открытым ключом, системы электронной подписи, управление ключами;

б) симметричные криптосистемы, асимметричные криптосистемы, системы

электронной подписи, управление ключами;

в) симметричные криптосистемы, криптосистемы с закрытым ключом, системы электронной подписи, управление ключами;

г) симметричные криптосистемы, криптосистемы с открытым ключом, системы электронной защиты, блокировку ключами.

4. Выберите правильный ответ.

Алфавит – это:

а) множество символов латинского алфавита;

б) конечное множество используемых для кодирования информации знаков;

в) бесконечное множество используемых для кодирования информации знаков;

г) конечное множество используемых для кодирования информации цифр.

5. Выберите правильный ответ.

Текст – это:

а) неупорядоченный набор из элементов алфавита;

б) упорядоченный набор слов;

в) упорядоченный набор из элементов алфавита;

г) неупорядоченный набор слов.

6. Выберите правильный ответ.

Шифрование – это:

а) процесс получения данных;

б) процесс суммирования информации;

в) процесс зашифрования и расшифрования;

г) процесс преобразования данных.

7. Выберите правильный ответ.

Криптосистемы подразделяются на:

а) симметричные и асимметричные;

б) числовые и символьные;

в) открытые и закрытые;

г) положительные и отрицательные.

8. Выберите правильный ответ.

Один и тот же ключ используется в:

а) симметричных криптосистемах;

б) асимметричных криптосистемах;

в) символьных криптосистемах;

г) числовых криптосистемах.

9. Выберите правильный ответ.

Электронной подписью называется:

а) подпись в конце текста;

б) набор символов, позволяющий проверить подлинность сообщения;

в) присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения;

г) присоединяемое к тексту его название, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения;

10. Выберите правильный ответ.

Криптостойкость – это:

а) характеристика шифра, определяющая его стойкость к расшифрованию без знания ключа;

б) характеристика шифра, определяющая его стойкость к расшифрованию с использованием ключа;

в) характеристика шифра, определяющая его стойкость к шифрованию без знания ключа;

г) характеристика шифра, определяющая его стойкость к копированию без знания ключа.

11. Выберите правильный ответ.

Моноалфавитные подстановки – это:

а) вид преобразований, заключающийся в замене символов исходного текста на другие по более или менее сложному правилу;

б) вид преобразований, заключающийся в добавлении символов по более или менее сложному правилу;

в) вид преобразований, заключающийся в удалении символов исходного текста по более или менее сложному правилу;

г) вид преобразований, заключающийся в преобразовании символов исходного текста по более или менее сложному правилу.