МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Оренбургский государственный университет»

Кафедра математических методов и моделей в экономике

УТВЕРЖДАЮ
Декан факультета экономики и управления
_____ С.Н. Ларе
(подпись, расшифровка подп
"23" апреля 201

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ДВ.2.2 Математические методы защиты информации»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
01.03.04 Прикладная математика
(код и наименование направления подготовки)

Применение математических методов к решению инженерных и экономических задач
(наименование направленности (профиля) образовательной программы)

Тип образовательной программы
Программа академического бакалавриата

Квалификация
Бакалавр

Форма обучения
Очная

Оренбург 2015

Рабочая программа дисциплины «*Б.1.В.ДВ.2.2 Математические методы защиты информации***» /сост.**
О.Н. Яркова - Оренбург: ОГУ, 2015

Рабочая программа предназначена студентам очной формы обучения по направлению подготовки 01.03.04 Прикладная математика

824847

Содержание

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

формирование теоретических знаний о математических методах построения криптографических алгоритмов и практических навыков их применения для защиты информации.

Задачи:

- освоение основных понятий криптографии и математических методов защиты информации;
- ознакомление с наиболее распространенными типами шифров и математическими методами их криптоанализа;
- освоение математических методов построения криптографических протоколов идентификации и аутентификации;
- изучение математических методов построения алгоритмов электронной цифровой подписи;
- приобретение навыков шифрования, расшифрования информации;
- приобретение навыков реализации алгоритмов идентификации и аутентификации;
- приобретение навыков разработки собственного программного обеспечения для решения задач защиты информации.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам (модулям) по выбору вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *Б.1.Б.10 Математический анализ, Б.1.Б.11 Линейная алгебра и аналитическая геометрия, Б.1.Б.12 Дискретная математика, Б.1.Б.13 Математическая логика и теория алгоритмов, Б.1.Б.20 Численные методы, Б.1.Б.21 Программирование для электронно-вычислительных машин, Б.1.Б.22 Программные и аппаратные средства электронно-вычислительных машин, Б.1.В.ОД.4 Разработка и применение прикладного программного обеспечения, Б.1.В.ОД.5 Основы информатики*

Требования к входным результатам обучения, необходимым для освоения дисциплины

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции
Знать: базовые понятия математического анализа, линейной алгебры, математической логики, дискретной математики, позволяющие самостоятельно решать прикладные математические задачи технологии разработки алгоритмов и программ, позволяющие осуществлять самостоятельную работу с персональным компьютером (ПК) в качестве пользователя и программиста; **Уметь:** решать прикладные математические задачи; самостоятельно разрабатывать алгоритмы решения широкого круга задач; планировать вычислительный эксперимент; работать с научно-технической литературой и технической документацией по программному обеспечению ПЭВМ. **Владеть:** навыками решения прикладных математических задач; навыками самостоятельной работы с персональным компьютером на уровне программиста;	ОПК-1 готовностью к самостоятельной работе
Знать: базовые понятия математического анализа, линейной алгебры, математической логики, дискретной математики, позволяющие самостоятельно решать прикладные математические задачи; технологии программирования, позволяющие использовать современные математические методы и современные прикладные программные средства для решения прикладных задач в том числе защиты информации	ОПК-2 способностью использовать современные математические методы и современные прикладные программные средства и осваивать современные технологии

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции
Уметь: использовать методы использовать методы математического анализа, линейной алгебры, дифференциального исчисления, дискретной математики, математической логики и теории алгоритмов, численных методов и современные прикладные программные средства для решения прикладных задач в том числе защиты информации; самостоятельно разрабатывать алгоритмы решения широкого круга задач; планировать вычислительный эксперимент; разрабатывать программы на языке высокого уровня для решения задач обработки данных в предметной области; работать с современными системами программирования; **Владеть:** навыками решения прикладных задач с использованием методов математического анализа, линейной алгебры, дифференциального исчисления, дискретной математики, математической логики и теории алгоритмов, численных методов и современных прикладных программных средств; навыками проектирования вычислительных алгоритмов для решения широкого круга задач; анализа сложности и эффективности алгоритмов; оформления программной документации; навыками численного решения прикладных задач в приведенной выше предметной области с использованием современных прикладных программных средств	программирования
Знать: базовые понятия математического анализа, линейной алгебры, дифференциального исчисления, дискретной математики, математической логики и теории алгоритмов, алгоритмы численных методов решения прикладных задач; пакеты прикладных программ для численного решения практических задач на электронных вычислительных машинах **Уметь:** применять стандартные пакеты прикладных программ для решения прикладных задач; разрабатывать, отлаживать, тестировать собственные программные средства при реализации численных методов решения прикладных задач **Владеть:** навыками решения математических задач с использованием стандартных пакетов прикладных программ; навыками разработки, отладки, тестирования собственных программных средств при реализации методов решения прикладных задач	ПК-1 способностью использовать стандартные пакеты прикладных программ для решения практических задач на электронных вычислительных машинах, отлаживать, тестировать прикладное программное обеспечение
Знать: алгоритмы численных методов решения прикладных задач; вычислительную технику и программные средства позволяющие реализовывать указанные алгоритмы; технологии разработки, отладки, тестирования параллельных программ, позволяющие настраивать программные среды для реализации , тестирования, отладки и запуска параллельных вычислительных алгоритмов **Уметь:** настраивать, тестировать и осуществлять проверку (в том числе собственных разрабатываемых) программных средств при реализации алгоритмов численных методов решения прикладных задач; самостоятельно настраивать операционную систему (ОС) и программные среды для реализации, тестирования, отладки и запуска параллельных вычислительных алгоритмов **Владеть:** навыками настройки, тестирования и осуществления проверки (в том числе собственных разрабатываемых) программных средств при реализации алгоритмов численных методов решения прикладных задач; навыками настройки операционной системы, программных сред для реализации, тестирования, отладки и запуска параллельных вычислительных алгоритмов	ПК-2 способностью и готовностью настраивать, тестировать и осуществлять проверку вычислительной техники и программных средств
Знать: современные технологии программирования, способы и механизмы управления данными в процессе разработки, отладки,	ПК-3 способностью и готовностью

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции
тестирования программ для решения широкого круга задач на ЭВМ; **Уметь:** разрабатывать программы на языке высокого уровня для решения задач обработки данных в предметной области; работать с современными системами программирования; самостоятельно настраивать операционную систему (ОС) для работы с ПК в качестве программиста, осуществлять поиск информации в сети Интернет; реализовывать алгоритмы численных методов решения прикладных задач с использованием современных языков программирования **Владеть:** навыками анализа сложности и эффективности алгоритмов; оформления программной документации, навыками настройки операционной системы (ОС) для работы с ПК в качестве программиста, навыками поиска информации в сети Интернет в процессе проектирования, разработки, отладки, тестирования программ для решения широкого круга задач на ЭВМ	демонстрировать знания современных языков программирования, операционных систем, офисных приложений, информационно-телекоммуникационной сети "Интернет" (далее - сеть Интернет"), способов и механизмов управления данными, принципов организации, состава и схемы работы операционных систем
Знать: подходы, позволяющие перейти от естественнонаучной сущности проблемы к формализованной задаче **Уметь:** перейти от естественнонаучной сущности проблемы к формализованной задаче; применять математические и численные методы при решении поставленной задачи и исследовать свойства полученного решения используя соответствующий естественнонаучный аппарат **Владеть:** навыками построения формализованных задач; навыками применения математических методов для решении практических задач, возникающих в ходе профессиональной деятельности; выбора оптимальных алгоритмов для решения практических задач; исследования свойств полученных решений используя соответствующий естественнонаучный аппарат	ПК-9 способностью выявить естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, готовностью использовать для их решения соответствующий естественнонаучный аппарат
Знать: базовые понятия математического анализа, линейной алгебры, дифференциального исчисления, дискретной математики, математической логики, алгоритмы численных методов решения прикладных задач **Уметь:** выбирать метод решения задачи конкретного класса, провести анализ полученного решения; принять решение на основе полученных результатов **Владеть навыками:** формализации прикладных задач; выбора оптимальных алгоритмов решения практических задач; анализа полученного решения; принятия решений на основе полученных результатов	ПК-10 готовностью применять математический аппарат для решения поставленных задач, способностью применить соответствующую процессу математическую модель и проверить ее адекватность, провести анализ результатов моделирования, принять решение на основе полученных результатов
Знать: базовые понятия программирования, алгоритмы и структуры данных, способы и механизмы управления данными в процессе разработки программ; базовые математические методы решения прикладных задач **Уметь:** применять знания для управления информацией при решении прикладных математических задач и разработке собственного ПО **Владеть:** навыками управления информацией при решении прикладных математических задач и разработке ПО	ПК-11 готовностью применять знания и навыки управления информацией
Знать: фундаментальные разделы математического анализа, линейной алгебры, дискретной математики, математической логики, численных методов, позволяющие самостоятельно изучать новые разделы фундаментальных наук **Уметь:** самостоятельно осваивать новые разделы фундаментальных наук на основе знаний математического анализа, линейной алгебры, дискретной математики, математической логики, численных методов,	ПК-12 способностью самостоятельно изучать новые разделы фундаментальных наук

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции
достаточных для решения задач защиты информации криптографическими методами **Владеть:** навыками познания новых разделов фундаментальных наук на основе знаний математического анализа, линейной алгебры, дискретной математики, математической логики, численных методов, используя информационный поиск в области решения прикладных задач криптографической защиты информации	

Постреквизиты дисциплины: *Б.2.В.П.2 Преддипломная практика*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: математические методы защиты информации, позволяющие осуществлять самостоятельную работу с персональным компьютером (ПК) **Уметь:** самостоятельно применять математические методы, программные средства для защиты информации **Владеть:** навыками самостоятельной работы с персональным компьютером с использованием информационных технологий и современных методов защиты информации	ОПК-1 готовностью к самостоятельной работе
Знать: основные криптографические алгоритмы; стандарты, модели и математические методы шифрования; современные математические методы и современные технологии построения алгоритмов шифрования, идентификации и аутентификации, цифровой подписи; **Уметь:** применять современные математические методы, современные прикладные программные средства и технологии программирования для решения задач защиты информации в предметной области; **Владеть:** навыками применения современных математических методов, прикладных программных средств и технологий программирования при реализации математических методов защиты информации в приведенной выше предметной области	ОПК-2 способностью использовать современные математические методы и современные прикладные программные средства и осваивать современные технологии программирования
Знать: основные криптографические алгоритмы; стандарты, модели и математические методы шифрования; математические методы построения алгоритмов шифрования, идентификации и аутентификации, цифровой подписи; **Уметь:** разрабатывать программы на языке высокого уровня для решения задач защиты информации в предметной области; разрабатывать, отлаживать, тестировать собственные программные средства при реализации методов защиты информации при решении прикладных задач **Владеть:** навыками анализа эффективности методов защиты информации, протоколов идентификации и аутентификации; навыками разработки, отладки, тестирования собственных программных средств при реализации математических методов защиты информации в приведенной выше предметной области	ПК-1 способностью использовать стандартные пакеты прикладных программ для решения практических задач на электронных вычислительных машинах, отлаживать, тестировать прикладное программное обеспечение
Знать: основные криптографические алгоритмы; стандарты, модели и математические методы шифрования; математические методы по-	ПК-3 способностью и готовностью

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
строения алгоритмов шифрования, идентификации и аутентификации; **Уметь:** разрабатывать программы на языке высокого уровня для решения задач защиты информации; самостоятельно настраивать операционную систему (ОС) при решении задач защиты информации, осуществлять поиск информации в сети Интернет; реализовывать криптографические алгоритмы с использованием современных языков программирования **Владеть:** навыками анализа сложности и эффективности криптографических алгоритмов; навыками настройки операционной системы (ОС) при решении задач защиты информации, навыками поиска информации в сети Интернет в процессе проектирования, разработки, отладки, тестирования программ для решения задач защиты информации на ЭВМ	демонстрировать знания современных языков программирования, операционных систем, офисных приложений, информационно-телекоммуникационной сети "Интернет" (далее - сеть Интернет"), способов и механизмов управления данными, принципов организации, состава и схемы работы операционных систем
Знать: основные криптографические алгоритмы; типичные слабости реализации современных криптографических систем; стандарты, модели и математические методы шифрования; математические методы построения алгоритмов шифрования, идентификации и аутентификации; Уметь: применять математические методы для построения криптографических алгоритмов; правильно применять криптографические алгоритмы и протоколы в приведенной выше предметной области **Владеть навыками:** формализации прикладных задач; выбора оптимальных алгоритмов решения практических задач в перечисленной выше предметной области; анализа полученного решения; принятия решений на основе полученных результатов	ПК-10 готовностью применять математический аппарат для решения поставленных задач, способностью применить соответствующую процессу математическую модель и проверить ее адекватность, провести анализ результатов моделирования, принять решение на основе полученных результатов
Знать: математические методы защиты информации **Уметь:** применять знания для управления информацией при решении задач защиты информации **Владеть:** навыками управления информацией при решении задач защиты информации	ПК-11 готовностью применять знания и навыки управления информацией
Знать: фундаментальные разделы прикладной алгебры, позволяющие самостоятельно изучать новые разделы фундаментальных наук **Уметь:** самостоятельно осваивать новые разделы фундаментальных наук на основе знаний прикладной алгебры и криптографических методов защиты информации **Владеть:** навыками познания новых разделов фундаментальных наук на основе знаний прикладной алгебры и криптографических методов защиты информации	ПК-12 способностью самостоятельно изучать новые разделы фундаментальных наук

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**42,25**	**42,25**
Лекции (Л)	22	22
Практические занятия (ПЗ)	10	10

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Лабораторные работы (ЛР)	10	10
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение индивидуального творческого задания (ИТЗ);* *- выполнение расчетно-графического задания (РГЗ);* *- написание реферата (Р);* *- написание эссе (Э);* *- самостоятельное изучение разделов (перечислить);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к практическим занятиям;* *- подготовка к коллоквиумам;* *- подготовка к рубежному контролю и т.п.)*	**65,75** +	**65,75** +
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**диф. зач.**	

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение	6	1			5
2	Математические основы криптологии	27	5	4	4	14
3	Симметричные системы шифрования	14	2	2	2	8
4	Асимметричные криптосистемы	20	4	2	2	12
5	Криптографические протоколы	19	4	1	2	12
6	Электронная цифровая подпись	13	4	1		8
7	Надежность криптосистем	9	2			7
	Итого:	108	22	10	10	66
	Всего:	108	22	10	10	66

4.2 Содержание разделов дисциплины

№ 1 Введение Основные понятия и определения. История развития криптографии. Классификация криптографических систем. Законодательные и правовые основы защиты компьютерной информации и информационных технологий.

№ 2 Математические основы криптологии Элементы теории делимости: общий наибольший делитель, общее наименьшее кратное, непрерывные дроби и алгоритм Евклида, простые числа, разложение на простые сомножители. Сравнимые по модулю m числа. Сравнения, свойства сравнений, вычеты, полная система вычетов, приведенная система вычетов, теоремы Эйлера и Ферма. Системы сравнений. Китайская теорема об остатках. Моноиды, группы, кольца, идеалы, поля, полиномиальные кольца над полями. Первообразные корни. Индексы и дискретные логарифмы. Примитивные многочлены, неприводимые многочлены и их построение. Рекуррентные последовательности.

№ 3 Симметричные системы шифрования Простейшие системы шифрования (шифр замены, перестановки, шифры Вернама, Вижинера, гаммирование). Современные симметричные криптосистемы. Блочные и поточные шифры. Шифр DES, режимы работы DES, AES, ГОСТ 28147-89. Поточные шифры: РСЛОС, RC4. Стойкость криптографических систем и алгоритмов Энтропия,

теоретическая и практическая стойкость, вычислительная стойкость. Теоретико-информационная стойкость. Вычислительная и временная сложность алгоритма.

№ 4 Асимметричные криптосистемы Общая схема функционирования систем с открытыми ключами, основанными на односторонних функциях. Криптосистема RSA и ее модификации. Криптосистема Эль Гамаля. Криптосистема Рабина.

№ 5 Криптографические протоколы Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля. Взаимная проверка подлинности пользователей. Протоколы с нулевой передачей знаний. Схемы обязательств. Распределение ключей Выбор ключа, время жизни ключа, разделение секрета. Схемы обмена секретными ключами: Шамира, Диффи-Хеллмана, протоколы основанные на эллиптических кривых.

№ 6 Электронная цифровая подпись Целостность данных и аутентификация сообщений. Хэш-функции (MD4, SHA). Алгоритмы ЭЦП, основанные на односторонних функциях: RSA, Эль Гамаля, Шнорра, Нибберга-Руппеля.

№ 7 Надежность криптосистем. Виды атак. Стойкость актуальных алгоритмов шифрования.

В блок **4.3 Лабораторные работы**

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2	Реализация алгоритмов нахождения НОД, канонического разложения составного числа, построения подходящих дробей	2
2	2	Реализация алгоритмов решения сравнений и систем линейных сравнений	2
3	3	Реализация шифра замены, перестановки, шифра Вернама, Вижинера	2
4	4	Реализация асимметричных алгоритмов шифрования (RSA/Эль Гамаля)	2
5	5	Реализация протоколов идентификации	2
		Итого:	10

В блок **4.4 Практические занятия (семинары)**

№ занятия	№ раздела	Тема	Кол-во часов
1	2	Сравнимые по модулю m числа. Сравнения, свойства сравнений, вычеты, полная система вычетов, приведенная система вычетов, теоремы Эйлера и Ферма.	2
2	2	Нахождение первообразных корней. Составление таблиц индексов. Неприводимые многочлены. Построение рекуррентных последовательностей	2
3	3	Поточные системы шифрования (РСЛОС, алгоритм RC4)	2
4	4	Асимметричные криптосистемы (RSA, El Gamal)	2
5	5	Эллиптические кривые и их свойства. Протокол распределения ключей основанный на эллиптических кривых.	1
6	6	Схемы электронной цифровой подписи (на основе алгоритмов RSA, El Gamal)	1
		Итого:	10

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Виноградов И.М. Основы теории чисел. – Спб.: Лань, 2009. (ентл 10)

2. Новиков, Ф. А. Дискретная математика для программистов [Текст] : учеб. для вузов / Ф. А. Новиков. - СПб. : Питер, 2009 - 384 с. (ентл 16)

3. Хорев, П.Б., Методы и средства защиты информации в компьютерных системах [Текст] : учеб. пособие / П. Б. Хорев .- 4-е изд., стер. - М. : Академия, 2008. - 256 с. (фнб 10)

4. Мельников, В. П. Защита информации [Текст] : учебник для подготовки бакалавров по направлению 230100 "Информатика и вычислительная техника" / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе; под ред. В. П. Мельникова. - Москва : Академия, 2014. - 297 с.

5. Сергеева Ю. С. Защита информации. Конспект лекций [Электронный ресурс] / Сергеева Ю. С. - А-Приор, 2011. Режим доступа: - http://biblioclub.ru/index.php?page=book_view&book_id=72670

6. Башлы П. Н. Информационная безопасность и защита информации[Электронный ресурс] / Башлы П. Н. - ИЦ РИОР, 2013. Режим доступа: - http://znanium.com/bookread2.php?book=405000

5.2 Дополнительная литература

1. Методы и средства защиты информации в сетях [Электронный ресурс] / Лаборатория книги, 2011. Режим доступа: - http://biblioclub.ru/index.php?page=book_view&book_id=140796
2. Биркгоф, Г. Современная прикладная алгебра = Modern Applied Algebra [Текст] : пер. с англ. / Г. Биркгоф, Т.К. Барти.- 2-е изд., стер. - СПб. : Лань, 2005. - 400 с.
3. Судоплатов С.В., Овчинникова Е.В. Элементы дискретной математики: учеб. для вузов / С.В. Судоплатов. – Новосибирск: НГТУ, 2002.
4. Бабенко, Л. К. Параллельные алгоритмы для решения задач защиты информации [Текст] : [монография] / Л. К. Бабенко, Е. А. Ищукова, И. Д. Сидорова. - Москва : Горячая линия-Телеком, 2014. - 304 с.
5. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии [Текст]: [монография] / О. Н. Василенко. - М. : МЦНМО, 2003. - 328 с.
6. Криптография: шаг за шагом: Учебник. - М. : Навигатор, 2002 + CD-ROM.
7. Нечаев, В.И. Элементы криптографии. Основы теории защиты информации: Учеб. пособие / В.И. Нечаев. - М. : Высш. шк., 1999. - 109 с.
8. Программирование алгоритмов защиты информации: учебное пособие/ А.В. Домашев, В.О. Попов, Д.И. Правиков и др. – М.: Нолидж, 2000
9. Жельников В. Криптография от папируса до компьютера / В. Жельников. - М. : ABF, 1996. - 336с.
10. Зегжда, Д.П. Основы безопасности информационных систем: Учеб. пособие / Д.П. Зегжда, А.М. Ивашко. - М. : Горячая линия - Телеком, 2000. – 452 с.
11. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
12. ГОСТ Р 34.11-94 Информационная технология. Криптографическая защита информации. Функция хэширования.

Методическая литература

1. Василего, И. П., Теория чисел в криптографии [Текст] : метод. указ. / И. П. Василего . - Оренбург : ОГУ, 2004. - 20 с

2. Шалкина, Т. Н. Методы и средства защиты компьютерной информации [Электронный ресурс] : метод. указ. к лабор. практикуму / Т. Н. Шалкина. - Оренбург : ОГУ – 2006

3. Шалкина, Т. Н. Методы и средства защиты компьютерной информации [Текст] : метод. указ. к лаб. практикуму / Т. Н. Шалкина ; М-во образования и науки РФ, ГОУ высш. проф. образования "ОГУ" . - Оренбург : ГОУ ОГУ, 2007. - 44 с. - Библиогр.: с. 44

4. Шалкина, Т. Н. Методы и средства защиты информации в вычислительных системах и сетях [Электронный ресурс] : учеб. пособие / Т. Н. Шалкина ; М-во образования и науки РФ, Гос. образов. учреждение высш. проф. образования "ОГУ". - Электрон. текстовые дан. (1 файл: 1,39 МБ). - Оренбург : ГОУ ОГУ, 2007. -Adobe Acrobat Reader 5.0

5.3 Периодические издания

1. Обозрение прикладной и промышленной математики

5.4 Интернет-ресурсы

– http://www.securitylab.ru/ информационный портал по ИТ безопасности
– http://www.osp.ru/ сайт издательства «Открытые системы»
– http://www.citforum.ru/ форум по информационным технологиям, методам защиты информации

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

Лицензионное ПО

Пакет настольных приложений
Microsoft Office (Word, Excel, PowerPoint, OneNote, Outlook, Publisher, Access)

ПО для решения широкого спектра научных и прикладных задач:
MathCad 14 – математический пакет (лицензия ОГУ, выделена на каф. ММиМЭ на 10 ПК)
MathWorks MATLAB R2013b + Fuzzy Logic Toolbox + Wavelet Toolbox

Средства для разработки и проектирования
Microsoft Visual Studio
Rad Studio 5 (конкурентная лицензия на факультет на 20 рабочих станций)

Приложения
Microsoft Visio - средство для создания широкого спектра диаграмм

6 Материально-техническое обеспечение дисциплины

Для проведения лабораторного практикума предназначен компьютерный класс (ауд. 6204).

Лекции проводятся в аудитории 3217, оснащенной мультимедийным оборудованием.

ЛИСТ
согласования рабочей программы

Направление подготовки: 01.03.04 Прикладная математика
код и наименование

Профиль: Применение математических методов к решению инженерных и экономических задач

Дисциплина: Б.1.В.ДВ.2.2 Математические методы защиты информации

Форма обучения: очная
(очная, очно-заочная, заочная)

Год набора 2015

РЕКОМЕНДОВАНА заседанием кафедры
Кафедра математических методов и моделей в экономике
наименование кафедры

протокол № 9 от "13" 04 2015 г.

Ответственный исполнитель, заведующий кафедрой
Кафедра математических методов и моделей в экономике — Реннер А.Г.
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
Доцент кафедры ММиМЭ — Яркова О.Н.
должность *подпись* *расшифровка подписи*

должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Заведующий кафедрой математических методов и моделей в экономике — Реннер А.Г.
наименование кафедры *подпись* *расшифровка подписи*

Председатель методической комиссии по направлению подготовки
01.03.04 Прикладная математика — Реннер А.Г.
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
Н.Н. Грицай
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
Н.В. Лужнова
личная подпись *расшифровка подписи*

Рабочая программа зарегистрирована в ОИОТ ЦИТ
Начальник отдела информационных образовательных технологий ЦИТ
Е.В. Дырдина
личная подпись *расшифровка подписи*