МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра прикладной математики

УТВЕРЖДАЮ
Декан факультета математики и информационных технологий

_____ Герасименко С.А.
(подпись, расшифровка подписи)

"24" апреля 2015 г.

РАБОЧАЯ ПРОГРАММА

МОДУЛЯ

«Б.1.В.ОД.17 Математические методы защиты информации»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
01.03.02 Прикладная математика и информатика
(код и наименование направления подготовки)

Общий профиль
(наименование направленности (профиля) образовательной программы)

Тип образовательной программы
Программа академического бакалавриата

Квалификация
Бакалавр

Форма обучения
Очная

Оренбург 2015

Рабочая программа модуля «*Б.1.В.ОД.17 Математические методы защиты информации***» /сост. О.С. Арапова - Оренбург: ОГУ, 2015**

Рабочая программа предназначена студентам очной формы обучения по направлению подготовки 01.03.02 Прикладная математика и информатика

Содержание

1 Цели и задачи освоения модуля

Цель (цели) освоения модуля:

– формирование у студентов представлений о роли математики в развитии методов защиты информации и развитие навыков решения задач криптографии.

Задачи:

– освоение терминологического аппарата теории защиты информации и фундаментальных математических понятий криптологии;

– освоение базовых математических алгоритмов и методов, лежащих в основе методов защиты информации;

– изучение подходов к созданию современных криптосистем;

– приобретение навыков применения математических методов к решению прикладных задач защиты информации.

2 Место модуля в структуре образовательной программы

Модуль относится к обязательным дисциплинам (модулям) вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты модуля: *Б.1.Б.11 Математический анализ, Б.1.В.ОД.19 Дополнительные главы математического анализа*

Требования к входным результатам обучения, необходимым для освоения модуля

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения модуля	Компетенции
Знать: основные методы математического анализа; **Уметь:** применять методы математического анализа на практике; **Владеть:** навыками решения типовых задач математического анализа и задач практической направленности.	ОПК-1 способность использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с прикладной математикой и информатикой
Знать: области применения методов математического анализа; **Уметь:** интерпретировать результаты решения основных задач математического анализа; **Владеть:** навыками формирования выводов по полученным результатам решения задач математического анализа.	ПК-1 способность собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям
Знать: современные научные исследования и разработки в области математического анализа; **Уметь:** оценивать возможности применения методов математического анализа в различных прикладных областях науки и техники; **Владеть:** навыками решения задач математического анализа.	ПК-2 способность понимать, совершенствовать и применять современный математический аппарат

Постреквизиты модуля: *Б.2.В.П.1 Преддипломная практика*

3 Требования к результатам обучения по модулю

Процесс изучения модуля направлен на формирование следующих результатов обучения

Планируемые результаты обучения по модулю, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: основные этапы развития криптографии и их характеристики; основные понятия теории защиты информации; математические понятия криптологии; основные типы шифров, криптографических систем, криптографических протоколов; принципы построения шифров, криптографических систем и криптографических протоколов; алгоритмы решения конкретных математических задач, используемых в криптографических системах и протоколах; **Уметь:** применять изученные алгоритмы и методы в решении задач защиты информации; собирать, обрабатывать и интерпретировать данные в области защиты информации; ориентироваться в различных видах криптосистем и современном программном обеспечении в области защиты информации; **Владеть:** математическими методами, лежащими в основе решения задач защиты информации; технологией программирования математических алгоритмов и методов криптографии;	ПК-3 способностью критически переосмысливать накопленный опыт, изменять при необходимости вид и характер своей профессиональной деятельности

4 Структура и содержание модуля

4.1 Структура модуля

Общая трудоемкость модуля составляет 4 зачетных единиц (144 академических часов).

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**45,25**	**45,25**
Лекции (Л)	30	30
Лабораторные работы (ЛР)	14	14
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- самостоятельное изучение разделов (схемы обмена секретными ключами: широкоротой лягушки, Ниджейма-Шредера, Отвэй-Риса; цифровые сертификаты);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к коллоквиумам;* *- подготовка к рубежному контролю и т.п.)*	**98,75** *12,75* *45* *21* *8* *12*	**98,75** *12,75* *45* *21* *8* *12*
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**Экзамен**	

Разделы модуля, изучаемые в 6 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в криптографию	3	1	–	–	2
2	Стойкость криптографических систем	12	4	–	–	8
3	Принципы построения симметричных криптографических алгоритмов	23	3	–	4	16
4	Распределение ключей	24	4	–	2	18
5	Принципы построения асимметричных криптографических алгоритмов	34	6	–	4	24
6	Криптографические Хэшфункции и электронная цифровая подпись	34	6	–	4	24
7	Криптографические протоколы	8	4	–	–	4
8	Надежность криптосистем	6	2	–	–	4
	Итого:	144	30	–	14	100
	Всего:	144	30	–	14	100

4.2 Содержание разделов модуля

1 Введение в криптографию. Краткая история развития криптографических методов. Основные понятия криптографии. Термины и определения. Классификация шифров.

2 Стойкость криптографических систем. Модели шифров и открытых текстов. Алгебраические модели шифров. Вероятностные модели шифров. Математические модели открытых сообщений. Криптографическая стойкость шифров. Теоретико-информационный подход к оценке криптостойкости шифров. Практическая стойкость шифров. Имитостойкость и помехоустойчивость шифров. Имитация и подмена сообщения. Способы обеспечения имитостойкости. Помехостойкость шифров.

3 Принципы построения симметричных криптографических алгоритмов. Математические методы формирования псевдослучайных последовательностей. Блочные и поточные шифры. Шифры DES, режимы работы DES, AES, ГОСТ 28147-89. Поточные шифры: РСЛОС, RC4, шифр Рона.

4 Распределение ключей. Выбор ключа, время жизни ключа, разделение секрета. Схемы обмена секретными ключами: широкоротой лягушки, Ниджейма-Шредера, Отвэй-Риса, Цербер. Односторонние функции и схемы формирования ключа: Шамира, Диффи-Хеллмана.

5 Принципы построения асимметричных криптографических алгоритмов. Общая схема функционирования систем с открытыми ключами, основанных на односторонних функциях. Криптосистема RSA и ее модификации. Криптосистема Эль Гамаля. Криптосистема Рабина.

6 Криптографические Хэшфункции и электронная цифровая подпись. Криптографические хэш-функции. Блочно-итерационные и шаговые функции. Ключевые функции хэширования. Бесключевые функции хэширования. Электронно-цифровая подпись. Задачи и особенности электронно-цифровой подписи. Ассиметричные алгоритмы цифровой подписи на основе RSA. Алгоритм цифровой подписи Фиата – Фейге – Шамира. Алгоритм цифровой подписи Эль-Гамаля. Алгоритм цифровой подписи Шнорра. Алгоритм цифровой подписи Ниберга-Руппеля. Алгоритм цифровой подписи DSA.

7 Криптографические протоколы. Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля. Взаимная проверка подлинности пользователей. Идентификация с нулевой передачей знаний. Схемы обязательств. Системы электронного голосования. Цифровые сертификаты: Системы перераспределения доверия: PGP, SSL, X509 (PKIX), SPKI. Неявные сертификаты.

8 Надежность криптосистем. Виды атак: Атака Винера на RSA, атаки на RSA основанные на решетках, атака Хостада, атака Франклина-Рейтера, частичное раскрытие ключа. Стойкость актуальных алгоритмов шифрования. Доказуемая стойкость со случайным оракулом. Доказуемая стойкость без случайного оракула.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1, 2	3	Поточные шифры: РСЛОС, RC4, шифр Рона.	4
3	4	Алгоритмы Шамира, Диффи-Хеллмана.	2
4, 5	5	Криптосистемы RSA , Эль Гамаля, Рабина.	4
6	6	Алгоритм цифровой подписи Шнорра.	2
7	7	Алгоритм цифровой подписи DSA.	2
		Итого:	14

5 Учебно-методическое обеспечение модуля

5.1 Основная литература

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

2 Борисов, М. А. Основы программно-аппаратной защиты информации [Текст] : учеб. пособие для вузов / М. А. Борисов, И. В. Заводцев, И. В. Чижов.- 2-е изд. - М. : Книжный дом "ЛИБРОКОМ", 2013. - 370 с. : ил. - (Основы защиты информации). - Библиогр.: с. 365-370 и в подстроч. примеч. - ISBN 978-5-397-03251-3.

5.2 Дополнительная литература

1 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. - (Высшее образование. Бакалавриат). - Библиогр.: с. 291-293. - ISBN 978-5-4468-0332-3.

2 Новиков, Ф. А. Дискретная математика для программистов [Текст] : учеб. пособие для вузов / Ф. А. Новиков.- 3-е изд. - СПб. : Питер, 2009. - 384 с. - (Учебник для вузов). - Библиогр.: с. 368-369. - Предм. указ.: с. 370-371. - ISBN 978-5-91180-759-7.

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. : ил. - (Высшее профессиональное образование). - Библиогр.: с. 251-252. - ISBN 978-5-7695-5118-5.

5.3 Периодические издания

1 Обозрение прикладной и промышленной математики

5.4 Интернет-ресурсы

– http://www.securitylab.ru/
– http://www.osp.ru/
– http://www.citforum.ru/

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

*(*Microsoft Office
Microsoft Windows
MathCad

6 Материально-техническое обеспечение модуля

- учебная аудитория;
- библиотечный фонд университета;
- компьютерный класс, оснащенный современной техникой (PENTIUM 3, PENTIUM 4, INTEL CORE 2);
- LCD – проектор EPSON EMP-X3;
- Ноутбук ASUS A6RP;
- Экран для проектора ЭКСКЛЮЗИВ MW 213*213.

К рабочей программе прилагаются:

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.

ЛИСТ
согласования рабочей программы

Направление подготовки: 01.03.02 Прикладная математика и информатика
код и наименование

Профиль: Общий профиль

Модуль: Б.1.В.ОД.17 Математические методы защиты информации

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

Год набора 2015

РЕКОМЕНДОВАНА заседанием кафедры
Кафедра прикладной математики
наименование кафедры

протокол № 7 от "16" 03 2016 г.

Ответственный исполнитель, заведующий кафедрой
Кафедра прикладной математики — подпись — Болодурина И.П.
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
ст. преподаватель кафедры прикладной математики — подпись — Арапова О.С.
должность *подпись* *расшифровка подписи*

–
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
01.03.02 Прикладная математика и информатика — личная подпись — Болодурина И.П.
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
личная подпись — Истомина Т.В.
личная подпись *расшифровка подписи*

Начальник отдела информационных образовательных технологий ЦИТ
личная подпись — Дырдина Е.В.
личная подпись *расшифровка подписи*

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