МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра прикладной математики

УТВЕРЖДАЮ
Декан факультета математики и информационных технологий

С.А. Герасименко
(подпись, расшифровка подписи)

"26" февраля 2016 г.

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«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

Год набора 2016

Рабочая программа дисциплины «*Б.1.В.ОД.17 Математические методы защиты информации***» /сост. С.В. Ханжин - Оренбург: ОГУ, 2016**

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

Содержание

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

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 математич*еских* алгоритмов и методов, лежащих в основе способов защиты информации;

– изучение различных подходов к созданию современных криптосистем;

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

2 Место дисциплины в структуре образовательной программы

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

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

Требования к входным результатам обучения, необходимым для освоения дисциплины

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции
Знать: основы математического анализа и дополнительные главы математического анализа; **Уметь:** применять методы математического анализа на практике; **Владеть:** навыками решения типовых задач математического анализа и задач практической направленности.	ОПК-1 способностью 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 способностью 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:** основными навыками решения задач математического анализа.	ПК-2 способностью понимать, совершенствовать и применять современный математический аппарат

Постреквизиты дисциплины: *Б.2.В.П.1 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: 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 дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины 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:	**98,75**	**98,75**
- самостоятельное изучение разделов (схемы обмена секретными ключами: широкоротой лягушки, Ниджейма-Шредера, Отвэй-Риса; цифровые сертификаты);	*12,75*	*12,75*
- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;	*45*	*45*
- подготовка к лабораторным занятиям;	*21*	*21*
- подготовка к коллоквиумам;	*8*	*8*
- подготовка к рубежному контролю и т.п.)	*12*	*12*
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**Экзамен**	

Разделы дисциплины, 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 хэш-функции 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 дисциплины

1 Введение в криптографию. Краткая история развития криптографических методов. Основные понятия криптографии. Информация как объект защиты. Источники угроз и способы нарушения информационной безопасности. Предмет криптографии и основные определения. Классификация шифров.

2 Стойкость криптографических систем. Математическая модель шифра. 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 дисциплины

5.1 Основная литература

1 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.

2 Горбунов В. А. Математические методы в теории защиты информации [Электронный ресурс] / Горбунов В. А. - Московский государственный горный университет, 2004. Режим доступа: http://biblioclub.ru/index.php?page=book&id=83664/

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.

4 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.

5.3 Периодические издания

1 Математические вопросы криптографии: журнал. - М. : Агентство "Роспечать" (http://www.mathnet.ru/php/journal.phtml?jrnid=mvk&option_lang=rus)

2 Защита информации. Инсайд: журнал. - М. : ВИНИТИ РАН (http://www.inside-zi.ru/pages/about.html)

3 Вестник компьютерных и информационных технологий : журнал. - М. : Агентство "Роспечать", 2017.

4 Информационные технологии : журнал. - М. : Агентство "Роспечать", 2017.

5.4 Интернет-ресурсы

http://www.securitylab.ru/ - информационный портал, оперативно и ежедневно рассказывающий о событиях в области защиты информации, интернет права и новых технологиях.

http://www.osp.ru/ - «Открытые системы» - ведущее российское издательство, выпускающее широкий спектр журналов для профессионалов и активных пользователей в сфере ИТ, цифровых устройств, телекоммуникаций.

http://www.citforum.ru/ - большой архив разнообразной информации по IT-технологиям.

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

1. Операционная система Microsoft Windows

2. Open Office/LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.

3. ПО для работы с файлами PDF Adobe Acrobat 8.0 Pro Russian Version

4. Антивирус Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition на 2 года

5. Свободная интегрированная среда разработки приложений (IDE) на языках программирования Java, Python, PHP, JavaScript, C, C++, Ада[3] и ряда других - NetBeans IDE

6. Технорма/Документ - Технорма / Документ [Электронный ресурс] : [система программных продуктов] / ООО Глосис-Сервис, ФБУ КВФ Интерстандарт. – Версия 1.11.36. – Электрон. дан. и прогр. –[Москва; Санкт-Петербург], [1999–2013]. – Режим доступа осуществляется в локальной сети ОГУ.

6 Материально-техническое обеспечение дисциплины

Вид помещения	Мебель и технические средства обучения
Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения занятий семинарского типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ОГУ
Учебные аудитории для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с подключения к сети «Интернет» и обеспечением доступа в электронную информационно-

Вид помещения	Мебель и технические средства обучения
	образовательную среду ОГУ
Помещения для самостоятельной работы	Комплекты ученической мебели Компьютеры с подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ОГУ

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. Режим доступа: http://artlib.osu.ru/web/books/metod_all/1092_20110804.pdf

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. Режим доступа: http://artlib.osu.ru/web/books/metod_all/2492_20110921.pdf

ЛИСТ
согласования рабочей программы

Направление подготовки: 01.03.02 Прикладная математика и информатика
код и наименование

Профиль: Общий профиль

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

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

Год набора 2016

РЕКОМЕНДОВАНА заседанием кафедры
Кафедра прикладной математики
наименование кафедры

протокол № 7 от "29" января 2016 г.

Ответственный исполнитель, заведующий кафедрой
прикладной математики

наименование кафедры	*подпись*	*расшифровка подписи*
		И.П. Болодурина

Исполнители:

должность	*подпись*	*расшифровка подписи*
преподаватель кафедры ПМ		С.В. Ханжин

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
01.03.02 Прикладная математика и информатика

код наименование	*личная подпись*	*расшифровка подписи*
		И.П. Болодурина

Заведующий отделом комплектования научной библиотеки

личная подпись	*расшифровка подписи*
	Н.Н. Грицай

Уполномоченный по качеству факультета

личная подпись	*расшифровка подписи*
	И.В. Крючкова

Рабочая программа зарегистрирована в ОИОТ ЦИТ
Начальник отдела информационных образовательных технологий ЦИТ

личная подпись	*расшифровка подписи*
	Е.В. Дырдина