

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра алгебры и дискретной математики



УТВЕРЖДАЮ

Декан факультета математики и информационных технологий

С.А. Герасименко

(подпись, расшифровка подписи)

"30" октября 2015 г.

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ДВ.6.2 Основы криптоанализа»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

02.03.01 Математика и компьютерные науки
(код и наименование направления подготовки)

Алгоритмы и приложения компьютерной математики
(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.6.2 Основы криптоанализа» /сост.
А.Н. Благовисная - Оренбург: ОГУ, 2015**

Рабочая программа предназначена студентам очной формы обучения по направлению подготовки 02.03.01 Математика и компьютерные науки

Содержание

1 Цели и задачи освоения дисциплины	
2 Место дисциплины в структуре образовательной программы	
3 Требования к результатам обучения по дисциплине	
4 Структура и содержание дисциплины	
4.1 Структура дисциплины	
4.2 Содержание разделов дисциплины	
4.3 Практические занятия (семинары)	
5 Учебно-методическое обеспечение дисциплины	
5.1 Основная литература	
5.2 Дополнительная литература	
5.3 Периодические издания	
5.4 Интернет-ресурсы	
5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий	
6 Материально-техническое обеспечение дисциплины	
Лист согласования рабочей программы дисциплины	
Дополнения и изменения в рабочей программе дисциплины	
Приложения:	
Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	
Методические указания для обучающихся по освоению дисциплины	

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

- формирование системы знаний об объектах и методах криптоанализа.

Задачи:

- изучение базовых конструкций, используемых при исследовании и раскрытии криптоалгоритмов;

- овладение основными математическими понятиями и идеями, используемыми в методах криптоанализа;

- приобретение навыков решения задач криптоанализа.

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.14 Фундаментальная и компьютерная алгебра, Б.1.Б.16 Дискретная математика, математическая логика и их приложения в информатике и компьютерных науках*

Требования к входным результатам обучения, необходимым для освоения дисциплины

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции
Знать: - содержание ключевых понятий и определений, используемых в теории и практике решения алгебраических задач; - основные понятия теории множеств, способы задания множеств, операции над множествами, их свойства, представление множеств и результатов операций над ними диаграммами Эйлера-Венна; - основы алгебры бинарных отношений, графическое представление бинарных отношений, свойства бинарных отношений, специальные виды бинарных отношений; отношение эквивалентности и отношение порядка, примеры таких отношений; - описание бинарных отношений и операций над ними матрицами и действиями над ними; - определения основных комбинаторных схем и способы подсчета их количества; - виды функций, оценки числа функций, действующих на конечных множествах; - бином Ньютона, полиномиальную формулу, формулу включений-исключений, примеры их применений; - основные понятия теории графов; - задание графов матрицами; - основные алгоритмы на графах: фронта волны, Форда-Беллмана, Дейкстры, поиска максимального потока в сети, метод ветвей и границ; - булевы функции, способы их задания и представления формулами; - свойства булевых операций; - описание контактных схем булевыми многочленами; - примеры полных систем булевых функций, алгоритм проверки системы булевых функций на полноту; - элементарные функции k-значной логики, примеры полных систем функций;	ОПК-1 готовностью использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в будущей профессиональной деятельности

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции
- алгоритм распознавания полноты, представление функций из P_k полиномами, особенности функций k-значной логики; Уметь: - применять прикладное программное обеспечение для решения задач в профессиональной деятельности, науке и образовании; - использовать методы дискретной математики для решения задач соответствующего содержания; Владеть: - навыками пользования прикладного программного обеспечения для решения задач в профессиональной деятельности, науке и образовании; - методами дискретной математики и математической логики для решения теоретических задач теоретической механики в будущей профессиональной деятельности.	
Знать: - принципы построения научного исследования в соответствующей области наук; Уметь: - обосновать актуальность, новизну, теоретическую и практическую значимость собственного исследования, определять методологию исследования, уметь делать выводы из проведенного исследования и определять перспективы дальнейшей работы, анализировать собранный эмпирический материал и делать достоверные выводы, отстаивать собственную научную концепцию в дискуссии, выступать оппонентом и рецензентом по научным работам; Владеть: - навыками работы с источниками научной литературе, владеть логикой научного исследования, научным стилем изложения собственной концепции.	ОПК-4 способностью находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем
Знать: - методы теории групп, колец, полей, векторных пространств; - корректные постановки классических задач; - аппарат алгебры высказываний и границы применимости языка исчисления высказываний для анализа логической выводимости; - аппарат логики предикатов, возможности применения формул логики предикатов для записи математических утверждений, для анализа логической выводимости; Уметь: - сформулировать и доказать основные результаты изучаемых разделов, применять алгебраические методы; - понимать корректность постановок задач; - формулировать утверждения любой природы (не только математической) на языке логических исчислений; - понять поставленную задачу; - формулировать результат; - строго доказать утверждение; - грамотно пользоваться языком предметной области; Владеть: - понятийным аппаратом алгебраической теории в прикладных задачах; - навыками самостоятельного построения алгоритма и его анализа; - методами дискретной математики и математической логики для решения и анализа теоретических и прикладных задач.	ПК-2 способностью математически корректно ставить естественнонаучные задачи, знание постановок классических задач математики
Знать: - новые научные результаты, связанные с алгеброй;	ПК-3 способностью строго доказать утверждение,

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения дисциплины	Компетенции
- метод резолюций как алгоритм проверки логической выводимости и основу логического программирования; - основные концепции теории алгоритмов; - вычислимость по Тьюрингу, по Черчу, по Маркову; Уметь: - использовать современные методы для исследования и решения научных и практических задач; использовать новые знания и применять их в своей профессиональной деятельности; - ориентироваться в постановках задач; - обрабатывать полученные формулы с помощью равносильных преобразований или переходов к логическим следствиям; - анализировать и синтезировать информацию, полученную из любых источников; Владеть: - способностью проводить научные исследования и получать новые научные результаты; - умением самостоятельно увидеть следствия сформулированного результата; - знанием корректных постановок классических задач; - пониманием корректности постановок задач; - пониманием того, что фундаментальное знание является основой компьютерных наук; - выделением главных смысловых аспектов в доказательствах; - владением методами математического и алгоритмического моделирования при анализе и решении прикладных и инженерно-технических проблем.	сформулировать результат, увидеть следствия полученного результата

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: - математические основы криптоанализа; Уметь: - решать задачи алгебры, математической логики, теории чисел, дискретной математики, теории вероятностей и математической статистики, возникающие при раскрытии шифров; Владеть: - навыками интерпретации математических моделей процессов передачи, преобразования информации и раскрытия шифров.	ОПК-1 готовностью использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов,

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
	теоретической механики в будущей профессиональной деятельности
<u>Знать:</u> - основные понятия криптоанализа, - математические основы теории стойких шифров; <u>Уметь:</u> - применять знания из различных разделов математики при решении задач криптоанализа; <u>Владеть:</u> - простейшими математическими методами решения задач криптоанализа.	ПК-1 способностью к определению общих форм и закономерностей отдельной предметной области
<u>Знать:</u> - постановки классических задач криптоанализа; <u>Уметь:</u> - формулировать математические задачи, лежащие в основе создания стойких криптографических конструкций; <u>Владеть:</u> - навыками постановки практических задач криптографии.	ПК-2 способностью математически корректно ставить естественнонаучные задачи, знание постановок классических задач математики

4 Структура и содержание дисциплины

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	144	144
Контактная работа:	40,25	40,25
Лекции (Л)	16	16
Практические занятия (ПЗ)	24	24
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа:	103,75	103,75
- выполнение индивидуального творческого задания (ИТЗ);	54	54
- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;	16	16
- подготовка к практическим занятиям;	24	24
- подготовка к коллоквиумам;	5,5	5,5
- подготовка к рубежному контролю и т.п.)	4,25	4,25
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	зачет	

Разделы дисциплины, изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в предмет	38	4	8		26
2	Основы криптоанализа симметричных криптосистем	60	8	10		42
3	Основы криптоанализа асимметричных криптосистем	46	4	6		36
	Итого:	144	16	24		104
	Всего:	144	16	24		104

4.2 Содержание разделов дисциплины

№ 1 Введение в предмет

Понятие криптоанализа. Соотношение понятий криптология, криптография, криптоанализ. История криптографии и криптоанализа. Этапы развития криптоанализа. Исторические шифры и методы их раскрытия.

Классический и современный криптоанализ. Понятие о методах криптоанализа. Классификации методов криптоанализа.

Математические основы теории стойких шифров. Работы Шеннона. Вероятность и шифры. Критерий Шеннона абсолютной стойкости шифра. Понятие совершенной криптосистемы. Примеры совершенных криптосистем. Вычислительно стойкие системы. Энтропия и извлечение информации из шифртекста. Ложные ключи и расстояние единственности.

№ 2 Основы криптоанализа симметричных криптосистем

Алгоритм Берлекемпа-Мессе и его роль в раскрытии шифров.

Статистический метод криптоанализа блочных шифров. Общая схема метода. Задача метода. Процедура статистической классификации. Алгоритм определения ключа и его параметры: объем, средняя трудоемкость, надежность.

Принципы корреляционного метода криптоанализа для поточных шифров. Статистические модели и расчет параметров алгоритма.

Принципы линейного метода криптоанализа. Алгоритмы Матцуи определения ключа. Линейный криптоанализ шифра DES.

Принципы дифференциального криптоанализа. Основные идеи алгоритма, лежащего в основе дифференциального криптоанализа. Примеры.

Основные идеи алгебраического криптоанализа. Понятие о методах решения систем булевых уравнений.

№ 3 Основы криптоанализа асимметричных криптосистем

Методы, основанные на алгоритмах решения задачи факторизации: методы Полларда, факторизации случайных квадратов, квадратичное решето. Криптоанализ алгоритма RSA.

Методы, основанные на дискретном логарифмировании: метод Полига-Хеллмана, метод «шаг младенца/шаг гиганта».

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1, 2	1	Методы раскрытия традиционных шифров.	4
3, 4	1	Теория информации и исследование криптосистем на стойкость.	4
5	2	Алгоритм Берлекемпа-Месси и его приложения в криптоанализе.	2
6	2	Линейный криптоанализ простых (учебных) шифров.	2
7	2	Дифференциальный криптоанализ простых (учебных) шифров.	2
8, 9	2	Системы булевых уравнений.	4
10, 11	3	Задача факторизации целого числа и методы её решения.	3
11, 12	3	Дискретное логарифмирование в мультипликативной группе кольца вычетов.	3
		Итого:	24

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Винберг, Э.Б. Алгебра [Электронный ресурс] / Э.Б. Винберг. – НЦНМО, 2011. – Режим доступа: http://biblioclub.ru/index.php?page=book_view&book_id=63299
2. Курош, А. Г. Курс высшей алгебры: учеб. для вузов / А. Г. Курош. – 17-е изд., стер. – СПб.: Лань, 2008. – 432 с.
3. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие [Электронный ресурс] / М.А. Иванов, И.В. Чугунков. – М.: МИФИ, 2012. – 400 с. Режим доступа: <http://biblioclub.ru/index.php?page=book&id=231673>
4. Фороузан, Б.А. Математика криптографии и теория шифрования [Электронный ресурс] /Б.А. Фороузан. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 511с. – Режим доступа: http://biblioclub.ru/index.php?page=book_view&book_id=428998

5.2 Дополнительная литература

1. Основы криптографии [Текст]: учеб. пособие для вузов / А. П. Алферов [и др.]. – М.: Гелиос АРВ, 2005. – 480 с.
2. Аграновский, А. В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. – Москва: Солон-Пресс, 2002. – 256 с.
3. Сمارт, Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. – Москва: Техносфера, 2006. – 528 с.

5.3 Периодические издания

1. Журнал «Дискретная математика».
2. Журнал «Дискретный анализ и исследование операций».
3. Журнал «Математические вопросы криптографии».
4. Журнал «Обозрение прикладной и промышленной математики».
5. Журнал «Прикладная дискретная математика».
6. Журнал «Фундаментальная и прикладная математика».

5.4 Интернет-ресурсы

1. http://www.mathnet.ru/index.phtml/?option_lang=rus (общероссийский математический портал Math-Net.Ru — это современная информационная система, предоставляющая российским и зарубежным математикам различные возможности в поиске информации о математической жизни в России)
2. <http://intuit.ru/> (сайт института дистанционного обучения "ИНТУИТ")
3. <http://cryptography.ru/about/> (сайт посвящен вопросам математической криптографии, содержит календарь конференций, семинаров и т. п., которые полностью или частично посвящены вопросам защиты информации, а также актуальные ссылки на сайты данных научных мероприятий)

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

Для выполнения ИТЗ используется любая из доступных на момент выполнения заданий сред программирования, имеющихся в распоряжении лаборатории кафедры. Среда и язык программирования выбираются студентами самостоятельно в соответствии с их индивидуальными учебными возможностями и предпочтениями.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных и практических занятий.

Для чтения лекций при необходимости используется переносной мультимедийный комплект: ноутбук, проектор, экран.

Для получения необходимой информации и самостоятельной работы студентов используются web-ресурсы Интернет и информационная библиотечная система.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.

Методические указания для обучающихся по освоению дисциплины (модуля) могут быть представлены в виде изданных печатным и (или) электронным способом методических разработок со ссылкой на адрес электронного ресурса, а при отсутствии таковых, в виде рекомендаций обучающимся по изучению разделов и тем дисциплины (модуля) с постраничным указанием глав, разделов, параграфов, задач, заданий, тестов и т.п. из рекомендованного списка литературы.

ЛИСТ

согласования рабочей программы

Направление подготовки: 02.03.01 Математика и компьютерные науки

код и наименование

Профиль: Алгоритмы и приложения компьютерной математики

Дисциплина: Б.1.В.ДВ.6.2 Основы криптоанализа

Форма обучения: очная

(очная, очно-заочная, заочная)

Год набора 2015

РЕКОМЕНДОВАНА заседанием кафедры

Кафедра алгебры и дискретной математики

наименование кафедры

протокол № 2 от "26" 09 2015г.

Ответственный исполнитель, заведующий кафедрой

Кафедра алгебры и дискретной математики

наименование кафедры

подпись

О.А. Пихтилькова

расшифровка подписи

Исполнители:

Игорь Петрович

должность

Вла

подпись

Благовоина Н.Н.

расшифровка подписи

должность

подпись

расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по направлению подготовки

02.03.01 Математика и компьютерные науки

код наименование

личная подпись

расшифровка подписи

Заведующий отделом комплектования научной библиотеки

Ирина

личная подпись

Т.В. Истомина

расшифровка подписи

Уполномоченный по качеству факультета

Владимир

личная подпись

Владимир Н.В.

расшифровка подписи

Рабочая программа зарегистрирована в ОИОТ ЦИТ

Начальник отдела информационных образовательных технологий ЦИТ

Е.В. Дырдина

личная подпись

расшифровка подписи

Дополнения и изменения в рабочей программе на 2016 год набора

Направление подготовки: 02.03.01 Математика и компьютерные науки (программа академического бакалавриата)

Профиль: Алгоритмы и приложения компьютерной математики (бакалавр)

Дисциплина: Б.1.В.ДВ.6.2 Основы криптоанализа

Форма обучения: очная

Внесенные изменения на 2016 год набора

УТВЕРЖДАЮ
/ Декан факультета математики и информационных технологий С.А. Герасименко
(подпись, расшифровка подписи)
"26" февраля 2016 г.

В рабочую программу вносятся следующие изменения.

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

- ✓ 1. Винберг, Э.Б. Алгебра [Электронный ресурс] / Э.Б. Винберг. – НЦНМО, 2011. – Режим доступа: http://biblioclub.ru/index.php?page=book_view&book_id=63299
- ✓ 2. Фороузан, Б.А. Математика криптографии и теория шифрования [Электронный ресурс] / Б.А. Фороузан. – М.: Национальный Открытый Университет «ИНТУИТ», 2016, 511с. Режим доступа: http://biblioclub.ru/index.php?page=book_view&book_id=428998
- ✓ 3. Алгебраические структуры и их приложения: учебное пособие [Электронный ресурс] / Л.В. Зяблицева, С.Ю. Корабельщикова, И.В. Кузнецова, С.А. Тихомиров; Министерство образования и науки Российской Федерации, Северный (Арктический) федеральный университет имени М.В. Ломоносова. – Архангельск: САФУ, 2015. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=436142>

5.2 Дополнительная литература

1. Сمارт, Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. – Москва: Техносфера, 2006. – 528 с.
2. Ян, С. Й. Криптоанализ RSA = Cryptanalytic Attacks on RSA [Текст] / С. Й. Ян. – М.: Ижевск: Ин-т компьютер. исслед., 2011. – 287 с.

5.4 Интернет-ресурсы

1. <http://eqworld.ipmnet.ru/indexr.htm> (международный научно-образовательный сайт «Мир математических уравнений», который содержит обширную учебную физико-математическую библиотеку и предназначен для широкого круга ученых, преподавателей вузов, инженеров, аспирантов и студентов в различных областях математики и других наук; все ресурсы сайта являются бесплатными для его пользователей).
2. <http://intuit.ru/> (сайт института дистанционного обучения "ИНТУИТ").
3. <http://cryptography.ru/about/> (сайт посвящен вопросам математической криптографии, содержит календарь конференций, семинаров и т. п., которые полностью или частично

посвящены вопросам защиты информации, а также актуальные ссылки на сайты данных научных мероприятий).

4. http://www.mathnet.ru/index.phtml/?option_lang=rus (общероссийский математический портал, современная информационная система, предоставляющая российским и зарубежным математикам различные возможности в поиске информации о математической жизни в России).

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

1. Операционная система Windows.
2. Офисный пакет Microsoft Office (Word, Excel, Power Point).
3. Среда разработки Visual Studio.

6 Материально-техническое обеспечение дисциплины

Для выполнения заданий предназначен компьютерный класс (ауд. № 1605), подключенный к локальной сети ОГУ и сети Интернет, оснащенный всем необходимым оборудованием.

Для чтения лекций используется переносной мультимедийный комплект: ноутбук, проектор, экран.

Для получения необходимой информации и самостоятельной работы студентов используются web-ресурсы Интернет и информационная библиотечная система.

Рабочая программа пересмотрена и одобрена на заседании кафедры алгебры и дискретной математики 18.02.16, протокол № 2 ✓ С.В.М. / Д.А.Михайлова
(дата, номер протокола заседания кафедры, подпись зав. кафедрой)

СОГЛАСОВАНО:

Заведующий отделом комплектования научной библиотеки

Грицай
личная подпись

Н.Н. Грицай

расшифровка подписи

Уполномоченный по качеству факультета

Крючкова
личная подпись

И.В. Крючкова

расшифровка подписи

Дополнения и изменения в рабочей программе на 2017 год набора

Направление подготовки: 02.03.01 Математика и компьютерные науки (программа академического бакалавриата)

Профиль: Алгоритмы и приложения компьютерной математики (бакалавр)

Дисциплина: Б.1.В.ДВ.6.2 Основы криптоанализа

Форма обучения: очная

Внесенные изменения на 2017 год набора

УТВЕРЖДАЮ
Декан факультета математики и информационных технологий _____ С.А. Герасименко
(подпись, расстановка подписи)

"22" февраля 2017 г.

В рабочую программу вносятся следующие изменения.

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Басалова, Г.В. Основы криптографии: курс лекций [Электронный ресурс] / Г.В. Басалова; Национальный Открытый Университет «ИНТУИТ». – Москва: Интернет-Университет Информационных Технологий, 2011. – 253с. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=233689>
2. Лапонина, О.Р. Криптографические основы безопасности [Электронный ресурс] / О.Р. Лапонина. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 244 с. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=429092>
3. Нестеров, С.А. Основы информационной безопасности: учебное пособие [Электронный ресурс] / С.А. Нестеров; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. – СПб.: Издательство Политехнического университета, 2014. – 322 с. – Режим доступа: <http://biblioclub.ru/index.php?page=book&id=363040>
- ✓ 4. Сمارт, Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. – Москва : Техносфера, 2006. – 528 с.

5.2 Дополнительная литература

1. Алферов А.П. Основы криптографии: учеб. пособие для вузов / А. П. Алферов [и др.]. – М.: Гелиос АРВ, 2005. – 480с.
2. Фороузан, Б.А. Математика криптографии и теория шифрования [Электронный ресурс] / Б.А. Фороузан. – М.: Национальный Открытый Университет «ИНТУИТ», 2016, 511с. – Режим доступа: http://biblioclub.ru/index.php?page=book_view&book_id=428998
3. Ян, С. Й. Криптоанализ RSA = Cryptanalytic Attacks on RSA [Текст] / С. Й. Ян. – М.: Ижевск: Ин-т компьютер. исслед., 2011. – 287 с.

5.4 Интернет-ресурсы

1. <http://eqworld.ipmnet.ru/indexr.htm> (международный научно-образовательный сайт «Мир математических уравнений», который содержит обширную учебную физико-математическую библиотеку и предназначен для широкого круга ученых, преподавателей вузов, инженеров, аспирантов и студентов в различных областях математики и других наук; все ресурсы сайта являются бесплатными для его пользователей).

2. <http://intuit.ru/> (сайт института дистанционного обучения "ИНТУИТ").
3. <http://cryptography.ru/about/> (сайт посвящен вопросам математической криптографии, содержит календарь конференций, семинаров и т. п., которые полностью или частично посвящены вопросам защиты информации, а также актуальные ссылки на сайты данных научных мероприятий).
4. http://www.mathnet.ru/index.phtml?option_lang=rus (общероссийский математический портал, современная информационная система, предоставляющая российским и зарубежным математикам различные возможности в поиске информации о математической жизни в России).
5. <https://arxiv.org/> (крупнейший бесплатный архив электронных публикаций научных статей и их препринтов по физике, математике, астрономии, информатике и биологии).

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

1. Операционная система Windows.
2. Офисный пакет Microsoft Office (Word, Excel, Power Point).
3. Для выполнения ИТЗ используется любая из доступных на момент написания работ сред программирования, имеющихся в распоряжении лаборатории кафедры. Среда и язык программирования выбираются студентами самостоятельно в соответствии с их индивидуальными учебными возможностями и предпочтениями.

6 Материально-техническое обеспечение дисциплины

Для выполнения заданий предназначен компьютерный класс (ауд. № 1605), подключенный к локальной сети ОГУ и сети Интернет, оснащенный всем необходимым оборудованием.

Для чтения лекций используется переносной мультимедийный комплект: ноутбук, проектор, экран.

Для получения необходимой информации и самостоятельной работы студентов используются web-ресурсы Интернет и информационная библиотечная система.

Рабочая программа пересмотрена и одобрена на заседании кафедры алгебры и дискретной математики 24.02.17, протокол № 7 И.В. Крючкова
(дата, номер протокола заседания кафедры, подпись зав. кафедрой)

СОГЛАСОВАНО:

Заведующий отделом комплектования научной библиотеки

И.Н. Грицай
личная подпись

Н.Н. Грицай

расшифровка подписи

Уполномоченный по качеству факультета

И.В. Крючкова
личная подпись

И.В. Крючкова

расшифровка подписи