Минобрнауки России

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

Кафедра алгебры и дискретной математики

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

Год набора 2018

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра алгебры и дискретной математики
наименование кафедры

протокол № 5 от "23" января 2018 г.

Заведующий кафедрой
Кафедра алгебры и дискретной математики _____ О.А. Пихтилькова
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
старший преподаватель _____ А.Н. Благовисная
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
02.03.01 Математика и компьютерные науки _____ О.А. Пихтилькова
код наименование *личная подпись* *расшифровка подписи*

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

Уполномоченный по качеству факультета
_____ И.В. Крючкова
личная подпись *расшифровка подписи*

№ регистрации _____

© Благовисная А.Н., 2018
© ОГУ, 2018

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*

Постреквизиты дисциплины: *Отсутствуют*

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, теоретической механики в будущей профессиональной деятельности
Знать: - *основные понятия криптоанализа,* - *математические основы теории стойких шифров;* **Уметь:**	ПК-1 способностью к определению общих форм и закономерностей отдельной предметной области

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
- применять знания из различных разделов математики при решении задач криптоанализа; **Владеть:** *- простейшими математическими методами решения задач криптоанализа.*	
Знать: *- постановки классических задач криптоанализа;* **Уметь:** *- формулировать математические задачи, лежащие в основе создания стойких криптографических конструкций;* **Владеть:** *- 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: *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к практическим занятиям;* *- подготовка к устным и письменным опросам;* *- подготовка к рубежному контролю)*	**103,75**	**103,75**
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 крипто-систем	60	8	10		42
3	Основы криптоанализа асимметричных крип-тосистем	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-Месси 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. Смарт, Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. – Москва: Техносфера, 2006. – 528 с.

2. Фомичев, В.М. Методы дискретной математики в криптологии [Электронный ресурс] / В.М. Фомичев. – Москва: Диалог-МИФИ, 2010. – 436 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=447668

3. 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&id=428998

5.2 Дополнительная литература

1. Аграновский, А.В. Практическая криптография: алгоритмы и их программирование [Электронный ресурс] / А.В. Аграновский, Р.А. Хади. – Москва: СОЛОН-ПРЕСС, 2009. – 256 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=117663

2. Адаменко, М.В. Основы классической криптологии. Секреты шифров и кодов [Электронный ресурс] / М.В. Адаменко. – Москва: ДМК Пресс, 2012. – 255 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=231860

3. Гультяева, Т.А. Основы теории информации и криптографии : конспект лекций [Электронный ресурс] / Т.А. Гультяева; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. – Новосибирск: НГТУ, 2010. – 88 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=228963

5.3 Периодические издания

1. Прикладная математика и механика: журнал. - М.: Агентство «Роспечать», 2016.

2. Вычислительные технологии: журнал. - М.: Агентство «Роспечать», 2016.

3. Вестник компьютерных и информационных технологий: журнал. – М.: Агентство «Роспечать», 2017-2018.

4. Информационные технологии: журнал. – М.: Агентство «Роспечать», 2017-2018.

5.4 Интернет-ресурсы

1. 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.

2. 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).

3. https://arxiv.org/ – крупнейший бесплатный архив электронных публикаций научных статей и их препринтов по физике, математике, астрономии, информатике и биологии.

4. https://www.gost.ru/portal/gost/ – портал Федерального агентства по техническому регулированию и метрологии.

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

1. Операционная система Microsoft Windows.
2. OpenOffice/LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Бесплатное средство просмотра файлов PDF Adobe Reader.
4. SCOPUS [Электронный ресурс]: реферативная база данных / компания Elsevier. – Режим доступа: https://www.scopus.com/, в локальной сети ОГУ.
5. Web of Science [Электронный ресурс]: реферативная база данных / компания Clarivate Analytics. – Режим доступа: http://apps.webofknowledge.com/, в локальной сети ОГУ.
6. Общероссийский математический портал Math-Net.Ru [Электронный ресурс]: профессиональная база данных для математиков – Режим доступа: http://www.mathnet.ru/index.phtml/?option_lang=rus

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

К рабочей программе прилагаются:

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