Минобрнауки России

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

Кафедра алгебры и дискретной математики

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ДВ.1.1 Математические основы криптографии»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
02.03.02 Фундаментальная информатика и информационные технологии
(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 рассмотрена и утверждена на заседании кафедры

Кафедра алгебры и дискретной математики
наименование кафедры

протокол № 7 от "17" февраля 2016 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*

_____ _____ _____
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
02.03.02 Фундаментальная информатика и информационные технологии
_____ А.Е. Шухман
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 _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

формирование у студентов представлений о роли математики в развитии методов защиты информации, 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 дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б.1.Б.12 Алгебра и теория чисел, Б.1.Б.14 Математическая логика и теория алгоритмов, Б.1.Б.18 Дискретная математика, Б.1.Б.21 Алгоритмы и анализ сложности*

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: *- основные понятия теории групп, колец, полей, используемые в математических методах защиты информации;* **Уметь:** *- решать задачи алгебры, математической логики, теории чисел, дискретной математики, теории вероятностей и математической статистики, возникающие в криптографии;* **Владеть:** *- алгоритмами фундаментальных разделов математики, используемыми в задачах шифрования и преобразования информации.*	ОПК-1 способностью использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с фундаментальной информатикой и информационными технологиями
Знать: *- постановки задач криптографии;* *- основные виды криптосистем;* **Уметь:** *- собирать, обрабатывать и анализировать публикации, содержащие теоретические сведения и практические результаты в области криптографии;* **Владеть:** *- навыками интерпретации математического знания в области защиты информации.*	ОПК-4 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
	безопасности
Знать: *- основные понятия криптографии,* *- математические основы криптологии;* **Уметь:** *- применять знания из различных разделов математики при решении задач криптографии и преобразования информации;* **Владеть:** *- простейшими математическими методами решения задач шифрования и преобразования информации.*	ПК-7 способностью разрабатывать и реализовывать процессы жизненного цикла информационных систем, программного обеспечения, сервисов систем информационных технологий, а также методы и механизмы оценки и анализа функционирования средств и систем информационных технологий
Знать: *- основы построения современных шифров;* **Уметь:** *- оценивать возможности и методы более рационального способа решения задач криптографии;* **Владеть:** *- навыками реализации базовых математических алгоритмов криптографии.*	ПК-8 способностью применять на практике международные и профессиональные стандарты информационных технологий, современные парадигмы и методологии, инструментальные и вычислительные средства

4 Структура и содержание дисциплины

4.1 Структура дисциплины

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

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**34,25**	**34,25**
Лекции (Л)	18	18
Практические занятия (ПЗ)	16	16
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение расчетно-графического задания (РГЗ);* *- написание реферата (Р);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю)*	**73,75**	**73,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 6 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в математические методы защиты информации	10	2	2		6
2	Элементы теории чисел, конечных полей, многочленов над конечными полями	30	0	10		20
3	Основы теоретико-информационной стойкости	10	2	0		8
4	Основы симметричной криптографии	38	8	2		28
5	Основы криптографии с открытым ключом	20	6	2		12
	Итого:	108	18	16		74
	Всего:	108	18	16		74

4.2 Содержание разделов дисциплины

№ 1 Введение в математические методы защиты информации

Предмет и объект защиты информации. Конфиденциальность, аутентичность, целостность. Криптология, криптография, криптоанализ. Исторические этапы развития криптологии и их характеристика. Примеры исторических шифров. Шенноновское описание традиционной криптосистемы. Классификация криптосистем. Группы методов атак на шифры.

№ 2 Элементы теории чисел, конечных полей, многочленов и последовательностей над конечными полями

Алгоритмы и понятия теории чисел, применяемые в криптографии. Элементы теории конечных полей. Строение, свойства конечных полей. Построение конечных полей. Многочлены над конечными полями.

№ 3 Основы теоретико-информационной стойкости

Понятие стойкости криптосистемы. Подходы к определению стойкости. Энтропия, ее свойства. Условная энтропия. Совершенная секретность по Шеннону, шифр Вернама. Ложные ключи и расстояние единственности.

№ 4 Основы симметричной криптографии

Традиционные шифры с симметричным ключом. Шифры подстановки и шифры перестановки. Блочные, поточные шифры. Криптосистемы Фейстеля, DES, ГОСТ 28147-89 и математический аппарат, используемый в них. Распределение симметричных ключей, протоколы Барроуза, Нидхейма-Шредера, Цербер.

№ 5 Основы криптографии с открытым ключом

Идеи криптографии с открытым ключом. Односторонние функции. Математические задачи и проблемы, лежащие в основе асимметричной криптографии. Алгоритм RSA. Электронная цифровая подпись. Понятие и свойства хэш-функции. Электронная подпись как модификация RSA. Система ЭЦП Эль-Гамаля.

4.3 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Роль математики в развитии методов защиты информации. Актуализация знаний курсов алгебры, дискретной математики, необходимых для изучения и понимания математических основ криптографии.	2
2	2	Модулярная арифметика. Основные понятия и методы, используемые в криптографии.	2
3, 4	2	Сравнения, системы сравнений.	4
5, 6	2	Арифметика конечных полей и многочленов над конечными полями.	4
7	4	Задача о разделении секрета.	2
8	5	Математические задачи криптографии с открытым ключом.	2
		Итого:	16

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

5.2 Дополнительная литература

1. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. – СПб.: Лань, 2004. – 176 с.

2. Отрыванкина, Т.М. Алгоритмы компьютерной алгебры: практикум / Т. М. Отрыванкина; М-во образования и науки Рос. Федерации, Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования «Оренбург. гос. ун-т», каф. приклад. математики. – Оренбург: ОГУ, 2007. – 26 с.

5.3 Периодические издания

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

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. https://www.gost.ru/portal/gost/ – портал Федерального агентства по техническому регулированию и метрологии.
3. «Криптографические протоколы» [Электронный ресурс]: онлайн-курс на платформе https://www.lektorium.tv/mooc – «Лекториум» / Разработчик курса: Computer Science клуб при ПОМИ РАН, режим доступа: https://www.lektorium.tv/course/22759

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. Springer [Электронный ресурс]: база данных научных книг, журналов, справочных материалов / компания Springer Customer Service Center GmbH . – Режим доступа: https://link.springer.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.

Дополнения и изменения к рабочей программе дисциплины (модуля)

«Б.1.В.ДВ.1.1 Математические основы криптографии»

Направление подготовки (специальность): 02.03.02 Фундаментальная информатика и информационные технологии
код и наименование

Направленность (профиль), специализация: Общий профиль

Год набора 2016
Форма обучения очная

Дополнения и изменения к рабочей программе на 2018/2019 учебный год рассмотрены и утверждены на заседании кафедры

Кафедра алгебры и дискретной математики
наименование кафедры

протокол № 1 от "27" августа 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
02.03.02 Фундаментальная информатика и информационные технологии
_____ А.Е. Шухман

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

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

В рабочую программу вносятся следующие дополнения и изменения:

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

5.3 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 – 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. «Криптографические протоколы» [Электронный ресурс]: онлайн-курс на платформе https://www.lektorium.tv/mooc – «Лекториум» / Разработчик курса: Computer Science клуб при ПОМИ РАН, режим доступа: https://www.lektorium.tv/course/22759