

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Алтайский государственный педагогический университет»
(ФГБОУ ВО «АлтГПУ»)

УТВЕРЖДАЮ
проректор по учебной работе и
международной деятельности

ОСНОВЫ КРИПТОГРАФИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Код, направление подготовки
(специальности):
01.03.04 Прикладная математика

Профиль (направленность):

Математическое моделирование и
обработка данных

Квалификация:
бакалавр

Форма обучения:
очная

Общая трудоемкость (час / з.ед.):
72 / 2

Форма контроля в семестре, в том
числе курсовая работа
зачет 2

Программу составил:

Мальцев Ю.Н., профессор кафедры алгебры и методики обучения математике, доктор физ.-мат. наук, профессор

Программа подготовлена на основании учебного плана в составе ОПОП

01.03.04 Прикладная математика: Математическое моделирование и обработка данных утвержденного Ученым советом ФГБОУ ВО «АлтГПУ» от «26» марта 2020 г., протокол № 6.

Программа утверждена:

на заседании кафедры алгебры и методики обучения математике Протокол от «25» февраля 2020 г. № 6

Срок действия программы: 2020 – 2024 гг.

Зав. кафедрой: доцент Исаев И.М., канд. физ.-мат. наук, доцент

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Целью дисциплины является изучение основ криптографии и элементов теории кодирования - важных разделов современной математики. В последние десятилетия важное значение приобрели вопросы, связанные с сохранением и передачей информации. Возникающие при этом задачи решает криптография – наука о методах преобразования информации в целях её защиты, а также теория кодирования, изучающая вопросы надежной передачи информации по каналу, находящемуся под воздействием «шума».

При изучении этих основ планируется использовать методы теории чисел и элементов абстрактной алгебры. Тем самым, планируется показать студентам применение абстрактной алгебры и теории чисел к важным прикладным задачам.

Задачи дисциплины:

- изложить элементы теории групп и теории сравнений;
- изложить конструкцию фактор-кольца коммутативного кольца, доказать существование конечных полей и изучить их строение;
- привести классические примеры шифров (Виженера, Хилла, Тритемиуса и др.);
- изложить криптосистему RSA, криптосистему без передачи ключей;
- доказать неравенство Крафта, изложить оптимальное кодирование Хаффмена и кодирование Фано;
- изложить схемы передачи закодированного сообщения и примеров кодов, исправляющих одну ошибку (код «проверки на четность» и код Хэмминга).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Требования к предварительной подготовке обучающегося:

вводный курс математики;
линейная алгебра и аналитическая геометрия.

2.2. Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

защита информации в БД;
производственная практика: научно-исследовательская работа;
производственная практика: преддипломная практика;
выполнение и защита выпускной квалификационной работы.

3. КОМПЕТЕНЦИИ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-6. Способен разрабатывать политику информационной безопасности на уровне БД.

4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ

Индикаторы достижения компетенции	Результаты обучения по дисциплине
ИПК - 6.1. Анализирует возможные угрозы для безопасности данных	Знает: теорию сравнений, теорему Лагранжа, метод построения конечного поля порядка; примеры классических шифров (Цезаря, Хилла, Тритемиуса и др.); RSA – криптосистему, криптосистему без передачи

ИПК - 6.2. Осуществляет выбор основных средств поддержки информационной безопасности на уровне БД	ключей; кодирование Фано и оптимальное кодирование Хаффмена. Умеет: решать системы линейных уравнений кольца классов вычетов и в конечном поле, находить циклический <u>порождающий</u> конечного поля, пользоваться теоремой Ферма – Эйлера; шифровать и дешифровать текст с помощью классических шифров; использовать RSA- криптосистему (для небольших простых чисел p, q); использовать криптосистему без передачи ключей (для небольших простых чисел p); кодировать двоичным кодом Фано; кодировать двоичным кодом Хаффмена). Владеет: методами теории чисел и аппаратом абстрактной алгебры для решения поставленных прикладных задач; теорией и практикой применения RSA – криптосистемы; оптимальным кодированием Хаффмена.
---	---

5. ОБЪЕМ ДИСЦИПЛИНЫ И РАСПРЕДЕЛЕНИЕ ВИДОВ УЧЕБНОЙ РАБОТЫ ПО СЕМЕСТРАМ

Профиль (направленность)	Семе стр	Всего часов	Количество часов по видам учебной работы				
			Лек.	Практ.	КСР	Сам. работа	Зачет
Математическое моделирование и обработка данных	2	72	14	14	2	42	
Итого		72	14	14	2	42	

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№	Раздел / Тема	Содержание	Лекц.	Практ.	Сам. работа
Семестр 2					
1.	Элементы алгебры и теории чисел	Определение группы, кольца. Теорема Лагранжа, теорема Коши. Кольцо классов вычетов по модулю p , теорема Ферма -Эйлера. Элементы теории сравнений. Алгоритм решения уравнений 1-й степени в кольце Z_p . Фактор-кольца коммутативных колец. Поля. Существование поля порядка p . Циклическость мультипликативной группы конечного поля.	4	4	14
2.	Элементы криптографии	Введение, история. Примеры шифров: квадрат Полибия, шифр Цезаря	4	4	12

		(дешифровка подстановочных шифров), перестановочный шифр, шифры Хилла, Тритемиуса, Виженера. Криптосистема RSA, криптосистема без передачи ключей.			
3.	Элементы теории кодирования	Основные определения. Неравенство Крафта. Кодирование Фано и оптимальное кодирование Хаффмена. Модель передачи закодированного сообщения. Примеры кодов: код «проверки на четность», код Хэмминга.	6	6	18
	Зачет				
	Итого		14	14	44

7. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ:

Курсовая работа не предусмотрена.

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ: Приложение 1.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

9.1. Рекомендуемая литература: Приложение 2.

9.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»:

Основы криптографии. //Национальный открытый университет «Интуит» [Электронный ресурс]. – Режим доступа: <https://www.intuit.ru/studies/courses/691/547/info-свободный>.

9.3. Перечень программного обеспечения:

1. Пакет Microsoft Office.
2. Пакет LibreOffice.
3. Пакет OpenOffice.org.
4. Операционная система семейства Windows.
5. Операционная система Linux.
6. Интернет браузер.
7. Программа для просмотра электронных документов формата pdf, djvu.

9.4. Перечень профессиональных баз данных и информационных справочных систем: Приложение 3

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

1. Оборудованные учебные аудитории, в том числе с использованием видеопроектора и подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Университета.

2. Аудитории для самостоятельной работы с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Университета.

3. Компьютерный класс с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Университета.

11. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ:

Студенту следует помнить, что дисциплина «Введение в криптографию» предусматривает обязательное посещение студентом лекций и практических занятий. Она реализуется через систему домашних работ, систему рефератов и индивидуальных работ. Самостоятельная работа студентов заключается в выполнении домашних заданий с целью подготовки к практическим занятиям (см. планы практических занятий) и подготовке рефератов. Контроль над самостоятельной работой студентов и проверка их знаний проводится в виде экзамена.

Дисциплина «Введение в криптографию» призвана сформировать у студентов целостное представление об основных понятиях курса «Введение в криптографию», обеспечить усвоение методов решения задач и доказательства теорем. Важной составной частью учебного процесса в вузе являются практические занятия. Они помогают студентам глубже усвоить учебный материал, приобрести навыки творческой работы с основной и дополнительной литературой и лекционным материалом. Практическое занятие представляет собой форму организации учебного процесса, в ходе которого студент должен приобрести новые учебные знания, их систематизировать и концептуализировать; оперировать базовыми понятиями и теоретическими конструкциями учебной дисциплины.

Целью практических занятий является приобретение студентами новых знаний, умений и навыков, необходимых для профессиональной деятельности, развитие у них естественно-научного мышления и интеллектуальных способностей как средства индивидуального освоения учебной дисциплины. Все это требует тщательной подготовки к практическим занятиям. При подготовке к практическим занятиям следует использовать всю рекомендованную литературу, размещенную на бумажных или электронных носителях. Готовясь к занятию, надо прочитать рекомендованную литературу и составить простые планы прочитанных текстов, а также решить предложенные задачи.

Особое внимание следует уделять связям между основными понятиями, рассматриваемыми в теме. Планы практических занятий, их тематика, рекомендуемая литература, цель и задачи ее изучения сообщаются преподавателем на вводных занятиях или в методических указаниях по данной дисциплине. На занятии студенты должны быть готовыми к выступлению по всем поставленным в плане вопросам, проявлять максимальную активность при их рассмотрении. Выступление студентов на занятии должно быть правильным, полным и аргументированным. Необходимо, чтобы выступление не сводилось к репродуктивному уровню (простому воспроизведению текста), не допускается и простое чтение конспекта. Важно, чтобы выступающий проявлял собственное отношение к тому, о чем он говорит, высказывал свое личное мнение, понимание, обосновывал его и мог сделать правильные выводы из сказанного. При этом студент может обращаться к записям конспекта лекций, непосредственно к первоисточникам, использовать знание математической литературы, факты из дополнительных источников. Вокруг такого выступления могут разгореться споры, дискуссии, к участию в которых должен стремиться каждый. Практическое занятие является важнейшей формой усвоения знаний. Важным фактором результативности данного вида занятий, его высокой эффективности является процесс подготовки. Прежде всего, студенты должны уяснить предложенный план занятия, осмыслить вынесенные для обсуждения вопросы, место каждого из вопросов в раскрытии темы занятия. Подготовка активизирует работу студента с книгой, требует обращения к литературе, учит рассуждать.

В процессе подготовки к семинару закрепляются и уточняются уже известные и осваиваются новые утверждения и факты. Сталкиваясь в ходе подготовки с недостаточно понятными моментами темы, студенты находят ответы самостоятельно или фиксируют свои вопросы для постановки и уяснения их на самом занятии. В ходе занятия студент учится публично выступать, видеть реакцию слушателей, логично, ясно, четко, грамотным математическим языком излагать мысли, приводить доводы, формулировать аргументы в

защиту своей позиции. В ходе семинара каждый студент опирается на свои конспекты, сделанные на лекции, собственные выписки из учебников, первоисточников, статей, другой математической литературы. Практическое занятие – эффективная форма закрепления полученных по обсуждаемой проблеме знаний, видения этой проблемы в целом, осознания ее соотнесенности с другими темами. Подготовку к семинарскому занятию следует начинать с ознакомления с соответствующим разделом учебника и лекции. Во время чтения лекции необходимо составить краткий план-конспект будущего ответа на практическом занятии, для чего целесообразно использовать специальную тетрадь для практических занятий. План ответа не должен представлять собой необработанную компиляцию учебной литературы; лучше, если он будет составлен в виде кратких, легко запоминающихся утверждений, которыми студент может пользоваться при ответе. В подготовке к практическим занятиям большое значение имеет рекомендованная лектором и ведущим практические занятия преподавателем учебная и научная литература. Различные вопросы по-разному раскрыты в учебниках, поэтому целесообразно иметь студенту один, два учебника (разных авторов), а также по отдельным вопросам обращаться и к иной учебной литературе. Залогом высоких учебных результатов студента является подготовка к практическим занятиям и работа на них на протяжении.

Методические рекомендации обучающимся с ограниченными возможностями здоровья (ОВЗ).

Специальные условия обучения в ФГБОУ ВО «АлтГПУ» определены «Положением об инклюзивном образовании» (утверждено приказом ректора от 25.12.2015 г. № 312/1п). Данным положением предусмотрено заполнение студентом при зачислении в ФГБОУ ВО «АлтГПУ» анкеты «Определение потребностей обучающихся в создании специальных условий обучения», в которой указываются потребности лица в организации доступной социально-образовательной среды и помощи в освоении образовательной программы.

Для лиц с ОВЗ, по их просьбе, могут быть адаптированы как сами задания, так и формы их выполнения по дисциплине. Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации по дисциплине в соответствии с потребностями студента, отмеченными в анкете, могут быть обеспечены специальные условия. При необходимости лицам с ОВЗ может быть предоставлено дополнительное время для подготовки к ответу на экзамене, выполнения заданий по самостоятельной работе.

Студент с ограниченными возможностями здоровья обязан:

- выполнять требования программы дисциплины;
- сообщить преподавателю о наличии у него ограниченных возможностей здоровья и необходимости создания для него специальных условий.

Список литературы

Код: 01.03.04

Направление: Прикладная математика: Математическое моделирование и обработка данных

Программа: ПМ01.03.04_2020.plx

Дисциплина: Основы криптографии

Кафедра: Математики и методики обучения математике

Тип	Книга	Количество
Основная	Басалова Г. В. Основы криптографии : учебное пособие / Г. В. Басалова. — Москва: ИНТУИТ; Саратов: Ай Пи Ар Медиа, 2020. — 282 с. — URL: http://www.iprbookshop.ru/89455.html . — Текст (визуальный) : электронный.	9999
Основная	Исаев И. М. Элементы абстрактной и компьютерной алгебры [Электронный ресурс] : учебное пособие / И. М. Исаев, А. С. Кузьмина ; Алтайский государственный педагогический университет. — Барнаул: АлтГПУ, 2015. — 104 с. — URL: http://library.altspu.ru/dc/pdf/kuzmina.pdf .	9999
Дополнительная	Введение в теоретико-числовые методы криптографии: учебное пособие для студентов вузов / М. М. Глухов [и др.]. — Санкт-Петербург; Москва; Краснодар: Лань, 2011. — 394 с.	40
Дополнительная	Танова Э. В. Введение в криптографию: как защитить свое письмо от любопытных: учебное пособие [для 10-11 классов] / Э. В. Танова. — Москва: БИНОМ. Лаборатория знаний, 2007. — 79 с.: ил.	17

Согласовано:

Преподаватель _____ (подпись, И.О. Фамилия)

Заведующий кафедрой _____ (подпись, И.О. Фамилия)

Отдел книгообеспеченности НПБ АлтГПУ _____ (подпись, И.О. Фамилия)