МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет математики и компьютерных наук

УТВЕРЖДАЮ:
Проректор по учебной работе, качеству образования – первый проректор
_____ Хагуров Т.А.
подпись
«27» мая 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ Б1.В.02 ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ КРИПТОГРАФИИ

Специальность 01.05.01 Фундаментальные математика и механика

Направленность (профиль) Фундаментальная математика и ее приложения, Вычислительная механика и компьютерный инжиниринг

Форма обучения Очная

Квалификация Математик. Механик. Преподаватель

Краснодар 2022

Рабочая программа дисциплины Теоретико-числовые методы криптографии составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки / специальности 01.05.01 Фундаментальные математика и механика

Программу составил(и):
А.В. Рожков, профессор, д.ф.-м.н., профессор

Рабочая программа дисциплины Теоретико-числовые методы криптографии утверждена на заседании кафедры функционального анализа и алгебры протокол № 9 «13» апреля 2022 г.
Заведующий кафедрой функционального анализа и алгебры
Барсукова В.Ю.

Утверждена на заседании учебно-методической комиссии факультета/института математики и компьютерных наук протокол № 5 «05» мая 2022 г.

Председатель УМК факультета/института Шмалько С.П.

Рецензенты:
Ганижева Л.Л. к.т.н., доцент кафедры наземного транспорта и механики КубГТУ
Лазарев В.А.. д.п.н., проф. кафедры теории функций КубГУ

Цели и задачи изучения дисциплины

1.1 Цель дисциплины

Цель освоения дисциплины – рассматривает задачи защиты информации математическими методами. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

1.2 Задачи дисциплины

Задачи освоения дисциплины «Теоретико-числовые методы криптографии»: получение базовых теоретических и исторических сведений о структуре и алгоритмах функционирования криптоалгоритмов. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли защиты информации в структуре информатизации и математических методов построения защищенных информационных систем.

Изучение теоретических основ предмета: Числовые функции, основные теоремы о евклидовых кольцах, алгоритмы решения линейных и квадратных уравнений в конечных полях, кольцах вычетов, алгоритмы нахождения наибольших общих делителей, алгоритмов проверки простоты чисел;

системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; алгебраических и теоретико-числовых принципов синтеза и анализа шифров; математических методов, используемых в криптоанализе и криптографии.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Теоретико-числовые методы криптографии» относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана и является одной из основных дисциплин в освоении математических знаний. Дисциплина «Теоретико-числовые методы криптографии» читается в 7 семестре Б1.В.02.

Знания, полученные в этом курсе, могут быть использованы в ходе практик, в других компьютерных дисциплинах. Слушатели должны владеть знаниями в рамках программы курсов «Алгебра», «Математический анализ», «Технология программирования и работа на электронно-вычислительной машине (ЭВМ)».

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ПК-1. Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики	
ПК-1.1 Знает основные понятия, идеи и методы фундаментальных математических дисциплин для решения базовых задач ПК-1.2 Умеет передавать результаты проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области ПК-1.3 Самостоятельно и корректно решает стандартные задачи фундаментальной и прикладной математики	Знать: о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности государства; о методологии создания систем защиты информации; Уметь: выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; Владеть: анализом информационной инфраструктуры государства; формальной постановкой и решением задачи обеспечения информационной безопасности компьютерных систем.

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ПК-1.4 Имеет навыки решения математических задач, соответствующих квалификации, возникающих при проведении научных и прикладных исследований	
ПК-2 Способен активно участвовать в исследовании новых математических моделей в естественных науках	
ПК-2.1 Умеет использовать математические модели и применять численные методы решения задач в естественных науках ПК-2.2 Разрабатывает новые математические модели в естественных науках ПК-2.3 Владеет навыками математической обработки результатов экспериментальных исследований составленных математических моделей	Знать: об основных задачах и понятиях криптографии; о классификации шифров; о методах криптографического синтеза и анализа; о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи; о нормативно-правовых основах защиты информации; Уметь использовать: типовые шифры замены и перестановки; принципы построения современных шифрсистем: основные математические методы, используемые в анализе типовых криптографических алгоритмов. Владеть: криптографической терминологией; навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шифров: навыками математического моделирования в криптографии

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2 Структура и содержание дисциплины

2.1 Распределение трудоемкости дисциплины по видам работ

Общая трудоемкость дисциплины «Теоретико-числовые методы криптографии» составляет 2 зачетные единицы (72 часов, из них – 36,2 часа контактной работы (16 лекций, 18 часов лабораторных занятий, 2 часа КСР, 0,2 часов ИКР); 35,8 часа самостоятельной работы).

Вид учебной работы	Всего часов	Семестры
		7-й
Аудиторные занятия (всего)	72	72
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа (семинары, практические занятия)	18	18
Иная контактная работа:		

Контроль самостоятельной работы (КСР)		2	2
Промежуточная аттестация (ИКР)		0,2	0,2
Самостоятельная работа, в том числе		35.8	35.8
Проработка учебного (теоретического) материала		11	11
Выполнение домашних заданий (решение задач)		20	20
Подготовка к текущему контролю		4,8	4,8
Контроль:			
Подготовка к экзамену			
Общая трудоемкость	**час.**	**72**	**72**
	в том числе контактная работа	**36.2**	**36.2**
	зач. ед	**2**	**2**

2.2 Структура дисциплины:

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов			
		Всего	Аудиторная работа		Самостоятельная работа
			Л	ЛЗ	
1	**2**	**3**	**4**	**5**	**6**
1	Модели шифров.	15	4	4	7
2	Мультипликативные функции.	16	4	4	8
3	Табличное и модульное гаммирование.	18	4	4	10
4	Построение больших простых чисел.	20.8	4	6	10,8
	Итого:		16	18	35,8

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа

№ п/п	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Модели шифров.	Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам	Проверка домашнего задания, реферативный доклад.
2	Мультипликативные функции.	Функция Эйлера и Мебиуса. Группы обратимых элементов в кольцах. Структура мультипликативной группы кольца вычетов. Обратимые элементы. Примитивные элементы.	Проверка домашнего задания, реферативный доклад.
3	Табличное и модульное гаммирование.	Случайные и псевдослучайные гаммы. Регистры сдвига с обратной связью Криптограммы, полученные при повторном использовании	Проверка домашнего задания, реферативный доклад.

		ключа. Анализ криптограмм, полученных применением неравновероятной гаммы.	
4	Построение больших простых чисел.	Алгоритмы проверки на простоту. Эллиптические кривые над конечными полями и алгоритмы вычисления на них. Электронная подпись.	экзамен

2.3.2 Занятия семинарского типа не предусмотрены

2.3.3 Лабораторные занятия.

№ п/п	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Модели шифров.	Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам	Проверка домашнего задания, реферативный доклад.
2	Мультипликативные функции.	Функция Эйлера и Мебиуса. Группы обратимых элементов в кольцах. Структура мультипликативной группы кольца вычетов. Обратимые элементы. Примитивные элементы.	Проверка домашнего задания, реферативный доклад.
3	Табличное и модульное гаммирование.	Случайные и псевдослучайные гаммы. Регистры сдвига с обратной связью Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы.	Проверка домашнего задания, реферативный доклад.
4	Построение больших простых чисел.	Алгоритмы проверки на простоту. Эллиптические кривые над конечными полями и алгоритмы вычисления на них. Электронная подпись.	Зачет, курсовая работа

2.3.4 Примерная тематика курсовых работ (проектов)
не предусмотрена

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

1. Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

2. Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

3. Методические указания по использованию интерактивных методов обучения. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5т от 05 мая 2022 г.

4. Методические указания по подготовке эссе, рефератов, курсовых работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5т от 05 мая 2022 г.

5. Методические указания по выполнению лабораторных работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

6. Методические указания по выполнению расчетно-графических заданий. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Таблица 4 – типовые задания для самоподготовки студентов

Перечень компетенций	Л	ЛЗ	Формы контроля
ОПК-1		+	Самостоятельная работа с доступом к источникам информации, отчет по реферату, зачет
ОПК-1 ПК-5	+		Обзор литературы, зачет
ОПК-1		+	Отчеты по практическим заданиям, реферативный доклад
ОПК-1	+	+	Дискуссия, зачет
ОПК-1	+		Реферативный доклад, зачет
ПК-5	+	+	Собеседование, зачет
ПК-5	+	+	Реферативный доклад, консультация
ОПК-1 ПК-5	+		Презентация, зачет

3. Образовательные технологии: Активные и интерактивные формы лекционных занятий, практических занятий, контрольных работ, тестовых заданий, типовых расчетов, докладов, сдача экзамена.

Вид занятия	**Используемые интерактивные образовательные технологии**
ЛЗ	Мультимедийная лекция-беседа: «Рекурсия. Быстрый алгоритм возведения в степень»
ПЗ	Дискуссия на тему: «Использование элементов алгебры в криптографии» с докладами-презентациями
ПЗ	Круглый стол на тему: «Теория чисел – алгоритмы проверки на простоту» с докладами-презентациями

Семестр	**Вид занятия**	**Используемые интерактивные образовательные технологии**	**Количество часов**
3	Лекционные занятия	Тема Алгоритм проверки на простоту.	2
		Тема Алгоритм тестирования. Тест Эдуарда Люка	2
		Тема Тесты псевдопростоты.	4

		Тема Числа Кармайкла. Разложение чисел на простые числа.	2
	Лабораторные занятия	Дискуссия на тему: «. Метод локализации. Алгоритм пополнения.» с докладами-презентациями	2
		Круглый стол на тему: «Алгоритмы факторизации целых чисел.» с докладами-презентациями	2
		Мозговой штурм» («мозговая атака»): Базисы Грёбнера.	4
		Компьютерная симуляция: Решение системы полиномиальных уравнений	2
Итого:			18

Вид занятия (Л, ЛЗ)	**Используемые интерактивные образовательные технологии**	**Количество часов**
Л	«Ручные и машинные шифры» (раздел 1) − *лекция в виде презентации.*	2
ЛЗ	«Анализ криптограмм» (раздел 3) - *занятие в виде презентации.*	2
Л	«Эллиптические кривые над конечными полями» (раздел) *– лекция в виде презентации.*	2

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций со студентом при помощи электронной информационно-образовательной среды ВУЗа.

В рамках реализации компетентностного подхода предусматриваются следующие основные виды активных и интерактивных форм проведения учебных занятий, которые указываются в рабочих программах дисциплин, профессиональных модулей, практик в рамках которых они реализуются:

– применение электронных образовательных ресурсов;

– компьютерные симуляции;

– деловые и ролевые игры;

– индивидуальные и групповые проекты;

– анализ производственных ситуаций;

– разбор конкретных ситуаций;

Проблемная лекция. Преподаватель в начале и по ходу изложения учебного материала создает проблемные ситуации и вовлекает студентов в их анализ. Разрешая противоречия, заложенные в проблемных ситуациях, обучаемые самостоятельно могут прийти к тем выводам, которые преподаватель должен сообщить в качестве новых знаний.

Лекция вдвоем. Представляет собой работу двух преподавателей, читающих лекцию по одной и той же теме и взаимодействующих как между собой, так и с аудиторией. В диалоге преподавателей и аудитории осуществляется постановка проблемы и анализ проблемной ситуации, выдвижение гипотез, их опровержение или доказательство, разрешение возникающих противоречий и поиск решений.

Лекция-визуализация. В данном типе лекции передача преподавателем информации студентам сопровождается показом различных рисунков, структурно-логических схем, опорных конспектов, диаграмм и т. п. с помощью ТСО и ЭВМ (слайды, видеозапись, дисплеи, интерактивная доска и т. д.).

Лекция-диалог и лекция-дискуссия. Содержание подается через серию вопросов, на которые студенты должны отвечать непосредственно в ходе лекции.

Лекция с разбором конкретных ситуаций по форме организации похожа на лекцию-дискуссию, в которой вопросы для обсуждения заменены конкретной ситуацией, предлагаемой обучающимся для анализа в устной или письменной форме. Обсуждение конкретной ситуации может служить прелюдией к дальнейшей традиционной лекции и использоваться для акцентирования внимания аудитории на изучаемом материале.

Дискуссия – это публичное обсуждение или свободный вербальный обмен знаниями, суждениями, идеями или мнениями по поводу какого-либо спорного вопроса, проблемы. Ее существенными чертами являются сочетание взаимодополняющего диалога и обсуждения-спора, столкновение различных точек зрения, позиций.

Коллоквиум – вид учебных занятий, представляющий собой обсуждение под руководством преподавателя широкого круга проблем, например, относительно самостоятельного большого раздела лекционного курса или отдельных частей какой-либо конкретной темы. Он может включать вопросы и темы из изучаемой дисциплины, не включенные в темы практических и семинарских занятий. Коллоквиум может проводиться в форме индивидуальной беседы преподавателя со студентом или как групповое обсуждение.

Разбор конкретных ситуаций (кейс-метод). Метод кейсов представляет собой изучение, анализ и принятие решений по ситуации, которая возникла в результате происшедших событий, реальных ситуаций или может возникнуть при определенных обстоятельствах в конкретной организации в тот или иной момент времени.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ПК-1.1 Способен решать актуальные и важные задачи фундаментальной и прикладной математики	Знать: о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности государства; о методологии создания систем защиты информации;	Контрольная работа №1- Значение информационной безопасности для субъектов информационных отношений.	1.Сущность и понятие информационной безопасности. 2.Значение информационной безопасности для субъектов информационных отношений. 3.Место информационной безопасности в системе национальной безопасности.
2	ПК-1.2 Демонстрирует навыки программирования подготовленных алгоритмов решения вычислительных задач, разработки структуры и программирования реляционных баз	Уметь: выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;	Вопросы для устного (письменного) опроса по теме, разделу Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.	4.Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности. 5. Источники, виды и методы дестабилизирующего воздействия

	данных, а также экспертных систем			на защищаемую информацию. 6. Каналы и методы несанкционированного доступа к конфиденциальной информации.
3	ПК-2.1 Демонстрирует навыки логичного и последовательного изложения материала научного исследования в устной и письменной форме	Знать: основные педагогические методы и идеи	Тест по теме, разделу Круглый стол, Кейс Защита персональных данных	7 Методы правовой защиты информации. 8. Правовые основы защиты государственной, коммерческой, служебной, профессиональной и личной тайны. 9. Защита персональных данных. 10.Правовая основа допуска и доступа персонала к защищаемым сведениям.
4	ПК-2.2 Конструирует предметное содержание и адаптирует его в соответствии с особенностями целевой аудитории	Владеть: анализом информационной инфраструктуры государства; формальной постановкой и решением задачи обеспечения информационной безопасности компьютерных систем.	Индивидуальная работа Система правовой ответственности за утечку информации и утрату носителей информации.	11. Система правовой ответственности за утечку информации и утрату носителей информации. 12. Правовые основы деятельности подразделений защиты информации

Контрольная работа

Вариант 1

Применения и разработки шифровальных средств ……

Вариант 2

Применения электронной подписи.…….

Вариант 3

Модели, стратегии и системы обеспечения информационной безопасности.

Вариант 4

Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

Вариант 5

Компьютерная система как объект информационной безопасности.

Список теоретических вопросов (для самостоятельных работ и зачета)

1. Защита персональных данных.
2. История криптографии; классические шифры, шифры гаммирования.
3. Принципы построения криптографических алгоритмов.
4. Различие между программными и аппаратными реализациями шифров.
5. Функция Эйлера и Мебиуса.
6. Группы обратимых элементов в кольцах.
7. Структура мультипликативной группы кольца вычетов.
8. Обратимые элементы.
9. Примитивные элементы.
10. Особенности использования вычислительной техники в криптографии вопросы организации сетей засекреченной связи.

11. Криптографические хеш-функции.
12. Электронная подпись.
13. Криптографические протоколы.
14. Предмет и задачи программно-аппаратной защиты информации.
15. Идентификация субъекта, понятие протокола идентификации.
16. Пароли и ключи, организация хранения ключей.

Список типовых практических заданий (для лабораторных занятий и зачета)

1. Применения и разработки шифровальных средств.
2. Применения электронной подписи.
3. Криптографические методы обеспечения информационной безопасности.
4. Алгоритмы проверки на простоту.
5. Эллиптические кривые над конечными полями.
6. Алгоритмы вычисления в конечных полях.
7. Электронная подпись по схеме Эль Гамаля.
8. Электронная подпись на основе RSA.
9. Случайные и псевдослучайные гаммы.
10. Регистры сдвига с обратной связью.
11. Схема Файстеля.
12. Подсчет количества точек на эллиптической кривой.
13. Операция сложения на эллиптической кривой.
14. Схема алгоритма RSA.
15. Криптограммы, полученные при повторном использовании ключа.
16. Анализ криптограмм, полученных применением неравновероятной гаммы.
17. Стандарт РФ. ГОСТ 28147 – 89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
18. Стандарт РФ. ГОСТ Р 34.11–2012. Информационная технология. Криптографическая защита информации. Функция хэширования.
19. Стандарт РФ. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной

Примерные практические - лабораторные работы

1. Нахождение примитивного элемента конечного поля.
2. Построение таблицы логарифма Якоби конечного поля.
3. Решение систем линейных уравнений над конечным полем.
4. Алгоритм быстрого возведения в степень.
5. Нахождение обратных элементов в конечном поле.
6. Расширения конечных полей.
7. Алгоритм шифрования AES: структура поля $GF(2^8)$, нахождение обратных элементов.
8. Алгоритм шифрования AES: фактор кольцо $GF(2^8)[x]/\text{ид}((x+1)^4)$, преобразование столбцов.

9. Алгоритм шифрования AES: Линейное преобразование, собственные значения матрицы $A=\begin{pmatrix}1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\\1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\end{pmatrix}$.
10. Алгоритм RSA – выбор секретных параметров p,q,d , вычисление открытого ключа n,e.
11. Рюкзачная система шифрования. Быстрорастущий вектор. Сокрытие быстрорастущего вектора после преобразования умножения по модулю.
12. Решение систем линейных уравнений по разным модулям.
13. Решение систем линейных уравнений в кольце целых чисел.
14. Линейный регистр сдвига с обратной связью
    $S_{n+k}=a_{k-1}S_{n+k-1}+a_{k-2}S_{n+k-2}+...+a_1S_{n+1}+a_0S_n+a, n=0,1,2,...$
15. Характеристический многочлен регистра сдвига
    $x^k=a_{k-1}x^{k-1}+a_{k-2}x^{k-2}+...+a_1x+a_0$
16. Нахождение явного вида значений регистра сдвига
    $S_n=\beta_1\alpha_1^{\,n}+\beta_2\alpha_2^{\,n}+...+\beta_k\alpha_k^{\,n}, n=0,1,2,...$,
    где $\alpha_1,\alpha_2,...,\alpha_k$ - корни характеристического многочлена, коэффициенты $\beta_1,\beta_2,...,\beta_k\in P$ являются решениями системы

$$\begin{cases}\beta_1\alpha_1^{\,0}+\beta_2\alpha_2^{\,0}+...+\beta_k\alpha_k^{\,0}=S_0\\ \beta_1\alpha_1^{\,1}+\beta_2\alpha_2^{\,1}+...+\beta_k\alpha_k^{\,1}=S_1\\ ...\\ \beta_1\alpha_1^{\,k-1}+\beta_2\alpha_2^{\,k-1}+...+\beta_k\alpha_k^{\,k-1}=S_{k-1}\end{cases}.$$

17. Матрица линейного регистра сдвига
$$A=\begin{pmatrix}0&0&...&0&0&a_0\\1&0&...&0&0&a_1\\0&1&...&0&0&a_2\\0&0&...&0&0&a_3\\...&...&...&...&...&...\\0&0&...&0&0&a_{k-3}\\0&0&...&1&0&a_{k-2}\\0&0&...&0&1&a_{k-1}\end{pmatrix}$$
    ее собственные значения и жорданова форма.
18. Квадратичный закон взаимности. Вычисление квадратичных вычетов и невычетов.
19. Извлечение квадратных корней по простому модулю $p\equiv 3(\mathrm{mod}\,4)\Rightarrow p=4k+3$.
20. Извлечение квадратных корней по простому модулю $\mathrm{p}\equiv 1(\mathrm{mod}4)\Rightarrow \mathrm{p}=4\mathrm{k}+1$.

Виды самостоятельной работы

Обязательными при изучении дисциплины «Теоретико-числовые методы криптографии» являются следующие виды самостоятельной работы:

- разбор и самостоятельное изучение теоретического материала по конспектам лекций и по учебным пособиям из списка источников литературы (п. 6.1);
- самостоятельное решение задач по темам лабораторных занятий (п. 6.2);
- подготовка к контрольным работам (п. 6.3);
- подготовка к реферативному докладу (п. 6.4);
- подготовка к зачету (п. 6.5).

Критерии оценивания результатов обучения

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, знает формы допускает незначительные ошибки; студент умеет правильно объяснять материал, иллюстрируя его примерами

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести примеры, довольно ограниченный объем знаний программного материала.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

5.1 Основная литература:

1. Рябко Б.Я, Фионов А.Н. Криптографические методы защиты информации, 2-е изд. [Электронный ресурс]. – М.: Горячая линия-Телеком, 2017. - URL: https://e.lanbook.com/reader/book/111097
2. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. [Электронный ресурс]. - СПб.: Лань, 2022. - https://reader.lanbook.com/book/210746

5.2 Дополнительная литература:

1. Бухштаб А.А. Теория чисел, 6-е изд. [Электронный ресурс]. - СПб.: Лань, 2022. -

https://reader.lanbook.com/book/189329/
2. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 4-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2020. – URL: https://e.lanbook.com/reader/book/151552

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Пакет компьютерной алгебры Sage 8.3. Официальный сайт http://sagemath.org/
2. Пакет компьютерной алгебры Gap4r9p3. Официальный сайт http://www.gap-system.org/
3. Пакет компьютерной алгебры PARI/GP 2.14 Официальный сайт http://pari.math.u-bordeaux.fr/

7,2 Методические указания к самостоятельной подготовке студентов для выполнения практических заданий лабораторных занятий

Для выполнения домашнего практического задания необходимо разобрать материал по соответствующей теме лабораторного занятия. При этом используются указания, данные преподавателем в ходе занятия, а также теоретико-практический материал, имеющийся в источниках из списка основной литературы. Если студент не смог понять приведенный в указанных источниках разбор типовых примеров в той степени, чтобы самостоятельно использовать предложенный алгоритм для решения задания, то он может получить консультацию преподавателя.

7.3. Методические указания к самостоятельной подготовке студентов к выполнению контрольных работ

В течение семестра проводятся три контрольных работы, каждая из которых длится 45 минут и состоит из трех практических и одного теоретического задания. Тематика трех контрольных работ соответствует тематике трех содержательных разделов дисциплины: Каждое задание оценивается по пятибалльной шкале, высокая оценка ставится при получении не менее 16 баллов, нижний порог успешности составляет 7 баллов. Для подготовки к контрольной работе необходимо выполнять задания в ходе лабораторных занятий, а также домашние задания. В процессе самоподготовки студенту желательно ознакомиться с разбором опорных по рассматриваемым темам задач, имеющихся в пособиях из списка литературы. Выше в пункте 6.2 приведен список заданий, который включает в себя все типы практических заданий контрольных работ.

7.4. Методические рекомендации к самостоятельной подготовке студентов к реферативному докладу

Каждый студент должен подготовить в течение семестра реферативный доклад по одной из тем, предназначенной для самостоятельного изучения. Для подготовки доклада желательно кроме основных источников литературы использовать дополнительные источники, а также Интернет-ресурс. Доклад может быть представлен студентом на лабораторном занятии, возможно, в виде презентации, если тема занятия соответствует теме доклада. Также студент может представить отчет о подготовке реферативного доклада в письменной форме в конце семестра. Оформление письменного отчета должно удовлетворять требованиям: а) текст набирается 14 шрифтом на бумаге формата А 4; б) на титульном листе кроме темы также указывается факультет, направление (бакалавриат), курс, группа, ФИО студента; в) содержание материала по объему составляет 4-5 страниц; г) список литературы содержит не менее двух источников (возможно, из списка литературы в пункте 7).

Примерные темы реферативных докладов

1. Алгебраическое и вероятностное определение шифр системы.
2. Криптосистемы с открытым ключом.

3. Понятие сертификата.
4. Криптосистема RSA. Выбор параметров.
5. Шифр AES
6. ГОСТ -89
7. Криптографические хэш-функции. Стандарты ГОСТ Р 34.11-2012 и SHA.
8. Схема Эль-Гамаля
9. Вычисления на эллиптической кривой.
10. Цифровая подпись. Схемы цифровой подписи.
11. Стандарты ГОСТ Р 34.
12. Стандарт DSS.
13. Анализ программного криптопродукта.

7.4. Методические указания к самостоятельной подготовке студентов к зачету

Согласно учебному плану дисциплины «Теоретико-числовые методы криптографии» итоговой формой контроля является зачет. Для допуска к зачету студент должен научиться на лабораторных занятиях решать практические задания по темам разделов 1-3 (табл. 4.1), выполнять домашние задания, а также успешно выполнить три контрольные работы. Типы практических заданий на зачет соответствуют заданиям из пункта 6.2. Также на зачете студентам предлагаются и теоретические задания, состоящие в письменном ответе на один из вопросов, приведенных в пункте 6.1. Количество практических и теоретических заданий зависит от активности и результативности работы студента в течение семестра. Если при условии хорошей посещаемости и активной работы на занятиях студент по трем контрольным работам и реферативному докладу заслужил высокие оценки, то он автоматически получает допуск к экзамену.

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods

https://experiments.springernature.com/sources/springer-protocols

13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/
2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка (http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование" http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
10. Справочно-информационный портал "Русский язык" http://gramota.ru/;
11. Служба тематических толковых словарей http://www.glossary.ru/;
12. Словари и энциклопедии http://dic.academic.ru/;
13. Образовательный портал "Учеба" http://www.ucheba.com/;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

6. Методические указания для обучающихся по освоению дисциплины (модуля).

Согласно учебному плану дисциплины «Информационная безопасность» итоговой формой контроля является зачет. Для сдачи зачета студент должен научиться на лабораторных занятиях решать практические задания по темам разделов 1-3, выполнять домашние задания. Типы практических заданий на зачет соответствуют заданиям. Также на зачете студентам предлагаются и теоретические задания, состоящие в письменном ответе

на один из вопросов. Количество практических и теоретических заданий зависит от активности и результативности работы студента в течение семестра.

Важнейшим этапом курса является самостоятельная работа по дисциплине (модулю).

Для подготовки к ответам на теоретические вопросы в ходе контрольных работ и на зачете студентам достаточно использовать материал лекций. Весь этот теоретический материал содержится в учебных пособиях из списка основной литературы. Для изучения теоретического материала, необходимого для подготовки реферативного доклада, кроме основных источников литературы возможно использование дополнительных источников и Интернет-ресурса. В случае затруднений, возникающих у студентов в процессе самостоятельного изучения теории, преподаватель разъясняет сложные моменты на консультациях.

7. Материально-техническое обеспечение по дисциплине (модулю)

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

При заполнении таблицы учитывать все виды занятий, предусмотренные учебным планом по данной дисциплине: лекции, занятия семинарского типа (практические занятия, лабораторные работы), а также курсовое проектирование, консультации, текущий контроль и промежуточную аттестацию.

При использовании лаборатории указать ее наименование «Лаборатория…».

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование:	
Учебные аудитории для проведения лабораторных работ. Лаборатория…	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование:	
Учебные аудитории для курсового проектирования (выполнения курсовых работ)	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование:	

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной	

	сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	
Помещение для самостоятельной работы обучающихся (ауд._____)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) Программы, демонстрации видео материалов (проигрыватель «Windows Media Player»). Программы для демонстрации и создания презентаций («Microsoft Power Point»).
2.	Семинарские занятия	Не предусмотрены
3.	Лабораторные занятия	Лаборатория, укомплектованная специализированной мебелью и техническими средствами обучения – компьютерами с предустановленными GAP и Sage
4.	Курсовое проектирование	Не предусмотрено
5.	Групповые (индивидуальные) консультации	Аудитория для групповых занятий
6.	Текущий контроль, промежуточная аттестация	Аудитория для групповых занятий
7.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.