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
«31» мая 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ Б1.О.32.02 ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ КРИПТОГРАФИИ

Специальность 01.05.01 Фундаментальные математика и механика

Направленность (профиль) Фундаментальная математика и ее приложения

Форма обучения Очная

Квалификация Математик. Механик. Преподаватель

Краснодар 2019

Рабочая программа дисциплины ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ КРИПТОГРАФИИ составлена в соответствии с требованиями ФГОС ВО от 12.09.2016 (пр. Минобрнауки РФ № 1173, от 12.09.2016) по специальности ФУНДАМЕНТАЛЬНЫЕ МАТЕМАТИКА И МЕХАНИКА

Составитель
Доктор физ.-мат. наук, профессор кафедры
функционального анализа и алгебры КубГУ_____А.В. Рожков

Рабочая программа рассмотрена и утверждена на заседании кафедры функционального анализа и алгебры протокол № 9 от «12» апреля 2019 г.
Зав. кафедрой функционального анализа
и алгебры кандидат физ.-мат. наук, доцент_____В.Ю. Барсукова

Рабочая программа обсуждена на заседании кафедры (выпускающей) функционального анализа и алгебры протокол № 9 от «12» апреля 2019 г.
Заведующий кафедрой (выпускающей) Барсукова В.Ю. _____

Рабочая программа одобрена на заседании учебно-методической комиссии факультета математики и компьютерных наук «24» апреля 2019 г. протокол № 2

Председатель УМК ФМ и КН
кандидат физ.-мат. наук, доцент _____Г.Н. Титов

Рецензенты:

Ганижева Л.Л. к.т.н., доцент кафедры наземного транспорта и механики КубГТУ
Дроботенко М.И. к.ф.-м.н., зав. кафедрой математических и компьютерных методов 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 относится к обязательной части Блока 1 "Дисциплины (модули)" учебного плана и является одной из основных дисциплин в освоении математических знаний. Дисциплина «Теоретико-числовые методы криптографии» читается в 6 семестре.

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, соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной дисциплины направлено на получение необходимого объёма теоретических знаний, отвечающих требованиям ФГОС ВО и необходимых для дальнейшего успешного изучения всех дисциплин высшей математики, с формированием следующих общепрофессиональных компетенций:

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ОПК-1	Способен находить, формулировать и решать актуальные и значимые проблемы фундаментальной математики и меха-	об основных задачах и понятиях криптографии; об этапах развития криптографии; о видах информации, подлежащей шифро-	использовать: типовые шифры замены и перестановки; частотные характеристики языков и их использование в криптоанализе;требования к	криптографической терминологией; навыками использования основных типов шифров и криптографических алго-

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
		ники	ванию:о классификации шифров	шифрам и основные характеристики шифров; принципы построения современных шифрсистем	ритмов;методами криптоанализа простейших шифров
2.	ОПК-3	Способен самостоятельно создавать и грамотно использовать прикладные программные средства на основе современных информационных технологий и сетевых ресурсов	О методах криптографического синтеза и анализа; о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи; о методах криптозащиты компьютерных систем и сетей	Использовать типовые поточные и блочные шифры, системы шифрования с открытыми ключами, криптографические протоколы; постановки задач криптоанализа и подходы к их решению; основные математические методы, используемые в анализе типовых криптографических алгоритмов	навыками математического моделирования в криптографии; современной научно-технической литературой в области криптографической защиты

2 Структура и содержание дисциплины

2.1 Распределение трудоемкости дисциплины по видам работ

Общая трудоемкость дисциплины «Теоретико-числовые методы криптографии» составляет 3 зачетные единицы (108 часов, из них – 79,2 часа контактной работы (34 лекций, 34 часов лабораторных занятий, 11 часов КСР, 0,2 часов ИКР); 28,8 часа самостоятельной работы).

Вид учебной работы	Всего часов	Семестры
		6-й
Аудиторные занятия (всего)	68	68
В том числе:		
Занятия лекционного типа	34	34
Занятия семинарского типа (семинары, практические занятия)		
Лабораторные работы	34	34
Иная контактная работа:		
Контроль самостоятельной работы (КСР)	4	4
Промежуточная аттестация (ИКР)	0,2	0,2
Курсовая работа	7	7
Самостоятельная работа, в том числе		
Проработка учебного (теоретического) материала	10	10
Выполнение домашних заданий (решение задач)	10	10

Подготовка к текущему контролю		8,8	8,8
Контроль:			
Подготовка к зачету			
Общая трудоемкость	**час.**	**108**	**108**
	в том числе контактная работа	**79,2**	**79,2**
	зач. ед	**3**	**3**

2.2 Структура дисциплины:

Разделы дисциплины, изучаемые в 6 семестре

№ раздела	Наименование разделов	Количество часов			
		Всего	Аудиторная работа		Самостоятельная работа
			Л	ЛЗ	
1	**2**	**3**	**4**	**5**	**6**
1	Модели шифров.	24	8	10	6
2	Мультипликативные функции.	22	8	8	6
3	Табличное и модульное гаммирование.	26	10	8	8
4	Построение больших простых чисел.	24.8	8	8	8,8
	Итого:		**34**	**34**	**28,8**

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 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. Элек-	экзамен

		тронная подпись.	

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)

1. Освоение процессов зашифрования и расшифрования для простейших шифров.
2. Свойства простейших шифров.
3. Расчет мощности ключевой системы различных шифров.
4. Оценка расстояния единственности для простейших шифров.
5. Криптоанализ шифра Виженера.
6. Расчет характеристик метода перебора ключей.
7. Вычисление характеристик двоичных функций.
8. Анализ схемы DES при небольшом числе итераций.
9. Вычисление характеристик датчиков псевдослучайных чисел.

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

N	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Проработка учебного (теоретического) материала	Методические указания по организации самостоятельной работы, утвержденные кафедрой функционального анализа и алгебры протокол № 9 от 12.04.2019 г
2	Выполнение домашних заданий (решение задач)	Методические указания по организации самостоятельной работы, утвержденные кафедрой функционального анализа и алгебры протокол № 9 от 12.04.2019 г
3	Подготовка к текущему контролю	Методические указания по организации самостоятельной работы, утвержденные кафедрой функционального анализа и алгебры протокол № 9 от 12.04.2019 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 ОПК-3	+		Обзор литературы, зачет
ОПК-1		+	Отчеты по практическим заданиям, реферативный доклад
ОПК-1	+	+	Дискуссия, зачет
ОПК-1	+		Реферативный доклад, зачет
ОПК-1 ОПК-3	+	+	Собеседование, зачет
ОПК-1 ОПК-3	+	+	Реферативный доклад, консультация
ОПК-1 ОПК-3	+		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	2

		числа.	
	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 4) – *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;

– психологические и иные тренинги;

– групповые дискуссии и др.

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-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.

«Мозговой штурм» («мозговая атака») представляет собой разновидность групповой дискуссии, которая характеризуется отсутствием критики поисковых усилий, сбором всех вариантов решений, гипотез и предложений, рожденных в процессе осмысления какой-либо проблемы, их последующим анализом с точки зрения перспективы дальнейшего использования или реализации на практике. «Мозговой штурм» включает три этапа: подготовительный, этап генерирования идей, этап анализа и оценки идей. Продолжительность «мозгового штурма», как правило, не менее 1,5–2 часов.

Дебаты – формализованное обсуждение, построенное на основе выступлений участников – представителей двух или более противостоящих, соперничающих команд (групп). Данная образовательная технология основывается на умении анализировать события, концентрироваться на обсуждаемой проблеме, собирать и обрабатывать информацию, творчески осмысливать возможности ее применения, определять собственную точку зрения по данной проблеме и защищать ее, организовывать взаимодействие в группе на основе соблюдения принятых правил и процедур совместной деятельности.

Ролевая игра – это эффективная отработка вариантов поведения в тех ситуациях, в которых могут оказаться обучающиеся (например, аттестация, защита или презентация какой-либо разработки, конфликт с однокурсниками и др.). Игра позволяет приобрести навыки принятия ответственных и безопасных решений в учебной ситуации. Признаком, отличающим ролевые игры от деловых, является отсутствие системы оценивания по ходу игры. Существенные признаки ролевой игры: – наличие игровой ситуации; – набор индивидуальных ролей; – несовпадение ролевых целей участников игры, принимающих на себя и исполняющих различные роли; – игровое взаимодействие участников игры; – проигрывание одной и той же роли разными участниками; – групповая рефлексия процесса и результата.

Компьютерная симуляция – это максимально приближенная к реальности имитация различных процессов (физических, химических, экономических, социальных и проч.) и (или) деятельности с использованием программного обеспечения образовательного назначения

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Учебная деятельность проходит в соответствии с графиком учебного процесса. Процесс самостоятельной работы контролируется во время аудиторных занятий и индивидуальных консультаций.

Оценочными средствами дисциплины являются средства текущего контроля (контрольные работы, ответ у доски и проверка домашних заданий) и итоговая аттестация (зачет). Зачет выставляется по результатам работы в семестре с учетом выполнения домашних заданий и итоговой контрольной работы.

Контрольные работы и реферативные доклады оцениваются по пятибалльной системе. Зачет оценивается по системе: зачтено, не зачтено. На лабораторных занятиях контроль осуществляется при ответе у доски и при проверке домашних заданий.

Самостоятельная работа студента включает в себя повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным занятиям, к контрольным работам и к зачету. Такой вид СРС контролируется в ходе проверки домашних заданий, заданий контрольных работ и в ходе зачета. Предполагается самостоятельное изучение студентами теоретического материала по темам реферативных докладов, указанных ниже в пункте 6.4. Контроль осуществляется во время консультаций (вызывных или по желанию студента), а также на лабораторных занятиях.

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).

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.

Перечень

электронных документов, которые могут быть представлены
в печатной форме с увеличенным шрифтом

1. Рожков А.В. «Темы исследовательских работ и методические указания по их написанию», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 г.
2. Рожков А.В. «Комментарии к лекциям по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 г.
3. Рожков А.В. «Решебник типовых задач по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 г.
4. Рожков А.В. «Алгебраические методы криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017.

5. Рябко Б.Я, Фионов А.Н. Криптографические методы защиты информации, 2-е изд. [Электронный ресурс]. – М.: Горячая линия-Телеком, 2012. - URL: http://e.lanbook.com/view/book/5193/
6. Аверченков В.И., Рытов М.Ю., Шпичак С.А. Криптографические методы защиты информации: учебное пособие, 2-е изд. [Электронный ресурс]. – М.: ФЛИНТА, 2017 https://e.lanbook.com/book/92914?category_pk=1537 .
7. Бухштаб А.А. Теория чисел, 4-е изд. [Электронный ресурс]. - СПб.: Лань, 2015. - URL: http://e.lanbook.com/view/book/65053/
8. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 3-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2015. – URL: http://e.lanbook.com/view/book/70724/
9. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. [Электронный ресурс]. - СПб.: Лань, 2011. - URL: http://e.lanbook.com/view/book/1540 /
10. Авдошин С.М., Набебин А.А. Дискретная математика. Модулярная алгебра, криптография, кодирование [Электронный ресурс]. – М.: ДМК пресс, 2017. – URL: https://e.lanbook.com/book/93575?category_pk=1537 .

Критерии оценивания по промежуточной аттестации

Зачет выставляется по результатам работы студента в течение семестра. Отметка «зачтено» выставляется студентам, которые регулярно посещали занятия, выполняли домашние работы, написали контрольные работы на положительные оценки. Отметка «незачтено» выставляется студентам, которые пропустили более 60 % занятий и написали контрольные работы на неудовлетворительные оценки.

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 [Электронный ресурс]. – М.: Горячая линия-Телеком, 2012. - URL: https://e.lanbook.com/reader/book/5193/#1
2. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. [Электронный ресурс]. - СПб.: Лань, 2011. - URL: https://e.lanbook.com/reader/book/68466/#1

5.2 Дополнительная литература:

1. Бухштаб А.А. Теория чисел, 4-е изд. [Электронный ресурс]. - СПб.: Лань, 2015. - URL: https://e.lanbook.com/reader/book/65053/#1
2. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 3-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2015. – URL: https://e.lanbook.com/reader/book/70724/#1

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 2.11 Официальный сайт http://pari.math.u-bordeaux.fr/

Методические указания для обучающихся по освоению дисциплины (модуля)

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 1 – 2. Для изу-

чения 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.

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.

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.

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 цифровой.

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.

Примерные контрольные (самостоятельные) 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
$S_{n+k}=a_{k-1}S_{n+k-1}+a_{k-2}S_{n+k-2}+\ldots+a_1S_{n+1}+a_0S_n+a, n=0,1,2,\ldots$

15. Характеристический многочлен регистра сдвига $x^k = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a_1 x + a_0$
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 $\mathrm{p} \equiv 1 (\mathrm{mod} 4) \Rightarrow \mathrm{p}=4\mathrm{k}+1$.

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.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

8.1. Перечень информационных технологий.

не предусмотрены

8.2 Перечень необходимого программного обеспечения

а) перечень лицензионного программного обеспечения:

№	Производитель	Наименование
1	Microsoft	Microsoft Windows 8, 10
2	Microsoft	Microsoft Office Professional Plus
4	WolframResearch	Mathematica
5	MapleSoft	Maple 18
6	Mathworks	MATLAB Wavelet Toolbox

в) Перечень свободно распространяемого программного обеспечения

№	Перечень свободно распространяемого программного обеспечения
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/GT 2.11. Официальный сайт http://pari.math.u-bordeaux.fr/
4.	Библиотека для работы с большими целыми числами GMP 6.1.2. Официальный сайт https://gmplib.org/
5.	Язык программирования Python. Официальный сайт https://www.python.org/
6.	Язык программирования Julia. Официальный сайт http://julialang.org/
7.	Язык программирования Cython. Официальный сайт http://cython.org/

8.	Компилятор PyPy, оптимизирующий код Python и Cython. Официальный сайт http://pypy.org/
9.	Python в облаке, интегрированная среда разработки Anaconda. Официальный сайт https://store.continuum.io/cshop/anaconda/
10.	Математические пакеты Python, проект SciPy. Официальный сайт http://www.scipy.org/
11.	Клиентская ОС Debian 9.5. Официальный сайт https://www.debian.org/index.ru.html
12.	Издательская система LaTeX/MiKTeX 2.9. Официальный сайт http://www.miktex.org/
13.	Утилиты Руссиновича https://technet.microsoft.com/ru-ru/library/bb545021.aspx
14.	Анализ защищенности сети Kali Linux 2018.3. https://www.kali.org/
15.	Анализ защищенности сети Snort 3.0. Официальный сайт https://www.snort.org/
16.	Офисная система Apache OpenOffice 4.1.5. Официальный сайт https://www.openoffice.org/ru/

8.3 Перечень необходимых информационных справочных систем

не предусмотрены

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

№	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)
2.	Лабораторные занятия	Специальное помещение, оснащенное доской, маркерами и мелом Компьютерные классы
3.	Групповые (индивидуальные) консультации	Аудитория (кабинет)
4.	Текущий контроль, промежуточная аттестация	Аудитория, (кабинет)
5.	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.

.