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.В.ДВ.01.02 КРИПТОГРАФИЯ И ЗАЩИТА ИНФОРМАЦИИ

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 «Криптография и защита информации» составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности 01.05.01 «Фундаментальные математика и механика»

Программу составили:
Рожков А.В., доктор физ.-мат. наук, профессор

Рабочая программа дисциплины «Криптография и защита информации» утверждена на заседании кафедры (разработчика) функционального анализа и алгебры
протокол № 9 «12» апреля 2019 г.
Заведующий кафедрой (разработчика) Барсукова В.Ю.

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

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук «24» апреля 2019 г, протокол № 2

Председатель УМК факультета Титов Г.Н.

Эксперты:

Наумова Н.А., доктор технических наук, профессор кафедры прикладной математики ФГБОУ ВО «Кубанский государственный технологический университет»
Иванисова О.В., кандидат физико-математических наук, доцент кафедры ВМИ КубГУ

1 Цели и задачи изучения дисциплины.

1.1 Цель освоения дисциплины.

Цель освоения дисциплины – рассмотрение задач информатизации и программно-аппаратных основ кодирования информации. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

1.2 Задачи дисциплины.

Задачи освоения дисциплины «Криптография и защита информации»: Получение базовых теоретических и практических сведений и навыков о структуре и алгоритмах кодирования информации. Математических основ анализа каналов связи с шумом. Основ теории кодов, исправляющих ошибки. Основ теории информации. Прежде всего алгебраических, связанных с вычислительными и числовыми вопросами алгебры и криптографии. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли вычислительных приемов и методов, при решении вопросов защиты информации.

Изучение теоретических основ предмета: Информационные объекты. Компьютерная алгебра и численный анализ информационных систем. Коды Хэмминга. Теория информации по Шеннону. Алгоритмы кодирования информации жестких и съемных дисков.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Криптография и защита информации» относится к части, определяемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана и является дисциплиной по выбору.

Данная дисциплина, как алгоритмическая основа криптографии, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления студентов. А также развитию навыков применения современных компьютерных средств для решения естественно-научных проблем.

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 компетенций (ОПК)

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-4	Способен ориентироваться в современных алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах	О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа.	Применять основные математические методы, используемые в анализе типовых алгоритмов.	использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений.

В результате освоения данной дисциплины обучающийся должен:

Знать:

об основных задачах и понятиях теории кодов;
о видах информации, подлежащей кодированию;
о классификации кодов;
о методах защиты компьютерных систем и сетей.
Уметь использовать:
коды с одной проверкой на четность;
линейные коды;
циклические коды;
групповые коды. Коды Хэмминга;
коды Боуза-Чоудхури-Хоквингемы;
основные математические методы, используемые в анализе типовых алгоритмов.
Владеть:
алгоритмами решение систем линейных уравнений по разным модулям;
методами построения генераторов псевдослучайных последовательностей;
алгоритмами построения кодов, исправляющих ошибки;
методами вычислений и построений кодов Хэмминга.

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 2 зач. ед. (72 часа), их распределение по видам работ представлено в таблице.

Вид учебной работы		Всего часов	Семестры (часы)			
			8			
Контактная работа, в том числе:						
Аудиторные занятия (всего):		**34**	**34**			
Занятия лекционного типа				-	-	-
Лабораторные занятия		34	34	-	-	-
Занятия семинарского типа (семинары, практические занятия)				-	-	-
		-	-	-	-	-
Иная контактная работа:						
Контроль самостоятельной работы (КСР)		4	4			
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:						
Курсовая работа		-	-	-	-	-
Проработка учебного (теоретического) материала		10	10	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		10	10	-	-	-
Реферат		4	4	-	-	-
Подготовка к текущему контролю		9,8	9,8	-	-	-
Контроль:						
Подготовка к экзамену		-	-			
Общая трудоемкость	**час.**	**72**	**72**	-	-	-
	в том числе контактная работа	**38,2**	**38,2**			
	зач. ед	**2**	**2**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в 7 семестре *(очная форма)*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Основные понятия и определения теории кодирования.	16			8	8
2	Свойства энтропии. Теорема Шеннона для кодирования в двоичном симметричном канале связи с шумом.	16			8	8
3	Алгебраические методы в теории кодов.	16			8	8
4	Теория кодов и криптография.	19.8			10	9.8
	Итого по дисциплине:				34	33.8

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

Не предусмотрены

2.3.2 Занятия семинарского типа.

Не предусмотрены

2.3.3 Лабораторные занятия.

№	Наименование лабораторных работ	Форма текущего контроля
1	3	4
1	Двоичный симметричный канал связи. Линейные коды. Границы объемов кодов. Код Хэмминга и его свойства. Способы построения новых кодов.	Р
2	Декодирование двоичных кодов. Декодирование линейного кода. Вероятность ошибки декодирования. Хеммингово расстояние, Хемминговы сферы и корректирующая способность..	Р
3	Двоичные коды Рида-Маллера. Групповые коды. Функция Эйлера и Мебиуса. Группы обратимых элементов в кольцах.	Э
4	Структура мультипликативной группы кольца вычетов. Обратимые элементы. Примитивные элементы. Коды Васильева.	Р
5	Поля Галуа, неприводимые многочлены. Псевдослучайные последовательности. Сложность и скорость выполнения алгоритмов.	Р
6	Порождающий и проверочный полиномы. Порождающий многочлен. Кодирование и декодирование двоичных циклических кодов	Э
7	Рекурсивные систематические сверточные коды. Свободное рассто-	Р

	яние. Связь с блоковыми кодами. Декодирование: Алгоритм Витерби в Хеммингoвой метрике.	
8	Декодирование по максимуму правдоподобия и метрики. Криптографические алгоритмы и протоколы. Блочные и поточные шифры. Однонаправленные функции. Сетевое кодирование и шифрование. Понятие о стеганографии.	Р

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т).

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены.

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

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Подготовка рефератов и научных сообщений	Рожков А.В. «Темы исследовательских работ и методические указания по их написанию», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 «12» апреля 2019 г.
2	Решение задач	Рожков А.В. «Лабораторная работа по теоретико-числовым методам криптографии по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 «12» апреля 2019 г.
3	Самостоятельное освоение теории	Рожков А.В. «Теоретико-числовые методы криптографии. Учебное пособие», утвержденное кафедрой функционального анализа и алгебры, протокол № 9 «12» апреля 2019 .
4	Решение задач	Рожков А.В. «Решебник типовых задач по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 «12» апреля 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 с 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,

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 31 августа 2017 г.
2. Рожков А.В. «Лабораторная работа по теоретико-числовым методам криптографии по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017 г.
3. Рожков А.В. «Теоретико-числовые методы криптографии. Учебное пособие», утвержденное кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017.
4. Рожков А.В. «Решебник типовых задач по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017 г

3. Образовательные технологии.

Активные и интерактивные формы, лекции, контрольные работы, реферативные доклады (по некоторым темам в виде презентации) и зачет. В течение семестра студенты решают задачи, указанные преподавателем, к каждому лабораторному занятию. Каждый студент готовит реферативный доклад по одной из ниже научных тем. Зачет выставляется после выполнения определенного количества (практических и теоретических) заданий контрольных работ и отчета по реферативному докладу. В случае невыполнения какого-то из приведенных требований, студенту для сдачи зачета предлагаются по усмотрению преподавателя некоторые практические и теоретические задания, подобные предложенным ниже.

К образовательным технологиям также относятся интерактивные методы обучения.

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;

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

4.1 Фонд оценочных средств для проведения текущего контроля.

Список теоретических вопросов (для подготовки к зачету)

1. Евклидовы кольца.
2. Кольца вычетов.
3. Функция Эйлера.
4. Функция Мебиуса.
5. Теорема Ферма.
6. Китайская теорема об остатках.
7. Однонаправленные функции.
8. Сложность разложения на множители.
9. Конечные поля.
10. Алгоритм извлечения квадратных корней в конечном поле.

11. Неприводимые многочлены над полями Галуа.
12. Период многочлена.
13. Решение систем линейных уравнений по разным модулям.
14. Генераторы псевдослучайных последовательностей.
15. Определение кода, исправляющего ошибки.
16. Расстояние Хэмминга.
17. Коды Хэмминга.
18. Линейные коды.
19. Циклические коды.
20. Групповые коды.
21. Матричные модели доступа.
22. Обыкновенные графы.
23. Ориентированные графы.
24. Графы с петлями и мультиграфы.
25. Нагруженные графы.
26. Коды Боуза-Чоудхури-Хоквингемы (БЧХ-коды).
27. Двоичные БЧХ-коды, исправляющие многократные ошибки.
28. Недвоичное кодирование.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Список типовых алгоритмов (для самостоятельных и лабораторных занятий)

1. Найти период последовательности, заданной формулой .
2. Решить систему линейных уравнений по разным модулям
3. Привести пример регистра сдвига с обратной связью. Записать регистр в матричной форме. Нарисовать электронную схему регистра.
4. Привести пример кода, исправляющего 3 ошибки.
5. Найти расстояние Хэмминга между конкретными кодирующими словами.
6. Найти расстояние Хэмминга между конкретными множествами кодирующих слов.
7. Закодировать кодом Хэмминга данный набор объектов (например, слов в алфавите).
8. Привести пример линейного кода.
9. Привести пример циклического кода.
10. Привести пример кода являющего групповым и кода групповым не являющегося.
11. На примере системы с тремя ресурсами и тремя пользователями привести пример матрицы доступа.
12. Матрицы доступа, реализованные в операционных системах семейства Linux.
13. Привести пример графа частично упорядоченного множества.
14. Привести пример графа с петлями.
15. Привести пример мультиграфа.
16. Матричная запись нагруженного графа.
17. Пример конечной реляционной алгебры.
18. Примеры операций в реляционной алгебре.
19. Привести примеры коммерческих реляционных баз данных.
20. Перечислить признаки распределенных баз данных.
21. Привести примеры кодов Боуза-Чоудхури-Хоквингемы (БЧХ-коды).
22. Привести пример двоичного БЧХ-коды, исправляющего 7 ошибок.
23. Привести примеры недвоичное кодирования.

Примерные темы реферативных докладов

1. Линейные регистры сдвига с обратной связью (доклад на лабораторном занятии в виде презентации).
2. Коды Хэмминга и сжатие информации (отчет в письменной форме).

3. Реляционные алгебры (доклад на лабораторном занятии).
4. Коммерческие продукт, реализующие модель распределенных баз данных (отчет в письменной форме).
5. Решение квадратных уравнений в конечных полях с использованием логарифмов Якоби (доклад на лабораторном занятии в виде презентации).
6. Обзор популярных БЧХ-кодов (доклад на лабораторном занятии в виде презентации).
7. Недостатки модели Белла-Ла Падула (отчет в письменной форме).

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

5.1 Основная литература:

1. Нестеров С.А. Основы информационной безопасности, 4-е изд. [Электронный ресурс]. - СПб.: Лань, 2018. – URL. https://e.lanbook.com/reader/book/103908/#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

5.2 Дополнительная литература:

1. Березкин Е.Ф. Основы теории информации и кодирования: учебное пособие, 2-е изд. [Электронный ресурс]. – М.: Издательство "Лань", 2018. - URL: https://e.lanbook.com/reader/book/108326/#1
2. Аверченков В.И. Аудит информационной безопасности, 2-е изд. [Электронный ресурс] – М.: Издательство "ФЛИНТА", 2011. – URL: https://e.lanbook.com/reader/book/20195/#1

1.3. Периодические издания:

Не предусмотрены

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

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

Согласно учебному плану дисциплины «Криптография и защита информации» 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.

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

8.1 Перечень информационных технологий.

8.2 Перечень необходимого программного обеспечения.

а) перечень лицензионного программного обеспечения:

№	Перечень лицензионного программного обеспечения
1.	Maple Soft Maple 18
2.	Mathcad 3
3.	Mathcad 14
4.	Microsoft office
5.	MS Windows 10 (x64)
6.	MS Office 2013, MS

в) Перечень свободно распространяемого программного обеспечения

№	Перечень свободно распространяемого программного обеспечения
1.	Пакет компьютерной алгебры Sage 8.2. Официальный сайт http://sagemath.org/
2.	Пакет компьютерной алгебры Gap4r9p1. Официальный сайт http://www.gap-system.org/
3.	Пакет компьютерной алгебры PARI/GT 2.9. 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 9.4. 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 2018.2. https://www.kali.org/
15.	Офисная система Apache OpenOffice 4.1.5. Официальный сайт https://www.openoffice.org/ru/

8.3 Перечень информационных справочных систем:

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 Maple 2018. http://www.maplesoft.com
4. http://www.pravo.gov.ru – официальный портал правовой информации
5. http://www.government.ru - интернет-портал Правительства РФ
6. http://graph.document.kremlin.ru - раздел «Документы» портала Президента России
7. http://minsvyaz.ru/ru - сайт Минкомсвязи РФ

8. http://www.rsoc.ru - сайт Федеральной службы Роскомнадзор
9. http://www.scrf.gov.ru – сайт Совета безопасности РФ
10. http://base.consultant.ru – сайт правовой информации «Консультант+»
11. http://www.fstec.ru – официальный сайт ФСТЭК России
12. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)/
13. Электронная библиотека http://gen.lib.rus.ec/

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

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лабораторные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения – компьютерами
2.	Групповые (индивидуальные) консультации	Аудитория, оснащенная мебелью, доской, маркерами и мелом
3.	Текущий контроль, промежуточная аттестация	Аудитория, оснащенная мебелью, доской, маркерами и мелом
4.	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.