Министерство образования и науки 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

_____ Иванов А.Г.
подпись

«30» апреля 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.10 Теоретико-числовые методы криптографии
(код и наименование дисциплины в соответствии с учебным планом)

Направление подготовки 01.04.01 Математика
(код и наименование направления подготовки/специальности)

Направленность Алгебраические методы защиты информации
(наименование направленности (профиля) специализации)

Программа подготовки академическая
(академическая /прикладная)

Форма обучения очная
(очная, очно-заочная, заочная)

Квалификация (степень) выпускника магистр
(бакалавр, магистр, специалист)

Краснодар 2017

Рабочая программа дисциплины Теоретико-числовые методы криптографии составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 01.04.01 Математика

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 № _15____ «_9___»__июня_____2017 г.

Заведующий кафедрой Барсукова В.Ю.

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук,
протокол № __3____ «__20__»__июня_____2017 г.
Председатель УМК факультета Титов Г.Н

Рецензенты:

Крамаренко Т.А., к.п.н. доцент кафедры системного анализа и обработки информации КубГАУ

Лазарев В.А. д.п.н., зав. кафедрой теории функций КубГУ

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Цель освоения дисциплины – рассматривает задачи информатизации и защиты информации. 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 (модуля) в структуре образовательной программы.

Дисциплина «Теоретико-числовые методы криптографии» относится к вариативной части Блока 1 "Дисциплины (модули)" учебного плана Б1.В.10.

Данная дисциплина, как математическая основа криптографии, критоанализа, теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления магистров

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 общекультурных/общепрофессиональных/профессиональных компетенций (ОК/ОПК/ПК)

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-4	Способностью к применению методов математического и алгоритмического моделирования при решении теоретических и прикладных	О компью-терной 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.

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
		задач			

В результате освоения данной дисциплины обучающийся должен:
Знать:
об основных задачах и понятиях криптографии;
об этапах развития криптографии;
о видах информации, подлежащей шифрованию;
о классификации шифров; о методах криптографического синтеза и анализа;
о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи;
о методах криптозащиты компьютерных систем и сетей;
Уметь использовать:
типовые шифры замены и перестановки;
частотные характеристики языков и их использование в криптоанализе;
требования к шифрам и основные характеристики шифров;
принципы построения современных шифрсистем:
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.
Владеть:
криптографической терминологией;
навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шифров:
современной научно-технической литературой в области криптографической защиты.

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 4 зач. ед. (144 часа), их распределение по видам работ представлено в таблице.

Вид учебной работы	Всего часов	Семестры (часы)			
		1			
Контактная работа, в том числе:					
Аудиторные занятия (всего):	**32**	**32**			
Занятия лекционного типа	16	16	-	-	-
Лабораторные занятия	-	-	-	-	-
Занятия семинарского типа (семинары, практические занятия)	16	16	-	-	-
	-	-	-	-	-
Иная контактная работа:					
Контроль самостоятельной работы (КСР)					
Промежуточная аттестация (ИКР)	0,3	0,3			
Самостоятельная работа, в том числе:					
Курсовая работа	-	-	-	-	-
Проработка учебного (теоретического) материала	38	38	-	-	-

Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		35	35	-	-	-
Реферат		4	4	-	-	-
Подготовка к текущему контролю		8	8	-	-	-
Контроль:						
Подготовка к экзамену		26,7	26,7			
Общая трудоемкость	**час.**	**144**	**144**	**-**	**-**	**-**
	в том числе контактная работа	**32,3**	**32,3**			
	зач. ед	**4**	**4**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 1 семестре *(очная форма)*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Модели шифров.	32	4	4		28
2	Мультипликативные функции.	32	4	4		28
3	Табличное и модульное гаммирование.	19	4	4		11
4	Построение больших простых чисел.	26	4	4		18
	Итого по дисциплине:		16	16		85

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.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Модели шифров.	Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам	Р
2	Мультипликативные функции.	Функция Эйлера и Мебиуса. Группы обратимых элементов в кольцах. Структура мультипликативной группы кольца вычетов. Обратимые элементы. Примитивные элементы.	Э
3	Табличное и модульное	Случайные и псевдослучайные гаммы. Регистры	Т

	гаммирование.	сдвига с обратной связью Криптограммы, полученные при повторном использовании 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.	Р

2.3.2 Занятия семинарского типа.

Не предусмотрены

№	Наименование раздела	Тематика практических занятий (семинаров)	Форма текущего контроля
1	2	3	4
1.			
2.			

2.3.3 Практические занятия.

№	Наименование практических работ	Форма текущего контроля
1	3	4
1	Блочные и поточные шифры. Понятие криптосистемы.	Р
2	Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам	Р
3	Функция Эйлера и Мебиуса. Группы обратимых элементов в кольцах.	Э
4	Структура мультипликативной группы кольца вычетов	Р
5	Случайные и псевдослучайные гаммы. Регистры сдвига с обратной связью	Р
6	Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы.	Э
7	Алгоритмы проверки на простоту.	Р
8	Эллиптические кривые над конечными полями и алгоритмы вычисления на них. Электронная подпись.	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 № 1 от 31 августа 2017 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 № 1 от 31 августа 2017 г.
3	Самостоятельное освоение теории	Рожков А.В. «Теоретико-числовые методы криптографии. Учебное пособие», утвержденное кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017.
4	Решение задач	Рожков А.В. «Решебник типовых задач по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017 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 экзамен. В течение семестра магистры решают задачи, указанные преподавателем, к каждому лабораторному занятию. Каждый магистр 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, магистру для сдачи зачета предлагаются по усмотрению преподавателя некоторые практические и теоретические задания, подобные предложенным ниже.

К образовательным технологиям также относятся интерактивные методы обучения. Интерактивность подачи материала по дисциплине «Теоретико-числовые методы криптографии» предполагает не только взаимодействия вида «преподаватель - магистр» и «магистр - преподаватель», но и «магистр - магистр». Все эти виды взаимодействия хорошо достигаются при изложении материала на занятиях в ходе дискуссий, а также на лабораторных занятиях в ходе изложения магистрами реферативных докладов (возможно в виде презентации).

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 экзамену)

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.
17. Антивирусы.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Список типовых алгоритмов (для самостоятельных занятий)

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. Нахождение примитивного элемента конечного поля.
17. Построение таблицы логарифма Якоби конечного поля.
18. Решение систем линейных уравнений над конечным полем.
19. Алгоритм быстрого возведения в степень.
20. Нахождение обратных элементов в конечном поле.
21. Расширения конечных полей.
22. Алгоритм шифрования AES: структура поля $GF(2^8)$, нахождение обратных элементов.
23. Алгоритм шифрования AES: фактор кольцо $GF(2^8)[\mathrm{x}]/\mathrm{ид}((\mathrm{x}+1)^4)$, преобразование столбцов.
24. Алгоритм шифрования AES: Линейное преобразование, собственные значения матрицы $A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$.
25. Алгоритм RSA – выбор секретных параметров p, q, d, вычисление открытого ключа n, e.
26. Рюкзачная система шифрования. Быстрорастущий вектор. Сокрытие быстрорастущего вектора после преобразования умножения по модулю.
27. Решение систем линейных уравнений по разным модулям.
28. Решение систем линейных уравнений в кольце целых чисел.
29. Линейный регистр сдвига с обратной связью
    $S_{n+k} = a_{k-1}S_{n+k-1} + a_{k-2}S_{n+k-2} + \ldots + a_1 S_{n+1} + a_0 S_n + a, n = 0,1,2,\ldots$
30. Характеристический многочлен регистра сдвига
    $x^k = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_1 x + a_0$
31. Нахождение явного вида значений регистра сдвига
    $S_n = \beta_1 \alpha_1{}^n + \beta_2 \alpha_2{}^n + \ldots + \beta_k \alpha_k{}^n, n = 0,1,2,\ldots$, где $\alpha_1, \alpha_2, \ldots, \alpha_k$ - корни характеристического многочлена, коэффициенты $\beta_1, \beta_2, \ldots, \beta_k \in P$ являются решениями системы $\begin{cases} \beta_1 \alpha_1{}^0 + \beta_2 \alpha_2{}^0 + \ldots + \beta_k \alpha_k{}^0 = S_0 \\ \beta_1 \alpha_1{}^1 + \beta_2 \alpha_2{}^1 + \ldots + \beta_k \alpha_k{}^1 = S_1 \\ \ldots \\ \beta_1 \alpha_1{}^{k-1} + \beta_2 \alpha_2{}^{k-1} + \ldots + \beta_k \alpha_k{}^{k-1} = S_{k-1} \end{cases}$.

32. Матрица линейного регистра сдвига

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & a_0 \\ 1 & 0 & \dots & 0 & 0 & a_1 \\ 0 & 1 & \dots & 0 & 0 & a_2 \\ 0 & 0 & \dots & 0 & 0 & a_3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & a_{k-3} \\ 0 & 0 & \dots & 1 & 0 & a_{k-2} \\ 0 & 0 & \dots & 0 & 1 & a_{k-1} \end{pmatrix}$$

ее собственные значения и жорданова форма.

33. Квадратичный закон взаимности. Вычисление квадратичных вычетов и невычетов.

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 28147-89 отечественного блочного шифра.
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 серии ГОСТ Р 34.
12. Стандарт *DSS*.
13. Анализ программного криптопродукта

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

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

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 «Теоретико-числовые методы криптографии» итоговой формой контроля является экзамен. Для сдачи экзамена магистр 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 магистрам предлагаются и теоретические задания, состоящие в письменном ответе на один из вопросов. Количество практических и теоретических заданий зависит от активности и результативности работы магистра 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 магистрам 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 магистров 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 14
3.	MS Windows 10 (x64)
4.	MS Office 2013, MS
5.	Office 2010, 7Zip

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.	Серверная ОС CentOS – 7. Официальный сайт https://www.centos.org/
17.	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 PARI/GP 2.11. Официальный сайт http://pari.math.u-bordeaux.fr/
4. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)/
5. 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.	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.	Практические занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения – компьютерами
3.	Групповые (индивидуальные) консультации	Аудитория, оснащенная мебелью, доской, маркерами и мелом
4.	Текущий контроль, промежуточная аттестация	Аудитория, оснащенная мебелью, доской, маркерами и мелом
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.

РЕЦЕНЗИЯ

на рабочую программу дисциплины

ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ КРИПТОГРАФИИ

Направление подготовки 01.04.01 Математика
Направленность Алгебраические методы защиты информации

Рабочая программадисциплины Теоретико-числовые методы криптографиидля магистров направленность «Алгебраические методы защиты информации» составлена доктором физико-математических наук, профессором кафедры функционального анализа и алгебры факультета математики и компьютерных наук Кубанского государственного университета Рожковым А.В.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования (ФГОС ВО) по направлению подготовки 01.04.01 Математика. Программа одобрена на заседании кафедры функционального анализа и алгебры и на заседании учебно-методического совета факультета математики и компьютерных наук.

Содержание рабочей программы – этоблочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам.Случайные и псевдослучайные гаммы. Регистры сдвига с обратной связью. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы.

Рабочая программа дисциплины Теоретико-числовые методы криптографиидля магистров направленность «Алгебраические методы защиты информации» сочетает теоретическую и практические части, что способствует более глубокому усвоению материала. Предложенные задания научно-исследовательского плана направлены на развитие практических навыков решения задач по направлению защита информации.

Считаю, что рабочая программа дисциплины Теоретико-числовые методы криптографиидля магистров направленность «Алгебраические методы защиты информации» может быть рекомендована для подготовки магистров направления подготовки 01.04.01 Математика.

Кандидат педагогических наук,
доцент кафедры системного анализа и обработки информации
ФГБОУ ВО «КубГАУ»

Т.А. Крамаренко

Личную подпись тов. Т.А. Крамаренко
ЗАВЕРЯЮ:
Специалист по кадрам

РЕЦЕНЗИЯ

на рабочую программу дисциплины
ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ КРИПТОГРАФИИ

Направление подготовки 01.04.01 Математика
Направленность Алгебраические методы защиты информации

Рабочая программа дисциплины Теоретико-числовые методы криптографиидля магистров направленность «Алгебраические методы защиты информации» составлена доктором физико-математических наук, профессором кафедры функционального анализа и алгебры факультета математики и компьютерных наук Кубанского государственного университета Рожковым А.В.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования (ФГОС ВО) по направлению подготовки 01.04.01 Математика. Программа одобрена на заседании кафедры функционального анализа и алгебры и на заседании учебно-методического совета факультета математики и компьютерных наук.

Освоившие программу дисциплины Теоретико-числовые методы криптографиибудут знать: типовые шифры замены и перестановки;частотные характеристики языков и их использование в криптоанализе; требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем: 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.

Рабочая программа дисциплины Теоретико-числовые методы криптографиидля магистров направленность «Алгебраические методы защиты информации» сочетает теоретическую и практические части.Получение базовых практических сведений и навыков о структуре и алгоритмах символьных математических вычислений.

Считаю, что рабочая программа дисциплины Теоретико-числовые методы криптографиидля магистров направленность «Алгебраические методы защиты информации» может быть рекомендована для подготовки магистров направления подготовки 01.04.01 Математика.

Доктор педагогических наук,
заведующий кафедрой теории функций
ФГБОУ ВО «КубГУ»

В.А. Лазарев