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
«29» мая 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ Б1.В.ДВ.09.01 ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И ЭЛЕКТРОННАЯ ПОДПИСЬ

Направление подготовки 02.03.01 Математика и компьютерные науки

Направленность (профиль) Алгебра, теория чисел и дискретный анализ

Форма обучения очная

Квалификация бакалавр

Краснодар 2020

Рабочая программа дисциплины Эллиптические кривые и электронная подпись составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 02.03.01 Математика и компьютерные науки

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

Рабочая программа дисциплины Эллиптические кривые и электронная подпись утверждена на заседании кафедры функционального анализа и алгебры
протокол № 9 от «10» апреля 2020 г.
Заведующий кафедрой (разработчика) Барсукова В.Ю. _____

Рабочая программа обсуждена на заседании кафедры функционального анализа и алгебры
протокол № 9 от «10» апреля 2020 г.
Заведующий кафедрой (выпускающей) Барсукова В.Ю. _____

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук,
протокол № 2 от «30» апреля 2020 г.
Председатель УМК факультета Шмалько С.П. _____

Рецензенты:

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

Дроботенко М.И. к.ф.-м.н., зав. кафедрой математических и компьютерных методов 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 «Эллиптические кривые и электронная подпись»: получение базовых теоретических и исторических сведений о структуре информатизации, ее развитии, применении этих знаний на практике, перспектив развития математических и компьютерных наук, месте и роли защиты информации в структуре информатизации.

Изучение теоретических основ предмета: автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите; информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите; технологии обеспечения информационной безопасности автоматизированных систем; системы управления информационной безопасностью автоматизированных систем;

Развитие навыков разработки алгоритмов и практического решения прикладных задач информатизации. Сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности автоматизированных систем; подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Эллиптические кривые и электронная подпись» относится к части, формируемой участниками образовательных отношений блока Б1 и является дисциплиной по выбору.

Курс «Эллиптические кривые и электронная подпись» продолжает, начатое на трех курсах математическое образование и студентов соответствующего направления подготовки. Знания, полученные в этом курсе, могут быть использованы в курсах защита операционных систем и баз данных, криптография, организационно-правовые методы защиты информации и др. Слушатели должны владеть знаниями в рамках программы курсов «Алгебра», «Дискретная математика», «Программирование», «Информатика», «Правоведение».

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 профессиональных компетенций

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-1	Способен демонстрировать базовые знания математических и естественных наук,	О компьютерной реализации информационных объектов.	Определять структуры данных в компьютерной алгебре.	навыками использования основных типов шифров и криптографически

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
2.	ПК-5	основ программирования и информационных технологий Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования	Связи компьютерной алгебры и численного анализа. Элементы теории сложности алгоритмов. об основных задачах и понятиях криптографии об этапах развития криптографии	использовать технику символьных вычислений. требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем.	х алгоритмов; методами криптоанализа простейших шифров: навыками математического моделирования в криптографии; современной научно-технической литературой в области криптографической защиты.

В результате освоения данной дисциплины обучающийся должен:
Знать:
об основных задачах и понятиях криптографии;
о классификации шифров; о нормативно-правовых документах в области защиты информации, о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи;
Уметь использовать:
требования к шифрам и основные характеристики шифров;
принципы построения современных шифрсистем:
типовые поточные и блочные шифры, системы шифрования с открытыми ключами, криптографические протоколы; 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; 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 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):	**48**	**48**			
Занятия лекционного типа	24	24	-	-	-
Лабораторные занятия	24	24	-	-	-

Занятия семинарского типа (семинары, практические занятия)				-	-	-
		-	-	-	-	-
Иная контактная работа:						
Контроль самостоятельной работы (КСР)		2	2			
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)				-	-	-
Реферат		5	5	-	-	-
Подготовка к текущему контролю		6,8	6,8	-	-	-
Контроль:						
Подготовка к экзамену		-	-			
Общая трудоемкость	**час.**	**72**	**72**	**-**	**-**	**-**
	в том числе контактная работа	**50,2**	**50,2**			
	зач. ед	**2**	**2**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 8 семестре *(очная форма)*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Об основных задачах и понятиях криптографии; о классификации шифров; о нормативно-правовых основах защиты информации	18	6		6	6
2	Эллиптические кривые над конечными полями и алгоритмы вычисления на них.	18	6		6	6
3	Табличное и модульное гаммирование.	18	6		6	6
4	Построение больших простых чисел.	15,8	6		6	3,8
	Итого по дисциплине:		**24**		**24**	**21,8**

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.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Об основных задачах и понятиях криптографии; о	Линейные рекуррентные последовательности ЛРП над полем. Характеристический многочлен и начальный вектор ЛРП. о нормативно-правовых	Р

	нормативно-правовых основах защиты информации.	основах защиты информации. О методах криптографического синтеза и анализа; о применениях криптографии в решении задач аутентификации, о методах криптографического синтеза и анализа. о классификации шифров; построения систем цифровой подписи.	
2	Эллиптические кривые над конечными полями и алгоритмы вычисления на них.	Приведение кривой к каноническому виду. Вычисления числа точек на эллиптической кривой. Сложение точек. Нахождение порядков точек. Нахождение порождающих точек эллиптической кривой.	Э
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.	Т
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

2.3.3 Лабораторные занятия.

№	Наименование лабораторных работ	Форма текущего контроля
1	3	4
1	Минимальный многочлен ЛРП, его единственность, вычисление по генератору и характеристическому многочлену. Биномиальная последовательность и ее минимальный многочлен. Биномиальный базис пространства ЛРП над полем.	Р
2	Вычисление периода ЛРП над конечным полем по ее минимальному многочлену. ЛРП максимального периода и ее свойства..	Р
3	Приведение кривой к каноническому виду. Вычисления числа точек на эллиптической кривой. Сложение точек.	Э
4	Нахождение порядков точек. Нахождение порождающих точек эллиптической кривой.	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. Эллиптические кривые над конечными полями и алгоритмы вычисления на них.	Р
8	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 № 9 от 10 апреля 2020 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 от 10 апреля 2020 г.
3	Самостоятельное освоение теории	Рожков А.В. «Теоретико-числовые методы криптографии. Учебное пособие», утвержденное кафедрой функционального анализа и алгебры, протокол № 9 от 10 апреля 2020 г.
4	Решение задач	Рожков А.В. «Решебник типовых задач по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 10 апреля 2020 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 № 9 от 10 апреля 2020 г.

2. Рожков А.В. «Лабораторная работа по теоретико-числовым методам криптографии по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 10 апреля 2020 г.
3. Рожков А.В. «Теоретико-числовые методы криптографии. Учебное пособие», утвержденное кафедрой функционального анализа и алгебры, протокол № 9 от 10 апреля 2020 г.
4. Рожков А.В. «Решебник типовых задач по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 10 апреля 2020 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. Интерактивность подачи материала по дисциплине «Эллиптические кривые и электронная подпись» предполагает не только взаимодействия вида «преподаватель - студент» и «студент - преподаватель», но и «студент - студент». Все эти виды взаимодействия хорошо достигаются при изложении материала на занятиях в ходе дискуссий, а также на лабораторных занятиях в ходе изложения студентами реферативных докладов (возможно в виде презентации).

Семестр	**Вид занятия**	**Используемые интерактивные образовательные технологии**	**Количество часов**
8	Лабораторные занятия	Тема Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты	4
		Тема . Криптоанализ шифров перестановки.	4
		Тема Одно алфавитные и многоалфавитные замены.	2
		Тема Вычисления средствами системы GAP4.	2
	Лабораторные занятия	Дискуссия на тему: «.Вопросы криптоанализа простейших шифров замены... с докладами-презентациями	2
		Круглый стол на тему: «Электронная подпись» с докладами-презентациями	4
		Стандартные алгоритмы криптографической зашиты данных.	2
		Компьютерная симуляция: Нерешенные проблемы. Варианты обобщения конструкции.	4
Итого:			24

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

Дискуссия Возможность дискуссии предполагает умение высказать собственную идею, предложить свой путь решения, аргументировано отстаивать свою точку зрения, связно излагать мысли. Полезны следующие задания: составление плана решения задачи, поиск другого способа решения, сравнение различных способов решения, проведение выкладок для решения задачи и выкладок для проверки правильности полученного решения, рассмотрение задач с лишними и недостающими данными.. Студентам предлагается проанализировать варианты решения, высказать своё мнение. Основной объем использования интерактивных методов обучения реализуется именно в ходе дискуссий, как на лекционных, так и на лабораторных занятиях.

Визуализация. В данном типе занятий 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.)

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. Линейные рекурренты максимального периода и их свойства
2. Подсчет точек на эллиптической кривой.
3. Приведение эллиптической кривой к каноническому виду.
4. Сложение точек эллиптической кривой.
5. Вычисление в кольце многочленов над полем. НОД и НОК.
6. Нахождение обратных элементов по умножению.
7. Поля Галуа, примеры, проведение прямых вычислений.
8. Расширение полей.
9. Логарифм Якоби.
10. Примитивный элемент поля и его нахождение.
11. Решение одного линейного уравнения над кольцом вычетов.
12. Решение системы линейных уравнений над кольцом вычетов.
13. Решение системы линейных уравнений над кольцом целых чисел.
14. Различие между программными и аппаратными реализациями шифров.
15. Функция Эйлера и Мебиуса.
16. Группы обратимых элементов в кольцах.
17. Структура мультипликативной группы кольца вычетов.
18. Обратимые элементы.
19. Примитивные элементы.
20. Особенности использования вычислительной техники в криптографии вопросы организации сетей засекреченной связи.
21. Криптографические хеш-функции.
22. Электронная подпись.
23. Криптографические протоколы.
24. Предмет и задачи программно-аппаратной защиты информации.
25. Идентификация субъекта, понятие протокола идентификации.
26. Пароли и ключи, организация хранения ключей.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Список типовых алгоритмов (для самостоятельных и лабораторных занятий)

1. Приведение эллиптической кривой к каноническому виду.
2. Вычисления числа точек на эллиптической кривой.
3. Сложение точек на эллиптической кривой.

4. Нахождение порядков точек эллиптической кривой.
5. Нахождение порождающих точек эллиптической кривой.
6. Применения и разработки шифровальных средств.
7. Применения электронной подписи.
8. Эллиптические кривые над конечными полями
9. Алгоритмы вычисления в конечных полях.
10. Электронная подпись по схеме Эль Гамаля.
11. Электронная подпись на основе RSA.
12. Случайные и псевдослучайные гаммы.
13. Регистры сдвига с обратной связью.
14. Схема Файстеля.
15. Подсчет количества точек на эллиптической кривой.
16. Операция сложения на эллиптической кривой.
17. Схема алгоритма RSA.
18. Криптограммы, полученные при повторном использовании ключа.
19. Нахождение примитивного элемента конечного поля.
20. Построение таблицы логарифма Якоби конечного поля.
21. Решение систем линейных уравнений над конечным полем.
22. Алгоритм быстрого возведения в степень.
23. Нахождение обратных элементов в конечном поле.
24. Расширения конечных полей.
25. Алгоритм шифрования AES: структура поля $GF(2^8)$, нахождение обратных элементов.
26. Алгоритм шифрования AES: фактор кольцо $GF(2^8)[\mathrm{x}]/\mathrm{ид}((\mathrm{x}+1)^4)$, преобразование столбцов.
27. Алгоритм шифрования AES: Линейное преобразование, собственные значения матрицы $A=\begin{pmatrix}1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\\1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\end{pmatrix}$.
28. Алгоритм RSA – выбор секретных параметров p,q,d, вычисление открытого ключа n,e.
29. Рюкзачная система шифрования. Быстрорастущий вектор. Сокрытие быстрорастущего вектора после преобразования умножения по модулю.
30. Решение систем линейных уравнений по разным модулям.
31. Решение систем линейных уравнений в кольце целых чисел.
32. Линейный регистр сдвига с обратной связью
$S_{n+k}=a_{k-1}S_{n+k-1}+a_{k-2}S_{n+k-2}+\ldots+a_1S_{n+1}+a_0S_n+a, n=0,1,2,\ldots$
33. Характеристический многочлен регистра сдвига $x^k=a_{k-1}x^{k-1}+a_{k-2}x^{k-2}+\ldots+a_1x+a_0$
34. 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 $\beta_1, \beta_2, ..., \beta_k \in P$ являются решениями системы $\begin{cases} \beta_1 \alpha_1^{\,0} + \beta_2 \alpha_2^{\,0} + ... + \beta_k \alpha_k^{\,0} = S_0 \\ \beta_1 \alpha_1^{\,1} + \beta_2 \alpha_2^{\,1} + ... + \beta_k \alpha_k^{\,1} = S_1 \\ ... \\ \beta_1 \alpha_1^{\,k-1} + \beta_2 \alpha_2^{\,k-1} + ... + \beta_k \alpha_k^{\,k-1} = S_{k-1} \end{cases}$.

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, 2-е изд. [Электронный ресурс]. – М.: Горячая линия-Телеком, 2012. - URL: http://e.lanbook.com/view/book/5193/
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/

5.2 Дополнительная литература:

1. Виноградов И.М. Основы теории чисел. 14-е изд. [Электронный ресурс]. - СПб.: Лань, 2020. - URL: https://e.lanbook.com/reader/book/139285
2. Аверченков В.И., Рытов М.Ю., Шпичак С.А. Криптографические методы защиты информации: учебное пособие, 2-е изд. [Электронный ресурс]. – М.: ФЛИНТА, 2017 - URL: https://e.lanbook.com/book/92914.

5.3 Нормативно-правовые документы:

1. Федеральный закон. Об электронной подписи от 06.04.2011 № 63-ФЗ (ред. от 23.06.2016 N 220-ФЗ).

2. Федеральный закон. Об информации, информационных технологиях и о защите информации от 27.07.2006 № 149-ФЗ (ред. от 23.04.2018 N 102-ФЗ).

3. Постановление Правительства РФ. Об использовании простой электронной подписи при оказании государственных и муниципальных услуг от 25.01.2013 № 33 (ред. от 25.10.2017 № 1296).

4. ГОСТ Р 34.11–2012. Информационная технология. Криптографическая защита информации. Функция хэширования.

5. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

1.3. Периодические издания:

Не предусмотрены

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

Интернет-ресурсы:

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. Пакет компьютерной алгебры Maple 2018. http://www.maplesoft.com
5. http://www.pravo.gov.ru – официальный портал правовой информации
6. http://www.government.ru - интернет-портал Правительства РФ
7. http://graph.document.kremlin.ru - раздел «Документы» портала Президента России
8. http://minsvyaz.ru/ru - сайт Минкомсвязи РФ
9. http://www.rsoc.ru - сайт Федеральной службы Роскомнадзор
10. http://www.scrf.gov.ru – сайт Совета безопасности РФ
11. http://base.consultant.ru – сайт правовой информации «Консультант+»
12. http://www.fstec.ru – официальный сайт ФСТЭК России
13. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)/
14. Электронная библиотека http://gen.lib.rus.ec/

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

Согласно учебному плану дисциплины «Эллиптические кривые и электронная подпись» 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 Prime3
3.	Mathcad 14

4.	Microsoft office
5.	MS Windows 10 (x64)
6.	MS Office 2013, MS
7.	Office 2010, 7Zip

в) Перечень свободно распространяемого программного обеспечения

№	Перечень свободно распространяемого программного обеспечения
1.	Пакет компьютерной алгебры Sage 8.1. 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 2018.1. 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. http://www.pravo.gov.ru – официальный портал правовой информации
2. http://www.government.ru - интернет-портал Правительства РФ
3. http://graph.document.kremlin.ru - раздел «Документы» портала Президента России
4. http://minsvyaz.ru/ru - сайт Минкомсвязи РФ
5. http://www.rsoc.ru - сайт Федеральной службы Роскомнадзор
6. http://www.scrf.gov.ru – сайт Совета безопасности РФ
7. http://base.consultant.ru – сайт правовой информации «Консультант+»
8. http://www.fstec.ru – официальный сайт ФСТЭК России
9. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)/
10. 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.	Семинарские занятия	Не предусмотрены
3.	Лабораторные занятия	Лаборатория, укомплектованная специализированной мебелью и техническими средствами обучения – компьютерами
4.	Групповые (индивидуальные) консультации	Аудитория для групповых занятий
5.	Текущий контроль, промежуточная аттестация	Аудитория для групповых занятий
6.	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

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И ЭЛЕКТРОННАЯ ПОДПИСЬ

Направление подготовки 02.03.01 Математика и компьютерные науки
Направленность Алгебра, теория чисел и дискретный анализ

Рабочая программа дисциплины Эллиптические кривые и электронная подпись для студентов направленность Алгебра, теория чисел и дискретный анализ 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 02.03.01 Математика и компьютерные науки. Программа одобрена на заседании кафедры функционального анализа и алгебры и на заседании учебно-методического совета факультета математики и компьютерных наук.

Студенты, освоившие дисциплину Эллиптические кривые и электронная подпись должны знать: требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем: типовые поточные и блочные шифры, системы шифрования с открытыми ключами, криптографические протоколы; основные математические методы, используемые в анализе типовых криптографических алгоритмов. Владеть: криптографической терминологией; навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шифров.

Рабочая программа дисциплины Эллиптические кривые и электронная подпись для студентов направленность Алгебра, теория чисел и дискретный анализ 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 Эллиптические кривые и электронная подпись для студентов направленность Алгебра, теория чисел и дискретный анализ может быть рекомендована для подготовки студентов направления подготовки 02.03.01 Математика и компьютерные науки.

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

Т.А. Крамаренко