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
_____ Т.А. Хагуров
подпись
«28» мая 2021 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 2021

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат:
4E23D21DF7CC6DF6D9D04D6AEAE74F342DA725D9
Владелец: Хагуров Темыр Айтечевич
Действителен: с 13.05.2021 до 13.08.2022

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

02.03.01 Математика и компьютерные науки
(Алгебра, теория чисел и дискретный анализ)

код и наименование направления подготовки

Программу составил(и):
А.В. Рожков, профессор, д.ф.-м.н., профессор _____
И.О. Фамилия, должность, ученая степень, ученое звание подпись

Рабочая программа дисциплины Эллиптические кривые и электронная подпись
утверждена на заседании кафедры функционального анализа и алгебры
протокол № 9 «13» апреля 2021 г.
Заведующий кафедрой функционального анализа и алгебры
Барсукова В.Ю. _____
фамилия, инициалы подпись

Утверждена на заседании учебно-методической комиссии факультета/института математики и компьютерных наук
протокол № 3 «12» мая 2021 г.
Председатель УМК факультета/института Шмалько С.П. _____
фамилия, инициалы подпись

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 «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 вариативной части Блока 1 "Дисциплины (модули)" учебного плана Б1.В.ДВ.09.01.

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 (ПК)

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ПК-1 Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий	
ПК-1.1 Способен решать актуальные и важные задачи фундаментальной и прикладной математики ПК-1.2 Демонстрирует навыки программирования подготовленных алгоритмов решения вычислительных задач, разработки	Знать: О компьютерной реализации инфор-мационных объектов. Связи компьютерной алгебры и численного анализа Уметь: Применять основные математиче-ские методы, используемые в анализе типовых алгоритмов

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
структуры и программирования реляционных баз данных, а также экспертных систем ПК-1.4 Собирает и анализирует научно- техническую информацию с учетом базовых представлений, полученных в области фундаментальной математики, механики, естественных наук, программирования и информационных технологий	Владеть навыками: использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений.
ПК-5 Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования	
ПК-5.1 Анализирует поставленные задачи и выбирает эффективные математические методы при создании алгоритмов и вычислительных программ для решения современных задач математики и механики ПК-5.2 Описывает математические модели, формулирует, теоретически обосновывает и реализует программно численные методы для решения поставленных задач ПК-5.3 Применяет в профессиональной деятельности методику исследования и создания новых моделей, методов и технологий в математике, механике и естественных науках	Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа. 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; Уметь: Определять структуры данных в компьютерной алгебре. использовать технику символьных вычислений. требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем. Владеть: классификации систем компьютерной алгебры; ориентироваться в типовых архитектурах вычислительных процессов; использования библиотеки алгоритмов и пакетов расширения; криптографической терминологией

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):	**30**	**30**			
Занятия лекционного типа	10	10	-	-	-
Лабораторные занятия	20	20	-	-	-
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:		**37.8**	**37.8**			
Курсовая работа		-	-	-	-	-
Проработка учебного (теоретического) материала		8	8	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)				-	-	-
Реферат		3	3	-	-	-
Интер часы		10	10			
Подготовка к текущему контролю		16,8	16,8	-	-	-
Контроль:						
Подготовка к экзамену		-	-			
Общая трудоемкость	**час.**	**72**	**72**	**-**	**-**	**-**
	в том числе контактная работа	**34,2**	**34,2**			
	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	16	2		4	10
2	Эллиптические кривые над конечными полями и алгоритмы вычисления на них.	19	3		6	10
3	Табличное и модульное гаммирование.	16	2		4	10
4	Построение больших простых чисел.	16,8	3		6	7,8
	Итого по дисциплине:		10		20	37,8

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 нормативно-правовых основах защиты информации.	Линейные рекуррентные последовательности ЛРП над полем. Характеристический многочлен и начальный вектор ЛРП. о нормативно-правовых 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.	Р
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 № 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,

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 беседа: «Алгоритмы проверки на простоту..
ЛЗ	Дискуссия на тему: «Ключевая система шифра. с докладами-презентациями
ЛЗ	Круглый стол на тему: «Эллиптические кривые над конечными полями и алгоритмы вычисления на них.» с докладами-презентациями

Семестр	Вид занятия	Используемые интерактивные образовательные технологии	Количество часов
3	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.

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;

– анализ производственных ситуаций;

Практические занятия с запланированными ошибками. После объявления темы преподаватель сообщает, что в ней будет сделано определенное количество ошибок различного типа: содержательные, методические, поведенческие и т. д. Студенты в конце лекции должны назвать ошибки.

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.).

Разбором конкретных ситуаций по форме организации похожа на 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.

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

Компьютерная симуляция – это максимально приближенная к реальности имитация различных процессов и (или) деятельности с использованием программного обеспечения образовательного назначения.

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 $GF(2^8)[x]/\text{ид}((x+1)^4)$, 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
$S_{n+k}=a_{k-1}S_{n+k-1}+a_{k-2}S_{n+k-2}+...+a_1S_{n+1}+a_0S_n+a, n=0,1,2,...$
33. Характеристический многочлен регистра сдвига $x^k=a_{k-1}x^{k-1}+a_{k-2}x^{k-2}+...+a_1x+a_0$
34. 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 $\begin{cases} \beta_1 \alpha_1^{\,0} + \beta_2 \alpha_2^{\,0} + ... + \beta_k \alpha_k^{\,0} = S_0 \\ \beta_1 \alpha_1^{\,1} + \beta_2 \alpha_2^{\,1} + ... + \beta_k \alpha_k^{\,1} = S_1 \\ ... \\ \beta_1 \alpha_1^{\,k-1} + \beta_2 \alpha_2^{\,k-1} + ... + \beta_k \alpha_k^{\,k-1} = S_{k-1} \end{cases}$.

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

Критерии оценивания результатов обучения

Оценка	Критерии оценивания по экзамену
Высокий уровень «5» (отлично)	оценку «отлично» заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку «хорошо» заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку «удовлетворительно» заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

Критерии оценивания по зачету:

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

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

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

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

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

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

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

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован.

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, 2017. - URL: https://e.lanbook.com/reader/book/111097

2. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. [Электронный ресурс]. - СПб.: Лань, 2021. - URL: https://e.lanbook.com/reader/book/153680

5.2 Дополнительная литература:

1. Бухштаб А.А. Теория чисел, 5-е изд. [Электронный ресурс]. - СПб.: Лань, 2020. - URL: https://e.lanbook.com/reader/book/147139/

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

5.3 Нормативно-правовые документы:

1. Федеральный закон. Об электронной подписи от 06.04.2011 № 63-ФЗ (ред. от 02.07.2021 N 359-ФЗ).

2. Федеральный закон. Об информации, информационных технологиях и о защите информации от 27.07.2006 № 149-ФЗ (ред. от 02.07.2021 N 355-ФЗ).

3. Постановление Правительства РФ. Об использовании простой электронной подписи при оказании государственных и муниципальных услуг от 25.01.2013 № 33 (ред. от 23.12.2020 № 2249).

4. ГОСТ Р 34.11–2018. Информационная технология. Криптографическая защита информации. Функция хэширования. Дата введения 2019-06-01.

5. ГОСТ Р 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Дата введения 2019-06-01.

5.3 Периодические издания:

Не предусмотрены

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

Электронно-библиотечные системы (ЭБС):

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

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

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

Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/
2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка (http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование" http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
10. Справочно-информационный портал "Русский язык" http://gramota.ru/;

11. Служба тематических толковых словарей http://www.glossary.ru/;
12. Словари и энциклопедии http://dic.academic.ru/;
13. Образовательный портал "Учеба" http://www.ucheba.com/;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

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

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:

№	Учебный год	Произво-дитель	Наименование	Лицензионный договор	Дата заключения договора
1	2018-2019	Microsoft	Microsoft Windows 8, 10	№73–АЭФ/223-ФЗ/2018 Соглашение Microsoft ESS 72569510	XX.11.2018
2	2018-2019	Microsoft	Microsoft Office Professional Plus	№73–АЭФ/223-ФЗ/2018 Соглашение Microsoft ESS 72569510	XX.11.2018

3	2018-2019	Microsoft	Microsoft Office 365 Professional Plus	№73–АЭФ/223-ФЗ/2018 Соглашение Microsoft ESS 72569510	XX.11.2018
4	2017-2018	Microsoft	Windows 8, 10	№77-АЭФ/223-ФЗ/2017 Соглашение Microsoft ESS 72569510	03.11.2017
5	2017-2018	Microsoft	Microsoft Office Professional Plus	№77-АЭФ/223-ФЗ/2017 Соглашение Microsoft ESS 72569510	03.11.2017
6	2017-2018	Microsoft	Microsoft Visio	№77-АЭФ/223-ФЗ/2017 Соглашение Microsoft ESS 72569510	03.11.2017
7	2018-2019	Новые облачные технологии	МойОфис Частное Облако	№02-еп/223-ФЗ/2018	29.01.2018
8	2018-2019	Новые облачные технологии	МойОфис Стандартный	№02-еп/223-ФЗ/2018	29.01.2018
9	2018-2019	WolframResearch	Mathematica		
10	2017-2018	COMSOL	COMSOL	№51-АЭФ/223-2017	17.07.2017
11	2017-2018	COMSOL	LiveLink for MATLAB	№51-АЭФ/223-2017	17.07.2017
12	2017-2018	StatSoft	Statistica	№74-АЭФ/44-ФЗ/2017	05.12.2017
13	2016-2017	MapleSoft	Maple 18	№127-АЭФ/2014	29.07.2014
14	2016-2017	ABBYY	FineReader 12	№127-АЭФ/2014	29.07.2014
15	2016-2017	Embarcadero	RAD Studio XE6	№127-АЭФ/2015	30.07.2014
16	2016-2017	Corel	CorelDRAW Graphics Suite X7	№127-АЭФ/2015	30.07.2014
17	2016-2017	ABBYY	PDF Transformer+	№127-АЭФ/2014	29.07.2014
18	2016-2017		PROMT Professional 9.5	№127-АЭФ/2014	29.07.2014
19	2016-2017	Mathworks	MATLAB Wavelet Toolbox	№127-АЭФ/2014	29.07.2014
20	2016-2017	Mathworks	Simulink, Signal Processing Toolbox	№127-АЭФ/2014	29.07.2014

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 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 с предустановленными GAP и Sage
4.	Курсовое проектирование	Не предусмотрено
5.	Групповые (индивидуальные) консультации	Аудитория для групповых занятий
6.	Текущий контроль, промежуточная аттестация	Аудитория для групповых занятий

7.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.