

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

«Кемеровский государственный университет»

Математический факультет



Рабочая программа дисциплины
ОСНОВЫ КРИПТОГРАФИИ И ТЕОРИИ КОДИРОВАНИЯ

Направление подготовки
**02.03.02 Фундаментальная информатика и
информационные технологии**

Направленность (профиль) подготовки
Информатика и компьютерные науки

Уровень бакалавриата

Форма обучения
Очная

Кемерово 2015

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.....	3
2. Место дисциплины в структуре ПРОГРАММЫ БАКАЛАВРИАТА.....	4
3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся.....	4
3.1. Объем дисциплины (модуля) по видам учебных занятий (в часах)	5
4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	5
4.1 Разделы дисциплины (модуля) и трудоемкость по видам учебных занятий (в академических часах) для очной формы обучения.....	5
4.2 Содержание дисциплины, структурированное по темам (разделам) для очной формы обучения.....	6
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине.....	10
6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.....	11
6.1 Паспорт фонда оценочных средств по дисциплине.....	11
6.2 Типовые контрольные задания или иные материалы	12
6.3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций.....	21
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	23
8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), необходимых для освоения дисциплины.....	24
9. Методические указания для обучающихся по освоению дисциплины.....	25
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости).....	25
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.....	26
12. Иные сведения и (или) материалы	27
12.1. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья	27

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНесЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

Коды компетенции	Результаты освоения ООП Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ОК-3	- способность использовать основы экономических знаний в различных сферах жизнедеятельности;	Владеть: - способностью использовать основы экономических знаний в различных сферах жизнедеятельности;
ОПК-2	-способность применять в профессиональной деятельности современные языки программирования и языки баз данных, методологии системной инженерии, системы автоматизации проектирования, электронные библиотеки и коллекции, сетевые технологии, библиотеки и пакеты программ, современные профессиональные стандарты информационных технологий;	Уметь: - применять в профессиональной деятельности современные языки программирования и языки баз данных, методологии системной инженерии, системы автоматизации проектирования, электронные библиотеки и коллекции, сетевые технологии, библиотеки и пакеты программ, современные профессиональные стандарты информационных технологий;
ОПК-3	-способность к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям;	Владеть: -способностью к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям;

ПК-4	-способность решать задачи профессиональной деятельности в составе научно-исследовательского и производственного коллектива;	Уметь: - решать задачи профессиональной деятельности в составе научно-исследовательского и производственного коллектива;
ПК-6	-способность эффективно применять базовые математические знания и информационные технологии при решении проектно-технических и прикладных задач, связанных с развитием и использованием информационных технологий.	Уметь: -эффективно применять базовые математические знания и информационные технологии при решении проектно-технических и прикладных задач, связанных с развитием и использованием информационных технологий.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ПРОГРАММЫ БАКАЛАВРИАТА

Дисциплина «Основы криптографии и теории кодирования» относится к дисциплинам по выбору вариативной части направленности “Информатика и компьютерные науки”.

Для освоения данной дисциплины необходимы компетенции, сформированные в рамках освоения дисциплин: «Математический анализ-1», «Математический анализ-2», «Алгебра и геометрия», «Алгоритмы и анализ сложности».

В результате изучения данной дисциплины студенты освоят непростые математические принципы организации криптографической защиты информации, передаваемой и обрабатываемой техническими средствами, что является неотъемлемой составляющей подготовки учащихся по профилю “Информатика и компьютерные науки”.

Дисциплина изучается на 4 курсе в 7 семестре.

3. ОБЪЕМ ДИСЦИПЛИНЫ В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость (объем) дисциплины составляет 144 академических часа, что составляет 4 зачетных единиц (3Е).

3.1. Объём дисциплины (модуля) по видам учебных занятий (в часах)

Объём дисциплины	Всего часов	
	Для очной формы обучения	
Общая трудоемкость базового модуля дисциплины	144	
Контактная* работа обучающихся с преподавателем (по видам учебных занятий)	84	
Аудиторные занятия (всего)	48	
В том числе:		
Лекции	16	
Практические занятия (ПЗ)	32	
в т.ч. в активной и интерактивной формах	32	
Внеаудиторная работа	0	
Самостоятельная работа (всего)	60	
В том числе:		
Расчетно-графические работы	0	
Индивидуальные работы (работа с учебником, конспектом, интернет-сайтами)	48	
Подготовка к промежуточной аттестации	12	
Вид итогового контроля	Экзамен 36	

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Разделы дисциплины (модуля) и трудоемкость по видам учебных занятий (в академических часах) для очной формы обучения

№ п/п	Раздел Дисциплины	Общая трудоём- кость (часах)	Виды учебных занятий, включая са- мостоятельную работу обучающихся и трудоемкость (в часах)			Формы теку- щего контроля успеваемости	
			аудиторные учебные за- нятия		Самостоятельная работа обучаю- щихся		
			всего	лекции	практические занятия		
1.	Введение в крипто- графию.	12	2	2	8	Индивидуаль- ное лабора- торное задание	
2.	Методы симметрич- ных систем защиты информации.	16	2	8	6	Индивидуаль- ные лабора- торные зада- ния	
3.	Асимметричные сис- темы защиты инфор- мации.	20	2	8	10	Индивидуаль- ные лабора- торные зада- ния	
4.	Криптография на эл-	22	4	8	10	Индивидуаль-	

№ п/п	Раздел Дисциплины	Общая трудоём- кость (часах)	Виды учебных занятий, включая са- мостоятельную работу обучающихся и трудоемкость (в часах)			Формы теку- щего контроля успеваемости	
			аудиторные учебные за- нятия		Самостоятельная работа обучаю- щихся		
			всего	лекции	практические занятия		
	липтических кривых.					ные лабора- торные зада- ния	
5.	Методы установления подлинности и целостности данных.	14	2	2	10	Индивидуаль- ные лабора- торные зада- ния	
6.	Системы счисления.	10	2	2	6	Индивидуаль- ные лабора- торные зада- ния	
7.	Способы кодирования и декодирования информации.	14	2	2	10	Индивидуаль- ные лабора- торные зада- ния	
8.	Итоговый контроль	36				Экзамен	
		144	16	32	60	36	

4.2 Содержание дисциплины, структурированное по темам (разделам) для очной формы обучения

№	Наименование раздела дисциплины	Содержание
1.	Введение в криптографию.	Основные понятия, обозначения и задачи криптографии. Основные принципы криптографической защиты информации. Исторические примеры крипtosистем. Алгоритм создания и общепринятые требования для любой крипtosистемы. Функции шифрования. Односторонние функции. Простейшие шифры и их классификация. Примеры. Методы криptoанализа. Частотный анализ текста. Крипто-стойкость алгоритма шифрования. Абсолютно стойкие (совершенные) шифры. Модульная арифметика в криптографии. Решение сравнений. Возведение в большую степень по модулю.
<i>Содержание лекционного курса</i>		
1.1.	Введение в криптографию.	Основные понятия, обозначения и задачи криптографии. Основные принципы криптографической защиты информации. Исторические примеры крипtosистем. Алгоритм создания и общепринятые требования для любой крипtosистемы. Функции шифрования. Односторонние функции. Простейшие шифры и их классификация. Примеры. Методы криptoанализа. Частотный анализ текста. Крипто-стойкость алгоритма шифрования. Абсолютно стойкие (совершенные) шифры. Модульная арифметика в криптографии. Решение сравнений. Возведение в большую степень по модулю.

№	Наименование раздела дисциплины	Содержание
		ской защиты информации. Исторические примеры криптосистем. Алгоритм создания и общепринятые требования для любой криптосистемы. Функции шифрования. Односторонние функции. Простейшие шифры и их классификация. Примеры. Методы криptoанализа. Частотный анализ текста. Криптостойкость алгоритма шифрования. Абсолютно стойкие (совершенные) шифры.
1.2.	Модульная арифметика в криптографии.	Использование модульной арифметики в криптографии. Решение сравнений. Возведение в большую степень по модулю.

Темы практических занятий

1.1.	Математические основы криптографии.	Модульная арифметика в криптографии. Решение сравнений и их систем. Возведение в большую степень по модулю. Подготовка текста к шифрованию. Элементы шифрования (символы, блоки, биграммы, триграмммы).
2.	Методы симметричных систем защиты информации.	Особенности и типы симметричных криптосистем. Шифры замены. Квадрат Полибия. Шифр Виженера. Двоичный шифр Бэкона. Аффинные криптосистемы. Реализация однобуквенных, биграммных и триграммных преобразований. Возможности усложнения. Шифры перестановки. Столбцевая перестановка. Двойная перестановка. Решетка Кардано. Композиция шифров. Способы усложнения шифров. Стандарты симметричных криптосистем США – DES и России – ГОСТ 28147-89.

Содержание лекционного курса

2.1.	Особенности и типы симметричных криптосистем. Шифры замены.	Особенности и типы симметричных криптосистем. Шифры замены. Квадрат Полибия. Шифр Виженера. Двоичный шифр Бэкона. Аффинные криптосистемы. Реализация однобуквенных, биграммных и триграммных преобразований. Возможности усложнения, композиции.
2.2.	Шифры перестановки.	Столбцевая перестановка. Двойная перестановка. Решетка Кардано. Композиция шифров. Способы усложнения шифров. Стандарты симметричных криптосистем США – DES и России – ГОСТ 28147-89.

Темы практических занятий

2.1.	Шифры замены.	Исторические примеры шифров замены. Шифры Цезаря и Виженера и их программная реализация. Квадрат Полибия. Двоичный шифр Бэкона.
2.2.	Аффинные криптосистемы.	Аффинные криптосистемы. Реализация однобуквенных, биграммных и триграммных преобразований. Возможности усложнения, композиции.

№	Наименование раздела дисциплины	Содержание
2.3.	Шифры перестановки.	Столбцевая перестановка. Двойная перестановка. Решетка Кардано.
2.4.	Композиция шифров.	Способы усложнения шифров. Повышение криптостойкости.
3.	Асимметричные системы защиты информации.	Системы защиты с открытым ключом. Необходимые сведения из алгебры для криптосистемы RSA. Криптосистема RSA. Варианты реализации: простой, биграммный, блочный. Неудачный выбор параметров криптосистемы. Атаки на алгоритм RSA. Аутентификация на основе алгоритма RSA.

Содержание лекционного курса

3.1.	Системы защиты с открытым ключом.	Системы защиты с открытым ключом. Необходимые сведения из алгебры для криптосистемы RSA. Криптосистема RSA. Аутентификация на основе алгоритма RSA.
------	-----------------------------------	---

Темы практических занятий

3.1.	Алгоритм RSA.	Системы защиты с открытым ключом. Криптосистема RSA. Необходимые сведения из алгебры для криптосистемы RSA. Выбор параметров криптосистемы.
3.2.	Алгоритм RSA.	Биграммный и блочный варианты реализации.
3.3.	Атаки на алгоритм RSA.	Неудачный выбор параметров криптосистемы. Варианты атак на криптосистему RSA. Атака посредством метода Ферма. Атака в виде бесключевого чтения. Атака повторным шифрованием.
3.4.	Аутентификация RSA.	Подтверждение авторства и подлинности информации. Аутентификация по простому, биграммному и блочному типу RSA.
4.	Криптография на эллиптических кривых.	Основные свойства эллиптических кривых. Абелева группа точек эллиптической кривой. Криптосистемы на эллиптических кривых. Ключевой обмен и шифрование Эль-Гамаля с использованием точек эллиптических кривых. Системы защиты Диффи-Хеллмана и Мэсси-Омуры с использованием точек эллиптических кривых. Критерий простоты, использующий эллиптические кривые. Разложение на множители при помощи эллиптических кривых.

Содержание лекционного курса

4.1.	Эллиптические кривые.	Эллиптические кривые. Абелева группа точек эллиптической кривой. Криптосистемы на эллиптических кривых. Ключевой обмен и шифрование Эль-Гамаля с использованием точек эллиптических кривых.
4.2.	Криптосистемы на точках эллиптической кривой.	Системы защиты Диффи-Хеллмана и Мэсси-Омуры с использованием точек эллиптических

№	Наименование раздела дисциплины	Содержание
		кривых. Критерий простоты, использующий эллиптические кривые. Разложение на множители при помощи эллиптических кривых.
Темы практических занятий		
4.1.	Абелева группа точек эллиптической кривой.	Операции в абелевой группе точек эллиптической кривой. Сложение и удвоение точек, определение кратных точек.
4.2.	Криптосистема Эль-Гамаля.	Криптосистемы на эллиптических кривых. Ключевой обмен и шифрование / дешифрование Эль-Гамаля с использованием точек эллиптических кривых.
4.3.	Криптосистемы Диффи-Хеллмана и Мэсси-Омуры.	Ключевые обмены и системы защиты Диффи-Хеллмана и Мэсси-Омуры с использованием точек эллиптических кривых.
4.4.	Критерий простоты.	Критерий простоты, использующий эллиптические кривые.
4.5.	Факторизация.	Разложение на множители при помощи эллиптических кривых.
5.	Методы установления подлинности и целостности данных.	Аутентификация данных. Электронная цифровая подпись. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля.
Содержание лекционного курса		
5.1.	Аутентификация данных.	Аутентификация данных. Электронная цифровая подпись. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля.
Темы практических занятий		
5.1.	Генерация ЭЦП.	Аутентификация данных. Электронная цифровая подпись. Генерация цифровой подписи на основе криптосистемы Эль-Гамаля.
5.2.	Проверка ЭЦП.	Проверка цифровой подписи на основе криптосистемы Эль-Гамаля.
6.	Системы счисления.	Алгоритм перевода числа из десятичной системы счисления в двоичную и наоборот. Правила выполнения арифметических действий в различных системах счисления.
Содержание лекционного курса		
6.1.	Системы счисления.	Алгоритм перевода числа из десятичной системы счисления в двоичную и наоборот. Правила выполнения арифметических действий в различных системах счисления.
Темы практических занятий		
6.1.	Системы счисления.	Перевод числа из десятичной системы счисления в двоичную и наоборот. Арифметических действий в различных системах счисления.

№	Наименование раздела дисциплины	Содержание
7.	Способы кодирования и декодирования информации.	Способы кодирования. Эффективность кода. Метод Шеннона-Фано. Метод Хаффмена. Алфавитное кодирование. Алфавитное равномерное двоичное кодирование. Байтовый код. Алфавитное неравномерное двоичное кодирование. Азбука Морзе.
<i>Содержание лекционного курса</i>		
7.1.	Кодирование / декодирование информации.	Способы кодирования. Эффективность кода. Метод Шеннона-Фано. Метод Хаффмена. Алфавитное равномерное двоичное кодирование. Байтовый код. Алфавитное неравномерное двоичное кодирование. Азбука Морзе.
<i>Темы практических занятий</i>		
7.1.	Способы кодирования.	Метод Шеннона-Фано. Метод Хаффмена.

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. <http://www.cryptography.ru/> – научно-информационный ресурс, полностью посвященный математической криптографии.
2. <http://gouspo.ru/> – сайт, созданный для студентов средних и высших учебных заведений, представляющий научно-информационный ресурс по криптографии и теории кодирования, а также по связанных с ними областями теоретической и прикладной математики.
3. <https://www.python.org/> – сайт, содержащий необходимые дистрибутивы и полную информацию для языка программирования Python, который при использовании криптографических модулей, позволяет быстро и наглядно проводить шифрование/расшифрование по разным алгоритмам, а также создавать свои собственные криптографические приложения. Интерпретатор для Python можно использовать как программируемый высокогоревненный калькулятор, что также полезно при обучающем “ручном” шифровании/расшифровании, которое позволяет студентам глубже, полнее понять современные алгоритмы шифрования.
4. <http://sympy.org/> – сайт, посвященный пакету sympy, представляющему собой библиотеку Python символьных вычислений. Свободный пакет sympy содержит криптографический модуль sympy.crypto.crypto.py.
5. <http://univerty.ru/video/matematika/> Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научнопопулярная лекция по интересующему вас вопросу.
6. <http://www.iqlib.ru/> Электронная библиотека Iqlib образовательных и просветительских изданий. Образовательный ресурс, объединяющий в себе ин-

тернет-библиотеку и пользовательские сервисы для полноценной работы с библиотечными фондами. Свободный доступ к электронным учебникам, справочным и учебным пособиям. Аудитория электронной библиотеки IQlib – студенты, преподаватели учебных заведений, научные сотрудники и все те, кто хочет повысить свой уровень знаний.

7. <http://eqworld.ipmnet.ru/tu/library.htm> EqWorld – мир математических уравнений. Учебно-образовательная физико-математическая библиотека. Электронная библиотека содержит DjVu- и PDF-файлы учебников, учебных пособий, сборников задач и упражнений, конспектов лекций, монографий, справочников и диссертаций по математике, механике и физике. Все материалы присланы авторами и читателями или взяты из Интернета (из www архивов открытого доступа). Основной фонд библиотеки составляют книги, издававшиеся тридцать и более лет назад.
8. http://www.edu.ru/modules.php?op=modload&name=Web_Links&file=index&l_op=viewlink&cid=1314 Федеральный портал "Российское образование". Каталог образовательных ресурсов.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

(Перечень компетенций с указанием этапов их формирования; описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания; типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы; методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций)

6.1 Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции (или её части) / и ее формулировка – по желанию	наименование оценочного средства
1	Введение в криптографию	ПК-4, 6; ОПК-2,3	Инд. лабор. работа №1
2	Методы симметричных систем защиты информации.	ПК-4, ПК-6	Инд. лабор. работа №2,3,4
3	Асимметричные системы защиты информации.	ПК-4, ПК-6	Инд. лабор. работа №5-9
4	Криптография на эллиптических кривых.	ПК-4, ПК-6	Инд. лабор. работа №10-13
5	Методы установления подлинности и целостности данных.	ПК-4, ПК-6	Инд. лабор. работа №14,15
6	Системы счисления.	ПК-4, ПК-6	Инд. лабор. работа №16
7	Способы кодирования и декодирования информации.	ПК-4, ПК-6	Инд. лабор. работа №17
8	Экзамен	ПК-4, 6; ОПК-2,3; ОК-3	Экзамен

6.2 Типовые контрольные задания или иные материалы

6.2.1. Экзамен

a) типовые вопросы (задания):

1. Основные понятия, обозначения и задачи криптографии.
2. Основные принципы криптографической защиты информации. Исторические и литературные примеры крипtosистем.
3. Алгоритм создания и требования для любой крипtosистемы. Частотный анализ текста.
4. Функции шифрования. Односторонние функции.
5. Простейшие шифры и их классификация. Примеры.
6. Методы криptoанализа. Частотный анализ текста.
7. Криптостойкость алгоритма шифрования. Абсолютно стойкие (совершенные) шифры.
8. Модульная арифметика в криптографии. Решение сравнений.
9. Алгоритм возведения в степень по модулю методом повторного возведения в квадрат.
10. Методы факторизация натуральных чисел. Метод факторизации Ферма.
11. Тестирование чисел на простоту. Детерминированный метод пробных делений.
12. Тестирование чисел на простоту. Вероятностный метод Ферма.
13. Особенности и типы симметричных крипtosистем. Общие принципы шифрования и дешифрования с секретным ключом, примеры.
14. Шифры замены. Квадрат Полибия.
15. Шифры Цезаря и Виженера.
16. Двоичный шифр Бэкона.
17. Аффинные крипtosистемы. Формулы шифрования и дешифрования k-буквенных блоков.
18. Возможности повышения криптостойкости аффинных крипtosистем.
19. Шифры перестановки. Столбцевая перестановка. Двойная перестановка. Решетка Кардано.
20. Композиция шифров. Способы усложнения шифров.
21. Стандарты симметричных крипtosистем США – DES и России – ГОСТ 28147-89.
22. Криптография с открытым ключом. Общая схема алгоритмов.
23. Крипtosистема RSA.
24. Особенности простого, биграммного и блочного типов шифрования RSA.
25. Аутентификация с помощью алгоритма RSA.
26. Атака на алгоритм RSA посредством метода Ферма.
27. Атака на алгоритм RSA на основе Китайской теоремы об остатках.
28. Атака на алгоритм RSA методом повторного шифрования.
29. Атака на алгоритм RSA в виде бесключевого чтения.
30. Основные свойства эллиптических кривых.
31. Абелева группа точек эллиптической кривой над полем вещественных чисел. Формулы сложения и удвоения точек эллиптической кривой.
32. Абелева группа точек эллиптической кривой. Алгоритм нахождения кратных точек.
33. Построение эллиптической группы $E_p(a, b)$.
34. Определение порядка эллиптической кривой. Теорема Хассе.
35. Крипtosистемы на эллиптических кривых.
36. Ключевой обмен и шифрование с использованием группы точек эллиптической кривой. Аналог системы Эль-Гамала.

37. Ключевой обмен и шифрование с использованием группы точек эллиптической кривой.
Шифрование с ключевым обменом Диффи-Хеллмана.
38. Ключевой обмен и шифрование с использованием группы точек эллиптической кривой.
Шифрование с ключевым обменом Месси-Омуры.
39. Критерий простоты, использующий эллиптические кривые.
40. Разложение на множители при помощи эллиптических кривых.
41. Аутентификация данных. Электронная цифровая подпись.
42. Алгоритм цифровой подписи, основанный на группе точек эллиптической кривой. Генерация и проверка цифровой подписи.
43. Общая формула записи числа. Двоичная система счисления.
44. Алгоритм перевода числа из десятичной системы счисления в двоичную и наоборот.
45. Правила выполнения арифметических действий в различных системах счисления.
46. Способы кодирования. Эффективность кода. Повышение эффективности кодирования.
47. Декодирование эффективных кодов.
48. Алфавитное равномерное двоичное кодирование. Байтовый код.
49. Алфавитное неравномерное двоичное кодирование. Азбука Морзе.
50. Блочное двоичное кодирование.

Экзаменационные билеты

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Криптография с открытым ключом. Общая схема алгоритмов.
2. Абелева группа точек эллиптической кривой. Алгоритм нахождения кратных точек.
3. Сгенерируйте ЭЦП для сообщения с известным значением хеш-свертки $e = 6$, зная секретный ключ подписи $d = 12$ при данном значении выбранного случайным образом числа $k = 11$. Используйте кривую $E_{751}(-1, 1)$ и генерирующую точку $G = (416, 55)$ порядка $n = 13$.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Симметричные криптосистемы. Общие принципы шифрования и дешифрования с секретным ключом, примеры.
2. Ключевой обмен и шифрование с использованием группы точек эллиптической кривой. Аналог системы Эль-Гамаля.
3. Вычислить вручную значение $a^b \pmod{c}$, где $a = 2784$, $b = 1509$, $c = 1876$.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 3

1. Аффинные криптосистемы. Формулы шифрования и дешифрования k -буквенных блоков.
2. Абелева группа точек эллиптической кривой над полем вещественных чисел. Формулы сложения и умножения точек эллиптической кривой.
3. Проверьте подлинность ЭЦП $(r,s) = (5, 2)$ для сообщения с известным значением хеш-свертки $e = 7$, зная открытый ключ проверки подписи $Q = (384, 276)$. Используйте кривую $E_{751}(-1, 1)$ и генерирующую точку $G = (562, 89)$ порядка $n = 13$.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 4

1. Алгоритм RSA.
2. Построение эллиптической группы $E_p(a, b)$.
3. Вычислить вручную значение $a^b \pmod{c}$, где $a = 9928$, $b = 413$, $c = 82224$.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 5

1. Биграммное аффинное шифрование и варианты повышения его криптостойкости.
2. Определение порядка эллиптической кривой. Теорема Хассе.
3. С помощью аутентификации RSA по блочному типу, зная открытый ключ $(N, e) = (15340529, 11)$ некоторого пользователя, прочитать подписанное им сообщение, которое было зашифрованное с помощью его секретного ключа:

[274222, 418138, 13295380, 12308006, 8129207, 9153358, 6742899, 6166592, 5856356,
13426228, 6236914, 10161915, 13264927, 10810889]

Известно, что сообщение использует следующий алфавит:
 {А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я 0 1 2 3 4 5 6 7 8 9 , . ; ! ? - / @ ' > < }.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 6

1. Ключевой обмен и шифрование с использованием группы точек эллиптической кривой. Шифрование с ключевым обменом Диффи-Хеллмана.
2. Тестирование чисел на простоту. Детерминированный метод пробных делений.
3. С помощью аутентификации RSA по блочному типу, зная открытый ключ $(N, e) = (73101929, 17)$ некоторого пользователя, прочитать подписанное им сообщение, которое было зашифрованное с помощью его секретного ключа:

[1450188, 1715206, 1093452, 654506, 64222, 471468, 690382, 235326, 1064974, 1018936,
393299, 737947, 105430, 319499, 1502154, 1457309, 1095900, 1114257, 1159061]

Известно, что сообщение использует следующий алфавит:
 {А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я 0 1 2 3 4 5 6 7 8 9 , . ; ! ? - / @ ' > < }.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 7

1. Тестирование чисел на простоту. Вероятностный метод Ферма.
2. Генерация и проверка цифровой подписи.
3. С помощью аутентификации RSA по блочному типу, зная открытый ключ $(N, e) = (100224511, 13)$ некоторого пользователя, прочитать подписанное им сообщение, которое было зашифрованное с помощью его секретного ключа:

[7390786, 75346952, 19607770, 22406579, 26718200, 87407941, 21151654, 406682,
59573964, 98450550, 77721959, 25061258, 8719537, 5097858]

Известно, что сообщение использует следующий алфавит:

{А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Щ Ъ Ы Ъ Э Ю Я 0 1 2 3 4 5 6 7 8 9 , . ; ! ? - / @ ' > < }.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 8

1. Атака на алгоритм RSA на основе Китайской теоремы об остатках. Другие варианты атак.
2. Алгоритм цифровой подписи, основанный на группе точек эллиптической кривой.
3. Вычислить вручную значение $a^b \pmod{c}$, где $a = 1685$, $b = 809$, $c = 1876$.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 9

1. Основные принципы криптографической защиты информации. Исторические и литературные примеры криптосистем. Частотный анализ текста.
2. Особенности и примеры эллиптических криптосистем.
3. Сгенерируйте ЭЦП для сообщения с известным значением хеш-свертки $e = 8$, зная секретный ключ подписи $d = 6$ при данном значении выбранного случайным образом числа $k = 3$. Используйте кривую и генерирующую точку $G = (416, 55)$ порядка $n = 13$.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 10

1. Шифры замены. Шифры Цезаря и Виженера.
2. Аутентификация с помощью алгоритма RSA.
3. Используя метод факторизации Ферма, определить (p,q) в разложении $N = p \cdot q$ и зашифровать некоторое сообщение-пословицу открытым ключом $(N,e) = (15340529, 11)$ по биграммному типу RSA со своей личной подписью.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 11

1. Двоичная система счисления. Алгоритм перевода числа из десятичной системы счисления в двоичную и наоборот.
2. Методы факторизация натуральных чисел. Метод факторизации Ферма.
3. Провести шифрование Виженера некоторой пословицы (более 5 слов) с кодовым словом «Виженер».

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 12

1. Шифры замены. Шифры Бэкона и Полибия.
2. Ключевой обмен и шифрование с использованием группы точек эллиптической кривой. Шифрование с ключевым обменом Месси-Омуры.

3. Используя метод факторизации Ферма, определить (p,q) в разложении $N = p \cdot q$ и зашифровать некоторое сообщение-пословицу открытым ключом $(N,e) = (100224511, 13)$ по блочному типу RSA со своей личной подписью.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 13

1. Алгоритм создания и требования для любой криптосистемы. Типы шифров.
2. Атака на алгоритм RSA посредством метода Ферма. Другие варианты атак.
3. Перевести число 19 в двоичную систему, а число 243 в пятеричную систему счисления.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 14

1. Шифры перестановки. Столбцевая перестановка. Двойная перестановка. Решетка Кардано.
2. Атака на алгоритм RSA в виде бесключевого чтения. Другие варианты атак.
3. Для точек P, Q, R эллиптической кривой кривой $E_{751}(-1, 1)$ найти точку $3P - 2Q$, если $P = (58, 139)$, $Q = (82, 481)$.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 15

1. Стандарты симметричных криптосистем США – DES и России – ГОСТ 28147-89.
2. Алгоритм возведения в степень по модулю методом повторного возведения в квадрат.
3. С помощью аутентификации RSA по блочному типу, зная открытый ключ некоторого пользователя $(N,e) = (2741881, 17)$, прочитать подписанное им сообщение, которое было зашифрованное с помощью его секретного ключа:

[1586774, 2534057, 2024182, 1430822, 2210439, 875996, 1002166, 2584969, 2481441, 1779188, 2226423, 61826, 809088, 1133592, 2559077, 69172]

Известно, что сообщение использует следующий алфавит:
{А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Щ Ъ Ы Ъ Э Ю Я 0 1 2 3 4 5 6 7 8 9 , . ; ! ? - / @ ' > < }.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 16

1. Исторические и литературные примеры криптосистем. Частотный анализ текста.
2. Типы ключевого обмена с помощью группы точек эллиптической кривой $E_p(a, b)$.
3. Проверьте подлинность ЭЦП $(r,s) = (11,9)$ для сообщения с известным значением хеш-свертки $e = 4$, зная открытый ключ проверки подписи $Q = (384, 475)$. Используйте кривую $E_{751}(-1, 1)$ и генерирующую точку $G = (562, 89)$ порядка $n = 13$.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 17

1. Криптография с открытым ключом. Общая схема алгоритмов.

2. Построение эллиптической группы $E_p(a, b)$ и алфавита на точках эллиптической кривой.
3. С помощью аутентификации RSA по блочному типу, зная открытый ключ $(N, e) = (1847957, 23)$ некоторого пользователя, прочитать подписанное им сообщение, которое было зашифрованное с помощью его секретного ключа:

[1450188, 1715206, 1093452, 654506, 64222, 471468, 690382, 235326, 1064974, 1018936, 393299, 737947, 105430, 319499, 1502154, 1457309, 1095900, 1114257, 1159061]

Известно, что сообщение использует следующий алфавит:
{А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Щ Ъ Ы Ь Э Ю Я 0 1 2 3 4 5 6 7 8 9 , . ; ! ? - / @ ' > < }.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 18

1. Способы кодирования. Эффективность кода. Повышение эффективности кодирования.
2. Аутентификация и криптосистемы с открытым ключом.
3. Для точек P, Q, R эллиптической кривой $E_{751}(-1, 1)$ найти точку

$2P - 5Q$, если $P = (58, 139)$, $Q = (67, 667)$.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 19

1. Алгоритм создания и требования для любой криптосистемы. Типы шифров.
2. Ключевой обмен и шифрование с использованием группы точек эллиптической кривой. Шифрование с ключевым обменом Диффи-Хеллмана.
3. Используя метод факторизации Ферма, определить (p, q) в разложении $N = p \cdot q$ и зашифровать некоторое сообщение-пословицу открытым ключом $(N, e) = (1847957, 23)$ по блочному типу RSA со своей личной подписью.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 20

1. Симметричные криптосистемы. Общие принципы шифрования и дешифрования с секретным ключом, примеры.
2. Атака на алгоритм RSA на основе Китайской теоремы об остатках. Другие варианты атак.
3. Проверьте подлинность ЭЦП $(r, s) = (11, 1)$ для сообщения с известным значением хеш-свертки $e = 7$, зная открытый ключ проверки подписи $Q = (596, 433)$. Используйте кривую $E_{751}(-1, 1)$ и генерирующую точку $G = (562, 89)$ порядка $n = 13$.

б) критерии оценивания компетенций (результатов):

Экзаменационный билет содержит три вопроса. Два первых вопроса являются теоретическими об основных понятиях криптографии и изученных криptoалгоритмах. Ответы на них должны содержать описание методов и математических принципов организации криптографической защиты информации. Последний вопрос – практический, заключается в решении смоделированной криптографической задачи или вспомогательной математической задачи, лежащей в основе

некоторого криптоалгоритма. Третий вопрос предполагает описание математических моделей, подходов к их решению и различных конструкций в которых реализуются решения задач математического моделирования в данной области.

Теоретическая часть экзаменационного билета, состоящая из двух первых вопросов оценивается в

0 баллов – если ответ содержит ошибки или нет ответа на вопрос билета;

10 баллов – если ответ не полный, имеются неточно или отсутствует доказательство;

14 баллов – если в ответе содержатся несущественные ошибки или отсутствует часть доказательства;

20 баллов – если ответ полный, приведены доказательства.

Практическая часть экзаменационного билета, состоящая из одного практического задания оценивается

0 баллов – отсутствует решение задачи или допущены ошибки;

10 баллов – решение не полное, имеются неточно или часть задачи не решена;

14 баллов – в решении содержатся несущественные ошибки или отсутствуют пояснения;

20 баллов – решение полное, приведены пояснения.

Оценка за экзамен:

- «удовлетворительно», если удалось набрать 41 балл при условии, что сданы индивидуальные лабораторные работы и достигнут проходной рубежный балл в 11 баллов;
- для получения оценки «хорошо» необходимо набрать 66 баллов при том же условии;
- для получения оценки «отлично» необходимо набрать 86 баллов.
- «не удовлетворительно» в других случаях.

В экзаменационную ведомость выставляется две оценки:

- оценка за экзамен;
- количество баллов.

Студенту при сдаче экзамена необходимо показать овладение способностью применять в профессиональной деятельности современные языки программирования (ОПК-2); способностью к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей (ОПК-3); способностью решать задачи профессиональной деятельности в составе научно-исследовательского и производственного коллектива (ПК-4); способностью эффективно применять базовые математические знания и информационные технологии при решении проектно-технических и прикладных задач, связанных с развитием и использованием информационных технологий (ПК-6).

в) описание шкалы оценивания:

Баллы	отметки
0 - 40	неудовлетворительно
41 - 65	удовлетворительно
66-85	хорошо
86-100	отлично

6.2.2. Лабораторные работы

а) типовые вопросы и практические задания:

Список индивидуальных лабораторных заданий

- 1) Вычислить вручную значение $ab \pmod c$ и проверить с помощью программы BCALC для $a = 9928, b = 413, c = 82224$.
- 2) Шифрование и расшифрование текста по методу Виженера с помощью криптографического модуля в Python.
- 3) Дан текст, зашифрованный шифром Виженера. С помощью частотного анализа на Python и теста Казиски требуется определить кодовое слово и восстановить открытый текст.

Шифрованный текст:

влцдутжбюцхъяррмшбрхцэооэцгбрьцмийфктььюмшэсяцпунуящэйтаяэдкцибрыцгбрпац
къуцпъбсэгкцъгуущарцёэвърюоуюэкааэбрняфукабъарпяфкъиъжяффниояфывбнэнфу
югбрьсшъжэтбэёчююръегофкбъябашвёуъюаднчжчужцёэвлрнчулбюпцурунъшсю
ъзкцхъяррнрюяспэмасчкпэужъжыатуфуяртубурьпэшлафоуфбюацмнубсюкитайэд
йуноэгюожбгкбрънцэпотчмёодзцвбцищвщепчдчръньюскасэгъппэгюкдойрсрэвоопчи
шоказръбнэугнялёкьсрбёуыбдэулбюасшоуэтъшкреддугэфлбубуъчнчтрапэгюокиугюэмэг
юккъяэгяапуфуэзърадзъжчюрмфцхраююанчёчюыхъцомэфъцпоиръкнщпэтэузябашу
щбаяэйчдфрпэцъярьцъцпоилуфэдцойэдятрачкубуфнитаяэдкцикрннциоабугюубурьпий
эъжтгюркующоуфъэгясуоичщцдцсфырэдщэуяфшёчцюйршвяхвмкршрпгюопэуцчайт
ъэдкцибрыцяжтюрбуэтэбдуящэубъибрювъежагибрбагымпуноцшяжчекфодщоъчж
йуъцхчщвуэбдлдъэгясуахзцэбдэулькнъбжяцърёдъбюврнчуяфуоухфекъгцччгэжтан
опчынажпачкуъмэнкйрэфщэъбудэндадъярьеюэлэтчоубъцэфэвлнёэгфдсэвэёкбсчоукга
утэыпуббцкпэгючасъбэнэфъркацхёваетуфяепърювържадфёжбфутощоявъгупчршуите
ачичирамчюфчоуяюонкяжкыкгсцбрясшчийтъжрсщл

- 4) Шифрование и расшифрование текста по аффинному биграммному методу с помощью криптографического модуля в Python.
- 5) С помощью программы BCALC изучить атаку на алгоритм шифрования RSA при неудачном выборе параметров криптосистемы посредством метода Ферма разложения N на простые числа и расшифровать текст C, если $N=99595193774911, e=1908299$,

75790643190143
36869061035180
38422576553598

68899435645717
 16193161920958
 C : 98487458352335
 34167725433806
 96613844267045
 26583768908805
 73052827576371
 94695336463618
 69092596694070

- 6) Разноблочное шифрование и расшифрование («в ручную») пословиц по алгоритму RSA. Использовать четырехразрядные простые p и q .
- 7) Биграммное шифрование и расшифрование текста по алгоритму RSA с помощью криптографического модуля в Python.
- 8) С помощью программы PS изучить атаку на алгоритм шифрования RSA посредством повторного шифрования для параметров: $N=307080138389$, $e=358703$,

150223836156
 41077612181
 164221721708
 163231492773
 84606189584
 211632968571
 C : 76644428054
 67904620890
 263054305449
 31191567018
 224545225463
 30878012295
 216396046580

- 9) Аутентификация сообщений по e-mail.
- 10) Для точек P, Q, R эллиптической кривой $E_{751}(-1, 1)$ найти точку $2P + 3Q - R$, если $P = (58, 139)$, $Q = (67, 667)$, $R = (82, 481)$.
- 11) Для точки P эллиптической кривой $E_{751}(-1, 1)$ и натурального числа n найти точку nP , если $P = (62, 372)$, $n = 128$.
- 12) Зашифруйте открытый текст с помощью алфавита на точках эллиптической кривой $E_{751}(-1, 1)$ с генерирующей точкой $G = (0, 1)$, если
 открытый текст P = мысленный,
 открытый ключ B = (346, 242),
 значения случайных чисел k для букв открытого текста: 6, 17, 18, 11, 18, 2, 4, 2, 12.
 (таблица с алфавитом прилагается)
- 13) С помощью алфавита на точках эллиптической кривой $E_{751}(-1, 1)$ и генерирующей точки $G = (-1, 1)$, зная секретный ключ d , найти открытый текст для данного шифртек-

ста С, если

секретный ключ $d=29$,

шифртекст С: $\{(440, 539), (128, 672)\}; \{(489, 468), (282, 341)\};$
 $\{(489, 468), (45, 720)\}; \{(72, 254), (227, 299)\};$
 $\{(188, 93), (251, 506)\}; \{(72, 254), (319, 518)\};$
 $\{(745, 210), (129, 659)\}; \{(286, 136), (515, 684)\};$
 $\{(568, 355), (395, 414)\}$

(Для работы разрешается использовать интерпретатор Python или калькуляторы BCalc, Crypto.)

- 14) Сгенерируйте ЭЦП для сообщения с известным значением хэш-свертки e , зная секретный ключ подписи d при данном значении выбранного случайным образом числа k . Используйте кривую $E_{751}(-1, 1)$ и генерирующую точку $G = (416, 55)$ порядка $n = 13$ и параметры

$$e=9, d=3, k=5.$$

- 15) Проверьте подлинность ЭЦП (r, s) для сообщения с известным значением хэш-свертки e , зная открытый ключ проверки подписи Q . Используйте кривую $E_{751}(-1, 1)$ и генерирующую точку $G = (562, 89)$ порядка $n = 13$ и параметры

$$e=4, Q = (596, 318), (r, s) = (11, 4).$$

- 16) Перевести число 19 в двоичную систему ($q=2$); число 243 в пятеричную систему ($q=5$).

- 17) Записать данные числа в десятичной системе счисления: 1234_5 ; 101101_2 ; $332,41_5$.

б) *критерии оценивания компетенций (результатов):*

Критерии оценки лабораторных работ:

Незачтено – отсутствует решение задач или допущены ошибки, выполнено менее 30% работы;

Зачтено – в решении содержатся несущественные ошибки или отсутствуют пояснения, выполнено от 50% до 100% работы.

6.3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

Оценка знаний бакалавров проводится с использованием балльно-рейтинговой оценки по дисциплине в соответствии с Положением о балльно-рейтинговой системе оценки достижений студентов КемГУ (КемГУ-МСК-ППД-6.2.3-2.1.6.-136 от 26.06.2013).

Для положительной оценки необходимо выполнить все виды деятельности.

Каждый вид деятельности, домашние, лабораторные работы оцениваются определенным образом:

1. Лекции, практические занятия (наличие конспекта лекции и практикума) – 1 балл каждое занятие.
2. Работа в аудитории у доски – 1 балл за ответ.
3. Выполнение домашних работ – 2 балла каждая работа (+ 1 балл за своевременное выполнение).

4. Лабораторная работа - 5 балльная оценка за выполнение работы.

На практических занятиях контроль осуществляется при ответе у доски, при проверке домашних заданий, защите контрольных работ.

Если студент пропустил занятие, он может его «отработать» - прийти с выполненным заданием к преподавателю в часы консультаций.

Максимальное число баллов, которое может набрать студент – 100 баллов.

При выставлении оценки экзамена учитываются следующие параметры:

1. Наличие индивидуальных лабораторных работ.
2. Теоретическая часть экзаменационного билета, состоящая из двух вопросов:
0 баллов – ответ содержит ошибки или нет ответа на вопрос билета; 10 баллов – ответ не полный, имеются неточно или отсутствует доказательство; 14 баллов – в ответе содержатся несущественные ошибки или отсутствует часть доказательства; 20 баллов – ответ полный, приведены доказательства.
3. Практическая часть экзаменационного билета, состоящая из одного практического задания: 0 баллов – отсутствует решение задачи или допущены ошибки; 10 баллов – решение не полное, имеются неточно или часть задачи не решена; 14 баллов – в решении содержатся несущественные ошибки или отсутствуют пояснения; 20 баллов – решение полное, приведены пояснения.

Итоговая оценка экзамена выставляется на основании 3 параметров указанных выше.

Виды учебной работы	Баллы	Комментарии
Посещение занятий	0 – 10	Баллы выставляются пропорционально количеству посещений.
Активность	0 – 10	Бонусный балл 10 – всем студентам. Снимается по 1 баллу за каждое публичное замечание преподавателя за пассивность на занятии.
Домашние работы	0 – 10	За выполнение домашних заданий.
Лабораторные работы	0 – 30 (20+10)	За выполнение лабораторных работ – 0-20 баллов. Плюс бонус 0-10 баллов за своевременное и правильное выполнение лабораторных работ.
Экзамен	0 – 40	За экзамен. Проходной рубежный (экзаменационный) балл – 11 баллов.
ВСЕГО	0 – 100	100 – максимальный балл.

Оценка экзамена:

- «неудовлетворительно», если либо не сданы индивидуальные лабораторные работы, либо не достигнут проходной рубежный балл (за ответ на экзамене) в 11 баллов;
- «удовлетворительно», если удалось набрать 41 балл при условии, что сданы

индивидуальные лабораторные работы и достигнут проходной рубежный балл;

- для получения оценки «хорошо» необходимо набрать 66 баллов при том же условии;
- для получения оценки «отлично» необходимо набрать 86 баллов.

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

a) основная литература:

1. Фороузан, Бехроуз А. Криптография и безопасность сетей [Текст] : учебное пособие: [пер. с англ.] / Б. А. Фороузан. - Москва : БИНОМ : Интернет-Университет Информационных Технологий, 2010. - 783 с.
2. Глухов, М. М. Введение в теоретико-числовые методы криптографии [Электронный ресурс] : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. - Санкт-Петербург : Лань, 2011. - 400 с. on-line. http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1540
3. Глотова, М. Ю. Математическая обработка информации [Текст] : учебник и практикум для бакалавров / М. Ю. Глотова, Е. А. Самохвалова. - Москва : Юрайт, 2015. - 344 с.

б) дополнительная литература:

1. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Книга 1: Алгебраические и алгоритмические основы. URRS, Изд.2, доп. 2012. 360 с.
2. Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию. Книга 2: Протоколы криптографии на эллиптических кривых. URRS, Изд.2, доп. 2012. 304 с.
3. Акулич, И. Л. Математическое программирование в примерах и задачах [Электронный ресурс] : учебное пособие / И. Л. Акулич. - 3-е изд., стер. - Санкт-Петербург : Лань, 2011. - 352 с. on-line. - (Учебники для вузов. Специальная литература).
http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=2027
4. Червяков, Н.И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии [Электронный ресурс] : монография / Н.И. Червяков, А.А. Евдокимов, А.И. Галушкин [и др.]. — Электрон. дан. — М. : Физматлит, 2012. — 277 с. — Режим доступа:
http://e.lanbook.com/books/element.php?pl1_id=5300 — Загл. с экрана.
5. Карманов, В.Г. Математическое программирование [Электронный ресурс] : . — Электрон. дан. — М. : Физматлит, 2005. — 265 с. — Режим доступа:
http://e.lanbook.com/books/element.php?pl1_id=2194 — Загл. с экрана.
6. Копченова, Н. В. Вычислительная математика в примерах и задачах [Текст] : учебное пособие для вузов / Н. В. Копченова, И. А. Марон. - 3-е изд., стер.

- Санкт-Петербург : Лань, 2009. - 367
с.http://e.lanbook.com/books/element.php?pl1_id=198

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ" (ДАЛЕЕ - СЕТЬ "ИНТЕРНЕТ"), НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. <http://www.cryptography.ru/> – научно-информационный ресурс, полностью посвященный математической криптографии.
2. <http://gouspo.ru/> – сайт, созданный для студентов средних и высших учебных заведений, представляющий научно-информационный ресурс по криптографии и теории кодирования, а также по связанных с ними областями теоретической и прикладной математики.
3. <https://www.python.org/> – сайт, содержащий необходимые дистрибутивы и полную информацию для языка программирования Python, который при использовании криптографических модулей, позволяет быстро и наглядно проводить шифрование/расшифрование по разным алгоритмам, а также создавать свои собственные криптографические приложения. Интерпретатор для Python можно использовать как программируемый высокогоуровневый калькулятор, что также полезно при обучающем “ручном” шифровании/расшифровании, которое позволяет студентам глубже, полнее понять современные алгоритмы шифрования.
4. <http://sympy.org/> – сайт, посвященный пакету SymPy, представляющему собой библиотеку Python символьных вычислений. Свободный пакет SymPy содержит криптографический модуль `sympy.crypto.crypto.py`.
5. <http://univertv.ru/video/matematika/> Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вас вопросу.
6. <http://www.iqlib.ru/> Электронная библиотека IQlib образовательных и просветительских изданий. Образовательный ресурс, объединяющий в себе интернет-библиотеку и пользовательские сервисы для полноценной работы с библиотечными фондами. Свободный доступ к электронным учебникам, справочным и учебным пособиям. Аудитория электронной библиотеки IQlib – студенты, преподаватели учебных заведений, научные сотрудники и все те, кто хочет повысить свой уровень знаний.
7. <http://eqworld.ipmnet.ru/tu/library.htm> EqWorld – мир математических уравнений. Учебно-образовательная физико-математическая библиотека. Электронная библиотека содержит DjVu- и PDF-файлы учебников, учебных пособий, сборников задач и упражнений, конспектов лекций, монографий, справочников и диссертаций по математике, механике и физике. Все материалы присланы авторами и читателями или взяты из Интернета (из www)

архивов открытого доступа). Основной фонд библиотеки составляют книги, издававшиеся тридцать и более лет назад.

8. http://www.edu.ru/modules.php?op=modload&name=Web_Links&file=index&op=viewlink&cid=1314 Федеральный портал "Российское образование". Каталог образовательных ресурсов.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по изучению дисциплины представляют собой комплекс рекомендаций и разъяснений, позволяющих студенту оптимальным образом организовать процесс изучения данной дисциплины.

Методика изучения материала (на что необходимо обращать внимание при изучении материала):

- 1) первичное чтение одного параграфа темы;
- 2) повторное чтение этого же параграфа темы с фиксированием наиболее значительных по содержанию частей;
- 3) проработка материала данного параграфа (terminologический словарь, словарь персонажей);
- 4) после такого прохождения всех параграфов одной темы, повторное (третий раз) чтение параграфов этой темы с фиксированием наиболее значительных по содержанию частей;
- 5) прохождение тренировочных упражнений по теме;
- 6) прохождение тестовых упражнений по теме;
- 7) возврат к параграфам данной темы для разбора тех моментов, которые были определены как сложные при прохождении тренировочных и тестовых упражнений по теме;
- 8) после прохождения всех тем раздела, закрепление пройденного материала на основе решения задач.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ (ПРИ НЕОБХОДИМОСТИ)

1. Лекции с применением мультимедийных материалов, мультимедийная аудитория.

2. Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине в активной и интерактивной формах.

Овладение дисциплиной «Пропедевтика курса математики» предполагает использование следующих образовательных технологий (методов):

• **лекция (вводная, обзорная, репродуктивно-информационная, заключительная)** - целесообразность традиционной лекции состоит в решении следующих образовательных и развивающих задач курса: показать значимость курса для профессионального становления будущего педагога; представить логическую схему изучения представленного курса; сформировать мотивацию бакалавров на освоение

ние учебного материала; связать теоретический материал с практикой будущей профессиональной деятельности; представить научно-понятийную основу изучаемой дисциплины; систематизировать знания бакалавров по изучаемой проблеме; расширить научный кругозор бакалавра как будущего специалиста и т.д.;

• **лекция-беседа** - позволяет учитывать отношение бакалавра к изучаемым вопросам, выявлять проблемы в процессе их осмысливания, корректировать допускаемые ошибки и т.д.;

• **лекция-дискуссия** - представляет организацию диалоговой формы обучения, создающей условия для формирования оценочных знаний бакалавров, обусловливающих проявление их профессиональной позиции как будущего специалиста; формируется умение высказывать и аргументировать личную точку зрения; развивается способность к толерантному восприятию иных точек зрения и т.д.;

• **«мозговой штурм»** - метод коллективного генерирования идей и их конструктивная проработка при решении проблемных задач предполагает создание условий для развития умений выражать собственные взгляды, работать во взаимодействии с другими людьми и т.д.;

• **лекция с разбором конкретных ситуаций** – предполагает включение конкретных ситуаций, отражающих проблемы профессиональной деятельности; создаётся ситуация, позволяющая «перевод» познавательного интереса на уровень профессионального; активизируется возможность занять профессиональную позицию, развить умения анализа, сравнения и обобщения;

• **разработка программ исследования** – предполагает развитие умений системно представить программу изучения математических понятий в физике;

• **тренинг** по использованию методов исследования при изучении конкретных проблем математики – отрабатывается умение и навыки решения математических задач и построения математических моделей;

• **рефлексия** - обеспечивает самоанализ и самооценку достижения результатов познавательной деятельности.

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

При проведении лекционных и семинарских занятий используются мультимедийные средства, компьютерные классы, интерактивные доски, а также классическое учебное оборудование: кабинет методики преподавания, оборудованный доской, инструментами, раздаточным материалом, учебной и методической литературой, периодической литературой по предмету.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие рабочей программе дисциплины.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации.

Содержание учебной дисциплины представлено в сети Интернет.

Научная библиотека КемГУ обладает достаточным для образовательного процесса количеством экземпляров учебной литературы и необходимым минимумом периодических изданий для осуществления методического и научно - исследовательского процесса. Имеются основные отечественные академические и отраслевые научные и методические журналы, кабинет методики преподавания математики, оснащенный учебно-методической литературой и средствами обучения.

Электронно-библиотечные системы (электронная библиотека) издательства «Лань» и «Университетская библиотека online», электронная информационно-образовательная среда обеспечивают одновременный доступ не менее 25 процентов обучающихся по программе бакалавриата.

12. ИНЫЕ СВЕДЕНИЯ И (ИЛИ) МАТЕРИАЛЫ

12.1. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья по дисциплине осуществляется на основе образовательных программ, разработанных факультетом и адаптированных для обучения указанных обучающихся.

Обучение по образовательной программе инвалидов и обучающихся с ограниченными возможностями здоровья осуществляется факультетом с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Учебно-методическая документация по дисциплине предусматривает проработку лекционного материала и выполнение индивидуальных заданий с использованием учебно-методических материалов для самостоятельной работы обучающихся по дисциплине.

Составитель

доцент О.А. Сергеева