Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тульский государственный педагогический университет им. Л. Н. Толстого»
ФГБОУ ВО «ТГПУ им.Л.Н.Толстого»

УТВЕРЖДЕНА

на заседании Ученого совета университета

Протокол № 2

«11» февраля 2016 г.

Рабочая программа дисциплины «Теория чисел и элементы криптографии»

Трудоемкость: 4 зачетные единицы

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Рассмотрена на заседании кафедры алгебры, математического анализа и геометрии
протокол № 5 от «1» декабря 2015 г.
Заведующий кафедрой Добровольский Н.М.

Одобрена на заседании Ученого совета факультета
математики, физики и информатики
протокол № 5 от «17» декабря 2015 г.
Декан Реброва И.Ю.

СОДЕРЖАНИЕ

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

Достижение планируемых результатов обучения, соотнесенных с общими целями и задачами ОПОП, является целью освоения дисциплины.

Планируемые результаты освоения образовательной программы (код и название компетенции)	**Планируемые результаты обучения**	**Этапы формирования компетенции в процессе освоения образовательной программы**
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 (ОПК-3)	***Выпускник знает:*** основные факты и положения теории делимости и теории сравнений; арифметические алгоритмы, связанные с криптографическими системами ***Умеет:*** использовать базовые знания теории чисел для оценки сложности арифметических операций ***Владеет:*** навыками использования арифметических методов кодирования информации	3 этап из 4 (5 семестр)

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Теория чисел и элементы криптографии» относится к обязательным дисциплинам вариативной части учебного плана. Изучение данной дисциплины базируется на освоении студентами дисциплин модуля «Алгебра и геометрия» и предшествует изучению дисциплин «Алгоритмы и анализ сложности», «Компьютерная алгебра».

К началу изучения дисциплины студенты должны владеть базовыми знаниями по основам теории делимости. Знания и умения, полученные в результате освоения дисциплины «Теория чисел и элементы криптографии», будут использоваться при подготовке выпускной квалификационной работы, в научно-исследовательской и практической деятельности.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы	**Объем часов/ зачетных единиц по формам обучения**
	очная
Максимальная учебная нагрузка (всего)	***144/4***
Контактная работа обучающихся с преподавателем (всего)	***54***
в том числе:	
лекции с применением мультимедийных технологий и раздаточным материалом для студентов	*18*
лабораторные занятия с использованием современных информационных технологий по разработке алгоритмов и программ	*6*
практические занятия	*28*

контрольные работы	*2*
Самостоятельная работа студента (всего)	***90***
в том числе:	
внеаудиторная самостоятельная работа при подготовке к лабораторным и практическим занятиям	*36*
подготовка к контрольной работе	*4*
Выполнение заданий для самостоятельной работы в модульной объектно-ориентированной динамической учебной среде Moodle	*14*
Подготовка к экзамену	*36*
Промежуточная аттестация в форме: экзамена	

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Наименование темы		Содержание	Количество академических или астрономических часов по видам учебных занятий				
			Занятия лекционного типа	Занятия семинарского типа	Лабораторные работы	Консультации	Самостоятельная работа обучающихся
Тема 1. Теория делимости	1	*Делимость и простые числа. Основная теорема арифметики. НОД и НОК.*	2	2			4
	2	*Теорема Чебышева о распределении простых чисел*					
Тема 2. Цепные дроби	1	*Непрерывные дроби и их свойства*	2	2			4
	2	*Представление рациональных чисел цепными дробями.*					
Тема 3. Теория сравнений	1	*Числовые сравнения и их свойства. Полная и приведенная системы вычетов.*	2	2			4
	2	*Функция Эйлера. Теоремы Эйлера и Ферма.*					
	3	*Сравнения первой степени. Системы сравнений первой степени.*	2	2			10
	4	*Сравнения n-ной степени по простому модулю.*		2			
	5	*Сравнения n-ной степени по составному модулю.*		2			
	6	*Сравнения второй степени. Квадратичные вычеты и невычеты.*	2	2			4
	7	*Первообразные корни и индексы*		2			
Тема 4. Оценка сложности арифметических операций	1	*Свойства функций оценки сложности*	2	2			6
	2	*Сложность арифметических операций с целыми числами*					
	3	*Сложность алгоритма Евклида*	2	2			4
Тема 5. Арифметические алгоритмы	1	*Проверка простоты. Решето Эратосфена. Критерий Вильсона. Тест на основе малой теоремы Ферма*	2	2			6
	2	*Построение больших простых чисел*					
	3	*Алгоритмы факторизации целых чисел*	2	2	6		6
Тема 6. Криптографическая система RSA	1	*Выбор параметров системы RSA. Взаимосвязь между параметрами системы RSA*	2	4			6
		Экзамен				*2*	*34*
		ИТОГО: 144 часа	18	28	6	2	90

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ «ТЕОРИЯ ЧИСЕЛ И ЭЛЕМЕНТЫ КРИПТОГРАФИИ»

1. Методическая система, используемая автором программы, базируется на оптимальном сочетании активных форм и методов организации учебной деятельности студентов и самостоятельной работы студентов.
2. В системе LMS MOODLE представлены для студентов методические материалы: списки основной и дополнительной литературы, индивидуальные задания, вопросы к экзамену, балльно-рейтинговая система оценки успеваемости студентов.
3. Для активизации работы студентов в течение семестра и лучшего усвоения дисциплины предусмотрена балльно-рейтинговая система оценки успеваемости студентов.
4. Промежуточная аттестация принимается в форме экзамена. Студент получает два теоретических вопроса и 2 задачи по разным разделам курса. После отведенного на подготовку времени проводится индивидуальная беседа преподавателя со студентом, в процессе которой студент должен четко обосновать все свои действия, производимые в результате решения задачи.

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

6.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице пункта 1 рабочей программы.

Формирование компетенции «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» (ОПК-3) осуществляется в течение четырех этапов освоения основной профессиональной образовательной программы.

Первый этап формирования компетенции осуществляется в процессе освоения дисциплины базовой части «Линейная алгебра и многомерная геометрия». Второй этап формирования компетенции осуществляется в процессе освоения дисциплины базовой части «Основные алгебраические структуры». Третий этап формирования компетенции осуществляется в процессе освоения обязательной дисциплины вариативной части учебного плана «Теория чисел и элементы криптографии». Завершающий четвертый этап формирования компетенции осуществляется в процессе освоения дисциплины базовой части «Теория функций комплексного переменного и функциональный анализ».

6.2. Описание показателей, критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Дескриптор компетенций	Показатели оценивания	Критерии оценивания
Знания	основные факты и положения теории делимости и теории сравнений; арифметические алгоритмы, связанные с криптографическими системами	Оценка «отлично» выставляется, если студент в целом за семестр набрал от 81 до 100 баллов (при условии, что на экзамене набрано не менее 20 баллов).

Умения	использовать базовые знания теории чисел для оценки сложности арифметических операций	Оценка «хорошо» выставляется, если студент в целом за семестр набрал от 61 до 80 баллов (при условии, что на экзамене набрано не менее 20 баллов). Оценка «удовлетворительно» выставляется, если студент в целом за семестр набрал от 41 до 60 баллов (при условии, что на экзамене набрано не менее 10 баллов). Оценка «неудовлетворительно» выставляется, если студент в целом за семестр набрал менее 41 балла (или на экзамене набрал менее 10 баллов).
Навыки и опыт деятельности	навыками использования арифметических методов кодирования информации	

Процедура оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих данный этап формирования компетенций, происходит по шкале с оценками: «отлично»; «хорошо»; «удовлетворительно»; «неудовлетворительно».

Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал по дисциплине, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материалы рекомендованной литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.

Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.

Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.

Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

6.3.Типовые контрольные задания и иные материалы, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

Задания, направленные на формирование навыков использования основных фактов и положений теории делимости и теории сравнений

1. Разложить на простые множители: а) 2003; б) 2057.
2. Найти НОД(138, 48) и его линейное представление.
3. Разложить в цепную дробь: $\frac{127}{54}$.
4. Свернуть цепную дробь: [2; 1, 3, 2].
5. Вычислить функцию Эйлера $\varphi(124)$.

6. Решить сравнения первой степени:

а) $19x \equiv 14 \pmod{27}$; б) $18x \equiv 15 \pmod{27}$; в) $15x \equiv 17 \pmod{35}$.

7. Решить в натуральных числах систему уравнений

$$\begin{cases} x + y = 150, \\ (x, y) = 30. \end{cases}$$

8. Найти произведение наименьших натуральных решений сравнения

$$12x \equiv 9 \pmod{15}.$$

9. Решить систему сравнений первой степени

$$\begin{cases} 5x \equiv 1 \pmod{12}, \\ 5x \equiv 2 \pmod{8}, \\ 7x \equiv 3 \pmod{11}. \end{cases}$$

10. Установить, имеет ли решения сравнение: $x^2 \equiv 151 \pmod{587}$.

11. Решить сравнение, предварительно приведя его к двучленному:

$$4x^2 - 11x - 3 \equiv 0 \pmod{23}.$$

12. Решить в целых числах уравнения:

а) $x^2 - 10x - 11y + 5 = 0$, б) $258x - 175y = 113$.

13. Найти сумму наименьших натуральных частных решений сравнения $3x \equiv 9 \pmod{12}$.

14. Решить сравнения с помощью таблицы индексов: $5x^3 \equiv 33 \pmod{37}$.

15. Решить сравнение $x^{15} + 4x^{14} - 2x^{13} + 6x^{12} - 12x^3 + 6x^2 - 3 \equiv 0 \pmod{3}$.

16. Найти две последние цифры числа 2^{21}.

17. Найти последнюю цифру числа 3^{2005}.

18. Составить полную и приведенную систему вычетов по модулю 18.

19. Вычислить символ Лежандра: $\left(\frac{105}{743}\right)$.

Вариант тестового задания

1. Остаток от деления числа 35 на 7 равен: а) 5; б) 0; в) 6; г) 7; д) 8.
2. Произведение наименьшего положительного и наибольшего отрицательного вычетов класса решений системы сравнений

$$\begin{cases} 4x \equiv 3 \pmod{5} \\ 5x \equiv 2 \pmod{3} \end{cases}$$

равно: а) -15; б) -56; в) -65; г) -20; д) -6.

3. Сравнение $6x \equiv 18 \pmod{m}$ имеет 6 решений при m, равном:

а) 11; б) 12; в) 13; г) 14; д) 15.

4. Произведение наибольших отрицательных решений сравнения $3x \equiv 9 \pmod{12}$ равно:

а) 231; б) 45; в) -45; г) -15; д) -5.

5. Наименьшее натуральное число m, при котором $7^{15} \equiv m \pmod{13}$, равно:

а) 5; б) 4; в) 11; г) 2; д) 3.

6. Остаток от деления числа $6 \cdot 5^{61} - 3 \cdot 13^{61}$ на 12 равен; а) 9; б) 5; в) 4; г) 0; д) 3.
7. $\varphi(75)$ равно: а) 30; б) 40; в) 42; г) 44; д) 46.
8. Наибольшее натуральное значение m, при котором имеет место сравнение $200 \equiv 301 \pmod{m}$ равно: а) 100; б) 101; в) 102; г) 105; д) 107.

Задания, направленные на формирование навыков использования базовых знаний теории чисел к построению арифметических алгоритмов, связанных с криптографическими системами

Лабораторная работа: ***Факторизация составного числа***
Цель работы: Освоить простые алгоритмы факторизации составного числа.
Указание к работе: Ознакомиться с приведенными ниже методическими указаниями. Для криптографического вскрытия алгоритма шифрования RSA достаточно разложить часть открытого ключа на простые множители, поэтому задача факторизации составного числа приобрела большое практическое значение. Данная задача является обратной к задаче определения простоты конкретного числа.
Задание. Реализовать приложение, удовлетворяющее следующим требованиям:

1. Во входном файле хранятся входные данные, необходимые для работы программы (например, подлежащее факторизации число).
2. Программа проверяет заданное число на простоту с помощью теста на простоту. Если оно является простым, то процедура факторизации не выполняется.
3. Программа находит разложение заданного числа на произведение простых множителей.
4. Программа выдаёт список простых делителей заданного числа с указанием степени, с которой они входят в разложение числа, время и количество итераций основного цикла, потребовавшихся для разложения.

Далее представлены наиболее простые методы факторизации составного числа.
Метод Ферма.
Данный метод основан на поиске таких чисел x и y, что $x^2 \equiv y^2 \pmod n$, где n надо разложить на множители.
Теорема 1 (Эйлера о представлении числа в виде разности квадратов):
Если $n > 1$ нечетно, то существует взаимно однозначное соответствие между разложениями на множители $n = a \cdot b$ и представлениями в виде разности квадратов $n = x^2 - y^2$, $x > y > 0$. Здесь $x = \frac{a+b}{2}$, $x = \frac{a-b}{2}$, $a = x + y$, $b = x - y$.

Метод Ферма заключается в том, что при малых значениях параметра y в представлении $n = x^2 - y^2$ можно найти пару (x, y), перебирая в качестве кандидатов на значение x числа $\lfloor \sqrt{n} + 1 \rfloor$, $\lfloor \sqrt{n} + 2 \rfloor$, … и проверяя для каждого из них равенства $\left(\lfloor \sqrt{n} + j \rfloor\right)^2 - n = y^2$.

Алгоритм факторизации методом Ферма:
Вход: n – нечетное число, $p_1, \ldots, p_k$ – небольшие простые числа.

1. Проверить, делят ли нацело p_k, $i = \overline{1, k}$ число n. Если да, то делитель найден (остановка алгоритма).
2. Для каждого $x \in \left[\left\lceil \sqrt{n} \right\rceil ; \frac{n}{2} + 1\right]$ вычислить величину $t = x^2 - n$. Если были проверены все x из этого диапазона и ни один делитель не был найден, то число n – простое.
3. Проверить, является ли t полным квадратом. Если $t = y^2$, то n – составное и делитель найден ($a = x + y$, $b = x - y$, останов алгоритма); если t не является полным квадратом, то перейти к следующему x на шаге 2.

(p–1)-факторизация Полларда.
Предположим, что n – нечетное составное число, не имеющее небольших простых делителей. Обозначим через p – наименьший простой делитель числа n. Наша задача заключается в его нахождении.
Предположим, что число p–1 разлагается в произведение небольших простых делителей. Выберем число k, которое является параметром метода. Для успешной работы алгоритма нужно, чтобы выполнялось условие p–1 делит $M(k)$, где $M(k) = \text{НОК}(1, 2, \ldots, k)$ (вместо $M(k)$ можно использовать, например, $k!$).
В силу малой теоремы Ферма выполняется сравнение $2^{M(k)} \equiv 1 \pmod p$. Если при этом $2^{M(k)} \not\equiv 1 \pmod n$, то p делит НОД $(2^{M(k)} - 1, n)$, где $p > 1$, НОД $(2^{M(k)} - 1, n) < n$.
Таким образом, НОД $(2^{M(k)} - 1, n)$ является делителем числа n, кратным p.
Так как число k неизвестно, то оно ищется в алгоритме перебором.
Алгоритм метода (p–1)-факторизации Полларда:
Пусть k – целое число, например, $k < 10^6$ и c – небольшое целое, для которого выполняется условие НОД $(c, n) = 1$, например, $c = 2$.

1. Для каждого $i = \overline{1, k}$ вычисляется $m_i = c^{M(i)} \bmod n$ и проверяется тест шага 2.

2. Вычисляется d = НОД ($m_i - 1$, n). Если $1 < d < n$, то d – нетривиальный делитель числа n. В противном случае полагаем $i = i + 1$.

Оценка сложности данного метода в худшем случае составляет O ($n^{1/2} \cdot \log^{const} n$) арифметических операций. Однако в некоторых случаях алгоритм может быстро выдать делитель числа n.
На практике (p–1)-метод Полларда обычно используют до применения более сильных алгоритмов факторизации для того, чтобы отделить небольшие простые делители числа n.

Метод ρ-Полларда.
Алгоритм:

1. Случайным образом выбирается x_1 из множества {0, 1, … , n–1}. y = x_1, $k = 2$, $i = 1$.
2. $i = i + 1$. Вычисляется следующий элемент последовательности $x_i = f(x_{i-1}) \bmod n$, где $f(x) = x^2 + 1$.
3. Вычисляется d = НОД ($y - x_i$, n). Если $1 < d < n$, то d является делителем n (останов алгоритма), иначе выполняется переход на шаг 4.
4. Если $i < k$, то осуществляется переход на шаг 2.
5. Если $i = k$, то $y = x_i$, $k = 2 \cdot k$ и выполняется переход на шаг 2.

Возможно, что цикл значений по модулю n окажется больше, чем $\sqrt{n}$. Метод имеет эвристическую оценку сложности O ($n^{1/4}$) арифметических операций. Он очень популярен и обычно используется для отделения небольших простых делителей факторизуемого числа n.
Основная идея данного метода очень проста. Если период последовательности $x_i \bmod n$ может быть порядка n, то период последовательности$x_i \bmod p$ для простого делителя p числа n не превосходит p. Это значит, что y и x_i могут быть различными по модулю n, но совпадать по модулю p.
Существует такая константа c, что для любого $\lambda > 0$ вероятность не найти нетривиальный делитель n за $c \cdot \sqrt{\lambda} \cdot n^{1/4} \cdot \log^3 n$ битовых операций будет меньше, чем $e^{-\lambda}$.

Метод Лемана.
Алгоритм: Пусть n нечетно и $n > 8$.

1. Для a = 2, 3, … , [$n^{1/3}$] проверить, что a делит n. Если на этом шаге найдётся делитель числа n, то алгоритм заканчивает свою работу, иначе выполняется переход к шагу 2.
2. Для всех k = 1, 2, … , [$n^{1/3}$] и всех d = 0, 1, … , $\left[\frac{n^{1/6}}{4\sqrt{k}}\right]+1$ проверить, является ли число $\left(\left[\sqrt{4 \cdot k \cdot n}\right]+d\right)^2 - 4 \cdot k \cdot n$ квадратом натурального числа.
3. Если является, то для $A = \left[\sqrt{4 \cdot k \cdot n}\right]+d$ и $B = \sqrt{A^2 - 4 \cdot k \cdot n}$ выполнено сравнение $A^2 \equiv B^2 \pmod n$ (или $(A - B) \cdot (A - B) \equiv 0 \pmod n$). В этом случае вычисляется d^* = НОД ($A - B$, n).
4. Если $1 < d^* < n$, то d^* и (n / d^*) – делители числа n. Алгоритм останавливается.

Если данный алгоритм не нашел разложение n на два множителя, то n – простое число.
Данный алгоритм раскладывает n на множители за O ($n^{1/3}$) арифметических операций.

Замечание: Следует иметь в виду, что все представленные методы ищут только один делитель n. Поэтому необходимо примерять метод несколько раз, пока не получится полное разложение числа на простые множители.

Вопросы к экзамену

1. Делимость и простые числа. Основная теорема арифметики. НОД и НОК.
2. Теорема Чебышева о распределении простых чисел.
3. Непрерывные дроби и их свойства.
4. Представление рациональных чисел цепными дробями.
5. Числовые сравнения и их свойства. Полная и приведенная системы вычетов.
6. Функция Эйлера. Теоремы Эйлера и Ферма.
7. Сравнения первой степени. Системы сравнений первой степени.
8. Сравнения n-ной степени по простому модулю.
9. Сравнения n-ной степени по составному модулю.
10. Сравнения второй степени. Квадратичные вычеты и невычеты.
11. Первообразные корни и индексы.
12. Свойства функций оценки сложности.
13. Сложность арифметических операций с целыми числами.
14. Сложность алгоритма Евклида.
15. Сложность операций в кольце вычетов.
16. Проверка простоты. Решето Эратосфена. Критерий Вильсона. Тест на основе малой теоремы Ферма.

17. Построение больших простых чисел.
18. Алгоритмы факторизации целых чисел.
19. Выбор параметров системы RSA. Взаимосвязь между параметрами системы RSA.

6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и/или опыта деятельности, характеризующие этапы формирования компетенций

Составляющие итоговой оценки за дисциплину:

1) Текущий контроль (общий вес 60 баллов):

до 15 баллов – посещение занятий;

до 30 баллов – выполнение заданий в ходе практических занятий и заданий для самостоятельной работы

до 15 баллов – выполнение заданий в ходе лабораторных работ

2) Итоговый контроль заключается в проведении экзамена (общий вес - 40 баллов). Экзамен проводится по вопросам билетов с обязательным решением задач. Как правило, студент получает два вопроса из приведенного выше списка и две задачи, готовится в присутствии преподавателя и дает подробные комментарии. Студент, пропускавший занятия в ходе семестра, получает дополнительные вопросы и задачи по каждой пропущенной им теме (на усмотрение преподавателя). Шкала перевода баллов в оценку:

Оценка	**«отлично»**	**«хорошо»**	**«удовлетворительно»**	**«неудовлетворительно»**
Интервал количества баллов	81-100	61 - 80	41 - 60	0 - 40

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 (ОПК-3)

Планируемые результаты обучения	**Критерии оценивания с весовым коэффициентом**	**Показатели оценивания**				
		1	**2**	**3**	**4**	**5**
Выпускник знает основные факты и положения теории делимости и теории сравнений	когнитивный – 0.3	Знает о признаках делимости и сравнениях	Знает о признаках делимости и сравнениях и может привести примеры	Знает о признаках делимости и сравнениях, может привести примеры, выделить их в алгоритмах решения прикладных задач	Знает основные положения и факты теории делимости и теории сравнений, может выделить их в алгоритмах решения прикладных задач	Знает основные положения и факты теории делимости и теории сравнений и может эффективно применять их при решении конкретных практических задач информатики
Выпускник знает арифметические алгоритмы, связанные с криптографическими системами	когнитивный – 0,2	Знает о существовании криптосистем	Знает о существовании арифметических алгоритмов, используемых в криптосистемах	Знает арифметические алгоритмы, используемых в криптосистемах, и может описать их средствами языка для	Знает арифметические алгоритмы, используемых в криптосистемах, семантику команд и сущность процессов,	Знает тонкости процессов, происходящих в среде программирования при обработке арифметических алгоритмов, используемых в

				обработки в программе	происходящих в среде при их обработке	криптосистемах
Выпускник умеет использовать базовые знания теории чисел для оценки сложности арифметических операций	деятельностный – 0,25	Способен понять сложность арифметических операций с точки зрения теории чисел	Способен понять и объяснить сложность арифметических операций на основе положений теории чисел	Способен модифицировать алгоритм, использующий арифметические операции, с точки зрения его упрощения на основе положений теории чисел	Способен самостоятельно написать алгоритм, использующий арифметические операции, на основе положений теории чисел	Способен самостоятельно написать и оценить алгоритм, использующий арифметические операции, на основе положений теории чисел
Выпускник владеет навыками использования арифметических методов кодирования информации	деятельностный – 0,25	Владеет приемами использования арифметических методов кодирования информации	Способен способ реализации предложенного алгоритма, реализующего арифметические методы кодирования информации	Способен разработать алгоритм кодирования информации арифметическими методами и реализовать его программными средствами	Способен выбрать наиболее эффективные средства для программной реализации разработанного самостоятельно алгоритма кодирования информации арифметическими методами	Способен составить оптимальный алгоритм кодирования информации арифметическими методами, выбрать и обосновать свой выбор его программной реализации, оценить полученные результаты и предложить систему тестов

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

7.1 Основная литература:

1. Глухов М.М. и др. Введение в теоретико-числовые методы криптографии.- Лань, 2011. - 400с.

2. Минеев М.П., Чубариков В.Н. Лекции по арифметическим вопросам криптографии. М.: Научно-издательский центр «Луч», 2014. – 224 с.

7.2 Дополнительная литература:

1. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии (2-е издание, дополненное). М.: МЦНМО, 2006. - 336 с. ISBN: 5-94057-103-4

2. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002. – 104 с.

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Math.ru [Электронный ресурс]: портал математического образования / Отделение математических наук Российской Академии Наук ; Московский центр непрерывного математического образования. - М : [б. и.], 2011. - Загл. с титул. экрана. - Б. ц. URL: http://www.math.ru

2. МЦНМО [Электронный ресурс]: свободно распространяемые издания / Департамент образования г. Москвы, Математический институт имени В.А. Стеклова, МГУ имени М.В. Ломоносова, отделение математики РАН. - М : [б. и.], 2004. - Загл. с титул. экрана. - Б. ц. URL: http://www.mccme.ru/free-books

3. Exponenta.ru [Электронный ресурс] : образовательный математичекий сайт / AXOFT. - М : [б. и.], 2000. - Загл. с титул. экрана. - Б. ц. URL:http://exponenta.ru/

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Дисциплина «Теория чисел и элементы криптографии» направлена на формирование систематизированных теоретических знаний в области теории чисел и некоторых ее приложений к криптографии.

Самостоятельная работа студентов по дисциплине «Теория чисел и элементы криптографии» составляет 60% от всего объема часов, отводимого учебным планом на изучение дисциплины. В связи с этим успешное изучение материала данного курса в значительной степени зависит от качества самостоятельной подготовки студентов. С целью активизации самостоятельной работы студентов на каждом практическом занятии повторяется соответствующий теоретический материал и закрепляются основные навыки и умения владением математическим аппаратом.

В начале изучения курса студенты получают темы и вопросы практических занятий.

По второму разделу предусмотрено выполнение трех лабораторных работ.

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

1. Подписка Microsoft DreamSpark Premium - Сублицензионный договор № S-2042626/M18 от 04.06.2013:
   1.1. Средства для разработки и проектирования Visual Studio 2008, 2010, 2012 и 2013 Professional Editions;
   1.2. Операционная система Windows 7 Professional;
2. Операционная система Microsoft Windows XP Professional Russian – Лицензия № 16698685 от 08.08.2003 г.;
3. Программное обеспечение Microsoft Office XP Professional Win32 Russian– Лицензия № 16698685 от 08.08.2003 г.;
4. Веб-браузеры.
5. Доступ студентов через личные кабинеты к электронным библиотечным системам.
6. Возможность работы студентов на удаленном рабочем столе кафедры информатики и информационных технологий.

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ «ТЕОРИЯ ЧИСЕЛ И ЭЛЕМЕНТЫ КРИПТОГРАФИИ»

Специальные помещения должны представлять собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Лекционные аудитории должны быть укомплектованы техническими средствами обучения, служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, мультимедийное оборудование.

Перечень материально-технического обеспечения, необходимого для проведения лабораторных работ, включает в себя компьютерные классы.

Помещения для самостоятельной работы обучающихся должны быть оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду MOODLE.

12. АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ «ТЕОРИЯ ЧИСЕЛ И ЭЛЕМЕНТЫ КРИПТОГРАФИИ»

1. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Компетенция: *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 (ОПК-3)*

Выпускник знает:
основные факты и положения теории делимости и теории сравнений;
арифметические алгоритмы, связанные с криптографическими системами;
Умеет:
использовать базовые знания теории чисел для оценки сложности арифметических операций;
Владеет:

навыками использования арифметических методов кодирования информации.

В результате освоения дисциплины «Теория чисел и элементы криптографии» студент должен приобрести знания:

- основных фактов и положений теории делимости и теории сравнений;
- арифметических алгоритмов, связанных с криптографическими системами;

умения:

- использовать базовые знания теории чисел для оценки сложности арифметических операций;

навыки и (или) опыт деятельности:

- использования арифметических методов кодирования информации.

2. Место дисциплины «Теория чисел и элементы криптографии» в структуре ОПОП

Дисциплина «Теория чисел и элементы криптографии» относится к обязательным дисциплинам вариативной части учебного плана. Изучение данной дисциплины базируется на освоении студентами дисциплин модуля «Алгебра и геометрия» и предшествует изучению дисциплин «Алгоритмы и анализ сложности», «Компьютерная алгебра».

К началу изучения дисциплины студенты должны владеть базовыми знаниями по основам теории делимости. Знания и умения, полученные в результате освоения дисциплины «Теория чисел и элементы криптографии», будут использоваться при подготовке выпускной квалификационной работы, в научно-исследовательской и практической деятельности.

3. Объем дисциплины - 4 зачетные единицы.

4. Образовательный процесс осуществляется на русском языке.

5. Разработчики: Реброва Ирина Юрьевна, кандидат физико-математических наук, доцент.

13. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ «ТЕОРИЯ ЧИСЕЛ И ЭЛЕМЕНТЫ КРИПТОГРАФИИ»

Изменения к рабочей программе дисциплины отсутствуют.

Заведующий кафедрой АМАиГ  Н.М. Добровольский,
«1» декабря 2015 г.

Программа составлена в соответствии с требованиями ФГОС ВО.
Разработчик:

Фамилия, имя, отчество	Учёная степень	Учёное звание	Должность	Дата разработки	Подпись
Реброва Ирина Юрьевна	к.ф.-м.н.	Доцент	Декан	01.12.2015