Факультет	Математики, физики и информатики	
Кафедра	Алгебры, математического анализа и геометрии	
Направление подготовки	09.03.03 Прикладная информатика	
Направленность (профиль)	Прикладная информатика в здравоохранении	
Компьютерная алгебра и элементы криптографии		Б1.В.12

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 № 8 от «31» августа 2017 г.

Рабочая программа дисциплины «Компьютерная алгебра и элементы криптографии»

Трудоемкость: 4 зачетные единицы

Квалификация выпускника: Бакалавр

Форма обучения: очная

Год начала подготовки: 2014

Заведующий кафедрой Добровольский Н.М.

Декан факультета 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 принимать участие в управлении проектами создания информационных систем на стадиях жизненного цикла (ПК-17)	***Выпускник знает:*** особенности символьных алгоритмов. ***умеет:*** решать алгоритмические задачи в кольцах многочленов ***владеет*** навыками конструирования кодов	В соответствии с учебным планом и планируемыми результатами освоения ОПОП
Готовность к обеспечению информационной безопасности на уровне БД (ДПК-5)	***Выпускник знает:*** основные факты и положения теории защиты информации. ***умеет:*** решать задачи шифрования и дешифрования сообщений ***владеет***: навыками использования методов кодирования информации.	В соответствии с учебным планом и планируемыми результатами освоения ОПОП

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП БАКАЛАВРИАТА

Дисциплина «Компьютерная алгебра и элементы криптографии» относится к обязательным дисциплинам вариативной части учебного плана. Изучение данной дисциплины базируется на знаниях, умениях и видах деятельности, сформированных в процессе освоения дисциплин «Алгебра и геометрия», «Дискретная математика», «Методы программирования».

Освоение данной дисциплины необходимо для успешного изучения дисциплин «Системы компьютерной математики» и «Информационная безопасность».

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*
практические занятия	*24*
лабораторные занятия с использованием современных информационных технологий	*10*
контрольные работы	*2*
Самостоятельная работа студента (всего)	*54*
в том числе:	
самостоятельное изучение разделов, проработка и повторение лекционного материала и материала учебников и учебных пособий	*30*
внеаудиторная самостоятельная работа при подготовке к практическим и лабораторным занятиям	*20*
подготовка к контрольной работе	*4*
Контроль	*36*
Промежуточная аттестация в форме: экзамен	

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

Наименование темы (раздела)	Количество академических или астрономических часов по видам учебных занятий			
	Занятия лекционного типа	Занятия семинарского типа	Другие виды работ	Самостоятельная работа обучающихся
Тема 1. Основные алгебраические структуры	2	2		6
Тема 2.Факторизация целых чисел	4	6		12
Тема 3.Алгоритмические задачи в кольцах многочленов	4	10		12
Тема 4 Коды, исправляющие ошибки	4	6		12

Тема 5.Элементы криптографии	4	8		12
Контроль самостоятельной работы студентов			*2*	
Контроль			*36*	
ИТОГО: 144 часа	18	34	38	54

Тема 1. Основные алгебраические структуры.

Группы, циклические группы. Функция Эйлера и ее основные свойства. Кольца и поля. Сравнение чисел по модулю. Кольца и поля вычетов

Тема 2. Факторизация целых чисел.

Наибольший общий делитель. Алгоритм Евклида. Простые числа. Решето Эратосфена. Тесты простоты. Разложение целых чисел на множители.

Тема 3. Алгоритмические задачи в кольцах многочленов.

Алгоритм Евклида нахождения наибольшего общего делителя двух многочленов. Вычисление значений и корней полиномов. Факторизация многочленов. Системы уравнений и идеалы в кольцах многочленов. Базис Гребнера полиномиального идеала. Алгоритм Бухбергера вычисления базиса Гребнера.

Тема 4. Коды, исправляющие ошибки.

Коды, исправляющие ошибки. Коды Хемминга. Линейные коды. Проверочная и порождающая матрица линейного кода.

Тема 5. Элементы криптографии.

Исторический экскурс. Симметричные криптосистемы. Системы с открытым ключом. Выбор параметров системы RSA. Взаимосвязь между параметрами системы RSA.

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

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: теоретические сведения, 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 один теоретический вопрос и 2 задачи по разным разделам курса. После отведенного на подготовку времени состоится 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 компетенций «Способность принимать участие в управлении проектами создания информационных систем на стадиях жизненного цикла (ПК-17)», «Готовность к обеспечению информационной безопасности на уровне БД (ДПК-5)» осуществляется в несколько этапов в соответствии с учебным планом и планируемыми результатами освоения ОПОП, соотнесенными с планируемыми результатами обучения по каждой дисциплине и практике.

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

Дескриптор компетенций	Показатели оценивания	Критерии оценивания
Знания	– особенности символьных алгоритмов; – основные факты и положения теории защиты информации.	Оценка «отлично» выставляется, если студент в целом за семестр набрал от 81 до 100 баллов (при условии, что на экзамене набрано не менее 16 баллов). Оценка «хорошо» выставляется, если студент в целом за семестр набрал от 61 до 80 баллов (при условии, что на экзамене набрано не менее 16 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).
Умения	– решать алгоритмические задачи в кольцах многочленов; – решать задачи шифрования и дешифрования сообщений	
Навыки и опыт деятельности	– навыки конструирования кодов; – навыками использования 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.

Критерии оценивания компетенций формируются на основе балльно-рейтинговой системы с помощью всего комплекса методических материалов, определяющих процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих данный этап формирования компетенций.

Баллы, набранные студентом в течение семестра	Баллы за промежуточную аттестацию (экзамен)	Общая сумма баллов за модуль в семестр	Оценка
51 – 70	16 – 30	81 – 100	Отлично
31 – 70	16 – 30	61 – 80	Хорошо
11 –70	10 – 30	41 – 60	Удовлетворительно
0 – 20	0 – 9	0 – 40	Неудовлетворительно

6.3. 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

Примерны вариант индивидуального задания по теме «Многочлены от одной переменной»

1. Найти наибольший общий делитель многочленов f и g и его линейное представление, если $f = x^5 - 2x^4 + 3x^2 - x^3 - x - 2, g = x^5 - 5x^3 + 4x^2 - x^4 + 5x - 2$
2. Найти остаток от деления многочлена $f(x) = x^{105} + x + 1$ на $g(x) = x^2 - 1$.
3. Найти условия, при которых $x^2 + mx - 1$ делит $x^3 + px + q$
4. Используя схему Горнера определить значения и производные многочлена $f = x^5 - 4x^3 + 6x^2 - 8x + 10$ при x_0=2.
5. Постройте многочлен наименьшей степени с действительными (комплексными) коэффициентами, имеющий следующие корни: 2 и 1+i – простые корни, а 1 – корень кратности 2.
6. Уравнение $2x^3 + mx^2 + nx + 12 = 0$ имеет корни $x_1 = 1,\ x_2 = -2$. Найти третий корень уравнения.
7. Найти рациональные корни многочлена $x^3 - 6x^2 + 15x - 14$.
8. Определить кратность корня c=-1 многочлена $f(x) = 5x^4 + 14x^3 + 12x^2 + 2x - 1$.

Перечень лабораторных работ.

Лабораторные работы предполагают разработку (или использование известных) алгоритмов для решения конкретных задач по следующей тематике:

Лабораторная работа №1 «Факторизация составного числа».
Лабораторная работа №2 «Факторизация многочленов».
Лабораторная работа №3 «Базисы Гребнера полиномиального идеала».
Лабораторная работа №4 «Элементы криптографии 1»
Лабораторная работа №5 «Элементы криптографии 2»

Примерные задания для контрольной работы.

1. В циклической группе 10 порядка, порожденной элементом a, найти порядок элемента a^6 и выписать элементы, порожденной им циклической подгруппы.
2. Найти наибольший общий делитель 20354 и 1647.
3. Найдите наибольший общий делитель многочленов $f(x) = 3x^5 + 5x^4 - 16x^3 - 6x^2 - 5x - 6$ и $g(x) = 3x^4 - 4x^3 - x^2 - x - 2$
4. Вычислить S-полиномы многочленов $f = x^4y - z^2$ и $g = 3xz^2 - y$, используя чисто лексикографическое упорядочение.
5. Покажите, что $\{f_1 = y - x^2; f_2 = z - x^3\}$ не является базисом Гребнера для чисто лексикографического упорядочения.

Вопросы к экзамену.

1. Группы, циклические группы.
2. Функция Эйлера и ее основные свойства.
3. Сравнение чисел по модулю. Кольца и поля вычетов.
4. Делимость в кольце целых чисел.
5. Наибольший общий делитель Алгоритм Евклида.
6. Простые числа. Решето Эратосфена. Тесты простоты.
7. Разложение целых чисел на множители.
8. Алгоритм Евклида нахождения наибольшего общего делителя двух многочленов.
9. Вычисление значений и корней полиномов.
10. Интерполяционный многочлен Лагранжа.
11. Факторизация многочленов над кольцом целых чисел. Алгоритм Кронекера.
12. Кольца многочленов от нескольких переменных. Упорядочивание мономов.
13. Системы алгебраических уравнений и идеалы в кольцах многочленов.
14. Базис Гребнера полиномиального идеала.
15. Алгоритм Бухбергера вычисления базиса Гребнера полиномиального идеала.
16. Коды, исправляющие ошибки.
17. Линейные коды. Проверочная и порождающая матрица линейного кода.
18. Элементы криптографии. Системы с закрытым ключом.
19. Примеры простейших асимметричных криптосистем.
20. Системы с открытым ключом. RSA-код.

6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1. Описание балльно-рейтинговой системы по дисциплине.

Балльно-рейтинговая система оценки успеваемости студентов

Максимальное количество (100 баллов) распределяется по следующей схеме:

- максимальное число баллов, набранных студентом в течение семестра, составляет – 70;
- максимальное число баллов за промежуточную аттестацию (экзамен) – 30.

В течение семестра баллы распределяются следующим образом:

1. *Посещаемость занятий (до 10 баллов):* количество баллов равно целой части $10n/34$, где n – число посещенных лекционных и практических занятий (в часах); студент, пропустивший занятия по уважительной причине, имеет право отчитаться по пропущенным темам.

*2. Работа в семестре (до 60 баллов**):***

- индивидуального задания по теме *«Многочлены от одной переменной» (до 10 баллов);*

- выполнение и отчет по лабораторной работе № 1 «*Факторизация составного числа*»» (до 10 баллов);
- выполнение и отчет по лабораторной работе № 2 «*Факторизация многочленов*»» (до 10 баллов);
- выполнение и отчет по лабораторной работе № 3 *«Базисы Гребнера полиномиального идеала»* (до 10 баллов);

выполнение и отчет по лабораторной работе № 4 *«Элементы криптографии 1»* (до 5 баллов);

выполнение и отчет по лабораторной работе № 5 *«Элементы криптографии 2»* (до 5баллов);

- контрольная работа (до 10 баллов).

На экзамене ответ студента может быть максимально оценен в 30 баллов. Экзаменационный билет состоит из одного теоретического вопроса и двух задач, одна из которых непосредственно связана с теоретическим вопросом. За теоретический вопрос и решение каждой задачи можно получить до 10 баллов.

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

7.1. Основная литература

1. Балаба, И.Н. Абстрактная и компьютерная алгебра: Учебное пособие для студентов физико-мат. специальностей вузов / И.Н. Балаба, С.А. Пихтильков – Тула: Изд-во Тул. гос. пед. ун-та им. Л.Н. Толстого, 2008. – 129 с.
2. Васильева И. Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата / И. Н. Васильева. – М.: Издательство Юрайт, 2017. – 349 с. – (Серия: Бакалавр. Академический курс). – ISBN 978-5-534-02883-6. То же [Электронный ресурс]. - URL:https://www.biblio-online.ru/book/59BABD78-5536-4ED4-BB9D-55E2F19F80B2

7.2. Дополнительная литература

1. Панкратьев, Е.В. Элементы компьютерной алгебры: учебник / Е.В. Панкратьев; Национальный Открытый Университет "ИНТУИТ". - М.: Интернет-Университет Информационных Технологий, 2007. - 247 с. - (Основы информатики и математики). - ISBN 978-5-9556-0099-4; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=233322
2. Чечёта, С.И. Введение в дискретную теорию информации и кодирования: учебное пособие / С.И. Чечёта. - М.: МЦНМО, 2011. - 224 с. : табл., схем. - ISBN 978-5-94057-701-0; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=63307

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

1. Руконт [Электронный ресурс]: национальный цифровой ресурс / ООО «Агентство Книга-Сервис». - М.: [б. и.], 2011. - Загл. с титул. Экрана URL: http://www.rucont.ru

2. Университетская библиотека Online [Электронный ресурс]: электронная библиотечная система / ООО "Директ-Медиа». - М.: [б. и.], 2001. - Загл. с титул. экрана. - Б. ц. URL: www.biblioclub.ru

3. Универсальные базы данных East View [Электронный ресурс]: информационный ресурс / East View Information Services. - М.: [б. и.], 2012. - Загл. с титул. экрана. - Б. ц. URL: www.ebiblioteka.ru

4. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]: информационный портал / ООО "РУНЭБ»; Санкт-Петербургский государственный университет. - М.: [б. и.], 2005. - Загл. с титул. экрана. - Б. ц. URL: www.eLibrary.ru

5. Научно-информационный портал ВИНИТИ [Электронный ресурс]: информационный ресурс / ВИНИТИ РАН. - М.: [б. и.], 2004. - Загл. с титул. экрана. - Б. ц. URL: http://science.viniti.ru

6. 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

7. 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

8. Exponenta.ru [Электронный ресурс]: образовательный математический 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 «Компьютерная алгебра и элементы криптографии» направлена на формирование у студентов навыков решения различных алгоритмических задач в кольцах многочленов от одной и нескольких переменных, знакомит студентов с широким кругом задач компьютерной алгебры, с элементами теории кодирования и криптографии, существенно расширяет примеры алгоритмов. Усвоение данной дисциплины поможет лучше осознать проблемы компьютерной безопасности, приобрести опыт практического использования систем компьютерной алгебры, понять важность основных алгебраических структур при построении современного программного обеспечения.

Для успешного освоения дисциплины «Компьютерная алгебра и элементы криптографии» учебной программой предусмотрено выполнение лабораторных работ по следующим темам:

«*Факторизация составного числа*».
«Факторизация многочленов».
«Базисы Гребнера полиномиального идеала».
«Элементы криптографии 1»
«Элементы криптографии 2»

При выполнении лабораторных заданий и самопроверки полученных результатов можно использовать пакеты компьютерной алгебры.

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

При осуществлении образовательного процесса по дисциплине используются информационные технологии, охватывающие ресурсы (компьютеры, программное обеспечение и сети), необходимые для управления информацией (создание, хранение, управление, передача и поиск информации):

- технические средства: компьютерная техника и средства связи (ноутбук, проектор, экран, USB-накопители и т.п.);

- коммуникационные средства (проверка домашних заданий и консультирование посредством электронной почты);
- организационно-методическое обеспечение (электронные учебные и учебно-методические материалы);
- программное обеспечение (Microsoft Office (Excel, Power Point, Word и т.д.) поисковые системы, электронная почта и т.п.;
- среда электронного обучения ТГПУ им. Л.Н. Толстого http://moodle.tsput.ru.

Комплект лицензионного программного обеспечения

1. Операционная система Microsoft Windows XP Professional Russian – Лицензия № 16698685 от 08.08.2003 г.
2. Программное обеспечение Microsoft Office XP Professional Win32 Russian– Лицензия № 16698685 от 08.08.2003 г.
3. Программное обеспечение Microsoft Office Enterprise 2007 Russian - Лицензия №46138962 от 16.11.2009 г.
4. Операционная система Microsoft Windows Professional 7 Russian – Лицензия №48497058 от 13.05.2011 г.
5. Программа для распознавания текста ABBYY FineReader 9.0 Corporate Edition лицензионный сертификат - код позиции AF90-3U1V25-102, ABBYY FineReader 9.0 Corporate Edition Volume License Concurrent от 28 июля 2009 г.
6. Электронный словарь ABBYY Lingvo X3 Европейская версия - Код позиции AL14-2U1V05-102, ABBYY Lingvo x3 Европейская версия. Именная лицензия Concurrent от 28 июля 2009 г.
7. Комплексная Система Антивирусной Защиты Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 500-999 Node 2 year Educational Renewal License – Лицензия № 1894-150512-101810 от 12-05-2015 г.

Современные профессиональные базы данных и информационные справочные системы

1. Компьютерная информационно-правовая система «Гарант» - регистрационный номер клиента 71-70685-000033.
2. Официальный интернет-портал правовой информации http://pravo.gov.ru.
3. Портал Федеральных государственных образовательных стандартов высшего образования http://fgosvo.ru.
4. Портал "Информационно-коммуникационные технологии в образовании" http://www.ict.edu.ru.

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

Реализация дисциплины обеспечена материально-технической базой, соответствующей действующим противопожарным нормам и правилам.

Дисциплина обеспечена специальными помещениями для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещениями для самостоятельной работы. Аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Учебные помещения для проведения занятий лекционного и семинарского типа оборудованы мультимедийным демонстрационным оборудованием, для демонстрации учебно-наглядных пособий, обеспечивающих тематические иллюстрации, соответствующие рабочей учебной программе дисциплины.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ТГПУ им. Л.Н. Толстого, внутривузовское сетевое окружение. Для проведения лекций с использованием мультимедийных средств обучения необходима аудитория с мультимедийным комплексом.

12. АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

1. Планируемые результаты обучения при освоении дисциплины, соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины у студента должны быть сформированы следующие компетенции:

- *способность принимать участие в управлении проектами создания информационных систем на стадиях жизненного цикла (ПК-17)*
- *готовность к обеспечению информационной безопасности на уровне БД (ДПК-5).*

В результате освоения дисциплины студент должен приобрести:

знания

- особенности символьных алгоритмов;
- основные факты и положения теории защиты информации;

умения

- решать алгоритмические задачи в кольцах многочленов;
- решать задачи шифрования и дешифрования сообщений;

навыки

- навыки конструирования кодов;
- навыками использования методов кодирования информации.

2. Место дисциплины в структуре ОПОП.

Дисциплина «Компьютерная алгебра и элементы криптографии» относится к обязательным дисциплинам вариативной части учебного плана. Изучение данной дисциплины базируется на знаниях, умениях и видах деятельности, сформированных в процессе освоения дисциплин «Алгебра и геометрия», «Дискретная математика», «Методы программирования».

Освоение данной дисциплины необходимо для успешного изучения дисциплин «Системы компьютерной математики» и «Информационная безопасность».

3. Объем дисциплины: 4 зачетные единицы.

4. Образовательный процесс осуществляется на русском языке.

5. Разработчик: Балаба И.Н., д.ф.- м.н., доцент, профессор кафедры алгебры, математического анализа и геометрии.

13. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

2016-2017 учебный год

В рабочую программу внесены изменения в части обновления состава лицензионного программного обеспечения, профессиональных баз данных и информационно-справочных систем, к которым должен быть обеспечен доступ обучающимся.

Решение ученого совета университета, протокол №2 от 16 февраля 2017 г.

2017-2018 учебный год

Обновлен состав необходимого комплекта лицензионного программного обеспечения.

1. Операционная система Microsoft Windows XP Professional Russian – Лицензия № 16698685 от 08.08.2003 г.
2. Операционная система Microsoft Windows Professional 7 Russian – Лицензия №48497058 от 13.05.2011 г., договор № Пр/16/6 от 05 апреля 2016 года.
3. Операционная система Microsoft Windows 10 Professional Russian - контракт № ПР/ФЕН/15/18 от 23.10.2015 г., договор № Пр/16/6 от 05 апреля 2016 года.
4. Программное обеспечение Microsoft Office Enterprise 2007 Russian - Лицензия №46138962 от 16.11.2009 г.
5. Программное обеспечение Microsoft Office 2013 Professional - контракт № 405535 от 2 ноября 2015 года, контракт № ПР/ФЕН/15/18 от 23.10.2015 г.
6. Программа для распознавания текста ABBYY FineReader 9.0 Corporate Edition лицензионный сертификат - код позиции AF90-3U1V25-102, ABBYY FineReader 9.0 Corporate Edition Volume License Concurrent от 28 июля 2009 г.
7. Электронный словарь ABBYY Lingvo X3 Европейская версия - Код позиции AL14-2U1V05-102, ABBYY Lingvo x3 Европейская версия. Именная лицензия Concurrent от 28 июля 2009 г.
8. Комплексная Система Антивирусной Защиты Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 500-999 Node 2 year Educational Renewal License – Лицензия № 17E0-170518-102844-823-690 от 18-05-2017 г.

Обновлен состав современных профессиональных баз данных и информационных справочных систем, к которым обеспечен доступ обучающимся.

1. Компьютерная информационно-правовая система «Гарант» - регистрационный номер клиента 71-70685-000033.
2. Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.
3. Портал Федеральных государственных образовательных стандартов высшего образования http://fgosvo.ru.
4. Портал «Информационно-коммуникационные технологии в образовании» http://www.ict.edu.ru.
5. Web of Science Core Collection – политематическая реферативно-библиографическая и наукометрическая (библиометрическая) база данных http://webofscience.com.
6. Полнотекстовый архив ведущих западных научных журналов на российской платформе Национального электронно-информационного консорциума (НЭИКОН) http://neicon.ru.
7. Базы данных издательства Springer https://link.springer.com.

Изменения к рабочей программе дисциплины утверждены на заседании Ученого совета университета, протокол № 8 от 31 августа 2017 г.

Программа составлена в соответствии с требованиями ФГОС ВО.

Разработчик

Фамилия, имя, отчество	Учёная степень	Учёное звание	Должность
Балаба Ирина Николаевна	д.ф.-м.н.	доцент	профессор кафедры алгебры, математического анализа и геометрии