МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 51

УТВЕРЖДАЮ
Руководитель направления

д.т.н.,проф.
(должность, уч. степень, звание)

А.М. Тюрликов
(инициалы, фамилия)

(подпись)
«_19_» __мая_____ 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Алгебраическая алгоритмика»
(Наименование дисциплины)

Код направления подготовки/ специальности	11.03.02
Наименование направления подготовки/ специальности	Инфокоммуникационные технологии и системы связи
Наименование направленности	Программно-защищенные инфокоммуникации
Форма обучения	очная

Санкт-Петербург– 2021

Лист согласования рабочей программы дисциплины

Программу составил (а)

Зав. Каф. №51, к.т.н., доц.	19.05.2021	А.А, Овчинников
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 51

«19» мая 2021 г, протокол № 10

Заведующий кафедрой № 51

к.т.н.,доц.	19.05.2021	А.А. Овчинников
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Ответственный за ОП ВО 11.03.02(03)

доц.,к.т.н.,доц.	19.05.2021	Н.В. Марковская
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №5 по методической работе

доц.,к.т.н.,доц.	19.05.2021	О.И. Красильникова
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Аннотация

Дисциплина «Алгебраическая алгоритмика» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 11.03.02 «Инфокоммуникационные технологии и системы связи» направленности «Программно-защищенные инфокоммуникации». Дисциплина реализуется кафедрой «№51».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-3 «Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств инфокоммуникаций, использованию и внедрению результатов исследований»

ПК-6 «Способен оценивать параметры безопасности и защищать программное обеспечение и сетевые устройства администрируемой сети с помощью специальных средств управления безопасностью»

Содержание дисциплины охватывает круг вопросов, связанных с изучением алгоритмических структур и их применением для решения практических задач.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента, консультации.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме дифференцированного зачета.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский »

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью преподавания дисциплины «Алгебраическая алгоритмика» является изучение алгоритмических структур и их применение для решения практических задач. Изучение дисциплины должно воспитывать у обучающихся творческое мышление, навыки самостоятельного решения задач научного содержания, трудолюбие и настойчивость в достижении результатов, строгость математического мышления.

1.2. Дисциплина входит в состав части, формируемой участниками образовательных отношений, образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Профессиональные компетенции	ПК-3 Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств инфокоммуникаций, использованию и внедрению результатов исследований	ПК-3.В.1 владеет навыками организации сбора и изучения научно-технической информации по теме исследований и разработок
Профессиональные компетенции	ПК-6 Способен оценивать параметры безопасности и защищать программное обеспечение и сетевые устройства администрируемой сети с помощью специальных средств управления безопасностью	ПК-6.З.2 знает основные принципы, криптографические протоколы и программные средства обеспечения информационной безопасности сетевых устройств

2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- Введение в направление;
- Математика. Математический анализ

– Математическая логика и теория алгоритмов

– Дискретная математика

– Математика. Аналитическая геометрия и линейная алгебра

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут использоваться при изучении других дисциплин:

– Технологии программирования;

– Криптографические методы защиты информации.

3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№3
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	3/ 108	3/ 108
Из них часов практической подготовки	17	17
Аудиторные занятия, всего час.	51	51
в том числе:		
лекции (Л), (час)	34	34
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	17	17
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
Самостоятельная работа, всего (час)	57	57
***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Дифф. Зач.	Дифф. Зач.

Примечание: **кандидатский экзамен

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 3					
Раздел 1. Точная целочисленная арифметика. Основные алгоритмы	4		2		8
Раздел 2. Первообразные корни и квадратичные вычеты. Квадратные корни	4				8
Раздел 3. Основы абстрактной алгебры. Некоторые методы алгебраической алгоритмики	6				8

Раздел 4. Быстрые алгоритмы для конечных алгебраических структур	6		3		8
Раздел 5. Тесты проверки чисел на простоту и построение больших простых чисел	4		4		8
Раздел 6. Методы разложение чисел на множители	4		4		8
Раздел 7. Разложение на множители полиномов над конечными полями. Алгоритм Берлекэмпа	6		4		9
Раздел 1. Точная целочисленная арифметика. Основные алгоритмы	4		2		8
Итого в семестре:	34		17		57
Итого	34	0	17	0	57

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Тема 1.1. Временные оценки сложности арифметических операций. Делимость и алгоритм Евклида. Основная теорема арифметики. Распределение простых чисел. Тема 1.2. Сравнения с одним неизвестным. Отношение сравнимости. Полная система вычетов. Теорема Эйлера. Теорема Ферма. Сравнения 1-й степени.
2	Тема 2.1. Первообразные корни и квадратичные вычеты. Квадратные корни. Сравнение 2-й степени. Символы Лежандра и Якоби. Квадратичный закон взаимности. Методы решения сравнений 2-й степени. Первообразные корни. Квадратные корни: метод Цассенхауза-Кантора.
3	Тема 3.1. Кольца. Кольца: Евлидовы, Безу, Факториальные, Главных идеалов. Тема 3.2. Различные формы китайской теоремы об остатках Различные формы китайской теоремы об остатках. Модулярная арифметика и смешанная система счисления. Тема 3.3. Конечные поля. Неприводимые многочлены. Тема 3.4. Матричная алгебра над произвольным полем. Вычисления над конечными структурами. Тема 3.5. Характеры и χ - преобразования. Быстрые χ - преобразования.
4	Тема 4.1. Арифметические операции над целыми числами и полиномами. Сложность основных целочисленных алгоритмов. Алгоритмы арифметики в системе счисления с основанием *B*. Умножение в классах вычетов.

	Тема 4.2. Умножение с помощью быстрого преобразования Фурье. Дискретное преобразование Фурье. Алгоритм быстрого преобразования Фурье. Алгоритм Шенхаге-Штрассена для умножения целых чисел. Тема 4.3. Модульное умножение. Метод Монтгомери. Модульное возведение в степень.
5	Тема 5.1. Вероятностные тесты проверки чисел на простоту. Тест Ферма. Тест Соловэя-Штрассена. Тест Миллера-Рабина. Тема 5.2. Детерминированные алгоритмы проверки чисел на простоту. Проверка чисел Мерсенна. Проверка с использованием разложения числа n-1.
6	Тема 6.1. Методы разложение чисел на множители. Метод пробного деления. ρ - Метод Полларда. Факторизация Ферма и факторные базы. Метод квадратичного решета. Метод непрерывных дробей. Приложения в криптографической системе RSA.
7	Тема 7.1. Факторизация многочленов над конечными полями. Тема 7.2. Алгоритм Берлекемпа**.**

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено					
Всего					

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 3				
1	Проверка чисел на простоту.	2	2	1
2	Реализация алгоритма Шенхаге-Штрассена для умножения целых чисел	4	4	4
3	Вероятностные тесты проверки чисел на простоту	3	3	5
4	Методы разложения чисел на множители и криптографическая система RSA	2	2	6

5	Реализация протокола Диффи-Хеллмана.	2	2	7
6	Алгоритм Берлекемпа	4	4	7
	Всего	17		17

4.5. Курсовое проектирование/ выполнение курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 3, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	37	37
Подготовка к текущему контролю успеваемости (ТКУ)	10	10
Подготовка к промежуточной аттестации (ПА)	10	10
Всего:	57	57

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 7-11.

6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
[519.7 Е 78]	Элементы дискретной математики: учебное пособие/И. Л. Ерош, В. В. Михайлов; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб: ГОУ ВПО "СПбГУАП", 2008.	164
http://www.znanium.com/catalog.php?bookinfo=441493	Теоретико-численные методы в криптографии: Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск: Сибирский федеральный университет, 2011. – 160 с.	

7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
http://neerc.ifmo.ru/wiki/index.php?title	Алгоритмы алгебры и теории чисел. Конспекты лекций

8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
1	MS Office
2	MS Windows
3	MS Visual Studio
4	Matlab

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Фонд аудиторий ГУАП для проведения занятий лекционного и семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; переносной набор демонстрационного оборудования	
2	Вычислительная лаборатория Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; лабораторное оборудование (ПЭВМ - 12 шт., объединенных в локальную вычислительную сеть с выходом в вычислительную сеть ГУАП и Интернет)	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средствдля проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Дифференцированный зачёт	Список вопросов

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	– обучающийся глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	– обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	– обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений.

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
	Учебным планом не предусмотрено	

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
1	Классы чисел	ПК-3.В.1 ПК-6.З.2
2	Основная теорема арифметики	
3	Теоремы о простых числах	
4	Сравнения, система вычетов, решение линейных систем по модулю	
5	Китайская теорема об остатках	
6	Теорема Ферма	
7	Функция Эйлера	
8	Количество делителей, сумма делителей	
9	Определение кольца, подкольца, изоморфизмы колец	
10	Делители нуля, области целостности	
11	Единицы (обратимые элементы), группа обратимых элементов	
12	Сравнения 1-й степени.	
13	Евклидовы кольца	
14	Определение кольца, подкольца, изоморфизмы колец	
15	Символ Лежандра, критерий Эйлера	
16	Символ Якоби и его свойства	
17	Обобщенный квадратичный закон взаимности	
18	Алгоритм вычисления символа Якоби	
19	Методы разложения полиномов на множители над конечными полями	
20	Быстрые χ - преобразования	
21	Различные формы китайской теоремы об остатках	
22	Неприводимые многочлены.	
23	Вычисления над конечными структурами.	
24	Сложность основных целочисленных алгоритмов.	
25	Алгоритмы арифметики в системе счисления с основанием B.	
26	Метод Монтгомери. Модульное возведение в степень.	
27	Проверка чисел Мерсенна.	
28	Проверка с использованием разложения числа n-1	
29	Алгоритм Берлекэмпа	
30	Метод пробного деления.	
31	Факторизация Ферма и факторные базы.	
32	Метод квадратичного решета.	
33	Метод непрерывных дробей.	
34	ρ - Метод Полларда.	
35	Тест Ферма.	
36	Тест Соловэя-Штрассена.	
37	Тест Миллера-Рабина.	

38	Отношение сравнимости.	
39	Полная система вычетов.	
40	Сравнение 2-й степени.	
41	Квадратные корни: метод Цассенхауза-Кантора.	

Перечень тем для курсового проектирования/выполнения курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для курсового проектирования/выполнения курсовой работы

№ п/п	Примерный перечень тем для курсового проектирования/выполнения курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	Не предусмотрено	

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

11. Методические указания для обучающихся по освоению дисциплины

11.1. Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимися лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;

– получение опыта творческой работы совместно с преподавателем;

– развитие профессионально-деловых качеств, любви к предмету и самостоятельного творческого мышления.

– появление необходимого интереса, необходимого для самостоятельной работы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;

– научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);

– получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

Раздел 1. Точная целочисленная арифметика. Основные алгоритмы

Раздел 2. Первообразные корни и квадратичные вычеты. Квадратные корни

Раздел 3. Основы абстрактной алгебры. Некоторые методы алгебраической алгоритмики

Раздел 4. Быстрые алгоритмы для конечных алгебраических структур

Раздел 5. Тесты проверки чисел на простоту и построение больших простых чисел

Раздел 6. Методы разложение чисел на множители

Раздел 7. Разложение на множители полиномов над конечными полями. Алгоритм Берлекэмпа

Структура предоставления материала каждой лекции состоит из:

вступления (введения), где определяется тема, план и цель лекции. Обосновывается предмет лекции и ее актуальность, основная идея (проблема, центральный вопрос), связь с предыдущими и последующими занятиями, основные вопросы лекции;

изложения содержания, где реализуется научное содержание темы, все главные вопросы, приводится система доказательств с использованием наиболее целесообразных методических приемов. В ходе изложения применяются все формы и способы суждения, аргументации и доказательства. Все доказательства и разъяснения направлены на достижение поставленной цели, раскрытие основной идеи, содержания и научных выводов. Каждый учебный вопрос заканчивается краткими выводами, логически подводящими студентов к следующему вопросу лекции. Количество вопросов в лекции, как правило, от двух до четырех;

заключения, где обобщаются в кратких формулировках основные идеи лекции, логически завершая ее как целостное изучение темы. В нем могут даваться рекомендации о порядке дальнейшего изучения основных вопросов лекции самостоятельно по указанной литературе.

11.2. Методические указания для обучающихся по участию в семинарах

Учебным планом не предусмотрено

11.3. Методические указания для обучающихся по прохождению практических занятий

Учебным планом не предусмотрено

11.4. Методические указания для обучающихся по выполнению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;

– получение новой информации по изучаемой дисциплине;

– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

Вариант задания по каждой лабораторной работе обучающийся получает в соответствии с номером в списке группы. Перед проведением лабораторной работы обучающемуся следует внимательно ознакомиться с методическими указаниями по ее выполнению. В соответствии с заданием обучающийся должен подготовить необходимые данные, получить от преподавателя допуск к выполнению лабораторной работы, выполнить указанную последовательность действий, получить требуемые результаты, оформить и защитить отчет по лабораторной работе.

Структура и форма отчета о лабораторной работе

Отчет о лабораторной работе должен включать в себя: титульный лист, формулировку задания, теоретические положения, используемые при выполнении лабораторной работы, описание процесса выполнения лабораторной работы, полученные результаты и выводы.

Требования к оформлению отчета о лабораторной работе

По каждой лабораторной работе выполняется отдельный отчет. Титульный лист оформляется в соответствии с шаблоном (образцом) приведенным на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации». Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации».

Методические указания по прохождению лабораторных работ:

1. [519.7(075) Д 48] Дополнительные главы теории чисел: методические указания/ С.-Петерб. гос. ун-т аэрокосм. приборостроения; сост. С. В. Федоренко. - СПб: ГОУ ВПО "СПбГУАП", 2011. Количество экз. в библ. – 83.
2. [519.7(075) Д 48] Основные понятия теории чисел: методические указания/С.-Петерб. гос. ун-т аэрокосм. приборостроения; сост. С. В. Федоренко. - СПб.: Изд-во ГУАП, 2011. - 16 с. Количество экз. в библ. – 78.

11.5. Методические указания для обучающихся по прохождению курсового проектирования/выполнения курсовой работы

Учебным планом не предусмотрено

11.6. Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихсяявляются: учебно-методический материал по дисциплине.

Перечень тем для самостоятельного изучения:

Распределение простых чисел.

Сравнения 1-й степени.

Сравнение 2-й степени. Методы решения сравнений 2-й степени.

Квадратные корни: метод Цассенхауза-Кантора.

Кольца: Евлидовы. Безу. Факториальные. Главных идеалов.

Модулярная арифметика и смешанная система счисления.

Матричная алгебра над произвольным полем. Вычисления над конечными структурами.

Быстрые χ - преобразования.

Быстрые алгоритмы для конечных алгебраических структур

Сложность основных целочисленных алгоритмов. Алгоритмы арифметики в системе счисления с основанием *B.* Умножение в классах вычетов.

Алгоритм Шенхаге-Штрассена для умножения целых чисел.

Метод Монтгомери. Модульное возведение в степень.

Тест Ферма. Тест Соловэя-Штрассена. Тест Миллера-Рабина.

Проверка чисел Мерсенна. Проверка с использованием разложения числа n-1

Метод пробного деления. ρ - Метод Полларда. Факторизация Ферма и факторные базы. Метод квадратичного решета. Метод непрерывных дробей.

Алгоритм Берлекэмпа

11.7. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

Результаты текущего контроля учитываются при проведении промежуточной аттестации в соответствии с требованиями СТО ГУАП. СМК 3.76 «Положение о текущем контроле успеваемости и промежуточной аттестации студентов и аспирантов ГУАП, обучающихся по образовательным программам высшего образования».

11.8. Методические указания для обучающихся по прохождению промежуточной аттестации.

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя: дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Дифференцированный зачет проводится в устной форме. Дифференцированный зачет обучающихся проводится, как правило, в течение недели, предшествующей началу экзаменационной сессии, либо на последнем занятии в семестре по дисциплине (модулю). При явке на зачет обучающийся обязан иметь при себе зачетную книжку, которую он предъявляет преподавателю. Прием зачета без зачетной книжки не допускается. Если со стороны обучающегося во время зачета допущены нарушения учебной дисциплины (списывание, несанкционированное использование средств мобильной связи, аудио–плейеров и других технических устройств), нарушения правил внутреннего распорядка ГУАП, предпринята попытка подлога документов, НПР вправе удалить обучающегося с

зачета с занесением в ведомость оценки «неудовлетворительно». По результатам дифференцированного зачета положительная оценка заносится преподавателем в ведомость и зачетную книжку. Отрицательная оценка («неудовлетворительно») заносится только в ведомость. Неявка обучающегося на дифференцированный зачет отмечается в ведомости словами «не явился», либо «н/я». Директор института на основе ведомости выясняет причину отсутствия обучающегося на зачете и принимает решение о порядке последующей сдачи.

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой