

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

Кафедра № 25

УТВЕРЖДАЮ

Руководитель направления

д.т.н., проф.

(должность, уч. степень, звание)

А.М. Тюрликов

(инициалы, фамилия)



(подпись)

«21» июня 2023 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Специальные разделы математики»  
(Наименование дисциплины)


Код направления подготовки/ специальности	11.04.02
Наименование направления подготовки/ специальности	Инфокоммуникационные технологии и системы связи
Наименование направленности	Защищенные инфокоммуникационные системы
Форма обучения	очная

Санкт-Петербург– 2023

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц.,к.т.н.,доц.  
(должность, уч. степень, звание)

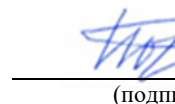
  
21.06.2023  
(подпись, дата)

А.А. Овчинников  
(инициалы, фамилия)

Программа одобрена на заседании кафедры № 25  
«21» июня 2023 г, протокол № 12/2022-23

Заведующий кафедрой № 25

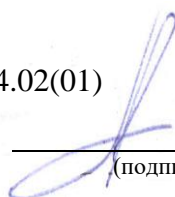
д.т.н.,проф.  
(уч. степень, звание)

  
21.06.2023  
(подпись, дата)

А.М. Тюрликов  
(инициалы, фамилия)

Ответственный за ОП ВО 11.04.02(01)

доц.,к.т.н.,доц.  
(должность, уч. степень, звание)

  
21.06.2023  
(подпись, дата)

А.А. Овчинников  
(инициалы, фамилия)

Заместитель директора института №2 по методической работе

доц.,к.т.н.,доц.  
(должность, уч. степень, звание)

  
21.06.2023  
(подпись, дата)

О.Л. Балышева  
(инициалы, фамилия)

## Аннотация

Дисциплина «Специальные разделы математики» входит в образовательную программу высшего образования – программу магистратуры по направлению подготовки/ специальности 11.04.02 «Инфокоммуникационные технологии и системы связи» направленности «Защищенные инфокоммуникационные системы». Дисциплина реализуется кафедрой «№25».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-2 «Способен самостоятельно выполнять экспериментальные исследования для решения научно-исследовательских и производственных задач с использованием современной аппаратуры и методов исследования»

ПК-4 «Способен к обеспечению информационной безопасности системного программного обеспечения инфокоммуникационной системы организации»

Содержание дисциплины охватывает круг вопросов, связанных с обеспечением фундаментальной математической подготовки в одной из наиболее важных областей современной прикладной математики – криптологии.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: практические занятия, самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме 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 является обеспечение фундаментальной математической подготовки в одной из наиболее важных областей современной прикладной математики – криптологии; ознакомление с рядом методов классической и современной алгебры и теории чисел, применяемых в криптографии; обучение алгебраическим методам решения ряда основных задач, возникающих при синтезе криптографических алгоритмов

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-2 Способен самостоятельно выполнять экспериментальные исследования для решения научно-исследовательских и производственных задач с использованием современной аппаратуры и методов исследования	ПК-2.3.1 знать методы, средства и практику планирования, организации, проведения и внедрения научных исследований и опытно-конструкторских разработок ПК-2.У.1 уметь проводить исследования характеристик телекоммуникационного оборудования и оценки качества предоставляемых услуг
Профессиональные компетенции	ПК-4 Способен к обеспечению информационной безопасности системного программного обеспечения инфокоммуникационной системы организации	ПК-4.3.3 знать принципы построения программно-аппаратных средств защиты информации

## 2. Место дисциплины в структуре ОП

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

– Математическое моделирование устройств и систем;

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

– Производственная практика

## 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
<b>Общая трудоемкость дисциплины, ЗЕ/ (час)</b>	3/ 108	3/ 108
<b>Из них часов практической подготовки</b>	34	34
<b>Аудиторные занятия, всего час.</b>	34	34
в том числе:		
лекции (Л), (час)		
практические/семинарские занятия (ПЗ), (час)	34	34
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
<b>Самостоятельная работа, всего (час)</b>	74	74
<b>Вид промежуточной аттестации:</b> зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Зачет	Зачет

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. Полиномиальная алгебра.		12			24
Раздел 2. Распределенные последовательности		10			24
Раздел 3. Функции		12			26
Итого в семестре:		34			74
Итого	0	34	0	0	74

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
	<b>Учебным планом не предусмотрено</b>

### 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
Семестр 3					
1	Представления различных программно реализованных преобразований в виде полиномов над универсальными алгебрами	Мозговой штурм	6	6	1
2	Фактор-кольца колец многочленов над кольцами вычетов, разложения их в прямые суммы, вид полиномиальных преобразований этих колец	Мозговой штурм	6	6	1
3	Построение биективных и равновероятных полиномиальных функций над кольцами вычетов, реализация функций усложнения	Мозговой штурм	4	4	2
4	Смешанный конгруэнтный метод, построение соответствующих псевдослучайных генераторов и (с использованием построенных ранее функций усложнения) построение простых алгоритмов для шифраторов гаммирования	Мозговой штурм	6	6	2
5	Задание функций на конечном поле с помощью	Мозговой штурм	6	6	3

	полиномов; построение биективных и транзитивных функций как композиций поразрядных логических операций (типа XOR,AND и т.п.) и сдвигов на основе преобразований треугольного вида				
6	Представление произвольной функции над конечным полем в виде полинома	Мозговой штурм	6	6	3
Всего			34	34	

#### 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
Учебным планом не предусмотрено				
Всего				

#### 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)	54	54
Подготовка к текущему контролю успеваемости (ТКУ)	10	10
Подготовка к промежуточной аттестации (ПА)	10	10
Всего:	74	74

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)
51(075) Б 93	Математическая логика [Текст] : учебное пособие / Д. В. Бутенина, В. М. Лагодинский ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2011. - 52 с	55
004 К 95	Инфокоммуникационные сети. Моделирование и оценка вероятностно-временных характеристик [Текст]: монография / О. И. Кутузов, Т. М. Татарникова; С.- Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2015. -382 с.	20
<a href="https://e.lanbook.com/book/210746">https://e.lanbook.com/book/210746</a>	Введение в теоретико-числовые методы криптографии : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург : Лань, 2022. — 400 с.	
004 К 95	Математические схемы и алгоритмы моделирования инфокоммуникационных систем [Текст]: учебное пособие / О. И. Кутузов, Т. М. Татарникова; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2013.- 147 с	64

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
https://e.lanbook.com/	Электронная библиотечная система
https://znanium.com/	Электронная библиотечная система

## 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 таблице 12.

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, выполнения курсовых работ, текущего контроля и промежуточной аттестации. Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; переносной набор демонстрационного оборудования	

## 10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средств для 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
Зачет	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	Характеристика сформированных компетенций
5-балльная шкала	
«отлично» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся глубоко и всесторонне усвоил программный материал;</li> <li>– уверенно, логично, последовательно и грамотно его излагает;</li> <li>– опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления;</li> <li>– умело обосновывает и аргументирует выдвигаемые им идеи;</li> <li>– делает выводы и обобщения;</li> <li>– свободно владеет системой специализированных понятий.</li> </ul>
«хорошо» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы;</li> <li>– не допускает существенных неточностей;</li> <li>– увязывает усвоенные знания с практической деятельностью направления;</li> <li>– аргументирует научные положения;</li> <li>– делает выводы и обобщения;</li> <li>– владеет системой специализированных понятий.</li> </ul>
«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы;</li> <li>– допускает несущественные ошибки и неточности;</li> <li>– испытывает затруднения в практическом применении знаний направления;</li> <li>– слабо аргументирует научные положения;</li> <li>– затрудняется в формулировании выводов и обобщений;</li> <li>– частично владеет системой специализированных понятий.</li> </ul>
«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> <li>– обучающийся не усвоил значительной части программного материала;</li> <li>– допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении;</li> <li>– испытывает трудности в практическом применении знаний;</li> <li>– не может аргументировать научные положения;</li> <li>– не формулирует выводов и обобщений.</li> </ul>

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
	<ol style="list-style-type: none"> <li>1. Применение методов алгебры в криптографических задачах.</li> <li>2. Понятие о шифрах, симметричном и асимметричном шифровании. Шифры гаммирования и колонной замены.</li> <li>3. Генератор исходной последовательности и функция усложнения как составные части шифрующего алгоритма.</li> <li>4. Понятие о псевдослучайных последовательностях.</li> <li>5. Определение универсальной алгебры, полинома над универсальной алгеброй и полиномиальной функции.</li> <li>6. Конгруэнция, фактор-алгебра, гомоморфизм, изоморфизм, эпиморфизм, мономорфизм.</li> <li>7. Определение равномерно распределенной последовательности, равновероятной функции, функции, сохраняющей меру и эргодической функции.</li> <li>8. Функции, сохраняющие меру на конечном множестве (биективные функции) и равновероятные функции.</li> <li>9. Регистр сдвига с линейной обратной связью и линейные рекуррентные последовательности над конечным полем.</li> <li>10. Период, аннулирующий, характеристический и минимальный многочлен. Критерий максимальности периода линейной рекуррентной последовательности.</li> <li>11. Представление конечного поля матрицами над простым полем.</li> <li>12. Представление кольца вычетов в виде прямой суммы с помощью китайской теоремы об остатках.</li> <li>13. Критерий биективности полинома на кольце вычетов.</li> <li>14. Линейные конгруэнтные генераторы.</li> <li>15. Понятие об однонаправленных функциях.</li> <li>16. Задача логарифмирования в конечном поле как математически трудная задача.</li> <li>17. Построение однонаправленных функций на основе операции возведения в степень в конечном поле.</li> <li>18. Роль примитивных элементов конечного поля для задачи построения однонаправленных функций на основе возведения в степень.</li> <li>19. Представление произвольной функции над конечным полем в виде полинома.</li> <li>20. Эффект «младшего бита» в выходной последовательности конгруэнтного генератора</li> </ol>	<p>ПК-2.3.1 ПК-2.У.1 ПК-4.3.3</p>

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 прохождению практических занятий

Практическое занятие является одной из основных форм организации учебного процесса, заключающаяся в выполнении обучающимися под руководством преподавателя комплекса учебных заданий с целью усвоения научно-теоретических основ учебной дисциплины, приобретения умений и навыков, опыта творческой деятельности.

Целью практического занятия для обучающегося является привитие обучающимся умений и навыков практической деятельности по изучаемой дисциплине.

Планируемые результаты при освоении обучающимся практических занятий:

- закрепление, углубление, расширение и детализация знаний при решении конкретных задач;
- развитие познавательных способностей, самостоятельности мышления, творческой активности;
- овладение новыми методами и методиками изучения конкретной учебной дисциплины;
- выработка способности логического осмысления полученных знаний для выполнения заданий;
- обеспечение рационального сочетания коллективной и индивидуальной форм обучения.

##### Требования к проведению практических занятий

Вариант задания по каждой задаче при выполнении практических и контрольных заданий обучающийся получает в соответствии с номером в списке группы. Перед решением задачи обучающемуся следует внимательно ознакомиться с условием задачи, с рассмотренными примерами, а также содержанием соответствующих тем лекционного курса. В соответствии с заданием обучающийся должен привести решение с

необходимыми вычислениями и пояснениями, получить требуемые результаты, оформить задание для сдачи преподавателю.

#### 11.2. 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 обучающихся являются:

- учебно-методический материал по дисциплине.

#### 11.3. 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».

#### 11.4. Методические указания для обучающихся по прохождению промежуточной аттестации.

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП». Зачет проводится в устной форме. 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–плееров и других технических устройств), нарушения правил внутреннего распорядка ГУАП, предпринята попытка подлога документов, преподаватель вправе удалить обучающегося с зачета с занесением в ведомость оценки «не зачтено». По результатам зачета «зачтено» заносится

преподавателем в ведомость и зачетную книжку. Отрицательная оценка («не зачтено») заносится только в ведомость. Неявка обучающегося на 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