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

Кафедра № 33

УТВЕРЖДАЮ
Руководитель программы

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

С.В. Беззатеев
(инициалы, фамилия)

(подпись)

«20» февраля 2026 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Специальные разделы математики в решении задач информационной безопасности»
(Наименование дисциплины)

Код научной специальности	2.3.6.
Наименование научной специальности	Методы и системы защиты информации, информационная безопасность
Наименование направленности (профиля) (при наличии)	
Год начала реализации программы	2026

Санкт-Петербург– 2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

д.т.н.,доц.	20.02.2026	С.В. Беззатеев
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33
«20» февраля 2026 г, протокол № 7

Заведующий кафедрой № 33

д.т.н.,доц.	20.02.2026	С.В. Беззатеев
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Ответственный за программу 2.3.6.(00)

д.т.н.,доц.	20.02.2026	С.В. Беззатеев
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №3 по методической работе

	20.02.2026	Н.В. Решетникова
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Аннотация

Дисциплина «Специальные разделы математики в решении задач информационной безопасности» входит в состав программы подготовки научных и научно-педагогических кадров в аспирантуре по научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность». Дисциплина реализуется кафедрой «№33».

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: лекции.

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

Общая трудоемкость освоения дисциплины составляет 1 зачетную единицу, 36 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 программы подготовки научных и научно-педагогических кадров в аспирантуре.

1.3. В результате изучения дисциплины аспирант должен:

знать:

- средства и способы обеспечения защиты от несанкционированного доступа

уметь:

- оценивать угрозы безопасности информации в компьютерных сетях

владеть:

- определять состав программно-аппаратных средств защиты информации в компьютерных сетях

2. Место дисциплины в структуре программы

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

«Математическая логика и теория алгоритмов»;

«Дискретная математика»;

«Теория вероятностей и математическая статистика»;

«Алгебраические проблемы криптографии».

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

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 1.

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№2
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	1/ 36	1/ 36
Из них часов практической подготовки, (час)		
Аудиторные занятия, всего час.	7	7
в том числе:		
лекции (Л), (час)	7	7
практические/семинарские занятия (ПЗ), (час)		
экзамен, (час)		
Самостоятельная работа (СР), всего (час)	29	29
Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач,	Зачет	Зачет

Экз.**)		

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 2.

Таблица 2 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	СРС (час)
Семестр 2			
Раздел 1. Введение			
Раздел 2. Полиномиальная алгебра. Тема 2.1. Шифры и их алгебраические модели. Тема 2.2. Элементы полиномиальной алгебры			
Раздел 3. Распределенные последовательности Тема 3.1. Элементы теории равномерно распределенных последовательностей. Тема 3.2. Линейные рекуррентные последовательности.			
Раздел 4. Функции. Тема 4.1. Равновероятные и биективные полиномиальные функции. Тема 4.2. Однонаправленные и полиномиальные функции над конечными полями.			
Итого в семестре:	7		29
Итого	7	0	29

Практическая подготовка заключается в непосредственном выполнении аспирантами 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 3.

Таблица 3 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	**Раздел 1. Введение.** Задачи и программа курса. Место изучаемой дисциплины в ряду других математических и общепрофессиональных дисциплин. Применение методов алгебры в криптографических задачах. Формы самостоятельной работы студентов по изучению курса.
2	**Раздел 2. Полиномиальная алгебра.** Тема 2.1. Шифры и их алгебраические модели. Понятие о шифрах, симметричном и асимметричном шифровании. Блочные и поточные шифры. Классические шифрующие алгоритмы. Шифры гаммирования и колонной замены. Блок-схемы шифрующих алгоритмов. Генератор исходной последовательности и функция усложнения как составные части шифрующего алгоритма. Основные криптографические

	требования к генератору исходной последовательности и функции усложнения. Понятие о псевдослучайных последовательностях. Тема 2.2. Элементы полиномиальной алгебры. Определение универсальной алгебры, полинома над универсальной алгеброй и полиномиальной функции. Универсальная алгебра, соответствующая процессору (множество входных слов как носитель, система команд как сигнатура). Полином над универсальной алгеброй, соответствующий программе для данного процессора. Конгруэнция, фактор-алгебра, гомоморфизм, изоморфизм, эпиморфизм, мономорфизм. Функции, совместимые со всеми конгруэнциями. Совместимость полиномиальной функции.
3	**Раздел 3. Распределенные последовательности** Тема 3.1. Элементы теории равномерно распределенных последовательностей. Определение равномерно распределенной последовательности, равновероятной функции, функции, сохраняющей меру и эргодической функции. Равномерно распределенные последовательности как "псевдослучайные", эргодические функции как законы генераторов исходных последовательностей, равновероятные функции как усложняющие преобразования. Равномерная распределенность периодической последовательности максимального периода на конечном множестве. Функции, сохраняющие меру на конечном множестве (биективные функции) и равновероятные функции. Эргодическиефункции на конечном множестве как транзитивные функции (функции, задающие полноцикловую подстановку). Теоремы об эргодичности (равновероятности) функции, индуцированной совместимой функцией на фактор-алгебре. Признаки и критерии равновероятности (эргодичности) полиномиальной функции на декартовом произведении универсальных алгебр. Тема 3.2. Линейные рекуррентные последовательности. Регистр сдвига с линейной обратной связью и линейные рекуррентные последовательности над конечным полем. Период,аннулирующий, характеристический и минимальный многочлен. Сопровождающая матрица. Примитивный многочлен. Критерий максимальности периода линейной рекуррентной последовательности. Представление конечного поля матрицами над простым полем. Сопровождающая матрица линейной рекуррентной последовательности максимального периода как примитивный элемент поля.
4	**Раздел 4. Функции** Тема 4.1. Равновероятные и биективные полиномиальные функции. Представление кольца вычетов в виде прямой суммы с помощью китайской теоремы об остатках. Сведение общей задачи к случаю колец примарных порядков. Критерий биективности полинома на кольце вычетов. Многомерные полиномиальные функции. Критерий биективности и достаточные условия равновероятности многомерной полиномиальной функции на кольце вычетов. Линейные конгруэнтные генераторы. Критерий транзитивностиполинома первой степени на кольце вычетов. Обобщения смешанного конгруэнтного метода. Тема 4.2. Однонаправленные и полиномиальные функции над конечными полями. Понятие об однонаправленных функциях. Асимметричное шифрование, распределение ключей. Задача логарифмирования в конечном поле как математически трудная задача. Построение однонаправленных функций на основе операции возведения в степень в конечном поле. Роль примитивных элементов конечного поля для задачи построения однонаправленных функций на основе возведения в степень. Представление произвольной

	функции над конечным полем в виде полинома. Интерполяция по Ньютону и Лагранжу. Полиномиальная полнота конечных полей. Преобразования треугольного вида. Критерии биективности и транзитивности преобразований треугольного вида над полем из двух элементов. Полиномиальные преобразования колец вычетов примарного порядка как преобразования треугольного вида над простым конечным полем. Эффект «младшего бита» в выходной последовательности конгруэнтного генератора.

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 4.

Таблица 4 – 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. Самостоятельная работа аспирантов

Виды самостоятельной работы и ее трудоемкость приведены в таблице 5.

Таблица 5 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 2, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	10	10
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	10	10
Домашнее задание (ДЗ)		
Подготовка к промежуточной аттестации (программы аспирантуры)	9	9
Всего:	29	29

5. Перечень учебно-методического обеспечения для самостоятельной работы аспирантов по дисциплине

Учебно-методические материалы для самостоятельной работы аспирантов указаны в п.п. 6-11.

6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 6.

Таблица 6– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)

004 М 87	Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие / Н. Н. Мошак, Т. М. Татарникова; С.- Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд- во ГУАП, 2014. - 121 с.	40
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	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
004.056.55 Е 78	Ерош, И. Л. Криптография. Первое знакомство: учебное пособие/ СПб.: ГОУ ВПО "СПбГУАП",2008. - 84 с.	323
004.05 В 75	Воронов, А. В., Волошина Н.В. Основы защиты информации: учебное пособие. СПб.: ГОУ ВПО"СПбГУАП", 2009. - 78 с.	74
519.7 Л 17 519.6/.8	Лазарева, С. В. Математические основы криптологии. Тесты простоты и факторизация: учебное пособие/ С. В. Лазарева, А. А. Овчинников; С.-Петерб. гос. акад. аэрокосм. приборостроения. - СПб: ГОУ ВПО "СПбГУАП", 2006	85
519.713 К 26	Карпов, Ю. Г. Теория автоматов. - СПб: ПИТЕР, 2003	11
519.6(075) Н73	Новиков, Ф. А. Дискретная математика для программистов: учебное пособие. - М. и др.: Питер, 2006.	100
004.4 К 84	Крук, Е.А. Методы программирования и прикладные алгоритмы: учебное пособие в 3 ч. Ч. 1 / Е. А. Крук, А. А. Овчинников; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2014. - 178 с.	45
04.4 К 84	Крук, Е.А. Методы программирования и прикладные алгоритмы: учебное пособие в 3 ч. Ч. 2 / Е. А. Крук, А. А. Овчинников; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2014. - 114 с.	45

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

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 7.

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

URL адрес	Наименование
http://e.lanbook.com/view/book/1540/	Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теоретико-числовые

	методы криптографии. Лань, 2011.

8. Перечень информационных технологий

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

Перечень используемого программного обеспечения представлен в таблице 8.

Таблица 8 – Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

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

Перечень используемых информационно-справочных систем представлен в таблице 9.

Таблица 9– 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 10.

Таблица 10 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Мультимедийная лекционная аудитория	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средств для проведения промежуточной аттестации аспирантов по дисциплине приведен в таблице 11.

Таблица 11 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Зачет	Список вопросов; Тесты; Задачи.

10.2. В качестве критериев оценки уровня освоения аспирантами дисциплины применяется 4-балльная шкала оценивания, которая приведена таблице 12. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 12 – Критерии оценки уровня освоения дисциплины

Оценка	Характеристика уровня освоения дисциплины
4-балльная шкала	

Оценка 4-балльная шкала	Характеристика уровня освоения дисциплины
«отлично» «зачтено»	– аспирант 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 по направлению подготовки/ специальности; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	– аспирант 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 по направлению подготовки/ специальности; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	– аспирант 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 по направлению подготовки/ специальности; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	– аспирант не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении подготовки/ специальности; – 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 13.

Таблица 13 – Вопросы (задачи) для экзамена

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

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 14.

Таблица 14 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета
	Применение методов алгебры в криптографических задачах. Понятие о шифрах, симметричном и асимметричном шифровании. Шифры гаммирования и колонной замены. Генератор исходной последовательности и функция усложнения как составные части шифрующего алгоритма. Понятие о псевдослучайных последовательностях. Определение универсальной алгебры, полинома над универсальной алгеброй и полиномиальной функции. Конгруэнция, фактор-алгебра, гомоморфизм, изоморфизм, эпиморфизм, мономорфизм.

	Определение равномерно распределенной последовательности, равновероятной функции, функции, сохраняющей меру и эргодической функции. Функции, сохраняющие меру на конечном множестве (биективные функции) и равновероятные функции. Регистр сдвига с линейной обратной связью и линейные рекуррентные последовательности над конечным полем. Период, аннулирующий, характеристический и минимальный многочлен. Критерий максимальности периода линейной рекуррентной последовательности. Представление конечного поля матрицами над простым полем. Представление кольца вычетов в виде прямой суммы с помощью китайской теоремы об остатках. Критерий биективности полинома на кольце вычетов. Линейные конгруэнтные генераторы. Понятие об однонаправленных функциях. Задача логарифмирования в конечном поле как математически трудная задача. Построение однонаправленных функций на основе операции возведения в степень в конечном поле. Роль примитивных элементов конечного поля для задачи построения однонаправленных функций на основе возведения в степень.

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 15.

Таблица 15 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания уровня освоения дисциплины, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации аспирантов ГУАП.

11. Методические указания для аспирантов по освоению дисциплины

11.1. Методические указания для аспирантов 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 аспирантами 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 – Введение.
Раздел 2 – Полиномиальная алгебра.
Тема 2.1 – Шифры и их алгебраические модели.
Тема 2.2 – Элементы полиномиальной алгебры.
Раздел 3 – Распределенные последовательности.
Тема 3.1 – Элементы теории равномерно распределенных последовательностей.
Тема 3.2 - Линейные рекуррентные последовательности.
Раздел 4 – Функции.
Тема 4.1 – Равновероятные и биективные полиномиальные функции.
Тема 4.2 - Однонаправленные и полиномиальные функции над конечными полями.

11.2. Методические указания для аспирантов по прохождению самостоятельной работы

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

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

11.3. Методические указания для аспирантов по прохождению текущего контроля успеваемости.

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

Возможные методы текущего контроля успеваемости аспирантов:

– устный опрос на занятиях;
– систематическая проверка выполнения индивидуальных заданий;
– защита отчётов по лабораторным работам;
– тестирование;
– контроль самостоятельных работ (в письменной или устной формах);
– иные виды, определяемые преподавателем.

11.4. Методические указания для аспирантов по прохождению промежуточной аттестации.

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

– дифференцированный зачет – это форма оценки знаний, полученных аспирантами при изучении дисциплины (модуля), при выполнении научно-исследовательских работ с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

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