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

Кафедра № 33

УТВЕРЖДАЮ
Ответственный за образовательную программу

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

Т.Н. Елина
(инициалы, фамилия)

(подпись)
«27» июня 2024 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Математические основы криптологии»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.03.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности	Безопасность компьютерных систем
Форма обучения	очная
Год приема	2024

Санкт-Петербург– 2024

Лист согласования рабочей программы дисциплины

Программу составил (а)

д.т.н.,доц.	27.06.2024	С.В. Беззатеев
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33
«27» июня 2024 г, протокол № 11

Заведующий кафедрой № 33

д.т.н.,доц.	27.06.2024	С.В. Беззатеев
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №3 по методической работе

	27.06.2024	Н.В. Решетникова
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

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

Кафедра № 33

УТВЕРЖДАЮ
Ответственный за образовательную программу

доц.,к.э.н.,доц.

(должность, уч. степень, звание)

Т.Н. Елина

(инициалы, фамилия)

(подпись)
«27» июня 2024 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Математические основы криптологии»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.03.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности	Безопасность компьютерных систем
Форма обучения	очная
Год приема	2024

Санкт-Петербург– 2024

Лист согласования рабочей программы дисциплины

Программу составил (а)

д.т.н.,доц.	27.06.2024	С.В. Беззатеев
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«27» июня 2024 г, протокол № 11

Заведующий кафедрой № 33

д.т.н.,доц.	27.06.2024	С.В. Беззатеев
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №3 по методической работе

	27.06.2024	Н.В. Решетникова
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Аннотация

Дисциплина «Математические основы криптологии» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 10.03.01 «Информационная безопасность» направленности «Безопасность компьютерных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-2 «Способен определять состав программно-аппаратных средств защиты информации в компьютерных сетях»

ПК-5 «Способен организовывать и проводить настройку программных, программно-аппаратных (в том числе крипто-графических) и технических средств и систем защиты от несанкционирован-ного доступа»

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, лабораторные работы, самостоятельная работа студента.

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

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа.

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 определять состав программно-аппаратных средств защиты информации в компьютерных сетях	ПК-2.У.1 умеет оценивать угрозы безопасности информации в компьютерных сетях
Профессиональные компетенции	ПК-5 Способен организовывать и проводить настройку программных, программно-аппаратных (в том числе крипто-графических) и технических средств и систем защиты от несанкционирован-ного доступа	ПК-5.З.2 знает средства и способы обеспечения защиты от несанкционированного доступа

2. Место дисциплины в структуре ОП

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:

– «Криптографические методы»;
– «Основы информационной безопасности»;
– «Проектирование систем обеспечения информационной безопасности»;
– «Защита информационных процессов»

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
		№5
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	2/ 72	2/ 72
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)	21	21
***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Дифф. Зач.	Дифф. Зач.

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)	ЛР (час)	КП (час)	СРС (час)
Семестр 5					
Раздел 1. Введение.	2				7
Раздел 2. Полиномиальная алгебра. Тема 2.1. Шифры и их алгебраические модели.Тема 2.2. Элементы полиномиальной алгебры.	11		6		7
Раздел 3. Распределенные последовательностиТема 3.1. Элементы теории равномерно распределенных последовательностей. Тема 3.2. Линейные рекуррентные последовательности.	11		5		7

Раздел 4. Функции. Тема 4.1. Равновероятные и биективныеполиномиальные функции. Тема 4.2. Однонаправленные и полиномиальные функции над конечнымиполями.	12		6		7
Итого в семестре:	34		17		21
Итого	34	0	17	0	21

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	**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,с овместимые 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 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 5				
1	Представления различных программно реализованных преобразований в виде полиномов над универсальными алгебрами	3	3	2
2	Фактор-кольца колец многочленов над кольцамивычетов, разложения их в прямые суммы, вид полиномиальных преобразований этих колец	3	3	2
3	Построение биективных и равновероятных полиномиальных функций над кольцами вычетов,реализация функций усложнения	2	2	3
4	Смешанный конгруэнтный метод, построение соответствующих псевдослучайных генераторов и (с использованием построенных ранее функций усложнения) построение простых алгоритмов для шифраторов гаммирования	3	3	3
5	Задание функций на конечном поле с помощью полиномов; построение биективных и транзитивных функций как	3	3	4
	композиций поразрядных логических операций (типа XOR, AND и т.п.) и сдвигов на основепреобразований треугольного вида			
6	Представление произвольной функции над конечным полем в виде полинома	3	3	4
	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 5, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	10	10
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	6	6
Домашнее задание (ДЗ)		

Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	5	5
Всего:	21	21

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)
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.: ГОУВПО "СПбГУАП",2008. - 84 с.	323
004.05 В 75	Воронов, А. В., Волошина Н.В. Основызащиты 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.-	85

	Петерб. гос. акад. аэрокосм. приборостроения. - СПб: ГОУ ВПО "СПбГУАП", 2006	
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 9.

Таблица 9 – 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 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем,используемых приосущ

Перечень используемых информационно-справочных систем представлен втаблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование

	Не предусмотрено

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществленияобразовательного 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	Лекционная аудитория	
2	Вычислительная лаборатория под управлением ОС Windowsверсии не ранее 7, объединенных в локальную сеть	

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; Тесты; Задачи.

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.

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«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	Применение методов алгебры в криптографическихзадачах. Понятие о шифрах, симметричном и асимметричномшифровании. 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.	ПК-2.У.1

	Критерий максимальности периода линейнойрекуррентной последовательности. Представление конечного поля матрицами над простымполем.	
2	Представление кольца вычетов в виде прямой суммы спомощью китайской теоремы об остатках. Критерий биективности полинома на кольце вычетов. Линейные конгруэнтные генераторы. Понятие об однонаправленных функциях. Задача логарифмирования в конечном поле какматематически трудная задача. Построение однонаправленных функций на основеоперации возведения в степень в конечном поле. Роль примитивных элементов конечного поля для задачипостроения однонаправленных функций на основе возведения в степень. Представление произвольной функции над конечнымполем в виде полинома. Эффект «младшего бита» в выходной последовательности конгруэнтного генератора.	ПК-5.З.2

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.

11.1. 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 – 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 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

налекциях;

- получение новой информации по изучаемой дисциплине;
- приобретение навыков самостоятельной работы с лабораторнымоборудованием 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, а также с содержанием соответствующего лекционного курса, при необходимости – изучить самостоятельно дополнительную литературу. В соответствии с заданием обучающийся должен подготовить необходимые данные, выполнить задание лабораторной работы, 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 (new.guap.ru) в разделе «Сектор нормативной документации». Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП (new.guap.ru) в разделе «Сектор нормативной документации».

11.3. 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 повышенияпрофессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются учебно-методические материалы по дисциплине.

Для развития у студентов навыков самостоятельного овладения теоретическим материалом ряд тем дисциплины на лекционных занятиях дается обзорно, что предполагает их самостоятельное детальное изучение.

Примерные темы для самостоятельного изучения:

- Применение методов алгебры в криптографических задачах.
- Понятие о псевдослучайных последовательностях.
- Совместимость полиномиальной функции.
- Функции, сохраняющие меру на конечном множестве.
- Примитивный многочлен.
- Обобщения смешанного конгруэнтного метода.

- Эффект «младшего бита» в выходной последовательности конгруэнтногогенератора.

11.4. 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. Форма проведения текущего контроля – защита отчетов по лабораторным работам. 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».

11.5. 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.

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».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программы высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

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