

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

Кафедра № 33

УТВЕРЖДАЮ
Руководитель образовательной программы

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

Т.Н. Елина
(инициалы, фамилия)
(подпись)

«20» февраля 2026 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Математические основы криптологии»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.03.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности/ специализации	Безопасность компьютерных систем
Форма обучения	очная
Год приема	2026

Санкт-Петербург– 2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

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


(подпись, дата)

С.В. Беззатеев
(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«20» февраля 2026 г, протокол № 7

Заведующий кафедрой № 33

д.т.н., проф.
(уч. степень, звание)


(подпись, дата)

С.В. Беззатеев
(инициалы, фамилия)

Заместитель директора института №3 по методической работе

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


(подпись, дата)

Н.В. Решетникова
(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/специализации «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 несанкционированного 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 (5 семестр).

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-2.3.2 знает принципы функционирования сетевых протоколов, включающих криптографические алгоритмы 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 криптографических) и технических средств и систем защиты от несанкционированного доступа	ПК-5.3.1 знает сетевые протоколы и их параметры настройки ПК-5.3.2 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»

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

- «Криптографические методы защиты информации»;
- «Основы информационной безопасности»

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/КР (час)	СР (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 последовательности Тема 3.1. Элементы теории равномерно распределенных последовательностей. Тема 3.2. Линейные рекуррентные последовательности.	11		5		7

Раздел 4. Функции. Тема 4.1. Равновероятные и биективные полиномиальные функции. Тема 4.2. Однонаправленные и полиномиальные функции над конечными полями.	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, совместимые со всемиконгруэнциями. 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. Эргодические функции на конечном множестве как транзитивные функции (функции, задающие полноцикловую подстановку). Теоремы об эргодичности (равновероятности) функции, индуцированной совместимой функцией на фактор-алгебре. Признаки и критерии равно вероятности (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 транзитивности полинома 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		2
2	Фактор-кольца колец многочленов над кольцами вычетов, разложениях в прямые суммы, вид полиномиальных преобразований этих колец	3		2
3	Построение биективных и равновероятных полиномиальных функций над кольцами вычетов, реализация функций усложнения	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
5	Задание функций на конечном поле с помощью полиномов; построение биективных и транзитивных функций как композиций поразрядных логических операций (типа XOR, AND и т.п.) и сдвигов на основе преобразований треугольного вида	3		4
6	Представление произвольной функции над конечным полем в виде полинома	3		4
Всего		17		

4.5. Выполнение курсового проекта/ 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. разделов 6-11.

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.-Петербург. 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.-Петербург. 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.-Петербург. 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	323

	"СПбГУАП", 2008. - 84 с.	
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 9.

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

URL адрес	Наименование
Lms.guap.ru	Система дистанционного обучения ГУАП (СДО ГУАП)
rsv.ru	Платформа «Россия – страна возможностей»
leader-id.ru	Платформа «Leader-ID»

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 при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
1	Гарант.ру: www.garant.ru/
2	ЭБС Лань: e.lanbook.com/books
3	ЭБС Знаниум: znanium.com/

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	Лекционная аудитория	
2	Мультимедийная лекционная аудитория	

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
Дифференцированный зачет	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	Характеристика сформированных компетенций
5-балльная шкала	
«отлично» «зачтено»	Обучающийся: – глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно связывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий. – правильно выполнил от 90% до 100% тестовых заданий**.
«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;

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
	– аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий. – правильно выполнил от 70% до 89% тестовых заданий**.
«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. – правильно выполнил от 51% до 69% тестовых заданий**.
«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. – правильно выполнил менее 51% тестовых заданий**.

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 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.	ПК-2.3.2
2	Определение равномерно распределенной последовательности, равновероятной функции, функции, сохраняющей меру и эргодической функции. Функции, сохраняющие меру на конечном	ПК-2.У.1

	множестве(биективные функции) и равновероятные функции. Регистр сдвига с линейной обратной связью и линейныерекуррентные последовательности над конечным полем.Период, аннулирующий, характеристический и минимальный многочлен. Критерий максимальности периода линейнойрекуррентной последовательности. Представление конечного поля матрицами над простымполем.	
3	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.	ПК-5.3.1
4	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-5.3.2

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

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

№ п/п	Примерный перечень тем для выполнения курсового проекта/ 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
1	1. Что является главным математическим фундаментом для алгоритмов асимметричной криптографии? А) Теория вероятностей и комбинаторика Б) Прикладная теория чисел (теория групп, колец и полей) В) Математический анализ и теория пределов Верный ответ: Б 2. Какую математическую задачу использует алгоритм RSA для обеспечения своей стойкости? А) Дискретное логарифмирование в конечных полях Б) Нахождение корней полинома высокой степени В) Факторизация (разложение) больших чисел на простые	ПК-2.3.2

	множители Верный ответ: В 3. Что определяет функция Эйлера $\phi(n)$ в теории чисел? А) Количество простых делителей числа n Б) Количество чисел от 1 до n, взаимно простых с n В) Наибольший общий делитель чисел Верный ответ: Б	
2	4. Чему равна функция Эйлера от простого числа p? А) $p-1$ Б) p В) 1 Верный ответ: А 5. Какой алгоритм применяется для быстрого нахождения наибольшего общего делителя (НОД) двух целых чисел? А) Алгоритм Эратосфена Б) Алгоритм Евклида В) Решето Сундарама Верный ответ: Б 6. Что вычисляет алгоритм (решето) Эратосфена? А) Остатки от деления Б) Простые числа до заданного значения В) Свойства эллиптических кривых Верный ответ: Б	ПК-2.У.1
3	7. Какое условие должно выполняться для того, чтобы число a имело обратное по модулю m (т.е. существовало $(a^{-1} \pmod m)$)? А) Числа a и m должны быть простыми Б) Число a должно быть больше числа m В) Наибольший общий делитель чисел a и m равен единице Верный ответ: В 8. Базовой математической структурой в криптосистеме Эль-Гамала является: А) Мультипликативная группа конечного поля или эллиптической кривой Б) Булева алгебра В) Кольцо многочленов без коэффициентов Верный ответ: А 9. Какой математический объект используется в современной криптографии для построения наиболее стойких систем при наименьшем размере ключа? А) Целые числа в кольце вычетов Б) Группы точек эллиптических кривых В) Матрицы малых размеров Верный ответ: Б	ПК-5.3.1
4	10. В чем заключается суть «задачи дискретного логарифмирования»? А) В разложении целого числа на множители Б) В поиске показателя степени x, при котором $g^x \equiv b \pmod p$ В) В переборе простых чисел Верный ответ: Б 11. Какая теорема утверждает, что для любого простого p и любого целого a, число $(a^p - a)$ делится на p? А) Теорема Эйлера Б) Малая теорема Ферма В) Китайская теорема об остатках Верный ответ: Б 12. На какой математической проблеме базируется алгоритм цифровой подписи (ГОСТ Р 34.10)?	ПК-5.3.2

	А) Дискретное логарифмирование в группе точек эллиптической кривой Б) Факторизация составных чисел В) Задача дискретного логарифмирования в мультипликативной группе поля Верный ответ: А	
--	---	--

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:

Модуль 1. Элементы теории чисел и модулярной арифметики

Введение: Цели криптологии. Понятия криптосистемы, шифра, ключа и стойкости.

Делимость целых чисел: Теорема о делении с остатком. Взаимно простые числа.

Алгоритм Евклида: Простая и расширенная формы. Поиск обратного элемента по модулю.

Сравнения по модулю: Свойства отношений сравнения. Кольца вычетов.

Фундаментальные теоремы: Малая теорема Ферма. Функция и теорема Эйлера. Китайская теорема об остатках (КТО).

Модуль 2. Алгебраические структуры в криптографии

Теория групп: Определение группы, подгруппы. Циклические группы. Порядок элемента.

Конечные поля (Поля Галуа): Поля вида $GF(p)$ и $GF(p^m)$. Арифметика многочленов над конечными полями (применяется в AES).

Тесты на простоту: Детерминированные и вероятностные тесты (Ферма, Миллера — Рабина, Соловея — Штрассена). Генерация больших простых чисел.

Модуль 3. Математические основы асимметричной криптографии

Односторонние функции: Понятие функции с «лазейкой» (trapdoor). Сложностно-теоретические проблемы.

Криптосистема RSA: Математическое обоснование. Процедура генерации ключей, зашифрования и расшифрования. Математические атаки на RSA.

Схема Диффи — Хеллмана и Эль-Гамала: Задача дискретного логарифмирования. Протокол распределения ключей и алгоритм шифрования.

Модуль 4. Теоретико-информационная стойкость и современные стандарты

Теория Клода Шеннона: Совершенная секретность. Энтропия источника сообщений. Расстояние единственности.

Математика симметричного шифрования: S-блоки (подстановки) и P-блоки (перестановки). Линейный и дифференциальный криптоанализ.

Эллиптические кривые (ECC): Математика точек на эллиптической кривой над конечными полями. Группа точек, сложение и удвоение точек. Стойкость ECDSA/ГОСТ.

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 на лекциях;
- получение новой информации по изучаемой дисциплине;
- приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

1. Задание и требования к проведению лабораторных работ

Формат заданий

Каждая лабораторная работа состоит из трех обязательных блоков:

- **Теоретический блок:** Самостоятельное изучение математического аппарата (теория чисел, общая алгебра).
- **Расчетно-аналитический блок:** Ручное решение «игрушечного» примера (с небольшими числами) для понимания математической сути алгоритма.

- **Программный блок:** Написание программного кода, реализующего алгоритм для работы с большими числами (без использования готовых высокоуровневых криптографических библиотек).

Общие требования к выполнению

- **Самостоятельность:** Запрещается использование готовых криптографических библиотек (например, PyCrypto, OpenSSL). Все базовые операции (расширенный алгоритм Евклида, быстрое возведение в степень по модулю) должны быть реализованы вручную.
- **Вариантность:** Каждому студенту выдаются индивидуальные входные параметры (модули, ключи, исходные сообщения).
- **Сроки выполнения:** Лабораторная работа должна быть защищена до контрольной точки (рубежного контроля) по данному модулю.

2. Структура и форма отчета о лабораторной работе

Отчет является официальным документом, подтверждающим выполнение работы. Он должен иметь следующую строгую структуру:

1. **Титульный лист** (установленного образца вуза).
2. **Цель работы** (чему студент должен научиться).
3. **Постановка задачи** (текст индивидуального задания, выданные преподавателем математические параметры).
4. **Краткие теоретические сведения** (основные математические определения, формулы, теоремы, на которых базируется лабораторная работа).
5. **Алгоритм реализации задачи** (пошаговое описание работы программы, математическая блок-схема).
6. **Ручной расчет** (пошаговый пример вычислений на малых числах).
7. **Результаты работы программы** (скриншоты работы ПО, примеры зашифрования/дешифрования, временные характеристики выполнения).
8. **Исходный код программы** (наиболее важные функции с комментариями).
9. **Выводы** (анализ полученных результатов, оценка вычислительной сложности алгоритма и его криптостойкости).

3. Требования к оформлению отчета

Оформление отчета должно соответствовать **ГОСТ 7.32** (Отчет о научно-исследовательской работе) или внутреннему стандарту кафедры.

Параметры текста и страницы

- **Формат страницы:** А4, книжная ориентация.
- **Поля:** Левое — 30 мм (для подшивки), правое — 10 (или 15) мм, верхнее и нижнее — 20 мм.
- **Шрифт:** Times New Roman, размер (кегель) — 14 пт (в таблицах допускается 12 пт).
- **Цвет шрифта:** Черный.
- **Межстрочный интервал:** 1.5 (полуторный).
- **Выравнивание текста:** По ширине страницы, с автоматическим переносом слов.
- **Абзацный отступ (красная строка):** 1,25 см.

Оформление специфических элементов криптологии

- **Математические формулы:** Должны быть набраны в редакторе формул (MS Equation, MathType или LaTeX).
- Все формулы выравниваются по центру, а их порядковый номер указывается в круглых скобках у правого края: (1).
- **Программный код:** Листинг программы оформляется моноширинным шрифтом (например, Courier New, размер 10–12 пт) с одинарным межстрочным интервалом. Большие куски кода выносятся в «Приложение».

- **Графика и таблицы:** Все графики (например, зависимости времени генерации ключа от его длины) и таблицы должны иметь сквозную нумерацию и названия (например, «Рисунок 1 – Блок-схема алгоритма RSA», «Таблица 2 – Результаты тестов на простоту»).

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.

В процессе выполнения самостоятельной работы у обучающегося 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.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

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.

1. Формы текущего контроля успеваемости

Контроль знаний проводится на протяжении всего семестра и включает в себя четыре основные формы:

- **Защита лабораторных работ:** Оценка практических навыков программирования криптоалгоритмов и ручных математических расчетов.
- **Тестирование (компьютерное или бланковое):** Проверка теоретических знаний, базовых понятий и формул (проводится в конце каждого учебного модуля).
- **Контрольные работы (коллоквиумы):** Письменное решение сложных математических задач без использования вычислительной техники (проверка владения аппаратом теории чисел).
- **Экспресс-опросы (летучки):** Короткие 5-минутные задания в начале лекций или практик для проверки усвоения материала прошлых занятий.

2. Критерии оценивания по видам контроля

Лабораторные работы

- **«Отлично» (высокий уровень):** Программа работает корректно на любых входных данных, код оптимизирован (например, используется быстрое возведение в степень, а не стандартное), студент демонстрирует глубокое понимание математической сути алгоритма, легко отвечает на дополнительные теоретические вопросы при защите, отчет оформлен строго по ГОСТу.
- **«Хорошо» (средний уровень):** Программа выполняет базовые функции, но содержит мелкие недочеты (нет валидации входных данных, не обработаны исключения). Студент ориентируется в алгоритме, но допускает незначительные ошибки при ответе на теоретические вопросы.

- **«Удовлетворительно» (минимальный уровень):** Программа работает нестабильно или только на «игрушечных» числах. Студент не может объяснить назначение отдельных функций в своем коде. Отчет имеет серьезные нарушения в оформлении.
- **«Неудовлетворительно»:** Код скопирован (плагиат), программа не компилируется/не запускается, студент не понимает математическую логику работы.

Тестирование и контрольные работы

Оценка выставляется на основе процента верно выполненных заданий или набранных баллов:

- **90% – 100%:** Отлично (выдающиеся знания)
- **74% – 89%:** Хорошо (полное понимание материала)
- **60% – 73%:** Удовлетворительно (базовые знания)
- **Менее 60%:** Неудовлетворительно (требуется повторное изучение)

3. Шкала оценивания и балльно-рейтинговая система (БРС)

Распределение баллов в течение семестра (примерная структура на 100 баллов):

Вид учебной деятельности	Количество в семестр	Макс. балл за единицу	Всего баллов
Выполнение и защита лабораторных работ	4 работы	10 баллов	40 баллов
Тестирование по модулям	4 теста	5 баллов	20 баллов
Контрольные (рубежные) работы	2 работы	15 баллов	30 баллов
Активность на практиках / Экспресс-опросы	—	—	10 баллов
ИТОГО за текущий контроль			100 баллов

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:

– 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».

1. Условия допуска к дифференцированному зачету

Для получения допуска к сдаче зачета обучающийся обязан выполнить обязательный минимум учебной программы в течение семестра:

- **Сдать все лабораторные работы** (с предоставлением оформленных и защищенных отчетов).
- **Пройти все этапы текущего контроля** (тесты, контрольные работы) с оценкой не ниже «удовлетворительно» (или набрать минимальный пороговый балл в рамках БРС — обычно не менее 45–60 баллов из 100).
- **Ликвидировать задолженности** по пропущенным занятиям (в случае их наличия).

2. Форма проведения промежуточной аттестации

Дифференцированный зачет проводится по утвержденному расписанию в **сочетании устной и письменной форм**:

1. **Билетная система:** Студент выбирает случайный экзаменационный билет.
2. **Структура билета:** Каждый билет включает 3 вопроса/задания:

- *Вопрос 1 (теоретический):* Математические основы, теоремы, доказательства или свойства алгебраических структур (например, «Свойства функции Эйлера и ее применение»).
- *Вопрос 2 (теоретико-практический):* Описание криптографического протокола, алгоритма или схемы, его математическая стойкость (например, «Алгоритм цифровой подписи ГОСТ Р 34.10»).
- *Вопрос 3 (практическая задача):* Ручной расчет криптографической операции (например, «Найти обратный элемент к числу $a=17$ по модулю $m=43$ с помощью расширенного алгоритма Евклида» или «Сгенерировать ключи в системе RSA для малых простых чисел»).

3. **Время на подготовку:** На подготовку ответов по билету и письменное решение задачи студенту выделяется **45–60 минут**.

3. Критерии оценивания на дифференцированном зачете

Итоговая оценка («отлично», «хорошо», «удовлетворительно», «неудовлетворительно») выставляется на основе качества ответов на все пункты билета, а также с учетом работы студента в семестре (БРС).

- **«Отлично»:** Студент в полном объеме владеет математическим аппаратом криптологии. Свободно оперирует понятиями теории чисел и общей алгебры. Без ошибок решил практическую задачу. Логично, последовательно и аргументированно изложил теоретические вопросы, продемонстрировал глубокую связь теории с практической реализацией шифров.
- **«Хорошо»:** Студент твердо знает материал, грамотно излагает суть математических методов. Задача решена верно, но в ходе решения или в ответе на теоретические вопросы были допущены незначительные неточности, которые студент самостоятельно исправил после наводящих вопросов преподавателя.
- **«Удовлетворительно»:** Студент демонстрирует поверхностные знания, путает формулировки сложных теорем. Практическая задача решена с арифметическими ошибками или решена не до конца. Ответ на билет фрагментарен, студент испытывает серьезные затруднения при ответе на дополнительные вопросы, но ориентируется в базовых понятиях (модулярная арифметика, алгоритм Евклида).
- **«Неудовлетворительно»:** Студент не знает базовых математических понятий дисциплины. Практическая задача не решена. Ответ на теоретические вопросы билета отсутствует либо содержит грубые ошибки. Компетенции не сформированы, зачет не выставляется.

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