МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
декан факультета прикладной
математики, информатики
и механики

_____А.И. Шашкин
подпись, расшифровка подписи
23.05.2020

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.Б.45 Теоретико-числовые методы в криптографии

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

математические методы защиты информации

3. Квалификация (степень) выпускника:

Специалист по защите информации

4. Форма обучения:

очная

5. Кафедра, отвечающая за реализацию дисциплины:

ERP-систем и бизнес-процессов

6. Составители программы:

Крыжановская Юлиана Александровна, старший преподаватель кафедры ERP-систем и бизнес-процессов

7. Рекомендована:

Научно-методическим советом факультета прикладной математики, информатики и механики 23.05.2020 г., протокол № 9

_____
отметки о продлении вносятся вручную)

8. Учебный год: 2024/2025 **Семестр(ы):** 9

9.Цели и задачи учебной дисциплины: Целью дисциплины является освоение студентом математического аппарата теории чисел для последующего успешного использования основных методов теории чисел в профессиональной деятельности. Задачами дисциплины являются: развитие у студентов соответствующих общекультурных, профессиональных и профессионально-специализированных компетенций; ознакомление с основами классической и современной теории чисел и численными− алгоритмами, имеющими практические приложения в криптографии; формирование умения строгой оценки эффективности применяемых алгоритмов с− математической точки зрения; формирование четкого осознания необходимости и важности математической подготовки для специалиста по компьютерной безопасности. Цели образовательного процесса достигаются посредством применения инновационных образовательных технологий в обеспечении компетентностного подхода.

10. Место учебной дисциплины в структуре ООП: Дисциплина «Теоретико-числовые методы в криптографии» входит в базовую часть учебного плана и изучается в 9 семестре.

№ п/п	Наименование дисциплин учебного плана, с которым организована взаимосвязь дисциплины рабочей программы
1	Б1.Б.37 Основы информационной безопасности
2	Б1.Б.43 Криптографические протоколы
3	Б1.Б.44 Криптографические методы защиты информации
4	Б1.Б.51.04 Криптографические стандарты

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ПК-4	Способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем.	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов.

12. Объем дисциплины в зачетных единицах/час. (*в соответствии с учебным планом)* — 6/216.

Форма промежуточной аттестации *(зачет/экзамен)* экзамен.

13. Виды учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			9 семестр		
Аудиторные занятия		100	100		
в том числе:	лекции	50	50		
	практические	0	0		
	лабораторные	50	50		
Самостоятельная работа		80	80		
Контроль		36	36		
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – __час.)*			Экз.		
Итого:			216		

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
		1. Лекции
1.1	Введение в математические проблемы криптографии. Основы теории чисел.	В криптографии важную роль играют простые числа. Рассмотрены основы теории делимости. Приведены простые (с методической точки зрения) алгоритмы выявления простоты числа и алгоритм нахождения всех простых чисел, не превосходящих заданного числа. Рассмотрены алгоритмы нахождения наибольшего общего делителя и представления наибольшего общего делителя двух чисел в виде линейной комбинации (с целыми коэффициентами) этих чисел. Показаны области использования непрерывных дробей в криптографии. Описаны важнейшие функции теории чисел, в том числе широко используемая в криптографии функция Эйлера. На содержательном уровне описаны основные проблемы и понятия криптографии. В традиционной криптографии довольно часто используют преобразование y=ax+b (mod) m. Рассмотрено использование таких преобразований для генерации псевдослучайных последовательностей. Делимость, простые числа, наибольший общий делитель. Алгоритм Евклида, расширенный алгоритм Евклида. Цепные дроби. Асимптотический закон распределения простых чисел. Мультипликативные функции.
1.2	Теория сравнений. Вычеты.	Доказаны важные для криптографии с открытым ключом теоремы Ферма и Эйлера о свойстве операции возведения в степень по заданному модулю. Полная система вычетов, приведенная система вычетов. Zn, Zp, Z*n, Z* p Обратный элемент в Zn Алгебраические структуры на целых числах. Теорема Эйлера, теорема Ферма, тест Ферма на простоту. Криптосистема RSA. Понижение степени сравнения.
1.3	Сравнения первой степени. Системы сравнений первой степени.	Исследовано нахождение решений сравнений первой степени и систем таких сравнений. В частности, доказана широко используемая в современной криптографии Китайская теорема об остатках. Приведены алгоритмы нахождения символов Лежандра и Якоби, значения которых позволяют решить вопрос о разрешимости сравнений второй степени по простому модулю.
1.4	Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.	Квадратичные сравнения. Символ Лежандра. Закон взаимности. Существование решений квадратичного сравнения по простому модулю. Решение квадратичных сравнений по простому модулю. Символ Якоби и его свойства. Тест Соловея-Штрассена на простоту. Тест Миллера-Рабина. Существование и количество решений квадратичного сравнения по составному модулю. Решение квадратичных сравнений по составному модулю. Квадраты и псевдоквадраты. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации. Числа Блюма. BBS-генератор. Криптосистемы Блюма-Гольдвассер, Гольдвассер-Микали.
1.5	Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа.	Циклическая группа Z* p (Up). Порождающий элемент и дискретный логарифм. Задача дискретного логарифмирования. Криптосистемы Диффи-Хэллмана и Эль-Гамаля. Теоремы Сэлфриджа и Поклингтона. (n-1) – тесты на простоту. Доказуемо простые числа общего вида. Числа Ферма, теорема Пепина, тест Пепина. Числа Мерсенна и тест Лукаса-Лемера. Теорема Диемитко и процедура генерации простых чисел ГОСТ Р34.10-94.
1.6	Алгоритмы криптоанализа шифров с открытым ключом.	Элементы теории сложности. Оценки сложности по времени, по объему требуемой памяти. Полиномиальная сложность, субэкспоненциальная сложность, экспоненциальная сложность алгоритмов. Сложность элементарных операций. Теоретико-числовые проблемы, лежащие в основе двухключевых

		криптосистем – факторизация, дискретное логарифмирование. Алгоритмы факторизации. Метод пробных делений, метод Ферма, метод квадратичного решета, ро-метод Полларда, p—1 – метод Полларда, методы случайных квадратов. Примеры, оценки сложности указанных алгоритмов. Алгоритмы дискретного логарифмирования. Метод прямого поиска, ро-метод Полларда, метод исчисления индексов, «шаг младенца-шаг великана». Примеры, оценки сложности указанных алгоритмов.
1.7	Конечные группы и поля многочленов.	Многочлены над Zp, Zn. Сложение, умножение, факторизация многочленов. Не приводимые многочлены. Поля Галуа.
2. Практические занятия		
3. Лабораторные работы		
3.1	Лабораторная работа №1. Введение в математические проблемы криптографии. Основы теории чисел.	*Теоретические сведения* 1. Простые числа. Основы теории делимости. Простые алгоритмы выявления простоты числа и алгоритм нахождения всех простых чисел, не превосходящих заданного числа. 2. Алгоритмы нахождения наибольшего общего делителя и представления наибольшего общего делителя двух чисел в виде линейной комбинации (с целыми коэффициентами) этих чисел. 3. функция Эйлера. Алгоритм Евклида, расширенный алгоритм Евклида. Цепные дроби. Асимптотический закон распределения простых чисел. Мультипликативные функции. *Практическая часть* 1. Реализовать программно рассмотренные алгоритмы.
3.2	Лабораторная работа №2. Теория сравнений. Вычеты.	*Теоретические сведения* 1. теоремы Ферма и Эйлера. 2. Полная система вычетов, приведенная система вычетов. Zn, Zp, Z*n, Z* p 3. Обратный элемент в Zn. Алгебраические структуры на целых числах. 4. Теорема Эйлера, теорема Ферма, тест Ферма на простоту. 5. Криптосистема RSA. 6. Понижение степени сравнения. *Практическая часть* 1. Программно реализовать операции и тесты.
3.3	Лабораторная работа №3 Сравнения первой степени. Системы сравнений первой степени.	*Теоретические сведения* 1. Нахождение решений сравнений первой степени и систем таких сравнений. 2. Китайская теорема об остатках. *Практическая часть* 1. Программно реализовать нахождение решения сравнений первой степени.
3.4	Лабораторная работа №4. Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.	*Теоретические сведения* 1. Квадратичные сравнения. 2. Символ Лежандра. 3. Решение квадратичных сравнений по простому модулю. 4. Символ Якоби и его свойства. 5. Тест Соловея-Штрассена на простоту. 6. Решение квадратичных сравнений по составному модулю. 7. Квадраты и псевдоквадраты. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации. 8. Числа Блюма. BBS-генератор. 9. Криптосистемы Блюма-Гольдвассер, Гольдвассер-Микали. *Практическая часть* 1. Реализовать программно применение одной из указанных тем.
3.5	Лабораторная работа №5. Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа.	*Теоретические сведения* 1. Циклическая группа Z* p (Up). 2. Порождающий элемент и дискретный логарифм. Задача дискретного логарифмирования. 3. Криптосистемы Диффи-Хэллмана и Эль-Гамаля. 4. Теоремы Сэлфриджа и Поклингтона. (n-1) – тесты на простоту. Доказуемо простые числа общего вида. 5. Числа Ферма, теорема Пепина, тест Пепина. Числа Мерсенна

		и тест Лукаса-Лемера. 6. Теорема Диемитко и процедура генерации простых чисел ГОСТ Р34.10-94 *Практическая часть* 1. Реализовать один из указанных методов
3.6	Лабораторная работа №6. Алгоритмы криптоанализа шифров с открытым ключом.	*Теоретические сведения* 1. Элементы теории сложности. 2. Алгоритмы факторизации. Метод пробных делений, метод Ферма, метод квадратичного решета, ро-метод Полларда, р—1 – метод Полларда, методы случайных квадратов. Алгоритмы дискретного логарифмирования. Метод прямого поиска, ро-метод Полларда, метод исчисления индексов, «шаг младенца-шаг великана». *Практическая часть* 1. Реализовать один из указанных методов
3.7	Лабораторная работа №7. Конечные группы и поля многочленов.	*Теоретические сведения* 1. Многочлены над Zp, Zn. 2. Сложение, умножение, факторизация многочленов. 3. Не приводимые многочлены. 4. Поля Галуа. *Практическая часть* 1. По вводимым данным сформировать Многочлены над Zp, Zn. 2. Реализовать сложение, умножение, факторизацию многочленов.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практические	Лабораторные	Самостоятельная работа	Контрольная работа	Всего
1	Введение в математические проблемы криптографии. Основы теории чисел.	4	0	6	8	2	20
2	Теория сравнений. Вычеты.	8	0	8	12	4	32
3	Сравнения первой степени. Системы сравнений первой степени.	4	0	8	12	6	30
4	Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.	8	0	8	12	6	34
5	Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа.	8	0	8	12	6	34
6	Алгоритмы криптоанализа шифров с открытым ключом.	8	0	8	12	6	34
7	Конечные группы и поля многочленов.	10	0	4	12	6	32
	Итого:	50	0	50	80	36	216

14. Методические указания для обучающихся по освоению дисциплины

Изучение теоретического материала, представленного в лекциях, основной и дополнительной рекомендуемой литературе, итоговое повторение теоретического материала. Подготовка к лабораторным работам, контрольной работе и экзамену.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

а) основная литература:

№ п/п	Источник
1	Василенко О. Н. Теоретико-числовые методы в криптографии [электронный ресурс] / О. Н. Василенко. – Электрон. Текстовые дан. – М.: МЦНМО, 2006.

б) дополнительная литература:

№ п/п	Источник
1	Диффи У. Защищенность и имитостойкость. Введение в криптографию / У. Диффи, М. Э. Хэллман. // ТИИЭР, т. 67, № 3, 1979.
2	Криптографические методы защиты информации : учебно-методическое пособие / сост.: Б. Н. Воронков, Ю. А. Крыжановская .— Воронеж : Издательский дом ВГУ, 2018 .— 113 с.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
1.	https://e.lanbook.com/ - ЭБС «Лань»
2.	www.lib.vsu.ru — Зональная научная библиотека ВГУ

* Вначале указываются ЭБС, с которыми имеются договоры у ВГУ, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)*

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения теоретико-числовых методов. Также предусмотрено получение консультаций по вопросам изучаемой дисциплине, изучение теоретического материала, представленного в лекциях, основной и дополнительной рекомендуемой литературе, выполнение индивидуальных и групповых заданий лабораторных работ, итоговое повторение теоретического материала. Также к СРС относится подготовка к контрольной работе и экзамену.

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Windows7, Microsoft Visual Studio Community. Мультимедийные лекционные демонстрации. Презентации на базе конспекта лекций.

18. Материально-техническое обеспечение дисциплины:

Лекционная аудитория оснащена специальной мебелью современным компьютером с подключенным к нему проектором и настенным экраном. Лаборатория оснащена современными компьютерами с установленным программным обеспечением, позволяющим выполнять: решение задач по освоению теоретико-числовых методов, применяемых в криптографии.

19. Фонд оценочных средств:

19.1. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции (или ее части)	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ПК-4. Способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем.	Знать теоретико-числовые методы защиты информации.	Раздел 1. Введение в математические проблемы криптографии. Основы теории чисел. Раздел 2. Теория сравнений. Вычеты. Раздел 3. Сравнения первой степени. Системы сравнений первой степени. Раздел 4. Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту. Раздел 5. Порождающий элемент и дискретный логарифм. Криптосистемы на	Устный опрос, лабораторные работы. Контрольная работа.

		их основе. Доказуемо простые числа. Раздел 6. Алгоритмы криптоанализа шифров с открытым ключом. Раздел 7. Конечные группы и поля многочленов	
	Уметь реализовывать алгоритмы защиты данных на основе теоретико-числовых методов.	Раздел 1. Введение в математические проблемы криптографии. Основы теории чисел. Раздел 2. Теория сравнений. Вычеты. Раздел 3. Сравнения первой степени. Системы сравнений первой степени. Раздел 4. Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту. Раздел 5. Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа. Раздел 6. Алгоритмы криптоанализа шифров с открытым ключом. Раздел 7. Конечные группы и поля многочленов	Устный опрос, лабораторные работы. Контрольная работа.
	Владеть навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов.	Раздел 1. Введение в математические проблемы криптографии. Основы теории чисел. Раздел 2. Теория сравнений. Вычеты. Раздел 3. Сравнения первой степени. Системы сравнений первой степени. Раздел 4. Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту. Раздел 5. Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа. Раздел 6. Алгоритмы криптоанализа шифров с открытым ключом. Раздел 7. Конечные группы и поля многочленов.	Устный опрос, лабораторные работы. Контрольная работа.
Промежуточная аттестация			КИМ

* В графе «ФОС» в обязательном порядке перечисляются оценочные средства текущей и промежуточной аттестаций.

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Промежуточная аттестация включает в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и результаты выполнения лабораторных работ, позволяющие оценить степень сформированности умений и навыков.

Для оценивания результатов обучения на зачете используется – зачтено, не зачтено

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Компетенция	Показатель сформированности компетенции	Шкала и критерии оценивания уровня освоения компетенции			
		5	4	3	2
ПК-4. Способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем.	Знает: – теоретико-числовые методы защиты информации.	Сформированные знания	Сформированные знания, но содержащие отдельные пробелы	Неполные знания	Фрагментарные знания или их отсутствие
	Умеет: – реализовывать алгоритмы защиты данных на основе теоретико-числовых методов.	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений
	Владеет: – навыками построения математических моделей	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные	Фрагментарные умения или

	элементов			умения	отсутствие умений

19.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

19.3.1 Примерный перечень вопросов к экзамену:

1. Простые числа. Основы теории делимости. Простые алгоритмы выявления простоты числа, алгоритм нахождения всех простых чисел, не превосходящих заданного числа.
2. Области использования непрерывных дробей в криптографии.
3. Важнейшие функции теории чисел.
4. Основные проблемы и понятия криптографии.
5. Преобразование y=ax+b (mod) m. Его использование для генерации псевдослучайных последовательностей.
6. Алгоритм Евклида, расширенный алгоритм Евклида. Цепные дроби.
7. Асимптотический закон распределения простых чисел. Мультипликативные функции. Функция Эйлера.
8. Теоремы Ферма и Эйлера. тест Ферма на простоту.
9. Полная система вычетов, приведенная система вычетов. Zn, Zp, Z*n, Z* p Обратный элемент в Zn Алгебраические структуры на целых числах.
10. Криптосистема RSA. Понижение степени сравнения.
11. Нахождение решений сравнений первой степени и систем таких сравнений.
12. Китайская теорема об остатках.
13. Алгоритмы нахождения символов Лежандра и Якоби.
14. Квадратичные сравнения. Закон взаимности. Существование решений квадратичного сравнения по простому модулю.
15. Решение квадратичных сравнений по простому модулю. Символ Якоби и его свойства.
16. Тест Соловея-Штрассена на простоту.
17. Тест Миллера-Рабина.
18. Существование и количество решений квадратичного сравнения по составному модулю.
19. Решение квадратичных сравнений по составному модулю. Квадраты и псевдоквадраты.
20. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации. Числа Блюма. BBS-генератор.
21. Криптосистемы Блюма-Гольдвассер, Гольдвассер-Микали.
22. Циклическая группа Z* p (Up).
23. Порождающий элемент и дискретный логарифм. Задача дискретного логарифмирования. Криптосистемы Диффи-Хэллмана и Эль-Гамаля.
24. Теоремы Сэлфриджа и Поклингтона. (n-1) – тесты на простоту. Доказуемо простые числа общего вида.
25. Числа Ферма, теорема Пепина, тест Пепина. Числа Мерсенна и тест Лукаса-Лемера.
26. Теорема Диемитко и процедура генерации простых чисел ГОСТ Р34.10-94.
27. Элементы теории сложности. Оценки сложности по времени, по объему требуемой памяти. Полиномиальная сложность.
28. субэкспоненциальная сложность, экспоненциальная сложность алгоритмов.
29. Сложность элементарных операций.
30. Факторизация, дискретное логарифмирование.
31. Алгоритмы факторизации.
32. Алгоритмы дискретного логарифмирования.
33. Сложение и умножение многочленов.
34. Разложение многочленов на сомножители. Неприводимые многочлены.
35. Различие понятий – кодирование и шифрование.
36. От каких характеристик кода зависит его корректирующая способность.

37. Сравните коды Хэмминга и циклические коды по эффективности контроля целостности информации.
38. Теоретико-числовые проблемы, лежащие в основе двухключевых криптосистем – факторизация, дискретное логарифмирование. Алгоритмы факторизации. Метод пробных делений, метод Ферма, метод квадратичного решета, ро-метод Полларда, p—1 – метод Полларда, методы случайных квадратов. Примеры, оценки сложности указанных алгоритмов. Алгоритмы дискретного логарифмирования.
39. Метод прямого поиска, ро-метод Полларда, метод исчисления индексов, «шаг младенца-шаг великана». Примеры, оценки сложности указанных алгоритмов.
40. Многочлены над Zp, Zn.
41. Сложение, умножение, факторизация многочленов.
42. Не приводимые многочлены.
43. Поля Галуа.

Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Декан факультета ПММ_____
_____Шашкин А. И.
подпись, расшифровка подписи
___.___.2016

Направление подготовки / специальность ___10.05.01_Компьютерная безопасность
шифр, наименование
Дисциплина__Теоретико-числовые методы криптографии _____

Вид контроля _____экзамен_____
промежуточный контроль - экзамен, зачет; текущий контроль с указанием формы

Контрольно-измерительный материал №_1_

1. Основные понятия теории чисел. Сравнения первой степени.

2. Алгоритмы криптоанализа шифров с открытым ключом.

Преподаватель _____ ____
подпись расшифровка подписи

19.3.2 Перечень практических заданий
Не предусмотрены

19.3.3 Тестовые задания
Не предусмотрены

19.3.4 Примерный перечень заданий для контрольных работ
Вариант 1.
1. Простые числа.
2. Теорема Эйлера.
3. Китайская теорема об остатках.
4. Тест Миллера-Рабина.
5. Криптосистемы Диффи-Хэллмана.
6. «шаг младенца-шаг великана».
7. Не приводимые многочлены.

Вариант 2.
1. Основы делимости.
2. Теорема Ферма.
3. Алгоритмы нахождения символов Лежандра и Якоби.
4. Тест Соловея-Штрассена.

5. Теорема Диемитко и процедура генерации простых чисел ГОСТ Р34.10-94
6. метод исчисления индексов
7. Поля Галуа.

19.3.5 Темы курсовых работ
Не предусмотрены

19.3.6 Темы рефератов
Не предусмотрены

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного опроса; лабораторных работ; контрольной работы. Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практическое задание, позволяющее оценить степень сформированности умений и навыков по работе с теоретико-числовыми методами в криптографии.

При оценивании используются качественные шкалы оценок. Критерии оценивания приведены выше.