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

УТВЕРЖДАЮ
Декан факультета прикладной математики, информатики и механики
Медведев С.Н.
31.03.2026 г

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.25 Методы представления, хранения и обработки информации

1. **Код и наименование направления подготовки:**

02.03.03 Математическое обеспечение и администрирование информационных систем

2. **Программа бакалавриата:**

Проектирование и разработка информационных систем

3. **Квалификация выпускника:** бакалавр

4. **Форма обучения:** очная

5. **Кафедра, отвечающая за реализацию дисциплины:** программного обеспечения и администрирования информационных систем

6. **Составители программы**: Барановский Е.С., к.ф.-м.н, заведующий кафедрой программного обеспечения и администрирования информационных систем

7. **Рекомендована:** НМС факультета Прикладной математики, информатики и механики № 6 от 17.03.2025 (изменения – протокол № 7 от 20.03.2026)

8. **Учебный год:** 2027/2028 **Семестр(ы):** 6

9. Цели и задачи учебной дисциплины

Цели освоения дисциплины:

Сформировать у студентов системное понимание математических основ представления, хранения и обработки информации, включая теоретико-числовые и алгебраические структуры. Научить выбирать адекватные математические модели и инструментальные средства (алгоритмы Евклида, сравнения, функции Эйлера, протоколы Диффи–Хеллмана, эллиптические кривые) для решения прикладных задач обработки и защиты информации. Развить способность применять типовые математические модели (группы, кольца, поля) на практике, анализировать результаты вычислений и интерпретировать их с точки зрения эффективности и корректности обработки данных. Подготовить студентов к использованию современных математических методов (включая ECDH) для решения задач целостности, конфиденциальности и аутентификации информации.

Задачи дисциплины:

- Изучить базовые математические модели теории чисел и алгебры (НОД, сравнения, кольца вычетов, мультипликативные группы) как инструменты описания информационных процессов.
- Освоить типовые алгоритмы обработки информации (расширенный алгоритм Евклида, решение сравнений и диофантовых уравнений, нахождение порядка элемента) и научиться применять их на практике.
- Сформировать умение выбирать подходящие математические методы (классические или основанные на эллиптических кривых) для реализации современных криптографических протоколов (Диффи–Хеллмана, Шнорра и др.) с учётом требований задачи.
- Развить навыки анализа результатов расчётов (оценка сложности, проверка разрешимости сравнений, интерпретация полученных ключей) и использования типовых моделей (поля, группы) для представления и обработки информации.
- Обеспечить опыт применения математических инструментальных средств (программная реализация алгоритмов, моделирование атак) для решения задач хранения и безопасной передачи информации.

10. Место учебной дисциплины в структуре ОПОП:
дисциплина относится к обязательным дисциплинам части, формируемой участниками образовательных отношений части Блока 1. блока Б1 учебного плана. Для изучения курса необходимы базовые знания в области алгебры и информатики.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения

ОПК-1	Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности	ОПК-1.3	Осуществляет выбор современных математических инструментальных средств для обработки исследуемых явлений в соответствии с поставленной задачей, анализирует результаты расчетов и интерпретирует полученные результаты	ЗНАТЬ: Основы теории чисел: свойства простых и взаимно простых чисел, алгоритм Евклида, основную теорему арифметики, распределение простых чисел. Базовые алгебраические структуры (группы, кольца, поля), понятие идеала и кольца вычетов, функцию Эйлера, теоремы Эйлера и Ферма. Методы решения сравнений и линейных диофантовых уравнений. Принципы криптографии с открытым ключом: односторонние функции, протокол Диффи–Хеллмана, атаку «человек посередине», протокол Шнорра. Основы эллиптических кривых в форме Вейерштрасса, теорему Хассе и алгоритм Диффи–Хеллмана на эллиптических кривых (ECDH). УМЕТЬ: Находить НОД и его линейное представление, проверять числа на простоту и раскладывать на множители, вычислять функцию Эйлера. Работать со сравнениями: упрощать их, решать линейные сравнения и диофантовы уравнения. Применять малую теорему Ферма и теорему Эйлера для вычисления остатков по модулю. Моделировать протоколы Диффи–Хеллмана и Шнорра, объяснять уязвимость к атаке MITM и способы её предотвращения. Выполнять операции на эллиптических кривых (сложение точек, скалярное умножение) и реализовывать ECDH для заданных параметров. ВЛАДЕТЬ: Навыками программной реализации расширенного алгоритма Евклида и модулярной арифметики на языке высокого уровня. Техникой решения сравнений и диофантовых уравнений как аналитически, так и алгоритмически. Практическими приёмами вычисления порядка элемента в поле, проверки примитивности и использования теоремы Эйлера для оптимизации вычислений. Опытом моделирования криптографических протоколов (DH, ECDH) в учебной среде, включая симуляцию атаки «человек посередине». Навыками работы с эллиптическими кривыми в малых полях (сложение, удвоение, скалярное умножение) и базовыми методами криптоанализа.
ОПК-2	Способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности	ОПК-2.1	Применяет типовые математические модели на практике	

12. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом —3/108

Форма промежуточной аттестации *экзамен*.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоемкость (часы)				
	Всего	В том числе в интерактивной форме	По семестрам		
			№ сем. 6	№ сем.	…..
Аудиторные занятия					
в том числе: лекции					
практические					
лабораторные					
Самостоятельная работа					
Форма промежуточной аттестации					
Итого:					

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
	1. Лекции		
1	Теоретико-числовые основы представления информации	Алгоритм Евклида, НОД и его линейное выражение. Свойства взаимно простых чисел. Бесконечность множества простых чисел, решето Эратосфена, тесты простоты. Единственность разложения на множители, каноническая форма. Плотность простых чисел, функция π(x). Определение и свойства сравнений по модулю.	Методы представления, хранения и обработки информации https://edu.vsu.ru/course/view.php?id=18851
2	Алгебраические структуры и кольцо вычетов	Группы (абелевы, циклические), подгруппы. Кольца, поля, идеалы (главные), факторкольца. Построение Z_m, полные и приведённые системы вычетов. Обратимые элементы, структура мультипликативной группы. Вычисление φ(m). Теоремы Эйлера и Ферма, их применение. Порядок элемента, существование первообразных корней в Z_m	
3	Решение сравнений, диофантовы уравнения и основы асимметричной криптографии	Понятие решения сравнения, равносильные преобразования. Линейные сравнения $a \cdot x \equiv b \pmod m$: условие разрешимости, алгоритм решения через обратный элемент или расширенный алгоритм Евклида. Связь с линейными диофантовыми уравнениями. Гаммирование как метод шифрования (XOR, гамма по модулю). Односторонние функции (возведение в степень, умножение простых чисел) и функции с секретом (потайной вход) как основа криптографии с открытым ключом.	
4	Криптографические протоколы и эллиптические	Протокол выработки общего секрета Диффи–Хеллмана на дискретном логарифме. Уязвимость к атаке «человек посередине» и способы защиты	

	кривые	(аутентификация). Протокол Шнорра — доказательство знания дискретного логарифма без его раскрытия. Эллиптические кривые над конечными полями, уравнение Вейерштрасса, базовая точка (генератор). Теорема Хассе о числе точек. ECDH — аналог Диффи–Хеллмана на эллиптических кривых, скалярное умножение как односторонняя функция.	
2. ***Лабораторные работы***			
1	Теоретико-числовые основы представления информации	1.1. Реализация расширенного алгоритма Евклида и нахождение линейного представления НОД. 1.2. Проверка числа на простоту методом перебора делителей и факторизация с использованием канонического разложения 1.3. Вычисление сравнений и упрощение выражений по модулю (арифметика вычетов).	Методы представления, хранения и обработки информации https://edu.vsu.ru/course/view.php?id=18851
2	Алгебраические структуры и кольцо вычетов	2.1 Исследование операций в кольце вычетов Z_m: построение таблиц сложения и умножения в Z_m. 2.2. Нахождение обратимых элементов и вычисление функции Эйлера φ(m) для заданного модуля. 2.3. Определение порядка элемента и поиск примитивных (образующих) элементов в поле Z_p.	
3	Решение сравнений, диофантовы уравнения и основы асимметричной криптографии	3.1. Решение линейных сравнений $a \cdot x \equiv b \pmod m$ и линейных диофантовых уравнений. 3.2. Программная реализация процедуры гаммирования (потокового шифрования) с различными гаммами. 3.3. Исследование односторонних функций: возведение в степень по модулю и факторизация как примеры функций с секретом	
4	Криптографические протоколы и эллиптические кривые	4.1. Моделирование протокола Диффи–Хеллмана и реализация атаки «человек посередине» 4.2. Реализация протокола аутентификации Шнорра (доказательство знания дискретного логарифма) 4.3. Вычисление точек на эллиптической кривой в форме Вейерштрасса и реализация алгоритма ECDH	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практи-ческие	Лабораторные	Самостоятельная работа	Всего
1	Теоретико-числовые основы представления информации	6	-	6	4	16
2	Алгебраические структуры и кольцо вычетов	6	-	6	8	20

3	Решение сравнений, диофантовы уравнения и основы асимметричной криптографии	8	-	8	8	24
4	Криптографические протоколы и эллиптические кривые	12	-	12	24	48
	Итого:	32	-	32	44	108

14. Методические указания для обучающихся по освоению дисциплины

Дисциплина реализуется по тематическому принципу, каждая тема представляет собой завершенный раздел курса. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины: вводятся основные понятия, изучаются базовые утверждения, разбираются основные алгоритмы и обсуждаются способы их программной реализации. Лабораторные работы предназначены для формирования умений и навыков, закрепленных компетенций по ОПОП. Они организовываются в виде выполнения отдельных заданий. По окончании изучения дисциплины проводится тестирование.

Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор заданий лабораторных работ, подготовку к зачету. Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации по соответствующей теме, чтобы систематизировать изучаемый материал, выполнять задания лабораторных работ.

Промежуточная аттестация по результатам обучения проводится в форме зачета с оценкой, контролирующего освоение ключевых положений дисциплины, составляющих основу знаний по дисциплине.

При использовании дистанционных образовательных технологий и электронного обучения следует выполнять все указания преподавателя по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

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

а) основная литература:

№ п/п	Источник
1	Пилиди, В.С. Математические основы защиты информации : учебное пособие / Пилиди В.С.Москва : ЮФУ, 2019308 с.Режим доступа: https://www.studentlibrary.ru/book/ISBN9785927533633.html
2	Хохлов, Г.И. Комбинаторная теория информации (информационная теория детерминированных процессов) : Монография / Г.И. ХохловЭлектрон. дан.Москва : Русайнс, 2016396 с. Режим доступа: https://book.ru/book/926201ISBN 978-5-4365-0429-2

б) дополнительная литература:

№ п/п	Источник

4	Алексеев, В.Е.Графы и алгоритмы. Структуры данных. Модели вычислений : учебник / Алексеев В.Е. ; Таланов В.А.Москва : ИНТУИТ, 2016. Режим доступа: https://www.studentlibrary.ru/book/ISBN5955600663.html
5	Макшанов, А. В. Современные технологии интеллектуального анализа данных : учебное пособие для спо / А. В. Макшанов, А. Е. Журавлев, Л. Н. Тындыкарь. — Санкт-Петербург : Лань, 2020. — 228 с. — ISBN 978-5-8114-5451-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/149343 (дата обращения: 25.02.2024). — Режим доступа: для авториз. пользователей.

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

№ п/п	Ресурс
6	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
7	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
8	Методы представления, хранения и обработки информации / Е.С. Барановский. — Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru/course/view.php?id=18851

16. Перечень учебно-методического обеспечения для самостоятельной работы

Для самостоятельной подготовки обучающийся пользуется конспектами лекций и литературой по тематике лекционного материала, заданий лабораторных работ.
Самостоятельная работа обучающегося должна включать подготовку к тестированию, лабораторным занятиям и подготовку к промежуточной аттестации. Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению лабораторных работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

При реализации дисциплины используются следующие образовательные технологии: логическое построение дисциплины, обозначение теоретического и практического компонентов в учебном материале. Применяются разные типы лекций (вводная, обзорная, информационная, проблемная). Дисциплина реализуется с применением информационно-коммуникационных технологий.

Информационно-коммуникативные технологии для реализации учебной дисциплины:
- технологии синхронного и асинхронного взаимодействия студентов и преподавателя посредством служб (сервисов) по пересылке и получению электронных сообщений, в том числе, по сети Интернет;
- сервис электронной почты для оперативной связи преподавателя и студентов.

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий, для организации самостоятельной работы обучающихся используется онлайн-курс, размещенный на платформе Электронного университета ВГУ (LMS moodle), а также другие Интернет-ресурсы, приведенные в п.15в.

18. Материально-техническое обеспечение дисциплины:

Лекционная аудитория должна быть оборудована учебной мебелью, компьютером, мультимедийным оборудованием (проектор, экран, средства звуковоспроизведения), допускается переносное оборудование.

Лабораторные работы должны проводиться в специализированной аудитории, оснащенной учебной мебелью и персональными компьютерами с доступом в сеть Интернет (компьютерные классы, студии), мультимедийным оборудованием (проектор, экран, средства звуковоспроизведения), Число рабочих мест в аудитории должно быть таким, чтобы обеспечивалась индивидуальная работа студента персональном компьютере.

Для самостоятельной работы необходимы компьютерные классы, помещения, оснащенные компьютерами с доступом к сети Интернет и платформе Электронного университета ВГУ (LMS moodle).

Программное обеспечение:
- ОС Windows 10, ОС Linux;
- пакет стандартных офисных приложений для работы с документами, таблицами и т.п. (МойОфис, LibreOffice);
- интернет-браузер (Mozilla Firefox, Яндекс).

19. Фонд оценочных средств:

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Теоретико-числовые основы представления информации	ОПК-1, ОПК-2	ОПК-1.3, ОПК-2.1	Лабораторные работы 1.1-1.3
2	Алгебраические структуры и кольцо вычетов	ОПК-1, ОПК-2	ОПК-1.3, ОПК-2.1	Лабораторные работы 2.1-2.3
3	Решение сравнений, диофантовы уравнения и основы асимметричной криптографии	ОПК-1, ОПК-2	ОПК-1.3, ОПК-2.1	Лабораторные работы 3.1-3.3
4	Криптографические протоколы и эллиптические кривые	ОПК-1, ОПК-2	ОПК-1.3, ОПК-2.1	Лабораторные работы 4.1-4.3
Промежуточная аттестация, форма контроля – зачет				Тест

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью лабораторных работ.

Перечень лабораторных работ.

Лабораторная работа № 1.1.
Реализация расширенного алгоритма Евклида и нахождение линейного представления НОД.

Лабораторная работа № 1.2.
Проверка числа на простоту методом перебора делителей и факторизация с использованием канонического разложения

Лабораторная работа №1.3.
Вычисление сравнений и упрощение выражений по модулю (арифметика вычетов).

Лабораторная работа № 2.1
Исследование операций в кольце вычетов Z_m: построение таблиц сложения и умножения в Z_m.

Лабораторная работа № 2.2.
Нахождение обратимых элементов и вычисление функции Эйлера φ(m) для заданного модуля.

Лабораторная работа № 2.3.
Определение порядка элемента и поиск примитивных (образующих) элементов в поле Z_p.

Лабораторная работа № 3.1.
Решение линейных сравнений $a \cdot x \equiv b \pmod m$ и линейных диофантовых уравнений.

Лабораторная работа № 3.2.
Программная реализация процедуры гаммирования (потокового шифрования) с различными гаммами.

Лабораторная работа № 3.3.
Исследование односторонних функций: возведение в степень по модулю и факторизация как примеры функций с секретом

Лабораторная работа № 4.1.
Моделирование протокола Диффи–Хеллмана и реализация атаки «человек посередине»

Лабораторная работа № 4.2.
Реализация протокола аутентификации Шнорра (доказательство знания дискретного логарифма)

Лабораторная работа № 4.3.
Вычисление точек на эллиптической кривой в форме Вейерштрасса и реализация алгоритма ECDH

Технология проведения
Студент выбирает вариант задания, ориентируясь на номер зачетки (последняя цифра). Файлы исходных данных заранее должны быть размещены на сервере (компьютере студента). Студенту разрешается пользоваться информацией из открытых источников.

Критерии оценивания:

- оценка «зачтено» выставляется студенту, если задания выполнены в полном объеме;
- оценка «не зачтено» - работа не выполнена или выполнена не в полном объеме.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: тест.

Примеры тестовых заданий.

1. Что такое линейное представление наибольшего общего делителя (НОД) двух чисел?
а) Запись НОД в виде суммы самих чисел
б) Представление НОД в виде линейной комбинации этих чисел с целыми коэффициентами
в) Разложение НОД на простые множители
г) Запись НОД в виде десятичной дроби

Правильный ответ: ***б***

2. Какие числа называются взаимно простыми?
а) Оба числа простые
б) Их НОД равен единице
в) Их НОД больше единицы
г) Одно из чисел равно единице

Правильный ответ: ***б***

3. Какое утверждение соответствует основной теореме арифметики?
а) Простых чисел бесконечно много
б) Любое натуральное число единственным образом раскладывается в произведение простых чисел
в) Любое простое число можно представить в виде суммы двух квадратов
г) НОД двух чисел всегда прост

Правильный ответ: ***б***

4. Какое из следующих свойств сравнений по модулю является верным?
а) Если $a \equiv b \pmod m$, то $a + c \equiv b - c \pmod m$
б) Если $a \equiv b \pmod m$ и $c \equiv d \pmod m$, то $a + c \equiv b + d \pmod m$
в) Если $a \equiv b \pmod m$, то $a \cdot c \equiv b \pmod m$ для любого c
г) Сравнения нельзя умножать на число

Правильный ответ: ***б***

5. Какая алгебраическая структура называется полем?
а) Множество с одной операцией (сложением), образующее группу
б) Коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим
в) Множество с двумя операциями, где сложение не ассоциативно
г) Группа с дополнительной операцией умножения, не имеющая нейтрального элемента

Правильный ответ: ***б***

6. Чему равно значение функции Эйлера $\varphi(10)$?
а) 10
б) 5
в) 4
г) 6

Правильный ответ: **в**

7. Малая теорема Ферма утверждает, что для простого p и целого a, не кратного p:
а) a^p ≡ 0 (mod p)
б) a^(p-1) ≡ 1 (mod p)
в) a^p ≡ a (mod p) только при a=1
г) a^(p+1) ≡ a (mod p)

Правильный ответ: ***б***

8. Как найти решение линейного сравнения a·x ≡ b (mod m), если НОД(a, m) = 1?
а) Разделить b на a с остатком
б) Умножить обе части на число, обратное к a по модулю m
в) Прибавить к обеим частям m
г) Решение не существует

Правильный ответ: ***б***

9. Какое из уравнений является линейным диофантовым?
а) $x^2 + y^2 = 25$
б) 6x + 9y = 15
в) 2^x + 3^y = 5
г) sin(x) + cos(y) = 1

Правильный ответ: ***б***

10. В чём суть процедуры гаммирования (потокового шифрования)?
а) Замена каждого символа на символ, отстоящий на фиксированное число позиций
б) Наложение (например, по XOR) открытого текста на последовательность (гамму)
в) Разбиение текста на блоки фиксированной длины и их перестановка
г) Сжатие текста с потерями

Правильный ответ: ***б***

11. Что такое односторонняя функция?
а) Функция, которую легко вычислить, но трудно обратить (найти прообраз)
б) Функция, которая имеет обратную, но её трудно вычислить
в) Функция, определённая только для положительных чисел
г) Функция, значение которой всегда равно нулю

Правильный ответ: ***а***

12. Какую проблему использует протокол Диффи–Хеллмана для выработки общего секрета?
а) Задачу факторизации больших чисел
б) Задачу дискретного логарифмирования в конечном поле
в) Задачу нахождения хеш-коллизий
г) Задачу поиска кратчайшего пути в графе

Правильный ответ: ***б***

13. В чём заключается атака «человек посередине» (MITM) на протокол Диффи–Хеллмана?
а) Злоумышленник подслушивает канал, но не может изменить сообщения
б) Злоумышленник подменяет открытые ключи сторон, встраиваясь между ними, и договаривается о ключах с каждой стороной отдельно
в) Злоумышленник перехватывает и уничтожает все сообщения
г) Злоумышленник использует квантовый компьютер

Правильный ответ: ***б***

14. Какое уравнение задаёт эллиптическую кривую в форме Вейерштрасса (над полем действительных чисел)?
а) $y = x^2 + ax + b$
б) $x^2 + y^2 = 1$
в) $y^2 = x^3 + ax + b$
г) y = a^x

Правильный ответ: ***в***

15. Что вычисляет алгоритм Диффи–Хеллмана на эллиптической кривой (ECDH)?
а) Общий секретный ключ двух сторон на основе их закрытых ключей и открытых точек кривой
б) Цифровую подпись сообщения
в) Хеш-значение эллиптической кривой
г) Количество точек на кривой

Правильный ответ: ***а***

Итоговый тест засчитывается, если студент дал правильные ответы на более чем 70% вопросов.

Для оценивания результатов обучения на зачете используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения:

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Итоговый тест зачтен. Выполнены все лабораторные работы.	Повышенный уровень	Отлично
Итоговый тест зачтен. Выполнены 10 или 11 лабораторных работ.	Базовый уровень	Хорошо
Итоговый тест зачтен. Выполнены 8 или 9 лабораторных работ.	Пороговый уровень	Удовлетвори-тельно
Итоговый тест не зачтен и/или менее 8 лабораторных работ.	–	Неудовлетвори-тельно

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

1. Какое множество образует группу относительно сложения?
а) Натуральные числа
б) Целые числа
в) Чётные натуральные числа
г) Неотрицательные целые числа

2. Если a и b взаимно просты, то их НОД равен:
а) 0
б) a
в) b
г) 1

Правильный ответ: ***г***

3. Каноническое разложение числа 84 на простые множители имеет вид:
а) $2^2 \cdot 3 \cdot 7$
б) $2 \cdot 3 \cdot 14$

в) $2^2 \cdot 21$
г) $2^3 \cdot 3 \cdot 7$

Правильный ответ: **а**

4. Какое из сравнений является верным по модулю 5?
а) $7 \equiv 2 \pmod 5$
б) $8 \equiv 4 \pmod 5$
в) $6 \equiv 0 \pmod 5$
г) $10 \equiv 1 \pmod 5$

Правильный ответ: **а**

*Правильный ответ: **б***

5. Какой элемент обязательно присутствует в любом кольце?
а) Нулевой элемент
б) Единичный элемент
в) Обратный элемент для каждого ненулевого
г) Делитель нуля

*Правильный ответ: **а***

6. Сколько обратимых элементов содержится в кольце вычетов Z_8?
а) 8
б) 4
в) 6
г) 2

*Правильный ответ: **б***

7. Функция Эйлера φ(12) равна:
а) 12
б) 8
в) 6
г) 4

Правильный ответ: **г**

8. Теорема Эйлера утверждает, что если a и m взаимно просты, то:
а) a^φ(m) ≡ 1 (mod m)
б) a^m ≡ a (mod m)
в) a^(m-1) ≡ 1 (mod m)
г) a^φ(m) ≡ 0 (mod m)

*Правильный ответ: **а***

9. Как называется элемент поля Zp, порядок которого равен p-1?
а) Нейтральный
б) Обратимый
в) Примитивный (образующий)
г) Нулевой

*Правильный ответ: **в***

10. Сколько решений может иметь линейное сравнение $a \cdot x \equiv b \pmod m$, если НОД(a, m) = d > 1 и d делит b?
а) 0

б) 1
в) d
г) бесконечно много

Правильный ответ: ***в***

11. Какое из следующих уравнений является линейным диофантовым?
а) 5x + 10y = 15
б) $x^2 – 2y = 0$
в) xy = 6
г) 2^x + y = 5

Правильный ответ: ***а***

12. Какое из следующих утверждений о функции с секретом верно?
а) Это функция, которая легко обратима для всех
б) Это односторонняя функция, у которой есть дополнительная информация (секрет), позволяющая эффективно обратить её
в) Это функция, которая не имеет обратной
г) Это функция, определённая только на секретных данных

Правильный ответ: ***б***

13. Как злоумышленник реализует атаку «человек посредине» (MITM) на протокол Диффи–Хеллмана?
а) Перехватывает и расшифровывает трафик, используя подобранный ключ
б) Устанавливает отдельные сеансы с Алисой и Бобом, подменяя их открытые ключи своими
в) Блокирует все сообщения между Алисой и Бобом
г) Вычисляет закрытый ключ по открытому, используя квантовый алгоритм

Правильный ответ: ***б***

14. Протокол аутентификации Шнорра предназначен для:
а) Шифрования сообщений
б) Доказательства знания секретного числа (дискретного логарифма) без его раскрытия
в) Выработки общего ключа
г) Сжатия данных

Правильный ответ: ***б***

15. Теорема Хассе об эллиптической кривой над конечным полем даёт оценку для:
а) Количества точек на кривой
б) Дискриминанта кривой
в) Порядка базовой точки
г) Длины секретного ключа

Правильный ответ: **а**

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).