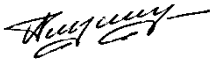
МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

УТВЕРЖДАЮ

Заведующий кафедрой
уравнений в частных производных
и теории вероятностей



А.В. Глушко
25.05.2023

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.04 Введение в теорию чисел

1. Код и наименование специальности: 10.05.04 Информационно-аналитические системы безопасности

2. Специализация: автоматизация информационно-аналитической деятельности

3. Квалификация выпускника: специалист по защите информации

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: кафедра уравнений в частных производных и теории вероятностей

6. Составители программы: Логинова Екатерина Александровна, кандидат физико-математических наук, доцент

7. Рекомендована: Научно-методическим советом математического факультета. Протокол № 0500-06 от 25.05.2023

8. Учебный год: 2024-2025 **Семестр:** 3

9. **Цели и задачи учебной дисциплины**

Целями освоения учебной дисциплины являются:
- формирование базовых знаний о теории чисел и её приложении к криптографии,
- приобретение практических навыков решения задач в целых числах.

Задачи учебной дисциплины:
- ознакомление с основными понятиями и фактами теории чисел;
- освоение методов решения базовых задач теории чисел;
- приобретение навыков применения основ теории чисел к задачам криптографии.

10. Место учебной дисциплины в структуре ООП: Блок 1, часть, формируемая участниками образовательных отношений.

Для успешного освоения дисциплины необходимы знания и умения, приобретенные в результате обучения по предшествующим и параллельно изучаемым дисциплинам: алгебра, геометрия, математический анализ, дискретная математика, информатика.

Дисциплина является предшествующей для дисциплин: формализованные модели и методы решения аналитических задач, методы и средства криптографической защиты информации.

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)	Индикатор(ы)	Планируемые результаты обучения
ПК-2	Способен организовывать работы по выполнению в информационно-аналитических системах требований защиты информации ограниченного доступа	ПК-2.1	Способен анализировать безопасность информации с помощью формальных моделей	Знать: Основные понятия теории чисел и криптографии Уметь: использовать алгоритмы работы с целыми числами при анализе безопасности информации Владеть: навыками решения задач с целыми числами

12. Объем дисциплины в зачетных единицах/час. — __2__/__72___.

Форма промежуточной аттестации зачет

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			8 семестр
Аудиторные занятия		50	50
в том числе:	лекции	34	34
	практические	16	16
	лабораторные	-	-
Самостоятельная работа		22	22
в том числе: курсовая работа (проект)		-	-
Форма промежуточной аттестации *(зачет)*		-	-
Итого:		72	72

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела

			дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Введение	Основные понятия криптографии и теории чисел	https://edu.vsu.ru/course/view.php?id=30027
1.2	Целые числа. Основная теорема арифметики	Основные понятия о множествах чисел. Свойства делимости целых чисел. Простые и составные числа. Основная теорема арифметики. Понятие о задачах распознавания простых чисел и факторизации целых чисел. Распределение простых чисел.	https://edu.vsu.ru/course/view.php?id=30027
1.3	Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. Соотношение Безу	Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. Расширенный алгоритм Евклида. Понятие и свойства взаимно простых чисел. Соотношение Безу.	https://edu.vsu.ru/course/view.php?id=30027
1.4	Диофантовы линейные уравнения	Диофантовы линейные уравнения: понятие и теоремы о них. Алгоритм решения диофантовых линейных уравнений с двумя неизвестными.	https://edu.vsu.ru/course/view.php?id=30027
1.5	Сравнение целых чисел	Определение сравнения по модулю. Арифметические свойства сравнений. Решение сравнений первой степени. Система сравнений первой степени.	https://edu.vsu.ru/course/view.php?id=30027
1.6	Классы вычетов	Отношение сравнимости как отношение эквивалентности. Множество классов вычетов.	https://edu.vsu.ru/course/view.php?id=30027
1.7	Теорема Ферма. Функции Эйлера. Теорема Эйлера	Малая теорема Ферма и её следствие. Функции Эйлера. Теорема Эйлера. Использование малой теоремы Ферма при тестировании простоты целых чисел. Числа Кармайкла.	https://edu.vsu.ru/course/view.php?id=30027
1.8	Первообразные корни и индексы	Показатель числа по модулю. Свойства показателей. Индексы и их свойства. Применение индексов при решении степенных сравнений.	https://edu.vsu.ru/course/view.php?id=30027
1.9	Задача дискретного логарифмирования. Применение к криптографии	Задача дискретного логарифмирования. Методы вычисления дискретного логарифма по простому модулю. Применение к криптографии. Алгоритм Диффи-Хеллмана создания общего секретного ключа. Схема Эль-Гамаля. Алгоритм создания открытого и секретного ключей. Алгоритм шифрования. Алгоритм расшифрования. Криптосистема Мэсси-Омуры. Алгоритм цифровой подписи DSA.	https://edu.vsu.ru/course/view.php?id=30027
2. Практические занятия			
2.1	Введение	Основные понятия криптографии и теории чисел	https://edu.vsu.ru/course/view.php?id=30027
2.2	Целые числа. Основная теорема арифметики	Основные понятия о множествах чисел. Свойства делимости целых чисел. Простые и составные числа. Основная теорема арифметики. Понятие о задачах распознавания простых чисел и факторизации целых чисел. Распределение простых чисел.	https://edu.vsu.ru/course/view.php?id=30027
2.3	Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. Соотношение Безу	Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. Расширенный алгоритм Евклида. Понятие и свойства взаимно простых чисел. Соотношение Безу.	https://edu.vsu.ru/course/view.php?id=30027
2.4	Диофантовы линейные уравнения	Диофантовы линейные уравнения: понятие и теоремы о них. Алгоритм решения диофантовых линейных уравнений с двумя неизвестными.	https://edu.vsu.ru/course/view.php?id=30027

2.5	Сравнение целых чисел	Определение сравнения по модулю. Арифметические свойства сравнений. Решение сравнений первой степени. Система сравнений первой степени.	https://edu.vsu.ru/course/view.php?id=30027
2.6	Классы вычетов	Отношение сравнимости как отношение эквивалентности. Множество классов вычетов.	https://edu.vsu.ru/course/view.php?id=30027
2.7	Теорема Ферма. Функции Эйлера. Теорема Эйлера	Малая теорема Ферма и её следствие. Функции Эйлера. Теорема Эйлера. Использование малой теоремы Ферма при тестировании простоты целых чисел. Числа Кармайкла.	https://edu.vsu.ru/course/view.php?id=30027
2.8	Первообразные корни и индексы	Показатель числа по модулю. Свойства показателей. Индексы и их свойства. Применение индексов при решении степенных сравнений.	https://edu.vsu.ru/course/view.php?id=30027
2.9	Задача дискретного логарифмирования. Применение к криптографии	Задача дискретного логарифмирования. Методы вычисления дискретного логарифма по простому модулю. Применение к криптографии. Алгоритм Диффи-Хеллмана создания общего секретного ключа. Схема Эль-Гамаля. Алгоритм создания открытого и секретного ключей. Алгоритм шифрования. Алгоритм расшифрования. Криптосистема Мэсси-Омуры. Алгоритм цифровой подписи DSA. Контрольная работа.	https://edu.vsu.ru/course/view.php?id=30027

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Введение	2	0	-	2	4
2	Целые числа. Основная теорема арифметики	4	2	-	2	8
3	Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. Соотношение Безу	4	2	-	2	8
4	Диофантовы линейные уравнения	4	2	-	2	8
5	Сравнение целых чисел	4	2	-	2	8
6	Классы вычетов	4	2	-	2	8
7	Теорема Ферма. Функции Эйлера. Теорема Эйлера	4	2	-	2	8
8	Первообразные корни и индексы	4	2	-	4	10
9	Задача дискретного логарифмирования. Применение к криптографии	4	2		4	10
	Итого:	34	16	-	22	72

14. Методические указания для обучающихся по освоению дисциплины:

В процессе преподавания дисциплины используются такие виды учебной работы, как лекции, практические занятия, а также различные виды самостоятельной работы обучающихся, на которую отводится 22 часа. На лекциях рассказывается теоретический материал, на практических занятиях решаются задачи и выполняются практические задания по теоретическому материалу, прочитанному на лекциях.

При изучении курса «Введение в теорию чисел» обучающимся следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий.

1. После каждой лекции обучающимся рекомендуется подробно разобрать прочитанный теоретический материал, выучить все определения и формулировки, разобрать примеры и задания, рассмотренные на лекции. Перед следующей лекций обязательно повторить материал предыдущей лекции.

2. Перед практическим занятием обязательно повторить лекционный материал. После практического занятия еще раз разобрать разобранные на этом занятии задания, после чего приступить к выполнению домашнего задания. Если при выполнении заданий возникнут вопросы, обязательно задать на следующем практическом занятии или в присутственный час преподавателю.

3. Выбрать время для работы с литературой по дисциплине в библиотеке.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и ресурсами сети Internet, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся заинтересованное отношение к конкретной проблеме.

Виды самостоятельной работы: конспектирование учебной и научной литературы; проработка учебного материала (по конспектам лекций, учебной и научной литературе); работа в электронной библиотечной системе; работа с информационными справочными системами, выполнение домашних заданий (практических и теоретических); выполнение контрольной работы; подготовка к практическим занятиям.

Самостоятельная учебная деятельность студентов по дисциплине «Введение в теорию чисел» предполагает изучение рекомендуемой преподавателем литературы по вопросам практических занятий, самостоятельное освоение понятийного аппарата, выполнение домашних заданий и подготовку к текущим аттестациям.

В конце семестра студенты сдают рефераты, содержащие дополнительные сведения по изученным в течение семестра темам: целые числа, основная теорема арифметики, наибольший общий делитель и наименьшее общее кратное, алгоритм Евклида, соотношение Безу, диофантовы линейные уравнения, сравнение целых чисел, классы вычетов, теорема Ферма, функции Эйлера, теорема Эйлера, первообразные корни и индексы, задача дискретного логарифмирования, применение к криптографии.

Выполняемые студентами самостоятельно задания подлежат последующей проверке преподавателем.

Наличие качественно выполненного реферата оценивается оценкой «зачтено», отсутствие реферата или наличие реферата, содержащего большое количество ошибочных сведений, сведения, не относящиеся к изучаемому курсу, сведения, полученные обучающимися на занятиях, оценивается оценкой «не зачтено».

Результаты текущих аттестаций учитываются преподавателем при проведении промежуточной аттестации.

Вопросы лекционных и практических занятий обсуждаются на занятиях в виде устного опроса – индивидуального и фронтального. При подготовке к лекционным и практическим занятиям, обучающимся важно помнить, что их задача, отвечая на основные вопросы плана занятия и дополнительные вопросы преподавателя, показать свои знания и кругозор, умение логически построить ответ, владение математическим аппаратом и иные коммуникативные навыки, умение отстаивать свою профессиональную позицию. В ходе устного опроса выявляются детали, которые по каким-то причинам оказались недостаточно осмысленными студентами в ходе учебных занятий. Тем самым опрос выполняет важнейшие обучающую, развивающую и корректирующую функции, позволяет студентам учесть недоработки и избежать их при подготовке к промежуточным аттестациям.

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

а) основная литература:

№ п/п	Источник
1	Бухштаб, А. А. Теория чисел / А. А. Бухштаб. — 7-е изд., стер. — Санкт-Петербург : Лань, 2023. — 384 с. — ISBN 978-5-507-47195-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/352355. — Режим доступа: для авториз. пользователей.
2	Ермолаева, Н. Н. Практические занятия по алгебре. Элементы теории множеств, теории чисел, комбинаторики. Алгебраические структуры : учебное пособие / Н. Н. Ермолаева, В. А. Козынченко, Г. И. Курбатова. — Санкт-Петербург : Лань, 2022. — 112 с. — ISBN 978-5-8114-1657-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/211595. — Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
1	Тропин, М. П. Теория чисел / М. П. Тропин. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 240 с. — ISBN 978-5-507-45436-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/269906. — Режим доступа: для авториз. пользователей.
2	Виноградов, И. М. Основы теории чисел / И. М. Виноградов. — 15-е изд., стер. — Санкт-Петербург : Лань, 2023. — 176 с. — ISBN 978-5-507-46129-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/298499. — Режим доступа: для авториз. пользователей.
3	Багина, Теория чисел, теория алгоритмов : учебное пособие / Багина. — Кемерово : КемГУ, 2022. — 101 с. — ISBN 978-5-8353-2846-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/233348. — Режим доступа: для авториз. пользователей.
4	Мартынов, Л. М. Алгебра и теория чисел для криптографии / Л. М. Мартынов. — 3-е изд., стер. — Санкт-Петербург : Лань, 2024. — 456 с. — ISBN 978-5-507-48774-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/362942. — Режим доступа: для авториз. пользователей.
5	Сборник задач по теории чисел : учебное пособие / составители А. Н. Васильева, В. Г. Ефремов. — Чебоксары : ЧГПУ им. И. Я. Яковлева, 2022. — 88 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/354089. — Режим доступа: для авториз. пользователей.
6	Черемисина, М. И. Избранные вопросы алгебры и теории чисел. Многочлены : учебное пособие / М. И. Черемисина. — Оренбург : ОГПУ, 2021. — 65 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/179894. — Режим доступа: для авториз. пользователей.

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

№ п/п	Ресурс
1	*http://www.lib.vsu.ru - электронный каталог ЗНБ ВГУ*
2	*http://www.kuchp.ru – электронный сайт кафедры уравнений в частных производных и теории вероятностей, на котором размещены методические издания*
3	https://edu.vsu.ru/ – *образовательный портал «Электронный университет ВГУ»/LMC Moodle*

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Тропин, М. П. Теория чисел / М. П. Тропин. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 240 с. — ISBN 978-5-507-45436-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/269906. — Режим доступа: для авториз. пользователей.
2	Виноградов, И. М. Основы теории чисел / И. М. Виноградов. — 15-е изд., стер. — Санкт-Петербург : Лань, 2023. — 176 с. — ISBN 978-5-507-46129-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/298499. — Режим доступа: для авториз. пользователей.
3	Багина, Теория чисел, теория алгоритмов : учебное пособие / Багина. — Кемерово : КемГУ, 2022. — 101 с. — ISBN 978-5-8353-2846-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/233348. — Режим доступа: для авториз. пользователей.

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

Дисциплина может реализовываться с применением дистанционных образовательных технологий, например, на платформе «Электронный университет ВГУ» (https://edu.vsu.ru/course/view.php?id=30027).

Перечень необходимого программного обеспечения: Microsoft Windows 10, LibreOffice 6 (*Writer (текстовый процессор), Calc (электронные таблицы), Impress (презентации), Draw (векторная графика), Base (база данных), Math (редактор формул)*), MATLAB, Gimp, WinDjView, Foxit Reader, 7-Zip, Mozilla Firefox.

18. Материально-техническое обеспечение дисциплины:

Специализированная мебель.

Для проведения лекционных и практических занятий используются аудитории, соответствующие действующим санитарно-техническим нормам и противопожарным правилам.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети Internet и обеспечением доступа в электронную информационно-образовательную среду ВГУ.

При реализации дисциплины с использованием дистанционного образования возможны дополнения материально-технического обеспечения дисциплины.

---

19. Оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Введение	ПК-2	ПК-2.1	Контрольная работа
2.	Целые числа. Основная теорема арифметики	ПК-2	ПК-2.1	Контрольная работа
3.	Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида. Соотношение Безу	ПК-2	ПК-2.1	Контрольная работа
4.	Диофантовы линейные уравнения	ПК-2	ПК-2.1	Контрольная работа
5.	Сравнение целых чисел	ПК-2	ПК-2.1	Контрольная работа
6.	Классы вычетов	ПК-2	ПК-2.1	Контрольная работа
7.	Теорема Ферма. Функции Эйлера. Теорема Эйлера	ПК-2	ПК-2.1	Контрольная работа
8.	Первообразные корни и индексы	ПК-2	ПК-2.1	Контрольная работа
9.	Задача дискретного логарифмирования. Применение к криптографии	ПК-2	ПК-2.1	Контрольная работа
Промежуточная аттестация форма контроля – _зачет_____				Перечень вопросов к зачету

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: контрольная работа

Пример варианта контрольной работы:

Вариант 1

1. Используя алгоритм Евклида, найти НОД чисел 5160 и 16920.
2. Решить диофантово уравнение $2x+3y=6$.
3. Решить сравнение $1287x \equiv 447 (\mathrm{mod}\, 516)$.

Описание технологии проведения.

В ходе контрольной работы обучающемуся выдается КИМ с тремя практическими заданиями. Ограничение по времени – 40 минут. Во время контрольной работы не разрешено пользоваться никакими справочными материалами.

Текущая аттестация по дисциплине с применением дистанционных образовательных технологий может проводиться на образовательном портале «Электронный университет ВГУ» (LMS Moodle, https://edu.vsu.ru/).

Требования к выполнению заданий (или шкалы и критерии оценивания). При текущем контроле уровень освоения учебной дисциплины и степень сформированности компетенции определяются оценками «зачтено» и «не зачтено», которые формируются следующим образом:

Контрольная работа 1

Оценки	Критерии
Зачтено	Обучающийся правильно выполнил не менее 50% предложенных заданий.
Не зачтено	Обучающийся правильно выполнил менее 50% предложенных заданий.

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: собеседование по билетам к зачету.

Перечень вопросов к зачету:

Основные понятия криптографии.

Основные понятия теории чисел.

Основные понятия о множествах чисел.

Свойства делимости целых чисел.

Простые и составные числа.

Основная теорема арифметики.

Понятие о задачах распознавания простых чисел и факторизации целых чисел.

Распределение простых чисел.

Наибольший общий делитель и наименьшее общее кратное.

Алгоритм Евклида.

Расширенный алгоритм Евклида.

Понятие и свойства взаимно простых чисел.

Соотношение Безу.

Диофантовы линейные уравнения: понятие и теоремы о них.

Алгоритм решения диофантовых линейных уравнений с двумя неизвестными.

Определение сравнения по модулю. Арифметические свойства сравнений.

Решение сравнений первой степени.

Система сравнений первой степени.

Отношение сравнимости как отношение эквивалентности.

Множество классов вычетов.

Малая теорема Ферма и её следствие.

Функции Эйлера. Теорема Эйлера.

Использование малой теоремы Ферма при тестировании простоты целых чисел.
Числа Кармайкла.
Показатель числа по модулю. Свойства показателей.
Индексы и их свойства.
Применение индексов при решении степенных сравнений.
Задача дискретного логарифмирования.
Методы вычисления дискретного логарифма по простому модулю.
Алгоритм Диффи-Хеллмана создания общего секретного ключа.
Схема Эль-Гамаля.
Алгоритм создания открытого и секретного ключей.
Алгоритм шифрования. Алгоритм расшифрования.
Криптосистема Мэсси-Омуры.
Алгоритм цифровой подписи DSA.

Примерный перечень практических заданий к зачёту:

1. Найти соотношение Безу для $(72;26)$.
2. Решить в целых числах уравнение $13x+9y=150$.
3. Решить сравнение $15x \equiv 39 (\mathrm{mod}\, 84)$.
4. Решить систему сравнений $\begin{cases} 7x \equiv 11 (\mathrm{mod}\, 18), \\ 8x \equiv 1 (\mathrm{mod}\, 27), \\ 9x \equiv 13 (\mathrm{mod}\, 28). \end{cases}$
5. Построить таблицы сложения и умножения в $\mathbb{Z}_6$.
6. Найти остаток от деления 171^{2147} на 52.
7. Найти, какому показателю принадлежит число 7 по модулю 16.
8. Составить таблицу индексов по модулю 11, используя наименьший натуральный первообразный корень по модулю 11.

Пример контрольно-измерительного материала:

Контрольно-измерительный материал № 1

1. Основные понятия теории чисел.
2. Решить систему сравнений $\begin{cases} 13x \equiv 7 (\mathrm{mod}\, 24), \\ 8x \equiv 5 (\mathrm{mod}\, 75). \end{cases}$

Описание технологии проведения.

Промежуточная аттестация по дисциплине «Введение в теорию чисел» проводится в форме зачета.

По решению кафедры оценки за зачет могут быть выставлены по результатам текущей успеваемости обучающегося в течение семестра, но не ранее, чем на заключительном занятии. Для этого обучающемуся необходимо написать контрольную работу на оценку «зачтено», посетить не менее 80% занятий, активно работать на занятиях. При несогласии обучающегося, ему дается возможность пройти промежуточную аттестацию на общих основаниях.

Промежуточная аттестация, как правило, осуществляется в конце семестра.

Промежуточная аттестация по дисциплине с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) может проводиться на образовательном портале «Электронный университет ВГУ» (LMS Moodle, https://edu.vsu.ru/).

Обучающиеся, проходящие промежуточную аттестацию с применением ДОТ, должны располагать техническими средствами и программным обеспечением, позволяющим обеспечить процедуры аттестации. Обучающийся самостоятельно обеспечивает выполнение необходимых

технических требований для проведения промежуточной аттестации с применением дистанционных образовательных технологий.

Идентификация личности обучающегося при прохождении промежуточной аттестации обеспечивается посредством использования каждым обучающимся индивидуального логина и пароля при входе в личный кабинет, размещенный в ЭИОС образовательной организации.

В ходе проведения аттестации обучающемуся необходимо ответить на вопросы КИМ, состоящего из одного теоретического и одного практического вопросов, и, возможно, дополнительные вопросы экзаменатора.

Результаты текущей аттестации обучающегося учитываются при проведении промежуточной аттестации следующим образом: обучающиеся, получившие за контрольную работу оценку «не зачтено» или не явившиеся на контрольную работу, получают дополнительное практическое задание или теоретический вопрос.

Требования к выполнению заданий, шкалы и критерии оценивания

Критерии оценивания компетенций	Шкала оценок
Обучающийся не владеет основами учебно-программного материала, обнаружил пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий, выполнил менее 50% заданий КИМ	«Не зачтено»
Обучающийся владеет знаниями основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, справился с выполнением заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой. Обязательным условием выставленной оценки является правильный ответ не менее, чем на 50% заданий КИМ.	"Зачтено"

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

ПК-2 Способен организовывать работы по выполнению в информационно-аналитических системах требований защиты информации ограниченного доступа

ПК-2.1 Способен анализировать безопасность информации с помощью формальных моделей

Знать: Основные понятия теории чисел и криптографии

Уметь: использовать алгоритмы работы с целыми числами при анализе безопасности информации

Владеть: навыками решения задач с целыми числами

Перечень заданий для оценки сформированности компетенций

1) закрытые задания (тестовые, средний уровень сложности):

1. Наибольший общий делитель чисел 447 и 745 равен:
а) 149,
б) 745,
в) 333015.

2. Наименьшее общее кратное чисел 447 и 745 равно:
а) 2235,
б) 149,
в) 333015.

3. Имеет ли уравнение $7x-5y=2$ решение в целых числах?
а) имеет;
б) не имеет;
в) нельзя дать однозначный ответ.

4. Имеет ли уравнение $3x+5y=10$ решение в целых числах?
а) имеет;
б) не имеет;
в) нельзя дать однозначный ответ.

5. Наименьшим числом Кармайкла является:
а) 561;
б) 222;
в) 1.

2) открытые задания (тестовые, средний уровень сложности):

1. Вставьте пропущенное прилагательное, отвечающее на вопрос «каких».

Множество $\mathbb{N}=\{1,2,3,...,n,...\}$ называют множеством _____ чисел.

2. Вставьте пропущенное прилагательное, отвечающее на вопрос «каким».

Натуральное число называется _____, если оно делится только на 1 и на само себя.

3. Вставьте пропущенное существительное в творительном падеже.

Если натуральное число k делится на каждое из целых чисел $a_1,...,a_n$ (каждое из которых отлично от нуля), то k называется их общим _____.

4. Вставьте пропущенное прилагательное, отвечающее на вопрос «каким».

Целые числа a и b называются взаимно _____, если НОД a и b равен 1.

5. Вставьте пропущенное существительное в родительном падеже.

Множество всех чисел, сравнимых с a по модулю m, называется классом _____ по модулю m.

Критерии и шкалы оценивания заданий ФОС:

1) Задания закрытого типа (выбор одного варианта ответа, верно/неверно):

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ.

2) Задания открытого типа (короткий текст):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

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