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

УТВЕРЖДАЮ
Заведующий кафедрой
алгебры и математических
методов гидродинамики

(Звягин В.Г.)
подпись, расшифровка подписи
17.04.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.15 Теоретико-числовые методы в криптографии

1. Шифр и наименование специальности:
01.05.01 Фундаментальные математика и механика

2. Профиль специализации: Современные методы теории функций в математике и механике

3. Квалификация выпускника: Математик. Механик. Преподаватель

4. Форма образования: очная

5. Кафедра, отвечающая за реализацию дисциплины: кафедра алгебры и математических методов гидродинамики

6. Составители программы: доцент, д.ф.-м.н. Звягин Андрей Викторович

7. **Рекомендована:** НМС математического факультета протокол № 0500-03 от 28.03.2024 г.

8. Учебный год: 2025-2026 **Семестр(-ы):** 4

9. Цели и задачи учебной дисциплины:

Цели учебной дисциплины:

- освоение основных понятий, фактов теории чисел
- установление связи теории чисел с криптографией
- овладение основными методами решения задач

Задачи учебной дисциплины:

- ознакомление с основными теоретико-числовыми понятиями и фактами
- формирование у студентов навыков, необходимых для разработки математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность
- формирование у студентов навыков, необходимых для проведения аттестации технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности или профилям защиты
- овладение основными методами решения задач, выработка навыков и умений по применению полученных знаний при решении задач теории чисел и других математических дисциплин.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к части, формируемой участниками образовательных отношений Блока 1.

Для его успешного освоения необходимы знания и умения, приобретенные в результате обучения по предшествующим дисциплинам: математический анализ, алгебра, линейная алгебра.

Студент должен свободно владеть математическим анализом, элементами линейной алгебры.

11. Компетенции обучающегося, формируемые в результате освоения дисциплины:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-3	Способен к построению моделей и оптимальному решению теоретических и прикладных задач математики и механики на основе методов теории функций и геометрии	ПК-3.1	Знает современные методы разработки и реализации математических моделей	Знать: современные методы разработки и реализации математических моделей Уметь: разрабатывать и реализовывать математические модели предметной области. Владеть: теоретическими подходами и современными методами разработки и реализации математических моделей;

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

Форма промежуточной аттестации: зачёт

13. Виды учебной работы:

Вид учебной работы	Трудоемкость (часы)	
	Всего	По семестрам
		4

Аудиторные занятия	50	50
в том числе: лекции	16	16
практические	34	34
лабораторные	-	-
Самостоятельная работа	58	58
Итого:	108	108

13.1 Содержание разделов дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК *
1. Лекции			
1	Элементы теории чисел	Делимость целых чисел. Алгоритм Евклида. Простые числа, основная теорема арифметики. Функция Эйлера и её свойства. Сравнения. Сравнения с одним неизвестным. Цепные дроби. p-адические числа. Алгебраические числа	
2	Разложение многочленов на множители над конечными полями	Алгоритм Берлекемпа. Сведение задачи разложения на неприводимые множители к нахождению корней (алгоритм Цессенхауза). Нахождение корней многочлена в полях малой характеристики. Нахождение корней многочлена в полях большой характеристики.	
3	Криптографические применения	Алгоритм Диффи-Хеллмана обмена ключами. Алгоритм RSA.	
2. Практические занятия.			
1	Элементы теории чисел	Делимость целых чисел. Алгоритм Евклида. Простые числа, основная теорема арифметики. Функция Эйлера и её свойства. Сравнения. Сравнения с одним неизвестным. Цепные дроби. p-адические числа. Алгебраические числа	
2	Разложение многочленов на множители над конечными полями	Алгоритм Берлекемпа. Сведение задачи разложения на неприводимые множители к нахождению корней (алгоритм Цессенхауза). Нахождение корней многочлена в полях малой характеристики. Нахождение корней многочлена в полях большой характеристики.	
3	Криптографические применения	Алгоритм Диффи-Хеллмана обмена ключами. Алгоритм RSA.	

13.2 Разделы дисциплины и виды занятий:

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабора-торные	Самостоятель-ная работа	Всего
1	Элементы теории чисел	4	11		19	34
2	Разложение многочленов на множители над конечными полями	6	12		19	37
3	Криптографические применения	6	11		20	37
	Итого:	16	34		58	108

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 58 часов. На лекциях рассказывается теоретический

материал, на практических занятиях решаются примеры по теоретическому материалу, прочитанному на лекциях. Самостоятельная работа обучающихся направлена на самостоятельное освоение всех тем и вопросов учебной дисциплины, предусмотренных программой. Самостоятельная работа является обязательным видом деятельности для каждого обучающегося, ее объем по учебному курсу определяется учебным планом. При самостоятельной работе обучающийся взаимодействует с рекомендованными материалами при минимальном участии преподавателя.

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. Вопросы, которые вызывают у обучающихся затруднения при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.

Для успешного и плодотворного обеспечения итогов самостоятельной работы разработаны учебно-методические указания к самостоятельной работе студентов над различными разделами дисциплины.

Все задания, выполняемые студентами самостоятельно, подлежат последующей проверке преподавателем.

При изучении курса «Теоретико-числовые методы в криптографии» 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 студентам рекомендуется подробно разобрать прочитанный теоретический материал, выучить все определения и формулировки теорем, разобрать примеры, решенные на лекции. Перед следующей лекций обязательно повторить материал предыдущей лекции.
2. Перед практическим занятием обязательно повторить лекционный материал. После практического занятия еще раз разобрать решенные на этом занятии примеры, после чего приступить к выполнению домашнего задания. Если при решении примеров, заданных на дом, возникнут вопросы, обязательно задать на следующем практическом занятии или в присутственный час преподавателю.
3. При подготовке к практическим занятиям повторить основные понятия по темам, изучить примеры. Решая задачи, предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить практические задачи.
4. Кроме обычного курса в системе «Электронный университет», все необходимые для усвоения курса материалы размещены также на сайте факультета https://math.vsu.ru/wp/?page_id=937.

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

а) основная литература:

№ п/п	Источник
1	Мартынов Л. М. Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. — Санкт-Петербург : Лань, 2020. — 456 с. — ISBN 978-5-8114-4424-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/140740
2	Герман О. Н. Теоретико-числовые методы в криптографии / О. Н. Герман, Ю. В. Нестеренко. – Москва : Академия, 2012. – 270 с. – ISBN 978-5-7695-6786-5

б) дополнительная литература:

№ п/п	Источник
3	Гречников Е. А. Вычислительно сложные задачи теории чисел : Учеб.пособие / Е. А. Гречников. МГУ им.М.В.Ломоносова. - М.: Изд-во МГУ, 2012.-310 с
4	Мартынов Л. М. Алгебра для криптографии : учебное пособие / Л. М. Мартынов. — Омск : ОмГУПС, [б. г.]. — Часть 1 — 2015. — 154 с. — ISBN 978-5-949-41131-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/129189
5	Мартынов Л. М. Алгебра для криптографии : учебное пособие / Л. М. Мартынов. — Омск : ОмГУПС, [б. г.]. — Часть 2 — 2015. — 150 с. — ISBN 978-5-949-41132-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/129188
6	Мартынов, Л. М. Алгебра для криптографии : учебное пособие / Л. М. Мартынов. — Омск : ОмГУПС, [б. г.]. — Часть 3 — 2018. — 83 с. — ISBN 978-5-949-41189-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/129190
7	Сингх С. Великая теорема Ферма : История загадки, которая занимала лучшие умы мира на протяжении 358 лет / Саймон Сингх ; Пер. с англ. Ю. А. Данилова.— М. : МЦНМО, 2000.— 288 с.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
8	*http://www.lib.vsu.ru-* Электронный каталог ЗНБ ВГУ
9	*https://math.vsu.ru/wp/?page_id=937 –* Сайт факультета

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Мартынов Л. М. Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. — Санкт-Петербург : Лань, 2020. — 456 с. — ISBN 978-5-8114-4424-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/140740
2	Гречников Е. А. Вычислительно сложные задачи теории чисел : Учеб.пособие / Е. А. Гречников. МГУ им.М.В.Ломоносова. - М.: Изд-во МГУ, 2012.-310 с
3	Мартынов Л. М. Алгебра для криптографии : учебное пособие / Л. М. Мартынов. — Омск : ОмГУПС, [б. г.]. — Часть 1 — 2015. — 154 с. — ISBN 978-5-949-41131-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/129189
4	Мартынов Л. М. Алгебра для криптографии : учебное пособие / Л. М. Мартынов. — Омск : ОмГУПС, [б. г.]. — Часть 2 — 2015. — 150 с. — ISBN 978-5-949-41132-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/129188
5	Мартынов, Л. М. Алгебра для криптографии : учебное пособие / Л. М. Мартынов. — Омск : ОмГУПС, [б. г.]. — Часть 3 — 2018. — 83 с. — ISBN 978-5-949-41189-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/129190
6	Сингх С. Великая теорема Ферма : История загадки, которая занимала лучшие умы мира на протяжении 358 лет / Саймон Сингх ; Пер. с англ. Ю. А. Данилова .— М. : МЦНМО, 2000 .— 288 с.
7	Герман О. Н. Теоретико-числовые методы в криптографии / О. Н. Герман, Ю. В. Нестеренко. – Москва : Академия, 2012. – 270 с. – ISBN 978-5-7695-6786-5
8	Положение об организации самостоятельной работы обучающихся в Воронежском государственном университете

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы:

Дисциплина может реализовываться с применением дистанционных образовательных технологий, например, на платформе «Электронный университет ВГУ».

Перечень необходимого программного обеспечения: операционная система Windows или Linux, Microsoft, Windows Office, LibreOffice 5*, Calc, Math,* браузер Mozilla Firefox, Opera или Internet.

18. Материально-техническое обеспечение дисциплины:

Специализированная мебель.

Для самостоятельной работы используется класс с компьютерной техникой, оснащенный необходимым программным обеспечением, электронными учебными пособиями и законодательно - правовой и нормативной поисковой системой, имеющий выход в глобальную сеть.

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

19. Фонд оценочных средств:

Оценочные средства для проведения текущей и промежуточной аттестаций

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	Элементы теории чисел	ПК-3	ПК-3.1	контрольная работа
2	Разложение многочленов на множители над конечными полями	ПК-3	ПК-3.1	контрольная работа
3	Криптографические применения	ПК-3	ПК-3.1	контрольная работа
Промежуточная аттестация Форма контроля - зачёт				Зачёт выставляется при успешной сдаче контрольной работы

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:

<u>Примерный перечень задач для контрольной работы:</u>

1. Задания контрольной работы №1:
   - Найти НОД и его линейное разложение: $au+bv=(a,b)$
   - Определить функцию Эйлера: $\varphi(b)$
   - Сформировать полную и приведенную системы вычетов: Z_m; $U(m)$
   - Найти обратный элемент: U_b в Z_p
   - Решить линейное сравнение: $ax \equiv b (\mathrm{mod} p)$

Параметры заданий (a, b, m, p) выдаются каждому студенту индивидуально.

2. Задания контрольной работы №2:
   - Определить вычет: $a^{52782} (\mathrm{mod}\ m)$
   - Решить степенное сравнение: $x^a \equiv q (\mathrm{mod}\ p)$
   - Найти символ Лежандра: $\left(\frac{m}{q}\right)$

Параметры заданий (a, m, p, q) выдаются каждому студенту индивидуально.

3. Задания контрольной работы №3:
   - Найти НОД многочленов: (f(X), g(X)):
     - $f(X) = a_0 + a_1 X + a_2 X^2 + a_3 X^3 + a_4 X^4 + a_5 X^5$
     - $g(X) = b_0 + b_1 X + b_2 X^2 + b_3 X^3 + b_4 X^4$
     - $a_i, b_j \in F_2, \quad i = \overline{0,5}, \quad j = \overline{0,4}$
   - Найти все точки эллиптической кривой $E_p(a,b)$: $Y^2 = X^3 + aX + b$
   - Найти сумму двух точек эллиптической кривой $P(x_1, y_1)$, $Q(x_2, y_2)$

Параметры заданий (a, b, p, коэффициенты многочленов) выдаются каждому студенту индивидуально.

Текущий контроль представляет собой проверку усвоения учебного материала практического характера, регулярно осуществляемую на занятиях.

Цель текущего контроля:
Определение уровня сформированности профессиональных компетенций, знаний и навыков деятельности в области знаний, излагаемых в курсе.
Задачи текущего контроля: провести оценивание
1. уровня освоения теоретических и практических понятий, научных основ профессиональной деятельности;
2. степени готовности обучающегося применять теоретические и практические знания и профессионально значимую информацию, сформированности когнитивных умений.
3. приобретенных умений, профессионально значимых для профессиональной деятельности.
Текущий контроль предназначен для проверки хода и качества формирования компетенций, стимулирования учебной работы обучаемых и совершенствования методики освоения новых знаний. Он обеспечивается проведением контрольных работ.
В ходе контрольной работы обучающемуся выдается КИМ с практическим перечнем заданий и предлагается решить данные задания. В ходе выполнения заданий можно пользоваться любой литературой, ограничение по времени 90 минут.
Если текущая аттестация проводится в дистанционном формате, то обучающийся должен иметь компьютер и доступ в систему «Электронный университет». Если у обучающегося отсутствует необходимое оборудование или доступ в систему, то он обязан сообщить преподавателю об этом за 2 рабочих дня. На контрольную работу в дистанционном режиме отводится ограничение по времени 120 минут.

Критерии оценки компетенций (результатов обучения) при текущей аттестации (контрольной работе):

– оценка «отлично» выставляется, если не менее чем на четыре пятых всех заданий контрольной работы даны правильные, полные и глубокие ответы, раскрывающие уверенное знание студентом понятий, закономерностей, принципов, фактов, содержащихся в конкретных материалах по теме; высокую сформированность у него аналитико-синтетических операций и их успешное применение при изложении изучаемого материала;

– оценка «хорошо» выставляется, если не менее чем на две трети всех заданий контрольной работы даны правильные, полные и глубокие ответы, раскрывающие достаточное знание студентом понятий, закономерностей, принципов, фактов, содержащихся в конкретных материалах по теме; хорошую сформированность у него аналитико-синтетических операций и в целом их адекватное применение при изложении изучаемого материала;

– оценка «удовлетворительно» выставляется, если правильно выполнено не менее половины всех заданий контрольной работы, при этом допускается недостаточная полнота и глубина ответов, в которых студентом продемонстрирован необходимый минимум знаний понятий, закономерностей, принципов, фактов, содержащихся в конкретных материалах по теме; слабая сформированность у него аналитико-синтетических операций, затруднения в их применении при изложении изучаемого материала;

– оценка «неудовлетворительно» выставляется, если с минимально необходимым уровнем решения выполнено менее половины всех заданий контрольной работы, ответы демонстрируют незнание или поверхностное знание студентов понятий, закономерностей, принципов, фактов, содержащихся в конкретных материалах по теме; несформированность у него аналитико-синтетических операций.

Количественная шкала оценок:

– оценка «отлично» выставляется, если безошибочно выполнено не менее 80% заданий контрольной работы, качество решения которых соответствует критерию оценки «отлично»;

– оценка «хорошо» выставляется, если безошибочно выполнено не менее 66% и не более 79% заданий контрольной работы, качество решения которых соответствует критериям оценки «хорошо»;

– оценка «удовлетворительно» выставляется, если безошибочно выполнено не менее 50% и не более 65% заданий контрольной работы, качество решения которых соответствует критериям оценки «удовлетворительно»;

– оценка «неудовлетворительно» выставляется, если безошибочно выполнено менее 50% заданий контрольной работы, качество решения которых соответствует критериям оценки «неудовлетворительно».

20.2. Промежуточная аттестация

Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины. Промежуточная аттестация по дисциплине «Теоретико-числовые методы в криптографии» проводится в форме зачета.

Промежуточная аттестация, как правило, осуществляется в конце семестра. Результаты текущей аттестации обучающегося по решению кафедры могут быть учтены при проведении промежуточной аттестации. При несогласии студента, ему дается возможность пройти промежуточную аттестацию (без учета его текущих аттестаций) на общих основаниях.

При проведении зачёта учитываются результаты контрольной работы и учитывается выставляемая преподавателем оценка за работу в ходе практических занятий.

Если у обучающегося есть положительная оценка по контрольной работе и положительная оценка работы в ходе обучения по практике, то зачёт выставляется. Если обучающийся не имеет положительной оценки контрольной работе или практике, он может ответить на соответствующие вопросы в ходе зачёта.

Примерный перечень вопросов:

1. Дать определение группы, абелевой группы, привести примеры.
2. Что такое порядок элемента в группе? (рассмотреть группы по сложению и умножению)
3. Какая группа называется циклической?
4. Как произвести разложение группы на подгруппы? (рассмотреть группы по сложению и умножению)
5. Как формируются смежные классы для подгруппы? (рассмотреть группы по сложению и умножению)
6. Дать определение кольца, привести примеры
7. Дать определение поля, поля Галуа. Привести примеры
8. Что такое область целостности?
9. Как задать многочлен над полем?
10. Что такое неприводимый многочлен над полем?

Для оценивания результатов обучения на зачете используются следующие **показатели:**

1) знание теоретических основ;
2) умение решать задачи лабораторной работы;
3) умение работать с информационными ресурсами;
4) успешное прохождение текущей аттестации.

Для оценивания результатов обучения на зачете используется **шкала:** «зачтено», «не зачтено».

Соотношение показателей, критериев и шкалы оценивания результатов обучения:

Критерии оценивания компетенций	**Шкала оценок**
«Зачтено» выставляется студенту, который прочно усвоил	«Зачтено»

предусмотренный программный материал; показал глубокие систематизированные знания, владеет приемами рассуждения и сопоставляет материал из разных источников: теорию связывает с практикой, другими темами данного курса, других изучаемых предметов; без ошибок выполнил практическое задание. Обязательным условием выставленной оценки является правильное решение контрольных работ, систематическая активная работа на лекционных и практических занятиях.	
«Не зачтено» Выставляется студенту, который не справился с заданиями билета, в ответах на другие вопросы допустил существенные ошибки. Не может ответить на дополнительные вопросы, предложенные преподавателем.	«Не зачтено»

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

1. Количество неприводимых делителей f(x) равно

а) n-rank(B-I)

б) n+rank(B-I)

Ответ: а)

2. Если rank(B-I)=n-1, то многочлен $f(x) \in F\left[x\right]$…

Ответ: неприводим

3. Справедливо ли равенство $x^q - x = \beta^{-1} \prod\limits_{c \in F_p} \left(S\left(\beta x\right) - c\right)$ для каждого $\beta \in F_q, \beta \neq 0$.

Ответ: да

4. Пусть $h(x) \in F\left[x\right]$ и выполнено сравнение $h(x)^q - h(x) \equiv 0 (\mathrm{mod}\, f(x))$. Тогда

а) $f(x) = \prod\limits_{c \in F} \left(f(x), h\left(x\right) - c\right)$

б) $f(x) = \prod\limits_{c \in F} \left(0, h\left(x\right) - c\right)$

Ответ: а)

5. Многочлен h(x) удовлетворяет сравнению $h(x)^q - h(x) \equiv 0 (\mathrm{mod}\, f(x))$, если и только если существуют элементы $c_j \in F, j = 1,...,k$ для которых выполнены сравнения

а) $h(x) \equiv c_j (\mathrm{mod}\, f_j(x))$

б) $h(x)^q - h(x) \equiv 0 (\mathrm{mod}\, f(x))$

Ответ: а)

6. Существуют в точности … многочленов $h(x) \in F\left[x\right]$, удовлетворяющих условиям: $h(x)^q - h(x) \equiv 0 (\mathrm{mod}\, f(x))$, $\deg h(x) < \deg f(x)$.

а) q^k

б) 0

в) 1

Ответ: а)

7. Многочлен $h(x) = a_0 + ...a_{n-1}x^{n-1} \in F\left[x\right]$ удовлетворяет условиям $h(x)^q - h(x) \equiv 0(\mathrm{mod}\ f(x))$, $\deg h(x) < \deg f(x)$ тогда и только тогда, когда вектор $\overline{a} = (a_0,...,a_{n-1}) \in F^n$ составляет решения системы уравнений …

а) $\overline{a} \cdot (B - I) = 0$

б) $(B - I) = 1$

Ответ: а)

8. Являются ли числа 3,17 и 6 взаимно простыми?
Правильный ответ: да

9. Для чисел 34 и 17 наибольший общий делитель равен?
Правильный ответ: 2

10. Являются ли числа 3,17 и 6 попарно простыми?
Правильный ответ: нет

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.

3) Задания открытого типа (число):

- 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).

Программа рекомендована НМС математического факультета протокол № 0500-03 от 28.03.2024 г.