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
14.04.2022 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.02.Эллиптические кривые и алгоритм EC DSA

1. Шифр и наименование направления подготовки:
01.04.01 Математика

2. Профиль подготовки: Математические модели гидродинамики

3. Квалификация выпускника: Магистр

4. Форма образования: Очная

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

6. Составители программы: доцент, к.ф.-м.н. Адамова Римма Сергеевна

7. **Рекомендована:** НМС математического факультета протокол № 0500-03 от 24.03.2022 г.

8. Учебный год: 2022-2023 **Семестр(-ы):** 1

9. Цели и задачи учебной дисциплины:

Целью курса является:

- усвоение основных свойств эллиптических кривых, их применения в теории защиты информации
- изучение свойств проективного пространства над полем комплексных чисел, топологии эллиптических кривых, методов их изучения.

Задачами курса является:

- развитие способности применения методов топологии эллиптических кривых при изучении реальных процессов и объектов с целью нахождения эффективных решений общенаучных и прикладных задач широкого профиля.

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Эллиптические кривые и алгоритм EC DSA» относится к части, формируемой участниками образовательных отношений Блока 1. Она непосредственно связана с такими дисциплинами как «Аналитическая геометрия», «Дифференциальная геометрия и топология», «Математический анализ».

Приступая к изучению данной дисциплины, студенты должны знать и уметь оперировать с основными понятиями из дифференциальной геометрии и топологии, теории математического анализа, аналитической геометрии.

11. Компетенции обучающегося, формируемые в результате освоения дисциплины:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-1	Способен решать задачи аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач математической гидродинамики	ПК-1.1	Обладает большим объемом знаний в области математической гидродинамики	Знать: зарубежную и отечественную литературу в области математической гидродинамики Уметь: формулировать постановки основных задач математической гидродинамики, формулировать и доказывать теоремы предметной области Владеть: источниками информации, теоретическими подходами к исследованию математической гидродинамики
		ПК-1.2	Умеет находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в области математической гидродинамики	Знать: современные методы проведения научных экспериментов, подходы к анализу научно-исследовательских работ Уметь: находить, формулировать и исследовать разрешимость в научно-исследовательской деятельности Владеть: методами исследования и решения классических моделей гидродинамики
		ПК-1.3	Имеет практический опыт научно-исследовательской деятельности в области математической гидродинамики	Знать: современные методы анализа научно-исследовательских работ, основы научно-исследовательской деятельности в области математической гидродинамики Уметь: определять и развивать тематику научного исследования Владеть: современными методами научного анализа в области математической гидродинамики
ПКВ-3	Способен осуществлять теоретическое обобщение	ПКВ-3.1	Обладает теоретическим аппаратом, необходимым для	Знать: теоретический аппарат обобщения научных данных и результатов экспериментов в моделях математической гидродинамики.

	научных данных и результатов экспериментов в моделях математической гидродинамики		обобщения научных данных и результатов экспериментов в моделях математической гидродинамики	Уметь: обобщать научные данные и результаты экспериментов в моделях математической гидродинамики. Владеть: методами, позволяющими при помощи теоретического аппарата обобщать научные данные и результаты экспериментов в моделях математической гидродинамики.
		ПКВ-3.2	Умеет структурировать и обобщать научные и экспериментальные данные, четко формулировать и излагать необходимую информацию	Знать: методы и способы структурирования и обобщения научных и экспериментальных данных, четкого формулирования и изложения необходимой информации. Уметь: структурировать и обобщать научные и экспериментальные данные, грамотно формулировать и излагать информацию. Владеть: методами, позволяющими структурировать и обобщать научные и экспериментальные данные, четко формулировать и излагать необходимую информацию.
		ПКВ-3.3	Имеет практический опыт обобщения подобной информации	Знать: практически используемые методы обобщения информации. Уметь: обобщать полученную информацию на практике. Владеть: практическими методами обобщения информации.

12. Объем дисциплины в зачетных единицах/час.(*в соответствии с учебным планом)* **—**3/108
Форма промежуточной аттестации зачёт

13. Трудоёмкость по видам учебной работы

Вид учебной работы	Трудоемкость (часы)	
	Всего	По семестрам
		1
Аудиторные занятия	32	32
в том числе: лекции	16	16
практические	16	16
лабораторные	-	-
Самостоятельная работа	76	76
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	Проективное пространство над полем	Определение вещественного проективного пространства. Проективные координаты. Преобразования системы координат	https://edu.vsu.ru/enrol/index.php?id=15954
2	Эллиптические кривые над полем вещественных чисел	Геометрия эллиптической кривой. Особые точки кривой, касательные, точки перегиба.	
3	Эллиптические кривые над	Свойства точек перегиба эллиптической кривой в комплексном проективном пространстве. Каноническое	

	полем комплексных чисел	уравнение. Приведение к каноническому виду. Топология Эллиптической кривой в комплексном проективном пространстве.	
4	Конечные поля. Эллиптические кривые над конечными полями	Расширения конечных полей. Первообразный корень. Изоморфизм конечных полей. Эллиптические кривые над конечными полями. Алгоритм цифровой подписи.	
2. Практические занятия			
1	Проективное пространство над полем	Определение вещественного проективного пространства. Проективные координаты. Преобразования системы координат	https://edu.vsu.ru/enrol/index.php?id=15954
2	Эллиптические кривые над полем вещественных чисел	Геометрия эллиптической кривой. Особые точки кривой, касательные, точки перегиба.	
3	Эллиптические кривые над полем комплексных чисел	Свойства точек перегиба эллиптической кривой в комплексном проективном пространстве. Каноническое уравнение. Приведение к каноническому виду. Топология Эллиптической кривой в комплексном проективном пространстве.	
4	Конечные поля. Эллиптические кривые над конечными полями	Расширения конечных полей. Первообразный корень. Изоморфизм конечных полей. Эллиптические кривые над конечными полями. Алгоритм цифровой подписи.	

13.2 Темы (разделы) дисциплины и виды занятий:

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Проективное пространство над полем	4	4	-	19	27
2	Эллиптические кривые над полем вещественных чисел	4	4	-	19	27
3	Эллиптические кривые над полем комплексных чисел	4	4	-	19	27
4	Конечные поля. Эллиптические кривые над конечными полями	4	4	-	19	27
	Итого:	16	16		76	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 лекциях рассказывается теоретический материал, на практических занятиях решаются примеры по теоретическому материалу, прочитанному на лекциях.

При изучении курса «Эллиптические кривые и алгоритм EC DSA» 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. 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.
3. 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. Учебно-методическое и информационное обеспечение дисциплины:

а) основная литература:

№ п/п	Источник
1	Адамова Р.С. Эллиптические кривые и алгоритм EC DSA : учебное пособие / Р.С. Адамова ; Воронеж : Издательский дом ВГУ, 2018. - 34 с.
2	Кострикин А.И. Введение в алгебру : учеб. для вузов : в 3 ч./ А.И.Кострикин.-М.: Физматлит, 2009.-Ч.2. Линейная алгебра. – 367 с.

б) дополнительная литература:

№ п/п	Источник
3	Фоменко А.Т. Наглядная геометрия и топология. Математические образы в реальном мире.−М.:Изд-во Моск. ун-та,1992.−432с.
4	Дьяконов В.П. Математическая система Maple V R3/R4/R5/−М.: Изд-во “Солон”, 1992.−399с.
5	Прасолов В.В, Соловьёв Ю.П. Эллиптические кривые и алгебраические уравнения.−М.: Изд-во”Факториал,1997.−288с.

в) базы данных, информационно-справочные и поисковые системы**:**

№ п/п	Источник
6	Электронный каталог ЗНБ ВГУ http://www.lib.vsu.ru/?p=4
7	Электронный курс https://edu.vsu.ru/enrol/index.php?id=15954
8	Сайт факультета https://math.vsu.ru/wp/?page_id=937

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

№ п/п	Источник
1	Прасолов В.В, Соловьёв Ю.П. Эллиптические кривые и алгебраические уравнения.−М.: Изд-во”Факториал,1997.−288с.
2	Кострикин А.И. Введение в алгебру : учеб. для вузов : в 3 ч./ А.И.Кострикин.-М.: Физматлит, 2009.-Ч.2. Линейная алгебра. – 367 с.
3	Адамова Р.С. Эллиптические кривые и алгоритм EC DSA : учебное пособие / Р.С. Адамова ; Воронеж : Издательский дом ВГУ, 2018. - 34 с.
4	Электронный каталог ЗНБ ВГУ http://www.lib.vsu.ru/?p=4
5	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 (при необходимости)

Дисциплина может реализовываться с применением дистанционных образовательных технологий, например, на платформе «Электронный университет ВГУ» (https://edu.vsu.ru/enrol/index.php?id=15954).
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	Проективное пространство над полем	ПК-1 ПКВ-3	ПКВ-3.1 ПКВ-3.2 ПК-1.1	Домашние задания, контрольная работа № 1
2	Эллиптические кривые над полем вещественных чисел	ПК-1 ПКВ-3	ПКВ-3.1 ПКВ-3.2 ПК-1.1 ПК-1.2	Домашние задания, контрольная работа № 1
3	Эллиптические кривые над полем комплексных чисел	ПК-1 ПКВ-3	ПКВ-3.1 ПКВ-3.2 ПК-1.1 ПК-1.2	Домашние задания, контрольная работа № 1
4	Конечные поля. Эллиптические кривые над конечными полями	ПК-1 ПКВ-3	ПКВ-3.3 ПК-1.3	Домашние задания, контрольная работа № 1
Промежуточная аттестация Форма контроля - зачёт		Зачет 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:

Домашние задания:

По теме 1. Проективное пространство над полем

Адамова Р.С. Эллиптические кривые и алгоритм EC DSA : учебное пособие / Р.С. Адамова ; Воронеж : Издательский дом ВГУ, 2018. - 34 с.

Задание:

1. Проверить критерий точки перегиба.
2. Привести примеры проективной плоскости и алгебраической кривой.

По теме 2. Эллиптические кривые над полем вещественных чисел

Адамова Р.С. Эллиптические кривые и алгоритм EC DSA : учебное пособие / Р.С. Адамова ; Воронеж : Издательский дом ВГУ, 2018. - 34 с.

Задание:

1. Привести пример уравнения эллиптической кривой и исследовать её точки перегиба.
2. Взять уравнение эллиптической кривой и выполнить сложение точек на данной кривой.

По теме 3 Эллиптические кривые над полем комплексных чисел

Адамова Р.С. Эллиптические кривые и алгоритм EC DSA : учебное пособие / Р.С. Адамова ; Воронеж : Издательский дом ВГУ, 2018. - 34 с.

Задание:
1. Доказать Теорему 15.

По теме 4. Конечные поля. Эллиптические кривые над конечными полями

Адамова Р.С. Эллиптические кривые и алгоритм EC DSA : учебное пособие / Р.С. Адамова ; Воронеж : Издательский дом ВГУ, 2018. - 34 с.

Задания:
1. Привести пример использования алгоритма формирования электронной подписи и проверить её истинность.

Примерный перечень задач для контрольной работы №1:

Контрольно-измерительный материал № 1.

1. Топология эллиптической кривой над полем комплексных чисел.
2. Особые точки кривой, касательные, точки перегиба.

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и 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 контрольной работы.
В ходе контрольной работы обучающемуся выдается КИМ с перечнем теоретических вопросов и предлагается ответить на данные вопросы. В ходе выполнения заданий нельзя пользоваться литературой и конспектом лекций, 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.

20.2. Промежуточная аттестация

Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины. Промежуточная аттестация по дисциплине «Эллиптические кривые и алгоритм EC DSA» проводится в форме зачёта. Предназначена для определения уровня освоения всего объема учебной дисциплины.
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 выставляется зачёт. Если обучающийся не имеет положительной оценки по контрольной работе или практике, или не согласен с этой оценкой, он может ответить на соответствующие вопросы в ходе зачёта.

Примерный перечень вопросов:

1	Алгебраическая кривая. Особые точки. Выход в проективное пространство. Касательная и точки перегиба.
2	Приведение уравнения эллиптической кривой над полем комплексных чисел к каноническому виду.
3	Топология эллиптической кривой над полем комплексных чисел.
4	Расширение полей. Структура конечных полей.
5	Алгоритм цифровой подписи на основе эллиптической кривой над конечным 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**
Всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой. Усвоение взаимосвязей основных понятий дисциплины в их значении для приобретаемой профессии.	Зачтено
Пробелы в знаниях основного учебно-программного материала, принципиальные ошибки в выполнении предусмотренных программой заданий.	Не зачтено

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

1. Назовите данную теорему:
   Для однородного многочлена (x, y, z) порядка n справедливо соотношение

   $\Phi_x' \cdot x + \Phi_y' \cdot y + \Phi_z' \cdot z = n\,\Phi$.
   Ответ: **Теорема Эйлера**
2. Какая точка алгебраической кривой называется точкой перегиба?

   Ответ: **Точка алгебраической кривой называется точкой перегиба, если кратность её как точки пересечения кривой и касательной в этой точке больше или равна 3.**

3. Назовите условия на базовую точку эллиптической кривой в алгоритме цифровой подписи EC DSA.
   Ответ: **Её порядок должен быть простым числом.**

4. Какая точка эллиптической кривой называется точкой конечного порядка?
   Ответ: **Точка эллиптической кривой называется точкой конечного порядка, если некоторое её кратное даёт нулевую точку.**

5. Из каких элементов состоит вещественная проективная плоскость?
   Ответ: **Из прямых в пространстве, проходящих через фиксированную точку.**

6. Каков порядок пересечения кривой и касательной к ней в точке касания?
   Ответ: **Равен 2 или больше.**

7. Дайте определение конечнопорождённой группы.
   Ответ: **Группа называется конечно порождённой, если все её элементы могут быть получены из конечного числа их и им противоположных применением групповой операции.**
8. Сколько особых точек у вещественной кривой с уравнением
   $x^3 - 2x^2 - xy + 2y = 0$ в проективной плоскости?
   Укажите правильный ответ:
   A) две,
   B) ни одной,
   C) одна,
   D) бесконечно много .
   Ответ: A)
9. Точкой перегиба эллиптической кривой $y^2 = x^3 + 1$ является точка
   A) (4, 6),
   B) (2, 3),
   C) (0,–1),
   D) (–1, 0).
   Ответ: C)
10. Эллиптическая кривая в комплексной проективной плоскости гомеоморфна

    A) окружности,
    B) паре не пересекающихся окружностей,
    C) тору,
    D) сфере.
    Ответ: C)

11. Сколько точек перегиба у вещественной эллиптической кривой в проективной плоскости?
    A) две,
    B) три,
    C) четыре,
    D) нет ни одной.
    Ответ: B)
12. Суммой двух точек (–2, 2) и (–1, 0) эллиптической кривой $y^2 = x^3 + 5x^2 + 4x$ является точка
    A) (–2, –2),
    B) (2, 6),
    C) (2, –6),
    D) (4, 4).
    Ответ: B)
13. Точка (2, 6) эллиптической кривой $y^2 = x^3 + 5x^2 + 4x$ является
    A) точкой перегиба этой кривой,

B) точкой порядка 2 в группе точек этой кривой,
C) точкой пересечения кривой с прямой $y = -2x-2$,
D) точкой касания кривой и прямой $y = 3x$.
Ответ: D)

14. Для точки $F(2, 3)$ эллиптической кривой $y^2 = x^3+ 1$ точка 2 F имеет координаты

A) (0, 1),
B) (4, 6),
C) (0, –1),
D) (0, 0).

Ответ: A)

15. Точкой перегиба эллиптической кривой $y^2=x^3 +64$ является точка

A) (2, –3),
B) (0, 8),
C) (–4, 0),
D) (4, 0).
Ответ: B)

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 24.03.2022 г.