Оценочные материалы при формировании рабочих программ дисциплин (модулей)

Направление: 01.03.02 Прикладная математика и информатика

Направленность (профиль): Системное программирование и компьютерные науки

Дисциплина: Эллиптические системы в криптографии

Формируемые компетенции:

1. Описание показателей, критериев и шкал оценивания компетенций.

Показатели и критерии оценивания компетенций

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения не ниже порогового

Шкалы оценивания компетенций при сдаче зачета

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
Пороговый уровень	Обучающийся: - обнаружил на зачете всесторонние, систематические и глубокие знания учебно-программного материала; - допустил небольшие упущения в ответах на вопросы, существенным образом не снижающие их качество; - допустил существенное упущение в ответе на один из вопросов, которое за тем было устранено студентом с помощью уточняющих вопросов; - допустил существенное упущение в ответах на вопросы, часть из которых была устранена студентом с помощью уточняющих вопросов	Зачтено
Низкий уровень	Обучающийся: - допустил существенные упущения при ответах на все вопросы преподавателя; - обнаружил пробелы более чем 50% в знаниях основного учебно-программного материала	Не зачтено

Описание шкал оценивания

Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения			
	Неудовлетворитель	Удовлетворительно	Хорошо	Отлично
	Не зачтено	Зачтено	Зачтено	Зачтено

Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстриро-вать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся демонстрирует способность к самостоятельному применению знаний при решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной	Обучающийся демонстрирует способность к самостоятельно-му применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных
Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Владеть	Неспособность самостоятельно проявить навык решения поставленной задачи по стандартному образцу повторно.	Обучающийся демонстрирует самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем.	Обучающийся демонстрирует самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.

2. Перечень вопросов и задач к экзаменам, зачетам, курсовому проектированию, лабораторным занятиям. Образец экзаменационного билета

1. Алгебраические структуры. Полугруппы. Моноиды. Группы. Кольца. Поля.
2. Делимость и деление с остатком в кольце целых чисел.
3. Наибольший общий делитель и его свойства. Алгоритм Евклида.
4. Простые и составные числа. Теорема Евклида. Основная теорема арифметики.
5. Сравнения. Кольца классов вычетов по простому и составному модулю. Полная и приведенная системы вычетов.
6. Функция Эйлера. Теоремы Ферма и Эйлера.
7. История изучения эллиптических кривых. Эллиптические кривые для криптографических алгоритмов и протоколов в ГОСТах и стандартах РФ.
8. Алгебраические кривые над полями. Приводимость алгебраических кривых.
9. Найти все F_5-точки кривой y^2=x^3+2.
10. Найти все точки эллиптической кривой E7(2,6)
11. Особые точки кубической кривой.
12. Построить кривую x^3-x^2+y^2=0 и найти ее касательные в точке (0, 0).
13. Построить действительную часть кривой x^3+x^2+y^2=0 и найти ее касательные в точке (0, 0).
14. Однородный полином. Равенство полных степеней полинома и однородного ему. Эквивалентность троек чисел (элементов) поля.
15. Геометрическое построение проективной плоскости.
16. Плоскость Фано (построение точек и прямых).
17. Найти точки проективной плоскости над полем Галуа F_3={0,1,2}.

18. Сложение точек на прямых, окружностях и других кривых второго порядка (на плоскости) как групповая операция.

19. Найти координаты суммы двух точек (x_1,y_1) и (x_2,y_2) параболы y=x^2 с фиксированной точкой E=(0,0).

20. Закон сложения точек плоской кубической кривой. Количество точек пересечения прямой и кубической кривой.

21. Найти координаты суммы двух точек кубической параболы y=x^3 с фиксированной точкой E=(0,0).

22. Определение эллиптической кривой над полем. Характеристика поля. Канонические уравнения эллиптической кривой.

23. Теорема о девяти точках кубической кривой.

24. Ассоциативность операции сложения точек кубической кривой.

25. Формулы координат суммы точек с различными абсциссами кривой Вейерштрасса.

26. Формулы удвоения точек кривой Вейерштрасса.

27. Бесконечно удаленная точка кривой Вейерштрасса. Правила сложения точек кривой Вейерштрасса.

28. Кратность точек кубической кривой. Неособенные кубические кривые. Точки перегиба неособенной кривой. Эллиптические кривые.

29. Доказать, что точка бесконечности кривой Вейерштрасса - точка перегиба.

30. Множество точек перегиба кривой Вейерштрасса и их свойства.

31. Приведение уравнения эллиптической кривой с заданной точкой перегиба к виду Вейерштрасса.

32. Приведение уравнения эллиптической кривой с заданной рациональной точкой к виду Вейерштрасса.

33. Точки кручения. Ранг эллиптической кривой. Теорема Морделла.

34. Найти порядок точки p=(2,3). на эллиптической кривой y^2=x^3+1.

35. Эллиптический вариант криптосистемы Месси-Омуры

36. Криптосистема Эль-Гомаля и задача дискретного логарифмирования на эллиптической кривой.

37. Аналог протокола Джеффи-Хеллмана на эллиптической кривой

38. Алгоритм Тонелли-Шенкса.

39. Задача кодирования открытого текста точками эллиптической кривой.

40. Факторизация чисел с помощью эллиптических кривых.

3. Тестовые задания. Оценка по результатам тестирования.

Задание 1 (ПК-3, ОПК-4)

Выберите правильный вариант ответа.

Условие задания: Выбрать правильное определение

 Неособая кривая третьего порядка над полем называется эллиптической кривой над этим полем, если на ней есть хотя бы одна точка.

 Кривая третьего порядка над полем называется эллиптической кривой над этим полем, если на ней есть хотя бы одна особая точка.

 Особая кривая третьего порядка над полем называется эллиптической кривой над этим полем, если на ней есть хотя бы одна точка.

Задание 2 (ПК-3, ОПК-4)

Установить историческую последовательность математиков, изучавших эллиптические функции:

1: Нильс Хенрик Абель

2: Карл Густав Якоби

3: Карл Вейерштрасс

Задание 3 (ПК-3, ОПК-4)

Установите соответствие между полем с определнной характеристикой и видом уравнения эллиптической кривой в нем

поле характеристики, отличной от 2 и 3	y2=x3+ax+b;
поле характеристики 3	y2+ay=x3+bx+c;
поле характеристики 2 (суперсингулярная кривая)	y2+ay=x3+bx+c;
поле характеристики 2 (несупесингулярная кривая)	y2+axy=x3+bx2+c;
	y2+ay=x2+bx+c

Задание 4 (ПК-3, ОПК-4)

Вставить число
Порядок группы точек кривой E7(2,6) равен ____ .
Правильный вариант ответа: 11;

Задание 5 (ПК-3, ОПК-4)
Вставить пропущенный термин
Точка P будет называться ____ , если кратные ей точки образуют все множество точек эллиптической кривой.
Правильные варианты ответа: генератором группы; генеретор группы.

Полный комплект тестовых заданий в корпоративной тестовой оболочке АСТ размещен на сервере УИТ ДВГУПС, а также на сайте Университета в разделе СДО ДВГУПС (образовательная среда в личном кабинете преподавателя).

Соответствие между бальной системой и системой оценивания по результатам тестирования устанавливается посредством следующей таблицы:

Объект оценки	Показатели оценивания результатов обучения	Оценка	Уровень результатов обучения
Обучающийся	60 баллов и менее	«Неудовлетворительно»	Низкий уровень
	74 – 61 баллов	«Удовлетворительно»	Пороговый уровень
	84 – 75 баллов	«Хорошо»	Повышенный уровень
	100 – 85 баллов	«Отлично»	Высокий уровень

4. Оценка ответа обучающегося на вопросы, задачу (задание) экзаменационного билета, зачета, курсового проектирования.

Оценка ответа обучающегося на вопросы, задачу (задание) экзаменационного билета, зачета

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворитель	Удовлетворитель	Хорошо	Отлично
	Не зачтено	Зачтено	Зачтено	Зачтено
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам.	Значительные погрешности.	Незначительные погрешности.	Полное соответствие.
Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать	Полное несоответствие критерию.	Значительное несоответствие критерию.	Незначительное несоответствие критерию.	Соответствие критерию при ответе на все вопросы.
Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.

Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко.	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер.
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.