Оценочные материалы при формировании рабочих программ дисциплин (модулей)

Направление подготовки / специальность: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Профиль / специализация: Безопасность автоматизированных систем на транспорте

Дисциплина: Основы криптографии

Формируемые компетенции: ОПК-10

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			
	Неудовлетворительно Не зачтено	Удовлетворительно Зачтено	Хорошо Зачтено	Отлично Зачтено
Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстрировать 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 поддержке в части современных проблем.	Обучающийся демонстрирует способность к самостоятельному применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных связей.

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.

Примерный перечень вопросов к зачету.

Компетенция ОПК-10:

1. Понятия «информационная безопасность» и «защита информации». Основные составляющие информационной безопасности.
2. Объекты защиты. Категории и носители информации.
3. Средства защиты информации.
4. Криптография. Основные термины и определения.
5. Классификация криптографических систем.
6. Шифры замены. Классификация и основные методы шифрования.
7. Шифры перестановки. Классификация и основные методы шифрования.
8. Шифры гаммирования. Классификация и основные методы шифрования.
9. Шифры гаммирования. Способы генерации гаммы. Генераторы гамм.
10. Схема режима шифрования DES-ECB.
11. Схема режима шифрования DES-CBC.
12. Схема режима шифрования DES-CPB и DES-OFB.
13. Тройной DES. Сферы применения различных режимов DES.
14. ГОСТ 28147-89. Схема режима шифрования простой замены.
15. AES. Краткая характеристика основных этапов зашифрования/расшифрования.
16. ГОСТ 34.12-2015. Схема шифрования блочного шифра "Кузнечик".
17. Шифрование с открытым ключом. Основные понятия.
18. Алгоритм шифрования RSA.
19. Алгоритм шифрования Эль-Гамаля.
20. Алгоритм шифрования на основе задачи об укладке ранца.
21. Эллиптические кривые. Основные понятия. Сложение и умножение точки.
22. Алгоритм шифрования на основе эллиптических кривых.
23. Сложность алгоритмов.
24. Простые числа.
25. Разложение числа на простые сомножители.
26. Нахождение начального списка простых чисел.
27. Тестирование числа на простоту.
28. Определение наибольшего общего делителя.
29. Основные сведения о криптоанализе и атаки на криптосистемы.
30. Классическая стеганография.
31. Компьютерная стеганография.
32. Общие сведения о кодировании.
33. Общедоступные кодовые системы.
34. Представление чисел в двоичном виде.
35. Секретные кодовые системы.

Примерные практические задачи (задания) и ситуации

Компетенция ОПК-10:

1. Зашифровать с помощью шифра Цезаря слово «безопасность».
2. Зашифровать с помощью полибианского квадрата фразу «защита данных».
3. Зашифровать с помощью системы Виженера слово «защита».
4. Зашифровать с помощью шифра блочной перестановки слово «производство».
5. Зашифровать с помощью шифра поворотной решетки фразу «секретное письмо».

3. Тестовые задания. Оценка по результатам тестирования.

Примерные задания теста

Задание 1 (ОПК-10)

Впишите понятие для приведенного определения:

_____ - свойство информации быть известной и доступной, только прошедшим проверку (авторизацию) субъектам системы (пользователям, программам, процессам).

Задание 2 (ОПК-10)

Проставьте правильную последовательность операций при генерации ключа в алгоритме RSA:

вычисление произведения двух простых чисел

нахождение значения функции Эйлера

выбор открытого ключа

выбор двух простых чисел

вычисление закрытого ключа

Задание 3 (ОПК-10)
Приведите соответствие между шифром и типом шифрозамен:

шифр Цезаря	числа
Полибианский квадрат	жесты
тюремный шифр	рисунки
шифр Тени	буквы
	звуки

Задание 5 (ОПК-10)
Выберите правильный вариант ответа.
Шифры, заведомо неподдающиеся вскрытию (при правильном использовании) (один):
1. идеальные;
2. совершенные;
3. невскрываемые;
4. безупречные.

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» / Не зачтено	Низкий уровень
	74 – 61 баллов	«Удовлетворительно» / Зачтено	Пороговый уровень
	84 – 75 баллов	«Хорошо» / Зачтено	Повышенный уровень
	100 – 85 баллов	«Отлично» / Зачтено	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			
	Неудовлетворительно	Удовлетворительно	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 свои мысли	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.	1. 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.