Оценочные материалы при формировании рабочих программ дисциплин (модулей)

Направление подготовки / специальность: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
Профиль / специализация: Безопасность информационных систем
Дисциплина: Криптографические методы защиты информации

Формируемые компетенции: ПК-2

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

Шкалы оценивания компетенций при сдаче экзамена

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
Низкий уровень	Обучающийся: -обнаружил пробелы в знаниях основного учебно-программного материала; -допустил принципиальные ошибки в выполнении заданий, предусмотренных программой; -не может продолжить обучение или приступить к профессиональной деятельности по окончании программы без дополнительных занятий по соответствующей дисциплине.	Неудовлетворительно
Пороговый уровень	Обучающийся: -обнаружил знание основного учебно-программного материала в объёме, необходимом для дальнейшей учебной и предстоящей профессиональной деятельности; -справляется с выполнением заданий, предусмотренных программой; -знаком с основной литературой, рекомендованной рабочей программой дисциплины; -допустил неточности в ответе на вопросы и при выполнении заданий по учебно-программному материалу, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Удовлетворительно
Повышенный уровень	Обучающийся: - обнаружил полное знание учебно-программного материала; -успешно выполнил задания, предусмотренные программой;	Хорошо

	-усвоил основную литературу, рекомендованную рабочей программой дисциплины; -показал систематический характер знаний учебно-программного материала; -способен к самостоятельному пополнению знаний по учебно-программному материалу и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности	
Высокий уровень	Обучающийся: -обнаружил всесторонние, систематические и глубокие знания учебно-программного материала; -умеет свободно выполнять задания, предусмотренные программой; -ознакомился с дополнительной литературой; -усвоил взаимосвязь основных понятий дисциплин и их значение для приобретения профессии; -проявил творческие способности в понимании учебно- программного материала.	Отлично

Шкалы оценивания компетенций при защите курсового проекта/курсовой работы

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
Низкий уровень	Содержание работы не удовлетворяет требованиям, предъявляемым к КР/КП; на защите КР/КП обучающийся не смог обосновать результаты проведенных расчетов (исследований); цель КР/КП не достигнута; структура работы нарушает требования нормативных документов; выводы отсутствуют или не отражают теоретические положения, обсуждаемые в работе; в работе много орфографических ошибок, опечаток и других технических недостатков; язык не соответствует нормам научного стиля речи.	Неудовлетворительно
Пороговый уровень	Содержание работы удовлетворяет требованиям, предъявляемым к КР/КП; на защите КР/КП обучающийся не смог обосновать все результаты проведенных расчетов (исследований); задачи КР/КП решены не в полном объеме, цель не достигнута; структура работы отвечает требованиям нормативных документов; выводы присутствуют, но не полностью отражают теоретические положения, обсуждаемые в работе; в работе присутствуют орфографические ошибки, опечатки; язык соответствует нормам научного стиля речи; при защите КР/КП обучающийся излагает материал неполно и допускает неточности в определении понятий или формулировке правил; затрудняется или отвечает не правильно на поставленный вопрос	Удовлетворительно
Повышенный уровень	Содержание работы удовлетворяет требованиям, предъявляемым к КР/КП; на защите КР/КП обучающийся смог обосновать все результаты проведенных расчетов (исследований); задачи КР/КП решены в полном объеме, цель достигнута; структура работы отвечает требованиям нормативных документов; выводы присутствуют, но не полностью отражают теоретические положения, обсуждаемые в работе; в работе практически отсутствуют орфографические ошибки, опечатки; язык соответствует нормам научного стиля речи; при защите КР/КП полно обучающийся излагает материал, дает правильное определение основных понятий; затрудняется или отвечает не правильно на некоторые вопросы	Хорошо
Высокий уровень	Содержание работы удовлетворяет требованиям, предъявляемым к КР/КП; на защите КР/КП обучающийся смог обосновать все результаты проведенных расчетов (исследований); задачи КР/КП решены в полном объеме, цель достигнута; структура работы отвечает требованиям нормативных документов; выводы присутствуют и полностью отражают теоретические положения, обсуждаемые в работе; в работе отсутствуют орфографические ошибки, опечатки; язык соответствует нормам научного стиля речи; при защите КР/КП обучающийся полно излагает материал, дает правильное определение основных понятий; четко и грамотно отвечает на вопросы	Отлично

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 (2 семестр).
Компетенция ПК-2:

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. Хэш-функции. Основные понятия и разновидности.
24. Хэш-функция. MD5.

Примерный перечень вопросов к экзамену (3 семестр).
Компетенция ПК-2:

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. Хэш-функции. Основные понятия и разновидности.
24. Хэш-функция. MD5.
25. Криптографические протоколы. Основные понятия.
26. Протоколы обмена ключами.
27. Протоколы аутентификации. Разновидности и краткая характеристика.
28. Парольная идентификация/аутентификация.
29. Протокол идентификации/аутентификации на основе шифрования с открытым ключом.
30. Сервер аутентификации Kerberos.
31. Идентификация/аутентификация с помощью биометрических данных.
32. Идентификационные карты (ID-cards) и электронные ключи.
33. Электронная цифровая подпись. Общие сведения и разновидности ЭЦП.

34. ЭЦП на базе алгоритма RSA.
35. Алгоритм цифровой подписи ГОСТ 34.10-94.
36. Алгоритм цифровой подписи ГОСТ 34.10-2001.
37. Протоколы контроля целостности. Разновидности и краткая характеристика.
38. Протоколы контроля целостности. Биты четности, контрольные цифры и числа.
39. Протоколы контроля целостности. Использование ЭЦП и MAC-кодов.
40. Протоколы контроля целостности. Коды Хэмминга и ECC.
41. Электронные платежи. Разновидности и краткая характеристика.
42. Цифровые деньги на базе "слепой" ЭЦП.
43. Биткойн. Блокчейн, сеть и узлы.
44. Биткойн. Адрес.
45. Биткойн. Транзакция.
46. Биткойн. Блок.
47. Биткойн. Дерево Меркла, майнинг и ветвления блокчейна.
48. Классическое («бумажное») голосования.
49. Электронное голосование. Разновидности и краткая характеристика.
50. Российский опыт электронного голосования.
51. Протоколы разбиения и разделения секрета.
52. Тайные многосторонние вычисления.
53. Сложность алгоритмов.
54. Простые числа.
55. Разложение числа на простые сомножители.
56. Нахождение начального списка простых чисел.
57. Тестирование числа на простоту.
58. Определение наибольшего общего делителя.
59. Основные сведения о криптоанализе и атаки на криптосистемы.
60. Классическая стеганография.
61. Компьютерная стеганография.
62. Общие сведения о кодировании.
63. Общедоступные кодовые системы.
64. Представление чисел в двоичном виде.
65. Секретные кодовые системы.

Примерные практические задачи (задания) и ситуации
Компетенция ПК-2:

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».

Образец экзаменационного билета
Дальневосточный государственный университет путей сообщения

Кафедра (к202) Информационные технологии и системы 3 семестр учебный год	Экзаменационный билет № по дисциплине КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ для направления подготовки / специальности 10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ	«Утверждаю» Зав. кафедрой Попов М.А., канд. техн. наук, доцент «___» _____ 20 __ г.
1. Криптографические протоколы. Основные понятия. (ПК-2)		
2. Идентификация/аутентификация с помощью биометрических данных. (ПК-2)		
3. Рассчитать четные паритетные биты для букв своей фамилии в кодировке Windows-1251. (ПК-2)		

Примечание. В каждом экзаменационном билете должны присутствовать вопросы, способствующих формированию у обучающегося всех компетенций по данной дисциплине.

Курсовая работа (ПК-2)

Тематика и содержание курсовой работы.
Разработать программу, реализующую процедуры шифрования и расшифрования по стандарту DES (Data Encryption Standard). В программе предусмотреть возможность шифрования/расшифрования в режимах: электронная кодовая книга ECB, сцепление блоков шифра CBC, тройной DES (EEE3, EDE3, EEE2 и EDE2). Программа должна выдавать промежуточные результаты шифрования/расшифрования.

Примерное содержание пояснительной записки.

Оглавление
Задание.
Введение.
1. Краткие сведения о стандарте шифрования DES.
2. Режим DES-ECB.
2.1. Общая схема шифрования.
2.2. Исходный текст процедуры шифрования.
2.3. Пример шифрования и расшифрования (исходное сообщение, ключ, ключевые элементы ki, начальная перестановка, полублокиHiи Li, f(ki, Li), Hi f(ki, Li), конечная перестановка).
3. Режим DES-CBC.
3.1. Общая схема шифрования.
3.2. Исходный текст процедуры шифрования.
3.3. Пример шифрования и расшифрования (исходное сообщение, ключ, синхропосылка, блоки исходного текста и зашифрованного сообщения).
4. Режим тройной DES.
4.1. Общие схемы шифрования.
4.2. Исходные тексты процедур шифрования.
4.3. Пример шифрования и расшифрования (исходное сообщение, ключи, результаты шифрования после применения каждого ключа).
5. Руководство пользователя программы.
Список литературы.

Вопросы к защите курсовой работы
1. Криптография. Основные термины и определения.
2. Классификация криптографических систем.
3. Схема режима шифрования DES-ECB.
4. Схема режима шифрования DES-CBC.
5. Схема режима шифрования DES-CPB и DES-OFB.
6. Тройной DES.
7. Сферы применения различных режимов DES.

3. Тестовые задания. Оценка по результатам тестирования.
Примерные задания теста

Задание 1 (ПК-2)
Впишите понятие для приведенного определения:
_____ - свойство информации быть известной и доступной, только прошедшим проверку (авторизацию) субъектам системы (пользователям, программам, процессам).

Задание 2 (ПК-2)
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 (ПК-2)
Приведите соответствие между шифром и типом шифрозамен:

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

Задание 5 (ПК-2)
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»	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			
	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.

Оценка ответа обучающегося при защите курсового работы/курсового проекта

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Соответствие содержания КР/КП методике расчета (исследования)	Полное несоответствие содержания КР/КП поставленным целям или их отсутствие	Значительные погрешности	Незначительные погрешности	Полное соответствие
Качество обзора литературы	Работа в значительной степени не является самостоятельной	В значительной степени в работе использованы выводы, выдержки из других авторов без ссылок на них	В ряде случае отсутствуют ссылки на источник информации	Полное соответствие критерию
Использование современных информационных технологий	Современные информационные технологии, вычислительная техника не были использованы	Современные информационные технологии, вычислительная техника использованы слабо. Допущены серьезные ошибки в расчетах	Имеют место небольшие погрешности в использовании современных информационных технологий, вычислительной техники	Полное соответствие критерию
Качество графического материала в КР/КП	Не раскрывают смысл работы, небрежно оформлено, с большими отклонениями от требований ГОСТ, ЕСКД и др.	Не полностью раскрывают смысл, есть существенные погрешности в оформлении	Не полностью раскрывают смысл, есть погрешность в оформлении	Полностью раскрывают смысл и отвечают ГОСТ, ЕСКД и др.
Грамотность изложения текста КР/КП	Много стилистических и грамматических ошибок	Есть отдельные грамматические и стилистические ошибки	Есть отдельные грамматические ошибки	Текст КР/КП читается легко, ошибки отсутствуют
Соответствие требованиям, предъявляемым к оформлению КР/КП	Полное не выполнение требований, предъявляемых к оформлению	Требования, предъявляемые к оформлению КР/КП, нарушены	Допущены незначительные погрешности в оформлении КР/КП	КР/КП соответствует всем предъявленным требованиям
Качество доклада	В докладе не раскрыта тема КР/КП, нарушен регламент	Не соблюден регламент, недостаточно раскрыта тема КР/КП	Есть ошибки в регламенте и использовании чертежей	Соблюдение времени, полное раскрытие темы КР/КП
Качество ответов на вопросы	Не может ответить на дополнительные вопросы	Знание основного материала	Высокая эрудиция, нет существенных ошибок	Ответы точные, высокий уровень эрудиции

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