Оценочные материалы при формировании рабочих программ дисциплин (модулей)

Направление подготовки / специальность: Инфокоммуникационные технологии и системы связи
Профиль / специализация: Защищенные системы и сети связи
Дисциплина: Основы криптографии с открытыми ключами
Формируемые компетенции: УК-2
ПК-6

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 экзамена или зачета с оценкой

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания Экзамен или зачет с оценкой
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; -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	Хорошо

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

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 экзамену, практическим занятиям.

Примерный перечень вопросов к экзамену:

Компетенция УК-2.

1. Основные понятия и определения криптологии.
2. Модели асимметричных криптосистем.
3. Протоколы аутентификации.
4. Алгоритмы гаммирования.
5. Псевдослучайные генераторы.
6. Криптографические хэш функции.
7. Порядок распределения ключей.
8. Методы экспоненциального ключевого обмена. Цифровая подпись, протоколы аутентификации.
9. Режим вероятностного шифрования. Описание. Характеристики.
10. Быстрые программные шифры.

Компетенция ПК-6

1. Симметричные криптосистемы.
2. Электронная цифровая подпись и ее алгоритмы.
3. Стандарты шифрования DES и ГОСТ.
4. Моноалфавитные и многоалфавитные подстановки.
5. Двухключевые системы шифрации.
6. Криптосистемы без передачи ключей.
7. Методы разграничения доступа.
8. Шифры на основе управляемых перестановочных и подстановочно-перестановочных сетей.
9. Режим псевдовероятностного шифрования.
10. Коммутативные шифры и бесключевое шифрование.

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

1. Изучение ассиметричных криптосистем, процедур аутентификации и ЭЦП.
2. Основные характеристики шифра простой перестановки и шифра двойной перестановки
3. Построение криптографической хэш-функции на основе блочного шифра и исследование ее свойств методами математической статистики и теории информации.
4. Блочные шифры. Программная реализация 4-битовых замен в 32-битовом слове согласно таблицам замены.
5. Блочные шифры. Программная реализация ГОСТ 28147-89.
6. Программная реализация схемы ЭЦП.
7. Эллиптические кривые над конечным полем. Программная реализация операций над точками эллиптической кривой над Zp.

Компетенция ПК-6

1. Основные характеристики биграммных шифров.
2. Программная реализация процедуры генерации доказуемо простых чисел.
3. Вычисление параметров имитостойкости, помехоустойчивости шифров.
4. Вероятностные характеристики текстов. Определение избыточности текста, языка. Расчет параметров шифров. Расстояние единственности, определение количества ложных ключей.
5. Компьютерная реализация и вскрытие шифров замены.
6. Ситуационные задачи на определение свойств информации, подлежащей криптографическому преобразованию.
7. Преобразование криптосистемы над Zp в криптосистему на эллиптической кривой.

Задание на РГР:
«Программная реализация криптографических алгоритмов»
1. Составление технического задания. (УК-2, ПК-6)
2. Изучение основных методов криптографической зашиты информации. (ПК-6)
3. Запись сообщений методом симметричных криптосистем. (УК-2)
4. Получение шифротекста методом шифра простой и сложной замены. (ПК-6)
5. Шифрование сообщения шифром многоалфавитной замены, гаммирования. (УК-2, ПК-6)

Примерный перечень вопросов к защите расчетно-графической работе:

Компетенция УК-2

1. Вероятностные шифры с секретным и открытым ключом.
2. Протоколы стойкого шифрования с ключом малого размера.
3. Ключевые и бесключевые хэш-функции
4. протоколы слепой цифровой подписи.
5. Мультиподпись. Описание. Характеристики. Область применения.
6. Дайте классификации шифров по различным признакам.
7. Особенности криптоанализа.
8. Сформулируйте основную задачу криптографии. Основные элементы.
9. Создайте собственный подстановочный шифр и оцените его криптостойкость.
10. На основе каких данныз строятся атаки на засекречивающие системы?

Компетенция ПК-6

1. Проблема защиты информации в условиях ограниченности ключевого материла.
2. Описание операций блочного шифрования с использованием булевых функций.
3. Особенности применения хэш-функций в протоколах цифровой подписи.
4. Использование криптосхемы RSA для построения мультиподписи.
5. Групповая и коллективная подпись. Область применения.
6. Чем определяется сложность взлома криптоалгоритмов?
7. Создайте собственный перестановочный шифр и оцените его криптостойкость.
8. В чем сущность задачи факторизации?
9. Основные принципы, задачи криптографии.
10. Как называется распределительный алгоритм, определяющий последовательность действий каждой из сторон? Для чего он нужен и его функции.

Образец экзаменационного билета

Дальневосточный государственный университет путей сообщения		
Кафедра (к206) Автоматика, телемеханика и связь 6 семестр, учебный год	Экзаменационный билет № по дисциплине Основы криптографии с открытыми ключами / специальности 11.03.02 Инфокоммуникационные технологии и системы связи профиль/специализация Защищенные системы и сети связяи	«Утверждаю» Зав. кафедрой Годяев А.И., д-р техн. наук, доцент «___» _____ 20 __ г.
1. Режим вероятностного шифрования. Описание. Характеристики. (УК-2)		
2. Двухключевые системы шифрации. (ПК-6)		

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

Задание 1 (УК-2)
Выберите правильный вариант ответа.

Какой криптографический метод защиты информации предназначен для обеспечения конфиденциальности информации?
- Хеширование
- Электронная подпись
- Шифрование
- Коды аутентичности сообщений

Задание 2 (ПК-6)
Выберите правильный вариант ответа.

Для решения какой задачи обеспечения информационной безопасности предназначено хеширование?
- Обеспечение конфиденциальности информации
- Обеспечение неотказуемости
- Обеспечение контроля целостности данных
- Проверка подлинности источника данных

Задание 3 (УК-2)
Выберите правильный вариант ответа.

Чем шифр «Магма» отличается от шифра, определенного в стандарте ГОСТ 28147-89?
- Длиной ключа
- Это два принципиально разных симметричных блочных шифра
- Невозможностью использования произвольной таблицы замен
- Количеством раундов

Задание 4 (ОПК-6)
Выберите правильный вариант ответа

Какова длина секретного ключа в шифре «Кузнечик»?
- 64 бита
- 128 бит
- 256 бит
- 512 бит

Задание 5 (УК-2)
Выберите правильный вариант ответа.

Какой из режимов работы симметричных блочных шифров не предназначен для обеспечения конфиденциальности информации?
- Режим простой замены
- Режим простой замены с зацеплением

 Режим выработки имитовставки
 Режим гаммирования

Задание 6 (ПК-6)
Выберите правильный вариант ответа.

Что является основной проблемой криптографии с открытым ключом?
 Обеспечение аутентичности закрытых ключей
 Обеспечение конфиденциальности закрытых ключей
 Обеспечение аутентичности открытых ключей
 Обеспечение конфиденциальности открытых ключей

Задание 7 (УК-2)
Выберите правильный вариант ответа.

Для чего в схемах электронной подписи используются функции хеширования?
 Для повышения криптографической стойкости схемы электронной подписи
 Для обеспечения контроля целостности подписываемого сообщения
 Для представления подписываемого сообщения произвольной длины в виде строки данных фиксированной длины
 Для представления подписанного сообщения произвольной длины в виде строки данных фиксированной длины

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.