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 стеганографии

Формируемые компетенции: ПК-3
ПК-6
ПК-16

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.

Примерный перечень вопросов к зачету

Компетенция ПК-3:

1. Классификация видов информации, подлежащей шифрованию.
2. Частотные характеристики открытых текстов.
3. Классические варианты крипто атак, распространенных в сети.
4. Режим обратной связи по шифртексту DES (CFB).
5. Виды крипто атак. Пояснить их сущность.
6. Сформулируйте правило Кирхгоффа относительно стойкости шифра.
7. Характеризуйте криптоанализ на основе шифротекста.

Компетенция ПК-6:

1. Дайте определение криптографического протокола.
2. Укажите особенности криптоанализа на основе выбранного шнфротексга.
3. Опишите криптоанализ на основе адаптированного открытого текста.
4. Каким образом реализуется криптоанализ на основе адаптированного шифротекста.

5. Охарактеризуйте понятие имитозащиты.
6. Дайте определение терминов «криптография» и «стеганография».
7. Опишите принцип реализации электронной цифровой подписи.

Компетенция ПК-16:
1. Стеганография, стегосистема. Классическая стеганография. ЦВЗ-системы. Системы встраивания информации (СВИ). Компьютерная стеганография.
2. Текстовая стеганография. Примеры.
3. Применение систем встраивания информации. Виды атак на СВИ. Требования по защищённости СВИ к различным видам атак в зависимости от назначения.
4. Основные компоненты СВИ. Обобщённая схема СВИ.
5. Основные компоненты СВИ. Детализированные схемы составных процессов встраивания и извлечения информации в СВИ.
6. Свойства СВИ. Требования к свойствам системы встраивания информации в зависимости от её назначения.
7. Непрерывные и дискретные изображения. Цветовые пространства. Восприятие цвета зрительной системой человека.

Примерный перечень вопросов к лабораторной работе

Компетенция ПК-3:
1. В чем заключается криптоанализ на основе известного открытого текста и соответствующего ему шифротекста?
2. Каким образом осуществляется контроль целостности информации?
3. Восприятие контраста зрительной системой человека. (закон Вебера).
4. Восприятие синусоидального сигнала. Функция контрастной чувствительности.
5. Эффект маскировки в изображениях.
6. Эффект маскировки в видео.
7. Показатели качества изображений.

Компетенция ПК-6:
1. Особенности представления звуковых сигналов и их восприятие человеком. Частотное и временное маскирование.
2. Показатели качества звуковых сигналов.
3. Этап преобразования контейнера в пространство признаков при встраивании информации. Встраивание информации в пространственной области.
4. Порядок встраивания информации в спектральной области. Понятие двумерного дискретного ортогонального преобразования.
5. Спектры ДПФ, ДП Хартли, ДКП и их использование в качестве пространств признаков для встраивания информации.
6. Дискретное вейвлет-преобразование как пространство признаков для встраивания информации.
7. Преобразование Фурье-Меллина.

Компетенция ПК-16:
1. Преобразование изображения при сжатии его в формате JPEG с точки зрения встраивания информации.
2. НЗБ-встраивание ЦВЗ. Простейшее стеганографическое НЗБ-встраивание. ±1-встраивание.
3. Общая идея методов QIM. Базовая система Simple-QIM. Использование методов группы QIM в качестве основы для хрупких СВИ.
4. Общая идея методов QIM. Модификации QIM: DM-QIM, DC-QIM.
5. Аддитивное и мультипликативное встраивание. Система PatchWork.
6. Особенности применения и требования при проектировании СВИ в видео. Система защиты DVD-дисков.
7. Стеганографические методы, использующие встраивание информации в квантованные коэффициенты блочного ДКП.

Расчетно-графическая работа " Принципы работы кэш-памяти. Алгоритмы замещения срок кэш-памяти"
Компетенции: ПК-3
ПК-6
ПК-16

Цель работы: Проверить работу различных алгоритмов замещения при различных режимах записи. Изучение влияния параметров кэш-памяти и выбранного алгоритма замещения на эффективность работы системы.

Задание: В качестве задания предлагается некоторая короткая "программа", которую необходимо выполнить с подключенной кэш-памятью (размером 4 и 8 ячеек) в шаговом режиме для следующих двух вариантов алгоритмов замещения. В данной работе все варианты задания одинаковы: исследовать эффективность работы кэш-памяти при выполнении двух разнотипных программ, написанных и отлаженных вами при выполнении лабораторных работ.

Примерный перечень вопросов к расчетно-графической работе

Компетенция ПК-3:

1. В чем смысл включения кэш-памяти в состав ЭВМ?
2. Как работает кэш-память в режиме обратной записи?
3. Как работает кэш-память в режиме сквозной записи?
4. Как зависит эффективность работы ЭВМ от размера кэш-памяти?
5. В какую ячейку кэш-памяти будет помещаться очередное слово, если свободные ячейки отсутствуют?
6. Какие алгоритмы замещения ячеек кэш-памяти вам известны?
7. Какие типы нарушителей рассматриваются в стеганографии?
8. Какое влияние оказывает сжатие графических изображений на алгоритмы встраивания стегосообщения?
9. Методы противодействия стеганографических актов.
10. Перечислите основные виды атак на стеганографии.

Компетенция ПК-6:

1. Как работает алгоритм замещения "очередь" при установленном флажке, с учетом бита записи в диалоговом окне?
2. Параметры кэш-памяти?
3. Какой алгоритм замещения будет наиболее эффективным в случае применения кэш-памяти большого объема (в кэш-память целиком помещается программа)?
4. Как скажется на эффективности алгоритмов замещения учет значения бита записи W при работе кэш-памяти в режиме обратной записи?
5. Как скажется на эффективности алгоритмов замещения учет значения бита записи W при работе кэш-памяти в режиме сквозной записи?
6. Для каких целей в структуру ячейки кэш-памяти включен бит использования. Как устанавливается и сбрасывается этот бит?
7. Что такое практическая стойкость стегосистемы?
8. Какие функции выполняет каждый элемент стегосистемы?
9. Провести сравнительный анализ современных стеганографических методов с точки зрения их стойкости к стегоаналитическим актам.
10. Что такое стеганографический контейнер? Приведите примеры.

Компетенция ПК-16:

1. Что такое стегоанализ, основанный на контролируемом обучении? Каковы его плюсы и минусы?
2. Каковы преимущества использования адаптивного правила выбора элементов стеганографического контейнера? Какие при этом могут возникнуть проблемы?
3. Почему JPEG является предпочтительным форматом для использования в качестве стеганографического контейнера?
4. Алгоритм JSteg. Его недостатки.
5. Алгоритм F5. Его достоинства и недостатки.
6. Алгоритм матричного кодирования.
7. RS-стегоанализ.
8. Какие специфические возможности предоставляет стеганография в отличие от других средств защиты информации?
9. Какие типы нарушений рассматриваются в стеганографии?
10. Что такое теоретическая и практическая стойкость стегосистемы?

3. Тестовые задания. Оценка по результатам тестирования.

Примерные задания теста:

Задание 1 (ПК-3)
Что такое Стеганография?

Варианты ответа:
а) Это наука о шифровании данных.
б) Это наука о скрытой передачи информации.

в) Это наука о методах получения доступа к зашифрованной информации без знания секретного ключа.
г) Это наука, объединяющая в себе криптографию и криптологию.

Задание 2 (ПК-6)

Что такое «цифровой водяной знак»?

Варианты ответа:
а) Информация, внедряемая в аудио или видеофайлы с целью защиты авторских прав.
б) Синоним электронно-цифровой подписи.
в) Синоним кода аутентификации сообщения.
г) Нет верного ответа.

Задание 3 (ПК-16)

Что из нижеперечисленного относится к преимуществам стеганографии по сравнению с криптографией?

Варианты ответа:
а) Сообщения, защищенные с помощью стеганографии, не привлекают к себе внимания.
б) Стеганография обладает меньшей вычислительной сложности.
в) Стеганография обеспечивает более высокий уровень безопасности.
г) Нет верного ответа.

Задание 4 (ПК-6)

Можно ли совместно использовать методы криптографии и стеганографии?

Варианты ответа:
а) Да, но такая конструкция всегда будет нестойкой.
б) Да.
в) Нет.
г) Ответ неизвестен.

Задание 5 (ПК-6)

Что такое контейнер (в стеганографическом смысле)?

Варианты ответа:
а) Любая информация, используемая для сокрытия тайного сообщения.
б) Информация, подлежащая сокрытию.
в) Секретный ключ, нужный для сокрытия информации
г) Такой термин в стеганографии не используется.

Задание 6 (ПК-16)

Метод замены младших битов при стеганографии изображений не может применяться к файлам с расширением ...

Варианты ответа:
а) метод замены младших битов применим к изображениям с любыми расширениями
б) png
в) jpeg
г) bmp

Задание 7 (ПК-6)

Наука о скрытой передаче информации путем скрытия самого факта передачи информации называется ...

Варианты ответа:

а) стегоанализом
б) криптографией
в) криптоанализом
г) стеганографией

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