Оценочные материалы при формировании рабочих программ дисциплин (модулей)

Направление подготовки / специальность: Информационная безопасность автоматизированных систем

Профиль / специализация: специализация N 9 "Безопасность автоматизированных систем на транспорте" (по видам)

Дисциплина: Информационная безопасность информационно- управляющих и информационно-логистических систем транспорта

Формируемые компетенции: ОПК-9.1.
ОПК-9.2.
ОПК-9.3.

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 экзаменам, зачетам, курсовому проектированию, лабораторным

занятиям. Образец экзаменационного билета.

Примерный перечень вопросов к экзамену.

Компетенция ОПК-9.1:

1. Дайте определение компьютерной атаки.
2. Что такое информационная безопасность и ее основные аспекты?
3. Какая система называется безопасной и какая надежной?
4. Приведите примеры однонаправленных функций.
5. Что такое хэш-функция?

Компетенция ОПК-9.2:

1. Что такое двукратный DES? Какая атака делает двукратный DES бесполезным?
2. Почему режим OFB (Output Feed Back – Обратная связь по выходу) алгоритма DES применяют для шифрования в спутниковых системах связи?
3. Какой режим работы алгоритма ГОСТ 28147-89 можно использовать при формировании ЭЦП?
4. Перечислите параметры (размер блока, размер ключа и число раундов) для трех версий AES?
5. Сколько преобразований имеется в каждой версии AES? Сколько ключей необходимо для каждой версии?
6. Что называется электронной цифровой подписью?
7. Для чего используется электронная цифровая подпись?

Компетенция ОПК-9.3:

1. Что такое персональные данные?
2. Что такое служебная тайна?
3. Что такое государственная тайна?
4. Что представляют персональные данные?
5. Что такое дайджест сообщения?

Примерные практические задачи (задания) и ситуации
Компетенция ОПК-9.1, ОПК-9.2, ОПК-9.3:
1. Особенности создания ролевой модели доступа.
2. Концепция разработки ИС в защищенном исполнении.
3. Этапы создания электронно-цифровой подписи.

Образец экзаменационного билета

<table>
<tr><td colspan="3">Дальневосточный государственный университет путей сообщения</td></tr>
<tr><td>Кафедра
(к202) Информационные технологии и системы
9
семестр, учебный год</td><td>Экзаменационный билет №
по дисциплине
Информационная безопасность информационно - управляющих и информационно-логистических систем транспорта
для направления подготовки / специальности
10.05.03 Информационная безопасность автоматизированных систем
профиль/специализация
10.05.03 специализация N 9 "Безопасность автоматизированных систем на транспорте" (по</td><td>«Утверждаю»
Зав. кафедрой
Попов М.А., канд. техн. наук, доцент
«___» _____ 20 __ г.</td></tr>
<tr><td colspan="3">1. Дайте определение компьютерной атаки. (ОПК-9.1)</td></tr>
<tr><td colspan="3">2. Что такое служебная тайна? (ОПК-9.3)</td></tr>
<tr><td colspan="3">3. Концепция разработки ИС в защищенном исполнении. (ОПК-9.1, ОПК-9.2, ОПК-9.3)</td></tr>
</table>

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

3. Тестовые задания. Оценка по результатам тестирования.

1. Фундаментальное правило криптоанализа, заключающееся в том, что стойкость шифра должна определяться только секретностью ключа, сформулировано (ОПК-9.1)**:**

а) Режевским;

б) Керкхоффом;

в) Шамиром;

г) Шенноном.

2. Хэш-функция предназначена для (ОПК-9.2)**:**

а) аутентификации текстов, передаваемых по телекоммуникационным каналам;

б) шифрования передаваемой информации;

в) увеличения скорости передачи данных;

г) сжатия подписываемого документа до нескольких десятков или сотен бит.

3. Какой из перечисленных алгоритмов является алгоритмом хэширования: (ОПК-9.1)

а) SHA;

б) RSA;

в) Эль-Гамаля;

г) DSA.

4. Что такое политики безопасности? (ОПК-9.1)

а) пошаговые инструкции по выполнению задач безопасности;

б) общие руководящие требования по достижению определенного уровня безопасности;

в) широкие, высокоуровневые заявления руководства;

г) детализированные документы по обработке инцидентов безопасности.

5. Какой из режимов работы алгоритма DES можно использовать для формирования электронной цифровой подписи: (ОПК-9.2)

а) ECB;

б) CBC;

в) CFB;

г) OFB.

6. Какой из режимов работы алгоритма DES используется в телекоммуникационных системах (ОПК-9.2)

а) ECB;

б) CBC;

в) CFB;

г) OFB.

7. Концепция асимметричных криптографических систем с открытым ключом основана на применении: (ОПК-9.1)

а) рядов Фурье;

б) расширенной теоремы Евклида;

в) однонаправленных функций;

г) теоремы Найквиста-Котельникова;

д) полей Галуа.

8. Какие утверждения верны для хэш-функции? (ОПК-9.1)

а) длина хэш-функции не зависит от длины исходного сообщения;

б) длина хэш-функции меняется в зависимости от длины исходного сообщения;

в) хэш-функция должна быть чувствительна к всевозможным изменениям в тексте, таким как вставки, выбросы, перестановки и т.п.;

г) хэш-функция должна обладать свойством необратимости, то есть задача подбора документа, который обладал бы требуемым значением хэш-функции, должна быть вычислительно неразрешима;

д) для вычисления значения хэша можно использовать симметричные криптостистемы.

9. Определите возможные значения открытого ключа алгоритма RSA, если P=3, Q=11: (ОПК-9.3)

а) 7;

б) 11;

в) 13;

г) 6;

д) 9;

е) 4.

10. Шифрование - это: (ОПК-9.2)

а) процесс создания алгоритмов шифрования;

б) процесс сжатия информации;

в) процесс криптографического преобразования информации к виду, когда ее смысл полностью теряется.

11. Можно ли отнести слабую аутентификацию к проблемам безопасности? (ОПК-9.3)

а) нет;

б) да;

в) в редких случаях.

12. Установите соответствие: (ОПК-9.1)

1) Информационная безопасность	А) процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов
2) Туннелирование	Б) защита от нанесения неприемлемого ущерба субъектам информационных отношений
3) Окно опасности	В) промежуток времени
4) Конфиденциальность	Г) защита от несанкционированного ознакомления

13. Установите соответствие: (ОПК-9.1)

1) TCP/IP	А) туннельный протокол, использующийся для поддержки виртуальных частных сетей
2) PPTP	Б) туннельный протокол типа точка-точка
3) VPN	В) обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети
4) L2TP	Г) набор сетевых протоколов передачи данных

14. Установите соответствие: (ОПК-9.1)

1) SKIP	А) протокол для обмена ключами шифрования
2) IPsec	Б) сетевой протокол межсетевых управляющих сообщений, входящий в стек протоколов TCP/IP
3) LDAP	В) набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP
4) ICMP	Г) протокол прикладного уровня для доступа к службе каталогов X.500

15. Напишите ответ. Требование безопасности повторного использования объектов противоречит … (ОПК-9.1)

16. Напишите ответ. Аутентификация на основе пароля, переданного по сети в зашифрованном виде, плоха, потому что не обеспечивает защиты от … (ОПК-9.3)

17. Напишите ответ. Окно опасности – это … (ОПК-9.3)

18. Напишите ответ. Потенциальная возможность определенным образом нарушить информационную безопасность - это … (ОПК-9.3)

19. Укажите последовательность уровней OSI, начиная с нижнего: (ОПК-9.2)

1) канальный;

2) сетевой;

3) физический;

4) транспортный.

20. Укажите последовательность уровней OSI, начиная с нижнего: (ОПК-9.2)

1) уровень представления;

2) транспортный;

3) прикладной;

4) сеансовый.

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.