Оценочные материалы при формировании рабочих программ дисциплин (модулей)

Направление подготовки / специальность: Информационная безопасность автоматизированных
Профиль / специализация: специализация N 9 "Безопасность автоматизированных систем на
Дисциплина: Основы информационной безопасности

Формируемые компетенции: УК-8
ОПК-1
ОПК-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		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 УК-8:

1. Сущность и основные отличия информационных войн.
2. Формы психологического воздействия. Убеждение и внушение.
3. Классификация и виды информационно-психологического оружия.
4. Классификация и виды информационно-технологического оружия.
5. Защита от неинформированности как вид информационной защиты. Право на доступ к информации.
6. Виды опасных для человека информационных воздействий. Избыточная информация. Реакции человека на информационную перегрузку.
7. Защита от опасной информации в формах клеветы, угроз, обмана, вредоносной пропаганды и агитации.
8. Ценность информации, чем она определяется.
9. Информация и эмоции.

10. Копирование как уникальное свойство информации.
11. Носители информации и их характеристика. Информация и сообщение.
12. Представление информации на физическом уровне. Свойства вещественных и энергетических носителей информации.
13. Формы и особенности представления компьютерной информации.
14. Особенности представления и защиты информации на уровне средств взаимодействия с носителем.
15. Логический уровень представления компьютерной информации. Уязвимость и особенности реализации защиты информации на логическом уровне.
16. Синтаксический уровень представления информации.
17. Виды и характеристика способов информационной защиты на синтаксическом уровне.
18. Признаковая информация и формы ее защиты.
19. Виды кодирования информации.
20. Способы сжатия и декомпрессии компьютерной информации.
21. Характеристика информации как объекта собственности.
22. Общая характеристика информационных угроз.
23. Угрозы конфиденциальности, целостности и доступности.
24. Субъекты (источники и носители) информационных угроз.
25. Информационные нарушители и их классификация
26. Угрозы информации, связанные с человеческим фактором.
27. Пользователи как источники информационных угроз
28. «Внешние» нарушители информационной безопасности
29. Характеристика информационных нарушителей с точки зрения их осведомленности, оснащенности и подготовленности
30. Демаскирующие признаки человека-нарушителя: геометрическая и биомеханическая модель
31. Демаскирующие признаки человека-нарушителя: физико-химическая и социальная модель
32. Демаскирующие признаки вредоносной программы
33. Демаскирующие признаки специальных технических средств
34. Модель абсолютной защиты для сложной информационной системы.
35. Стратегии информационной защиты.
36. Активные и пассивные способы обнаружения информационных угроз.
37. Стратегия пассивной защиты
38. Стратегия маскировки, имитации и дезинформации
39. Стратегия ликвидации источников и носителей информационных угроз
40. Сущность энергетического скрытия информации

Компетенция ОПК-1:

1. Информационное скрытие на логическом и синтаксическом уровнях
2. Модель канала связи.
3. Угрозы информации в каналах связи
4. Методы защиты информации в каналах связи.
5. Виды и способы сокрытия источников и получателей сообщений в открытых информационных сетях.
6. Характеристика, этапы и демаскирующие признаки удаленного доступа к сетевой ЭВМ.
7. Модель комплексной защиты информации и ее элементы.
8. Общая характеристика нормативно-правовой защиты информации.
9. Защищаемая законом информация. Особенности правовой защиты информации ограниченного доступа.
10. Основные принципы защиты сведений, составляющих государственную тайну.
11. Основные положения о защите коммерческой тайны
12. Сущность и основные принципы организационно-распорядительной защиты информации.
13. Инженерно-техническая защита информации: постулаты, тактические требования, основные элементы защиты.
14. Объекты информатизации и их классификация.
15. Защита от утечки информации по техническим каналам. Термины и определения. Каналы утечки.
16. Основные способы защиты информации от утечки по техническим каналам.
17. Основные принципы защиты информации от электронных средств негласного подслушивания.
18. Общие принципы защиты компьютерной информации и ЭВМ от вредоносных программ.
19. Общая характеристика систем управления доступом.
20. Системы управления физическим доступом. Специальные режимы работы СУФД.
21. Особенности систем управления логическим доступом. Виды удаленного доступа.

Компетенция ОПК-16:

1. Защита объектов информатизации, технических средств обработки информации и машинных носителей от дестабилизирующих факторов окружающей среды. Классификация дестабилизирующих воздействий и способов защиты от них.
2. Понятия об информационных и компьютерных преступлениях.
3. Основные причины и особенности компьютерных преступлений.
4. Уголовно наказуемые формы распространения и разглашения информации
5. Уголовно наказуемые формы фальсификации информации
6. Формы законного и незаконного собирания информации.
7. Незаконное хранение, передача, предоставление и использование информации.
8. Компьютерная система как орудие преступления.
9. Компьютерная система как средство совершения преступления и хранилище информации о преступной деятельности.
10. Государственные органы власти, обеспечивающие защиту информации в России.
11. Основные федеральные законы в области защиты информации.
12. Технология двухфакторной аутентификации.
13. Идентификация в вычислительной системе.
14. Циклические коды.
15. Недостатки систем хеширования.
16. Способы защиты информации.
17. Стратегии защиты информации.
18. Периметр охраняемой территории.
19. «Абсолютная» система защиты.

3. Тестовые задания. Оценка по результатам тестирования.

1. В каком правовом документе дается определение термина «информационная безопасность»?
а) Федеральный закон «О безопасности».

б) Стратегия национальной безопасности Российской Федерации до 2020 года.

в) Доктрина информационной безопасности Российской Федерации.

г) Конституция.

д) Федеральный закон «Об информации, информационных технологиях и о защите информации».

2. Основными аспектами деятельности (задачами) информационной безопасности выступают –
а) Конфиденциальность.

б) Доступность.

в) Системность.

г) Целостность.

д) Защита информации.

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.