

Оценочные материалы при формировании рабочих программ дисциплин (модулей)

Направление подготовки / специальность: Информационная безопасность
Профиль / специализация: специализация N 9 "Безопасность автоматизированных систем на
Дисциплина: Организационное и правовое обеспечение информационной безопасности

Формируемые компетенции: УК-9
УК-10
ОПК-5

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-9:

1. Информация как объект правового регулирования Законодательство РФ в области информационной безопасности
2. Правовой режим защиты государственной тайны
3. Правовые режимы защиты конфиденциальной информации
4. Лицензирование и сертификация в информационной сфере
5. Защита интеллектуальной собственности
6. Компьютерные правонарушения
7. Правовое регулирование оперативно-розыскных мероприятий (ОРМ) в оперативно-розыскной (ОРД) и частной детективной и охранной деятельности (ЧДОД)
8. Международное законодательство в области защиты информации
9. Информационная безопасность и современные информационные технологии
10. Организационные источники и каналы утечки информации.

11. Экономика информационной безопасности. Защита информации в экстремальных ситуациях
12. Система организационной защиты информации
13. Информационная безопасность объекта при осуществлении международного сотрудничества
14. Цели и задачи организационной защиты информации, её связь с правовой защитой информации.
15. Классификация технических каналов утечки информации. Каналы утечки информации в средствах и системах информатизации.

Компетенция УК-10:

1. Виды угроз информационной безопасности на объекте защиты и их характеристика.
2. Основные требования Управления Федеральной Службы по Техническому и Экспортному Контролю (ФСТЭК) к технической защите информации.
3. Средства и методы физической охраны объектов.
4. Основные способы осуществления мер по обеспечению безопасности информации. Содержание организационных (административных) мер.
5. Порядок проведения аттестации объектов информатизации. Этапы аттестации. Содержание 2-го этапа аттестации.
6. Модели нарушителей информационной безопасности на объекте. Характеристика нарушителя 4-го уровня.
7. Организационные мероприятия по защите конфиденциальной информации.
8. Основные организационно-распорядительные документы, разрабатываемые на объекте защиты.
9. Категории конфиденциальности информации. Информация первой категории.
10. Структура органов по защите информации в РФ.
11. Категории объектов информатизации. Краткая характеристика каждой категории.
12. Структура государственной системы противодействия иностранной технической разведки (ПД ИТР) и технической защиты информации в РФ.
13. Основные направления деятельности по защите информации на предприятии.
14. Функции и задачи службы безопасности объекта информатизации.
15. Требования защищённости средств вычислительной техники (СВТ) от несанкционированного доступа (НСД) к информации. Классы и группы защищённости СВТ от НСД.

Компетенция ОПК-5:

1. Типовая структура службы безопасности. Задачи, решаемые подразделениями службы безопасности.
2. Исходные данные по аттестуемому объекту информатизации.
3. Основные документы, регламентирующие деятельность подразделения (специалиста) по защите информации.
4. Требования к помещениям, в которых циркулирует защищаемая информация. Категорирование помещений. Определение границ контролируемых зон (КЗ).
5. Организация обучения персонала, её методы и формы.
6. Требования руководящих документов по порядку разработки и содержанию "Положения о подразделении (специалисте) по защите информации".
7. Организационные мероприятия, проводимые с целью защиты средств вычислительной техники (СВТ) и автоматизированных систем (АС) от несанкционированного доступа (НСД).
8. Классификационные требования к уровню подготовки главного инженера (руководителя подразделения) по защите информации.
9. Четыре основные составляющие национальных интересов РФ в информационной сфере.
10. Требования руководящих документов по порядку разработки и содержанию "Руководства по защите информации ...".
11. Внешние источники угроз безопасности информации.
12. Типовой перечень внутренних организационно-распорядительных документов по защите конфиденциальной информации.
13. Внутренние источники угроз безопасности информации.
14. Задачи, которые необходимо решить для реализации четвёртой составляющей национальных интересов РФ в информационной сфере.
15. Типовое положение о Совете (Технической комиссии) министерства, ведомства органа государственной власти субъекта Российской Федерации по защите информации от иностранных технических разведок и от её утечки по техническим каналам (Решение ГТК № 32 от 14 марта 1995 года).
16. Основные направления обеспечения защиты информации от несанкционированного доступа (НСД).
17. Положение по аттестации объектов информатизации от 25 ноября 1994 года. Основные тезисы.
18. Основные принципы защиты информации от несанкционированного доступа (НСД).
19. Порядок согласования и утверждения руководящих должностей по защите информации на предприятии и в организации.

3. Тестовые задания. Оценка по результатам тестирования.

Примерные задания теста

Задание 1 (УК-9)

Укажите 2 правильных ответа:

В Российской Федерации оказание услуг регламентируется (2 ответа):

20. Гражданским кодексом

21. Федеральным законом «О защите прав потребителей»

22. Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ

23. Федеральным законом «О техническом регулировании» от 27.12.2002 N 184-ФЗ

Задание 2 (УК-10)

Установите соответствие понятий продуктов:

L1: Промышленный продукт

L2: Программный продукт

L3: Продукт творчества (произведение искусства)

R1: Товар или услуга, которую можно предложить для рынка, и которая будет удовлетворять потребности потребителей

R2: Совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ

R3: Качественно новые материалы, духовные ценности или итог создания объективно нового

Задание 3 (ОПК-5)

Вставьте пропущенный термин

безопасность – практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации

+: Информационная

+: информационная

+: ИНФОРМАЦИОННАЯ

Задание 4 (ОПК-5)

Укажите последовательность действий при обнаружении в информационно-телекоммуникационных сетях, в том числе в сети интернет, информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, включая случай поступления уведомления о распространении такой информации от федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления, организаций или граждан. (Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

1: Генеральный прокурор РФ или его заместители направляют требование в Роскомнадзор о принятии мер по ограничению доступа к информационным ресурсам, распространяющим запрещённую информацию

2: Роскомнадзор направляет операторам связи требование о принятии мер по ограничению доступа к информационному ресурсу.

3: Роскомнадзор определяет провайдера хостинга или иное лицо, обеспечивающее размещение в информационно-телекоммуникационной сети

4: Роскомнадзор направляет провайдеру хостинга или иному лицу уведомление о нарушении порядка распространения информации с требованием принять меры по удалению такой информации

5: Роскомнадзор фиксирует дату и время направления уведомления в соответствующей информационной системе

6: После получения требования Роскомнадзора оператор связи ограничивает доступ к информационному ресурсу

7: В течение суток с момента получения уведомления провайдер хостинга обязан проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно удалить запрещённую информацию

8: Если владелец информационного ресурса удалил запрещённую информацию, он направляет уведомление об этом в Роскомнадзор.

9: После получения данного уведомления и проверки его достоверности Роскомнадзор обязан уведомить оператора связи о возобновлении доступа к информационному ресурсу

10: После получения уведомления от Роскомнадзора оператор связи незамедлительно возобновляет доступ к информационному ресурсу

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 балльной 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.