Оценочные материалы при формировании рабочих программ дисциплин (модулей)

Направление подготовки / специальность: Информатика и вычислительная техника
Профиль / специализация: Программирование интеллектуальных и автоматизированных систем
Дисциплина: Защита информации

Формируемые компетенции: УК-2
ОПК-3
ОПК-4

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	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 УК-2:

1. Национальная безопасность Российской Федерации. Основные понятия и регламентирующие документы
2. Информационная безопасность: понятие, терминология, цели, задачи, направления, основные регламентирующие документы
3. Основные угрозы информационной безопасности. Источники угроз. Уязвимости: понятие и классификация.
4. Классификация вредоносных программ. Виды воздействий вредоносных программ
5. Методы и средства защиты информации и информационных систем от воздействия вредоносного программного обеспечения
6. Защита информации: понятие, функции и задачи, способы и направления
7. Защита информации: методы и средства
8. Методы и средства управления доступом
9. Программные средства и методы защиты информации
10. Технические средства и методы защиты информации
11. Организационные и правовые средства и методы защиты информации

Компетенция ОПК-3:

12. Криптология: структура, предмет и методы. Криптография. Основные понятия, задачи, этапы развития.
13. Криптографические методы и системы защиты информации.
14. Шифры: понятие, классификация шифров. Модели шифров. Основные требования к шифрам.
15. Криптографический анализ. Анализ надежности криптосистем. Криптографическая стойкость шифров.
16. Симметричное и асимметричное шифрование в задачах защиты информации.
17. Основные шифры классической криптографии и их криптоанализ
18. Шифр перестановки: алгоритм и криптоанализ
19. Шифр подстановки: алгоритм и криптоанализ
20. Шифр Хилла: алгоритм и криптоанализ
21. Шифр Виженера: алгоритм и криптоанализ
22. Полибианский квадрат: алгоритм и криптоанализ
23. Блочные шифры. Сети Фейстеля
24. Алгоритм шифрования DES и его криптоанализ
25. Алгоритм шифрования AES и его криптоанализ
26. Режимы применения блочных шифров и их криптоанализ

Компетенция ОПК-4

27. Основные асимметричные криптосистемы и их криптоанализ
28. Алгоритм шифрования Эль Гамаля и его криптоанализ
29. Алгоритм шифрования RSA и его криптоанализ
30. Алгоритм шифрования Эль Гамаля на основе эллиптических кривых и его криптоанализ
31. Алгоритмы проверки подлинности сообщения. Message Authentication Codes. Анализ одного из методов (по выбору)
32. Основные алгоритмы и методы идентификации и аутентификации пользователей. Анализ одного из методов (по выбору)
33. Электронная подпись. Угрозы электронной подписи
34. Инфраструктура открытых ключей
35. Системы обнаружения атак и вторжений (Intrusion Detection Systems, IDSs)

36. Политика безопасности и механизмы защиты
37. Модель дискреционного доступа
38. Модели безопасности Белла-Ла Падулы и Биба
39. Ролевая модель контроля доступа
40. Системы разграничения доступа
41. Использование функций хэширования в информационной безопасности. Описание одного из алгоритмов (по выбору)
42. Применение случайных чисел в криптографии. Генераторы псевдослучайных чисел. Описание одного из алгоритмов (по выбору)

Примерные практические задачи (задания) и ситуации (ОПК-3)

1. С помощью линейного шифра (K=(3,7), N=32) зашифровать слово **школа**
2. С помощью сдвигового шифра (K=9, N=26) зашифровать слово **universe**
3. С помощью шифра Хилла $K = \begin{matrix} 3 & 9 \\ 7 & 11 \end{matrix}$, N=26 зашифровать слово **antropology**
4. С помощью шифра Виженера (K=USELESS, N=26, пробелы опускаются) зашифровать фразу **quis custodiet ipsos custodes**
5. С помощью шифра перестановки (K = 3 6 4 1 2 5) зашифровать слово **интроспекция**
6. С помощью LFSR (IV=10111, C=11111) сгенерировать последовательность из 10 элементов.
7. С помощью шифра с автоматическим выбором ключей (K=20, N=32) зашифровать слово **синхрофазотрон**
8. С помощью шифра постановки (K= QAZLPOKMWSXIJNCDEBHUVFRGYT, N=26) зашифровать слово **datasheet**
9. С помощью линейного шифра (K=(9,11), N=26) зашифровать слово **process**
10. С помощью сдвигового шифра (K=17, N=32) зашифровать слово **галактика**
11. С помощью шифра Хилла $K = \begin{matrix} 7 & 17 \\ 5 & 19 \end{matrix}$, N=32 зашифровать слово **победитель**
12. С помощью шифра Виженера (K=религия, N=32, пробелы опускаются) зашифровать фразу **иду в магазин за макаронами**
13. С помощью шифра перестановки (K = 5 4 1 2 3 6) зашифровать слово **pastafarian**
14. С помощью LFSR (IV=10001, C=00101) сгенерировать последовательность из 10 элементов.
15. С помощью шифра с автоматическим выбором ключей (K=3, N=26) зашифровать слово **mathematics**

С помощью шифра постановки (K= ЙФЯЭЪЮЖХЦЫЧЗДБЬЛЩУВСШОТМАКИРГПНЕ, N=32) зашифровать слово **распространение**

Образец билета к экзамену

Дальневосточный государственный университет путей сообщения		
Кафедра (к910) Вычислительная техника и компьютерная графика 1 семестр, 2021/2022 учебного года	Экзаменационный билет № 1 по дисциплине Защита информации для направления подготовки / специальности 09.03.01 Информатика и вычислительная техника профиль/специализация Программирование интеллектуальных и автоматизированных систем	«Утверждаю» Зав. кафедрой Пономарчук Ю.В., канд. физ.-мат. наук «___» _____ 20 __ г.
1. Информационная безопасность: понятие, терминология, цели, задачи, направления, основные регламентирующие документы (УК-2)		
2. Инфраструктура открытых ключей (ОПК-4)		
3. Задача (ОПК-3) С помощью LFSR (IV=10111, C=11111) сгенерировать последовательность из 10 элементов		

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

3. Тестовые задания. Оценка по результатам тестирования.

Примерные задания теста

Задание 1 (ОПК-3)

Последовательность действий при авторизации пользователя в системе

а) Предоставление доступа к системе или отказ в доступе
б) Получение информации о пользователе при его входе в систему
в) Регистрация пользователя и идентифицирующей его информации
г) Сравнение характеристик введенной пользователем информации при входе в систему с зарегистрированной учетной записью

Задание 2 (УК-2)

Вставьте пропущенное слово

_____ - это набор документированных норм, правил, практических приемов, регулирующих управление, защиту и распространение информации ограниченного доступа.

Задание 3 (ОПК-4)

Выберите несколько правильных ответов.

Принципами проектирования систем безопасности являются _____

а) По умолчанию доступ пользователю в систему не должен предоставляться
б) По умолчанию доступ пользователю в систему предоставляется
в) Необходимо проверять текущее состояние прав доступа
г) Устройство системы не должно быть секретом
д) Устройство системы должно быть секретом
е) Предоставлять каждому процессу как можно меньше привилегий
ж) Механизм защиты должен быть простым, одинаковым для всех и встроенным в самые нижние уровни системы
з) Механизм защиты должен быть сложным
и) Необходимо усложнять систему защиты
к) Необходимо сохранять систему защиты простой

Задание 5 (ОПК-3)
Выберите один ответ

а) К методам аутентификации относятся _____
б) Шифрование данных
в) Алгоритмы генерирования электронной подписи сообщения
г) Алгоритмы хэширования
д) Методы вычисления контрольной суммы содержания сообщения

Задание 6 (ОПК-1)
Вставьте пропущенное слово

_____ - это состояние ИС, при котором блокируется доступ к некоторому ее ресурсу

Задание 7 (ОПК-4)
Являются косвенными каналы утечки информации в ИС:

а) Использование подслушивающих устройств и хищение носителей информации
б) Дистанционное видеонаблюдение, незаконное подключение специальной аппаратуры к устройствам или линиям связи ИС и перехват побочных электромагнитных излучений и наводок
в) Использование подслушивающих устройств и перехват побочных электромагнитных излучений и наводок
г) Сбор производственных отходов с информацией и использование подслушивающих устройств

Задание 8 (УК-2)
Методы и средства защиты информации включают:

а) Организационно-правовые
б) Инженерно-технические
в) Физические
г) Криптографические
д) Программно-аппаратные
е) Эргономические

Задание 9 (ОПК-3)

Выберите один ответ

К информации ограниченного доступа НЕ относятся _____

а) Стандартные протоколы шифрования
б) Сведения, составляющие государственную тайну
в) Сведения, составляющие служебную тайну
г) Персональные данные
д) Сведения, составляющие коммерческую тайну

Задание 10 (ОПК-4)

Выберите один вариант ответа.

Комплекс программно-аппаратных средств, осуществляющий информационную защиту одной части компьютерной сети от другой путем анализа проходящего между ними трафика, называется ...

а) сетевой экран
б) система шифрования с открытым ключом
в) троянская программа
г) система FDDI

Задание 11 (УК-2)

Соответствие между видами сетевых экранов и их назначением.

а) сетевой экран сетевого уровня	б)
в) сетевой экран сеансового уровня	г) способен интерпретировать, анализировать и контролировать содержимое сообщений, которыми обмениваются приложения
д) сетевой экран прикладного уровня	е) решает задачу фильтрации пакетов по IP-адресам и портам приложений на основании списков доступа
ж) сетевой экран коммутационного уровня	з) отслеживает состояние соединений, фиксирует подозрительную активность, направленную на сканирование портов и сбор другой информации о сети

Ответ: _____

Задание 12 (ОПК-4)

Выберите несколько ответов.

К протоколам защищенного канала относятся следующие виды протоколов:

а) SSL
б) SDN
в) PDN
г) TLS
д) IPSec

Задание 13 (УК-2)

Шифры замены можно разделить на следующие группы:

а) комбинированные и квантовые шифры;
б) шифры маршрутной и поворотной замены;
в) шифры однозначной и многозначной замены;
г) алфавитные и лозунговые шифры

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 и рейтинговой системами оценивания знаний, умений, навыков и (или) опыта деятельности, 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 – 77 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.