

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гарант Максим Алексеевич
Должность: Ректор
Дата подписания: 14.03.2024 09:29:11
Уникальный программный ключ:
7708e7a47e66a8ee02711b293d7e78bd1e40bf88

Приложение
к рабочей программе дисциплины

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Защита информации в информационных системах

(наименование дисциплины(модуля))

09.04.02 Информационные системы технологии

(код и наименование)

Корпоративные информационные системы

(наименование)

Содержание

1. Пояснительная записка.
2. Типовые контрольные задания или иные материалы для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих уровень сформированности компетенций.
3. Методические материалы, определяющие процедуру и критерии оценивания сформированности компетенций при проведении промежуточной аттестации.

1. Пояснительная записка

Цель промежуточной аттестации – оценивание промежуточных и окончательных результатов обучения по дисциплине, обеспечивающих достижение планируемых результатов освоения образовательной программы.

Формы промежуточной аттестации: зачёт, *семестр 4*.

Перечень компетенций, формируемых в процессе освоения дисциплины

Код и наименование компетенции	Код индикатора достижения компетенции
ОПК-6: Способен использовать методы и средства системной инженерии в области получения, передачи, хранения, переработки и представления информации посредством информационных технологий	ОПК-6.2

Результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные материалы (семестр)
ОПК-6.2: Использует методы и средства системной инженерии в области получения, передачи, хранения, переработки и представления информации посредством информационных технологий	Обучающийся знает: правовые основы защиты компьютерной информации, модели и методы криптографической защиты и криптоанализа	Вопросы (№1 - №5)
	Обучающийся умеет: применять криптографические методы на программном уровне: создание и отладка модулей шифрования/дешифрования, подготовка к передаче и обработка приема специально структурированных данных	Задания (№1 - №5)
	Обучающийся владеет: базовыми знаниями и приемами вычислений модулярной арифметики, теории чисел для расширенного решения задач криптографической защиты информации	

Промежуточная аттестация (зачёт) проводится в одной из следующих форм:

- 1) ответ на билет, состоящий из теоретических вопросов и практических заданий;
- 2) выполнение заданий в ЭИОС СамГУПС.

2. Типовые¹ контрольные задания или иные материалы для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих уровень сформированности компетенций

2.1 Типовые вопросы (тестовые задания) для оценки знаниевого образовательного результата

Проверяемый образовательный результат:

Код и наименование индикатора достижения компетенции	Образовательный результат
ОПК-6.2: Использует методы и средства системной инженерии в области получения, передачи, хранения, переработки и представления информации посредством информационных технологий	Обучающийся знает: основные методы и средства защиты конфиденциальной информации; состав и организацию систем информационной безопасности, методы криптографических преобразований; основные стандарты и протоколы шифрования и электронной подписи; методы и средства обеспечения информационной безопасности компьютерных систем; современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования; современные подходы к построению систем защиты информации.
<i>Примеры вопросов</i>	
1. Основные понятия криптографической защиты информации	
2. Система шифрования RSA	
3. Основы теории чисел. Теоремы Ферма, Эйлера и Гаусса в теории чисел	
4. Модулярная арифметика и классы вычетов	
5. Проблемы теории чисел	

2.2 Типовые задания для оценки навыкового образовательного результата

Проверяемый образовательный результат:

Код и наименование индикатора достижения компетенции	Образовательный результат
ОПК-6.2: Использует методы и средства системной инженерии в области получения, передачи, хранения, переработки и представления информации посредством информационных технологий	Обучающийся умеет: определять и анализировать угрозы безопасности информации в зависимости от среды эксплуатации продуктов информационных технологий; использовать современные программные средства для защиты информации; принимать адекватные решения при выборе средств защиты информации на основе анализа угроз; разрабатывать и создавать типовые схемы защиты информации на основе современных средств обеспечения информационной безопасности; обоснованно выбирать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты.
ОПК-6.2: Использует методы и средства системной инженерии в области получения, передачи, хранения,	Обучающийся владеет: навыками разработки защищенных приложений; навыками создания защищенной среды с помощью аппаратно-программных средств защиты; навыками самостоятельного проектирования систем защиты информации; методами оценки эффективности систем защиты информации в компьютерных

¹ Приводятся типовые вопросы и задания. Оценочные средства, предназначенные для проведения аттестационного мероприятия, хранятся на кафедре в достаточном для проведения оценочных процедур количестве вариантов. Оценочные средства подлежат актуализации с учетом развития науки, образования, культуры, экономики, техники, технологий и социальной сферы. Ответственность за нераспространение содержания оценочных средств среди обучающихся университета несут заведующий кафедрой и преподаватель – разработчик оценочных средств.

переработки и представления информации посредством информационных технологий

системах.

Тестовые вопросы

1. Преобразование открытого текста сообщения в закрытый называется:

- 1) процедура шифрования;
- 2) алгоритм шифрования;
- 3) обеспечение аутентификации;
- 4) цифровая запись.

2. Входные параметры процесса шифрования {несколько верных ответов):

- 1) зашифрованный текст;
- 2) ключ;
- 3) открытый текст;
- 4) алгоритм.

3. Какие из сервисов реализуются при использовании криптографических преобразований {несколько верных ответов):

- 1) контроль целостности;
- 2) аутентификация;
- 3) шифрование;
- 4) алгоритм.

4. Что позволяет предотвратить использование криптографических преобразований:

- 1) отказ от информации;
- 2) обеспечение аутентификации;
- 3) утечку информации;
- 4) использование алгоритмов асимметричного шифрования.

5. Знание ключа позволяет:

- 1) использовать криптографические сервисы безопасности;
- 2) обеспечить аутентификацию;
- 3) предотвратить утечку информации;
- 4) выполнить обратное преобразование.

2.5. Перечень вопросов для подготовки обучающихся к промежуточной аттестации

I. Введение в криптографическую защиту информации

1. Основные понятия криптографической защиты информации
2. Система шифрования RSA
3. Основы теории чисел. Теоремы Ферма, Эйлера и Гаусса в теории чисел
4. Модулярная арифметика и классы вычетов
5. Проблемы теории чисел

II. Фундаментальные алгоритмы

6. Особенности алгоритмов в теории чисел
7. Алгоритм деления
8. Теорема деления
9. Алгоритм Эвклида
10. Расширенный алгоритм Эвклида

III. Факторизация чисел

11. Теорема о разложении
12. Существование разложения
13. Алгоритм Ферма разложения на множители
14. Фундаментальное свойство простых чисел
15. Единственность разложения
16. Числа Кармайкла и тест Миллера

IV. Простые числа

17. Полиномиальная формула
18. Экспоненциальные формулы: числа Мерсенна, числа Ферма
19. Решето Эратосфена

V. Арифметика остатков

20. Отношение эквивалентности
21. Сравнения
22. Арифметика остатков
23. Критерий делимости
24. Степени

25. Диофантовы уравнения

26. Деление по модулю

27. Теорема Ферма

28. Вычисление корней. Квадратные корни

VI. Системы сравнений

29. Линейные уравнения 30. Китайский алгоритм остатков: взаимно простые модули

31. Свойства степени. Алгоритм степени

VII. Группы

32. Арифметические группы

33. Подгруппы

34. Циклические подгруппы

35. Поиск подгрупп. Теорема Лагранжа

3. Методические материалы, определяющие процедуру и критерии оценивания сформированности компетенций при проведении промежуточной аттестации

Критерии формирования оценок по ответам на вопросы, выполнению тестовых заданий

- оценка **«отлично»** выставляется обучающемуся, если количество правильных ответов на вопросы составляет 100 – 90% от общего объёма заданных вопросов;
- оценка **«хорошо»** выставляется обучающемуся, если количество правильных ответов на вопросы – 89 – 76% от общего объёма заданных вопросов;
- оценка **«удовлетворительно»** выставляется обучающемуся, если количество правильных ответов на тестовые вопросы – 75–60 % от общего объёма заданных вопросов;
- оценка **«неудовлетворительно»** выставляется обучающемуся, если количество правильных ответов – менее 60% от общего объёма заданных вопросов.

Критерии формирования оценок по зачету

«Зачтено» – обучающийся демонстрирует знание всех разделов изучаемой дисциплины: содержание базовых понятий и фундаментальных проблем; умение излагать программный материал с демонстрацией конкретных примеров. Свободное владение материалом должно характеризоваться логической ясностью и четким видением путей применения полученных знаний в практической деятельности, умением связать материал с другими отраслями знания. Данная оценка выставляется при условии выполнения студентом всех лабораторных работ и не менее 80% обучающих элементов,

входящих в учебно-методический комплекс изучаемой дисциплины, а именно: практических работ, прохождения промежуточного тестирования и форум-опросов с правильным количеством ответов – 100 – 75 % от общего объёма заданных тестовых вопросов.

«Не зачтено» – выставляется в том случае, когда обучающийся демонстрирует фрагментарные знания основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем. У обучающегося слабо выражена способность к самостоятельному аналитическому мышлению, имеются

затруднения в изложении материала, отсутствуют необходимые умения и навыки, допущены грубые ошибки и незнание терминологии, отказ отвечать на дополнительные вопросы, знание которых необходимо для получения положительной оценки. Данная оценка выставляется при условии не выполнения студентом 80% всех обучающих элементов, входящих в учебно-методический комплекс

изучаемой дисциплины, а именно: лабораторных и практических работ, форум-опросов, прохождения промежуточного тестирования с правильным количеством ответов 59 % и менее от общего объёма заданных тестовых вопросов.

Кроме того, выбор значения балла-оценки может быть сделан преподавателем по данным балльно-рейтинговой системы, которая формируется автоматически при ведении электронного журнала.