МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ

Приложение
к рабочей программе дисциплины

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Защита информации

(наименование дисциплины (модуля)

Направление подготовки / специальность

09.03.01 Информатика и вычислительная техника

(код и наименование)

Направленность (профиль) / специализация

«Проектирование АСОИУ на транспорте»

(наименование)

Содержание

1. Пояснительная записка

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

Формы промежуточной аттестации: зачет в 8 семестре.

Перечень компетенций, формируемых в процессе освоения дисциплины

Код и наименование компетенции	Код индикатора достижения компетенции
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.2: Применять методы защиты информации при выполнении задач профессиональной обязанностей

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

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные материалы
ОПК-3.2: Применяет методы защиты информации при выполнении задач профессиональной деятельности	Обучающийся знает: основы теории чисел	Вопросы 1-10
	Обучающийся умеет: производить вычисления с большими числами	Задания 1-6
	Обучающийся владеет: методами модальной арифметики	Задания 7-12

Промежуточная аттестация (зачет) проводится в одной из следующих форм:
1) собеседование;
2) выполнение заданий в ЭИОС СамГУПС.

2. Типовые[1] контрольные задания или иные материалы для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих уровень сформированных компетенций

2.1 Типовые вопросы для оценки знаний образовательного результата

Проверяемый образовательный результат:

Код и наименование компетенции	Образовательный результат
ОПК-3.2: Применяет методы защиты информации при выполнении задач профессиональной деятельности	Обучающийся знает: основы теории чисел
Вопросы: 1. Основы шифрования и алгоритма RSA 2. Сравнения по модулю и арифметика остатков 3. Алгоритм Эвклида 4. Расширенный алгоритм Эвклида 5. Разложение на множители 6. Алгоритм Ферма разложения на множители 7. Фундаментальное свойство простых чисел 8. Числа Кармайкла и тест Миллера 9. Числа Мерсенна. Числа Ферма 10. Решето Эратосфена	

2.2 Типовые задания для оценки навыков образовательного результата

Проверяемый образовательный результат:

Код и наименование индикатора достижения компетенции	Образовательный результат
ОПК-3.2: Применяет методы защиты информации при выполнении задач профессиональной деятельности	Обучающийся умеет: производить вычисления с большими числами
Задания: 1 Определение простых чисел Задание: выбрать алгоритм факторизации и тест факторизации Задание: Получить модуль числа и сформировать классы; показать приемами модальной арифметики корректную принадлежность результатов к классам 3 Китайская теорема об остатках Задание: решить модальное уравнение 4. Тема «Вычисление символа Якоби» Задание: решить представление числа, определить четность чисел и значение символа Якоби 5. Тема «Криптография с открытым ключом» Задание: выбрать основание и модуль; сгенерировать закрытый ключ; провести факторизацию ключа; формировать открытый ключ- 6. Тема «Тест Соловэя-Штрассена» Задание: вычислить «вероятностно-простое» свойство числа, вычислить символ Якоби и сделать заключение о результате теста	
ОПК-3.2: Применяет методы защиты информации при выполнении задач профессиональной деятельности	Обучающийся владеет: методами модальной арифметики
Задания:	

[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.

7. Тема «Метод квадратичного решета»
Задание: вычислить факторную базу, составить элементы решета
8. Тема «Криптография с открытым ключом»
Задание: решение НОД алгоритмом Евклида, шифрование/дешифрование сообщений
9. Тема «Факторизация методом Ферма»
Задание: факторизовать заданное число, оформить ход факторизации таблично.
10. Тема «Тест Миллера-Рабина»
Задание: подготовить предварительные данные для итераций метода, показать, что тест Миллера-Рабина эффективней, чем тест Ферма
11. Тема «Факторизация (p-1) – метод Полларда»
Задание: решить каноническое разложение числа на простые множители, выполнить НОД факторизации по Полларду
12 Тема «Криптографическая обработка блока текста»
Задание: выбрать блок текста; назначить символ-разделения блоков; указать на соизмеримость модуля кодировки и длины кодируемого блока

2.3. 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

Примечание: по усмотрению преподавателя, вопросы на зачете могут быть заменены требованием решения практических задач, аналогичных примерам лабораторных работ.

3. Методические материалы, определяющие процедуру и критерии оценивания сформированных 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 результатам выполнения заданий

«Отлично/зачтено» – ставится за работу, выполненную полностью без ошибок и недочетов.

«Хорошо/зачтено» – ставится за работу, выполненную полностью, но при наличии в ней не более одной негрубой ошибки и одного недочета, не более трех недочетов.

«Удовлетворительно/зачтено» – ставится за работу, если обучающийся правильно выполнил не менее 2/3 всей работы или допустил не более одной грубой ошибки и двух недочетов, не более одной грубой и одной негрубой ошибки, не более трех негрубых ошибок, одной негрубой ошибки и двух недочетов.

«Неудовлетворительно/не зачтено» – ставится за работу, если число ошибок и недочетов превысило норму для оценки «удовлетворительно» или правильно выполнено менее 2/3 всей работы.

Виды ошибок:

- *грубые ошибки: незнание основных понятий, правил, норм; незнание приемов решения задач; ошибки, показывающие неправильное понимание условия предложенного задания.*
- *негрубые ошибки: неточности формулировок, определений; нерациональный выбор хода решения.*
- *недочеты: нерациональные приемы выполнения задания; отдельные погрешности в формулировке выводов; небрежное выполнение задания.*

Критерии формирования оценок по зачету

«Зачтено» - обучающийся демонстрирует знание основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем; приобрел необходимые умения и навыки, освоил вопросы практического применения полученных знаний, не допустил фактических ошибок при ответе, достаточно последовательно и логично излагает теоретический материал, допуская лишь незначительные нарушения последовательности изложения и некоторые неточности.

«Не зачтено» - выставляется в том случае, когда обучающийся демонстрирует фрагментарные знания основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем. У экзаменуемого 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.