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.
2. Типовые контрольные задания или иные материалы для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих уровень формирования компетенций.
3. Методические материалы, определяющие процедуру и критерии оценивания формирования 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: 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 |
| УК-10: Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности | УК-10.1 Раскрывает механизм проявления коррупционного поведения и определяет способы противодействия ему в профессиональной деятельности |
| УК-10.2 Обосновывает правовыми средствами свою гражданскую позицию в отношении терроризма и экстремизма и применяет способы противодействия им в профессиональной сфере |

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 |
| УК-10.1 Раскрывает механизм проявления коррупционного поведения и определяет способы противодействия ему в профессиональной деятельности | Обучающийся знает: способы и средства защиты информации от утечки по техническим каналам; организацию защиты информации от утечки по техническим каналам на объектах информатизации | Вопросы 11-19 |
| Обучающийся умеет: оценивать коррупционные риски в части защиты информации на объектах информатизации | Задания 13-15 |
| Обучающийся владеет: методами и средствами технической защиты информации на объектах информатизации | Задания 16-20 |
| УК-10.2 Обосновывает правовыми средствами свою гражданскую позицию в отношении терроризма и экстремизма и применяет способы противодействия им в профессиональной сфере | Обучающийся знает: антикоррупционные стандарты, основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы | Вопросы 19-25 |
| Обучающийся умеет: идентифицировать коррупционные риски в части защиты информации на объектах информатизации | Ситуационная задача |
| Обучающийся владеет: методами выявления проблем в организации технической защиты информации | Задания 21-23 |

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

1) собеседование;

2) выполнение заданий в ЭИОС СамГУПС.

**2. Типовые[[1]](#footnote-3) 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 RSA2. Сравнения по модулю и арифметика остатков3. Алгоритм Эвклида4. Расширенный алгоритм Эвклида5. Разложение на множители6. Алгоритм Ферма разложения на множители7. Фундаментальное свойство простых чисел8. Числа Кармайкла и тест Миллера9. Числа Мерсенна. Числа Ферма10. Решето Эратосфена  |
| УК-10.1 Раскрывает механизм проявления коррупционного поведения и определяет способы противодействия ему в профессиональной деятельности | Обучающийся знает: способы и средства защиты информации от утечки по техническим каналам; организацию защиты информации от утечки по техническим каналам на объектах информатизации |
| *Примерные вопросы:*11. Анализ уязвимостей системы 12. Классификация угроз информационной безопасности 13. Основные направления и методы реализации угроз 14. Неформальная модель нарушителя 15. Методы оценки уязвимости системы 16. Причины и виды утечки информации 17. Классификация каналов утечки информации 18. Технические каналы утечки информации 19. Информационные каналы утечки информации |
| УК-10.2 Обосновывает правовыми средствами свою гражданскую позицию в отношении терроризма и экстремизма и применяет способы противодействия им в профессиональной сфере | Обучающийся знает: антикоррупционные стандарты, основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы |
| *Примерные вопросы:*20. Содержание антикоррупционных стандартов .21. Обязанности государственных служащих в сфере противодействия коррупции 22. Ограничения23. Запреты 24.Требования к служебному поведению 25. Ответственность за несоблюдение ограничений, запретов, обязанностей, установленных в целях противодействия коррупции |

**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 чиселЗадание: выбрать алгоритм факторизации и тест факторизацииЗадание: Получить модуль числа и сформировать классы; показать приемами модальной арифметики корректную принадлежность результатов к классам3 Китайская теорема об остаткахЗадание: решить модальное уравнение4. Тема «Вычисление символа Якоби»Задание: решить представление числа, определить четность чисел и значение символа Якоби5. 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:*7. Тема «Метод квадратичного решета»Задание: вычислить факторную базу, составить элементы решета8. 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 Ферма11. Тема «Факторизация (p-1) – метод Полларда»Задание: решить каноническое разложение числа на простые множители, выполнить НОД факторизации по Полларду12 Тема «Криптографическая обработка блока текста»Задание: выбрать блок текста; назначить символ-разделения блоков; указать на соизмеримость модуля кодировки и длины кодируемого блока |
| УК-10.1 Раскрывает механизм проявления коррупционного поведения и определяет способы противодействия ему в профессиональной деятельности | Обучающийся умеет: оценивать коррупционные риски в части защиты информации на объектах информатизации |
| *Задания:*13. Определите наиболее коррупционноемкие направления деятельности организации N.14. Составьте Формализованное описание (карту) направлений деятельности организации N и составляющих их бизнес-процессов и подпроцессов. Карту рекомендуется дополнить результатами предварительного анализа возможных коррупционных правонарушений.15. Предложите модель угроз информационной безопасности организации N, описывающую угрозы информационной безопасности для всех выделенных в организации типов объектов среды и на всех уровнях иерархии информационной инфраструктуры. |
| УК-10.1 Раскрывает механизм проявления коррупционного поведения и определяет способы противодействия ему в профессиональной деятельности | Обучающийся владеет: методами и средствами технической защиты информации на объектах информатизации |
| *Задания:*16. ТемаМатематическая модель канала акустической утечки информации.17. Тема Математическая модель канала утечки информации применительно к техническим разведкам.18. Тема Автоматизация процессов охраны.19. Тема Система контроля и управления доступом.20. Тема Принципы работы системы видеонаблюдения и ее проектирование. |
| УК-10.2 Обосновывает правовыми средствами свою гражданскую позицию в отношении терроризма и экстремизма и применяет способы противодействия им в профессиональной сфере | Обучающийся умеет: идентифицировать коррупционные риски в части защиты информации на объектах информатизации |
| *Ситуационная задача*На основе процессной модели представьте все направления деятельности организации N в форме бизнес-процессов. Идентифицируйте коррупционных риски путем выделения в каждом анализируемом бизнес-процессе критических точек и общего описания возможностей для реализации коррупционных рисков в каждой критической точке. |
| УК-10.2 Обосновывает правовыми средствами свою гражданскую позицию в отношении терроризма и экстремизма и применяет способы противодействия им в профессиональной сфере | Обучающийся владеет: методами выявления проблем в организации технической защиты информации |
| *Задания:*21. Тема Звукоизоляция помещений системы зашумления.22. Тема Реализация защиты от утечки по цепям электропитания и заземления.23. Тема Разработка основной документации по инженерно-технической защите информации.  |

**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.

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. [↑](#footnote-ref-3)