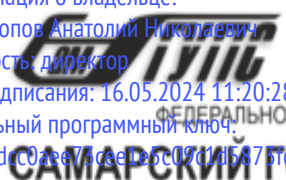


Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Попов Анатолий Николаевич  
Должность: директор  
Дата подписания: 16.05.2024 11:20:28  
Уникальный программный ключ:  
1e0c38dccc0aee71dce1e6c09d1d5875tc7497bc8



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

Приложение 2  
к рабочей программе дисциплины

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ  
ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

**Информационная безопасность**  
*(наименование дисциплины(модуля))*

Направление подготовки / специальность

**09.03.03 Прикладная информатика**  
*(код и наименование)*

Направленность (профиль)/специализация

**Прикладная информатика на железнодорожном транспорте**  
*(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.

### Перечень компетенций, формируемых в процессе освоения дисциплины

Код и наименование 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-3.1 Решает стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-3.2 Применяет методы защиты информации при выполнении задач профессиональной деятельности
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью
ОПК-4.1 Применяет стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
ОПК-4.2 Оформляет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам

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

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные материалы
ОПК-3.1 Решает стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	<b>ОПК-3.1.1</b> Обучающийся знает: способы и средства защиты информации от утечки по техническим каналам; организацию защиты информации от утечки по техническим каналам на объектах информатизации	Тесты 1-5
	<b>ОПК-3.1.2</b> Обучающийся умеет: оценивать коррупционные риски в части защиты информации на объектах информатизации	Задания 1-3
	<b>ОПК-3.1.3</b> Обучающийся владеет: методами и средствами технической защиты информации на объектах информатизации	Задания 4-8
ОПК-3.2 Применяет методы защиты информации при выполнении задач профессиональной деятельности	<b>ОПК-3.2.1</b> Обучающийся знает: антикоррупционные стандарты, основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	Тесты 6-10

	<b>ОПК-3.2.2</b> Обучающийся умеет: идентифицировать коррупционные риски в части защиты информации на объектах информатизации	Ситуационная задача
	<b>ОПК-3.2.3</b> Обучающийся владеет: методами выявления проблем в организации технической защиты информации	Задания 9-11
ОПК-4.1 Применяет стандарты оформления технической документации на различных стадиях жизненного цикла	<b>ОПК-4.1.1</b> Обучающийся знает: основы теории чисел	Вопросы 1-10
	<b>ОПК-4.1.2</b> Обучающийся умеет: производить вычисления с большими числами	Задания 12-15
	<b>ОПК-4.1.3</b> Обучающийся владеет: методами модальной арифметики	Задания 16-21
ОПК-4.2 Оформляет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам	<b>ОПК-4.2.1</b> Обучающийся знает: методы защиты информации	Тесты 11-15
	<b>ОПК-4.2.2</b> Обучающийся умеет: Применяет методы защиты информации при выполнении задач профессиональной деятельности	Вопросы 11-19
	<b>ОПК-4.2.3</b> Обучающийся владеет: Навыками применения методов защиты информации при выполнении задач профессиональной деятельности	Вопросы 20-25

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

- 1) собеседование;
- 2) выполнение заданий в ЭИОС СамГУПС.

## 2. Типовые<sup>1</sup> 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 компетенции	Образовательный результат
ОПК-3.1.1	Обучающийся знает: способы и средства защиты информации от утечки по техническим каналам; организацию защиты информации от утечки по техническим каналам на объектах информатизации
<p>1. Что из ниже перечисленного относится к проблемам информации (<i>выберите несколько вариантов ответа</i>)?</p> <ol style="list-style-type: none"> <li>1) обеспечение целостности;</li> <li>2) обеспечение неделимости;</li> <li>3) обеспечение достоверности;</li> <li>4) обеспечение чистоты;</li> <li>5) обеспечение защиты от различного вида угроз.</li> </ol> <p>2. Процесс обеспечения информационных потребностей общества на основе применения новейших информационных технологий — это...</p> <ol style="list-style-type: none"> <li>1) компьютеризация;</li> <li>2) информатика;</li> </ol>	

<sup>1</sup>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.

- 3) информатизация;
- 4) информационная индустрия;
- 5) автоматизация.

3. Информационная система — это...

- 1) посредник между потребителем информации и информационным массивом;
- 2) ряд компьютеров, объединенных в локальную сеть;
- 3) совокупность технических средств обработки информации;
- 4) группа людей, ответственная за обработку, накопление, хранение и выдачу информации;
- 5) средства массовой информации, функционирующие на территории определенного государства.

4. Какие свойства информации являются наиболее важными в практическом применении (выберите несколько вариантов ответа)?

- 1) ценность;
- 2) популярность;
- 3) достоверность;
- 4) чистота;
- 5) своевременность.

5. Что является основной причиной старения информации?

- 1) физическая изношенность носителя;
- 2) появление новой информации, с поступлением которой прежняя информация оказывается неверной;
- 3) устаревание знаковой системы, посредством которой выражена информация;
- 4) уменьшение потребности в информации;
- 5) величина длительности хранения информации: чем больше длительность, тем информация старше.

**ОПК-3.2 .1**

Обучающийся знает: антикоррупционные стандарты, основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы

6. Совокупность взаимосвязанных и взаимообусловленных процессов выявления, анализа, ввода и отбора информации, выдачи с помощью различных средств ее потребителю для принятия управленческого решения — это...

- 1) процессы обработки информации;
- 2) циркуляция информации;
- 3) информационные процессы;
- 4) процессы перераспределения информации;
- 5) вычислительные процессы.

7. Организационно-упорядоченная совокупность людей, информационных ресурсов, технических средств и технологий обработки информации, имеющая своей целью сбор, обработку, накопление, хранение, актуализацию, поиск и выдачу информации — это...

- 1) автоматизированная инфраструктура;
- 2) информационная система;
- 3) информационная структура;
- 4) автоматизированная система;
- 6) информационный ресурс.

8. Что понимается под безошибочностью данных?

- 1) свойство данных не иметь явных ошибок;
- 2) свойство данных полностью соответствовать области их применения;
- 3) свойство данных не иметь скрытых случайных ошибок;
- 4) свойство данных соответствовать нескольким областям человеческой деятельности;
- 5) свойство данных не иметь противоречий в собственной структуре;

9. Назовите свойство данных, которое заключается в том, что время их сбора и переработки соответствует динамике изменения ситуации:

- 1) идентичность;
- 2) оперативность;
- 3) динамичность;
- 4) адаптивность;

5) актуальность.	
10. Каким свойством обладают данные, соответствующие состоянию объекта (явления)?	
1) идентичность; 2) объективность; 3) эквивалентность; 4) неотрывность; 5) целостность.	
ОПК- 4.2.1	Обучающийся знает: методы защиты информации
11. Что является источником информации, обладающей свойством «общественная природа»?	
1) живые организмы, несущие в своем строении определенную биологическую информацию; 2) структура и состояние современного общества; 3) отношения между людьми; 4) познавательная деятельность людей, общества; 5) состояние окружающей среды.	
12. Что подразумевается под целостностью информации (выберите не-сколько вариантов ответа)?	
1) принадлежность информации одному источнику; 2) неделимость информации; 3) актуальность информации; 4) непротиворечивость информации; 5) защищенность информации от разрушения и несанкционированного изменения.	
13. Меры каких уровней необходимо принимать при обеспечении защиты интересов субъектов информационных отношений?	
1) социального; 2) законодательного; 3) исполнительного; 4) административного; 5) экономического; 6) процедурного; 7) функционального; 8) программно-технического; 9) программно-аппаратного.	
14. Что относится к основным составляющим информационной безопасности (выберите несколько вариантов ответа)?	
1) защита информации; 2) компьютерная безопасность; 3) экологическая безопасность; 4) защищенность информации и поддерживающей инфраструктуры; 5) защита от информации; 6) защищенность потребностей граждан.	
15. Что относится к первоочередным задачам защиты информации (выберите несколько вариантов ответа)?	
1) обеспечение качества информационных ресурсов; 2) обеспечение целостности информационных ресурсов; 3) обеспечение доступности информационных ресурсов; 4) обеспечение надежности информационных ресурсов; 5) обеспечение конфиденциальности информационных ресурсов.	
ОПК-4.1.1	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 навыкового образовательного результата

Проверяемый образовательный результат:

Код и наименование компетенции	Образовательный результат
ОПК-3.1.2	Обучающийся умеет: оценивать коррупционные риски в части защиты информации на объектах информатизации
<p>Задания:</p> <ol style="list-style-type: none"> <li>1. Определите наиболее коррупционнoемкие направления деятельности организации N.</li> <li>2. Составьте Формализованное описание (карту) направлений деятельности организации N и составляющих их бизнеспроцессов и подпроцессов. Карту рекомендуется дополнить результатами предварительного анализа возможных коррупционных правонарушений.</li> <li>3. 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.</li> </ol>	
ОПК-3.2.3	Обучающийся владеет: методами и средствами технической защиты информации на объектах информатизации
<p>Задания:</p> <ol style="list-style-type: none"> <li>4. Тема Математическая модель канала акустической утечки информации.</li> <li>5. Тема Математическая модель канала утечки информации применительно к техническим разведкам.</li> <li>6. Тема Автоматизация процессов охраны.</li> <li>7. Тема Система контроля и управления доступом.</li> <li>8. Тема Принципы работы системы видеонаблюдения и ее проектирование.</li> </ol>	
ОПК-3.2.2	Обучающийся умеет: идентифицировать коррупционные риски в части защиты информации на объектах информатизации
<p>Ситуационная задача</p> <p>На основе процессной модели представьте все направления деятельности организации N в форме бизнес-процессов.</p> <p>Идентифицируйте коррупционных риски путем выделения в каждом анализируемом бизнес-процессе критических точек и общего описания возможностей для реализации коррупционных рисков в каждой критической точке.</p>	
ОПК-3.2.3	Обучающийся владеет: методами выявления проблем в организации технической защиты информации
<p>Задания:</p> <ol style="list-style-type: none"> <li>9. Тема Звукоизоляция помещений системы шумления.</li> <li>10. Тема Реализация защиты от утечки по цепям электропитания и заземления.</li> <li>11. Тема Разработка основной документации по инженерно-технической защите информации.</li> </ol>	
ОПК-4.2.2	Обучающийся умеет: Применяет методы защиты информации при выполнении задач профессиональной деятельности

<p>Примерные вопросы:</p> <ol style="list-style-type: none"> <li>11. Анализ уязвимостей системы</li> <li>12. Классификация угроз информационной безопасности</li> <li>13. Основные направления и методы реализации угроз</li> <li>14. Неформальная модель нарушителя</li> <li>15. Методы оценки уязвимости системы</li> <li>16. Причины и виды утечки информации</li> <li>17. Классификация каналов утечки информации</li> <li>18. Технические каналы утечки информации</li> <li>19. Информационные каналы утечки информации</li> </ol>	
ОПК-4.2.3	Обучающийся владеет: Навыками применения методов защиты информации при выполнении задач профессиональной деятельности
<p>Примерные вопросы:</p> <ol style="list-style-type: none"> <li>20. Содержание антикоррупционных стандартов.</li> <li>21. Обязанности государственных служащих в сфере противодействия коррупции</li> <li>22. Ограничения</li> <li>23. Запреты</li> <li>24. Требования к служебному поведению</li> <li>25. Ответственность за несоблюдение ограничений, запретов, обязанностей, установленных в целях противодействия коррупции</li> </ol>	
ОПК-4.1.2	Обучающийся умеет: производить вычисления с большими числами
<p>Задания:</p> <ol style="list-style-type: none"> <li>12. 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</li> <li>13. Китайская теорема об остатках Задание: решить модальное уравнение</li> <li>14. Тема «Вычисление символа Якоби» Задание: решить представление числа, определить четность чисел и значение символа Якоби</li> <li>15. Тема «Криптография с открытым ключом» Задание: выбрать основание и модуль; сгенерировать закрытый ключ; провести факторизацию ключа; сформировать открытый ключ. Тема «Тест Соловья-Штрассена» Задание: вычислить «вероятностно-простое» свойство числа, вычислить символ Якоби и сделать заключение о результате теста</li> </ol>	
ОПК-4.1.3	Обучающийся владеет: методами модальной арифметики
<p>Задания:</p> <ol style="list-style-type: none"> <li>16. Тема «Метод квадратичного решета» Задание: вычислить факторную базу, составить элементы решета</li> <li>17. Тема «Криптография с открытым ключом» Задание: решение НОД алгоритмом Евклида, шифрование/дешифрование сообщений</li> <li>18. Тема «Факторизация методом Ферма» Задание: факторизовать заданное число, оформить ход факторизации таблично.</li> <li>19. Тема «Тест Миллера-Рабина» Задание: подготовить предварительные данные для итераций метода, показать, что тест Миллера-Рабина эффективней, чем тест Ферма</li> <li>20. Тема «Факторизация (p-1) – метод Полларда» Задание: решить каноническое разложение числа на простые множители, выполнить НОД факторизации по Полларду</li> <li>21. Тема «Криптографическая обработка блока текста» Задание: выбрать блок текста; назначить символ-разделения блоков; указать на соизмеримость модуля</li> </ol>	



### **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 подгруп. 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 объема заданных вопросов;
- оценка **«хорошо»** выставляется обучающемуся, если количество правильных ответов на вопросы – 89 – 76% от общего объема заданных вопросов;
- оценка **«удовлетворительно»** выставляется обучающемуся, если количество правильных ответов на тестовые вопросы – 75–60 % от общего объема заданных вопросов;
- оценка **«неудовлетворительно»** выставляется обучающемуся, если количество правильных ответов – менее 60% от общего объема 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 с оценкой**

**«Отлично/зачтено»** – студент приобрел необходимые умения и навыки, продемонстрировал навык практического применения полученных знаний, не допустил логических и фактических ошибок

**«Хорошо/зачтено»** – студент приобрел необходимые умения и навыки, продемонстрировал навык практического применения полученных знаний; допустил незначительные ошибки и неточности.

**«Удовлетворительно/зачтено»** – студент допустил существенные ошибки.

**«Неудовлетворительно/не зачтено»** – студент демонстрирует фрагментарные знания изучаемого курса; отсутствуют необходимые умения и навыки, допущены грубые ошибки.

Экспертный лист  
оценочных материалов для проведения промежуточной аттестации по  
дисциплине «Основы информационной безопасности»

Направление подготовки / специальность

**09.03.03 Прикладная информатика**  
(код и наименование)

Направленность (профиль)/специализация

**Прикладная информатика на железнодорожном транспорте**  
(наименование)

**Бакалавр**  
квалификация выпускника

1. Формальное оценивание			
Показатели		Присутствуют	Отсутствуют
Наличие обязательных структурных элементов:		+	
– титульный лист		+	
– пояснительная записка		+	
– типовые оценочные материалы		+	
– методические материалы, определяющие процедуру и критерии оценивания		+	
Содержательное оценивание			
Показатели	Соответствует	Соответствует частично	Не соответствует
Соответствие требованиям ФГОС ВО к результатам освоения программы	+		
Соответствие требованиям ОПОП ВО к результатам освоения программы	+		
Ориентация на требования к трудовым функциям ПС (при наличии утвержденного ПС)	+		
Соответствует формируемым компетенциям, индикаторам достижения компетенций	+		

Заключение: ФОС рекомендуется/ не рекомендуется к внедрению; обеспечивает/ не обеспечивает объективность и достоверность результатов при проведении оценивания результатов обучения; критерии и показатели оценивания компетенций, шкалы оценивания обеспечивают/ не обеспечивают проведение всесторонней оценки результатов обучения.

Эксперт, должность, ученая степень, ученое звание \_\_\_\_\_ /

(подпись)