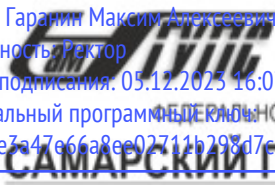


Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гарант Максим Алексеевич
Должность: Ректор
Дата подписания: 05.12.2023 16:07:49
Уникальный программный ключ:
7708e7a47e66a8ee02711b298d7e78bd1e40bf88

 **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 в информационных системах

(наименование дисциплины(модуля))

09.04.02 Информационные системы технологии

(код и наименование)

Цифровые технологии в образовании

(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: Использует информационные технологии защиты информации в области её получения, передачи, хранения, переработки и представления

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 информационные технологии защиты информации в области её получения, передачи, хранения, переработки и представления	Обучающийся знает: средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации	Вопросы (№1 - №5) Тестовые задания 1-5
	Обучающийся умеет: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения	Задания (№1 - №6)
	Обучающийся владеет: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической 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 информационные технологии защиты информации в области её получения, передачи, хранения, переработки и представления	Обучающийся знает: средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации
<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	
<i>Тестовые задания</i> 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.	

2.2 Типовые задания для оценки навыкового образовательного результата

Проверяемый образовательный результат:

Код и наименование индикатора достижения компетенции	Образовательный результат
--	---------------------------

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.

<p>ОПК-6.2: Использует информационные технологии защиты информации в области её получения, передачи, хранения, переработки и представления</p>	<p>Обучающийся умеет: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения</p>
<p>ОПК-6.2: Использует информационные технологии защиты информации в области её получения, передачи, хранения, переработки и представления</p>	<p>Обучающийся владеет: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации</p>
<p>Задание 1 Используя ГОСТ Р ИСО/МЭК 27002-2012, решить ситуационную задачу. Вы – начальник отдела по вопросам информационной безопасности в некоторой не крупной организации (20-30 человек). Вам необходимо разработать комплекс мероприятий (от 10 до 20) по следующему направлению: привлечение сторонних организаций к обработке информации. Цель: обеспечение информационной безопасности при передаче ответственности за обработку информации другой организации. Изучить разделы ГОСТ Р ИСО/МЭК 27002-2012.</p> <p>Задание 2 Вы – начальник отдела по вопросам информационной безопасности в некоторой не крупной организации (20-30 человек). Вам необходимо разработать требования к хранению, использованию и утилизации информации для вашей организации. Цель: обеспечение информационной безопасности при хранении, обработке, передаче и уничтожении информации.</p> <p>Задание 3 1. Создайте файл virus.doc (содержание – чистый лист) и выполните алгоритм восстановления файла (в предположении его заражения макровирусом). 2. Зафиксируйте этапы работы, используйте команду PrintScreen клавиатуры (скопированные таким образом файлы вставьте в новый Wordдокумент для отчета). 3. Сравните размеры файлов virus.doc и virus.rtf, используйте пункты контекстного меню «Свойства» (для этого выделите в «Проводнике» файл, нажмите правую кнопку мыши и выберите пункт «Свойства»).</p> <p>Задание 4 1. Посетить сайты наиболее известных разработчиков антивирусных программ: - Антивирус Касперского (http://www.kaspersky.ru/), - Доктор Web (http://www.drweb.com/), - NOD32 (http://www.esetnod32.ru/), - Avast! (http://www.avast-russia.com/). 2. Исходя из информации, представленной на сайтах разработчиков антивирусного ПО, проанализировать виды угроз, от которых гарантированно предоставляется защита. Анализ проводить по параметрам защиты от: 1) мошеннического ПО; 2) хакерских атак; 3) фишинга; 4) спама. Результаты представить в виде статистической гистограммы, используя средства программного продукта MS Excel. На основе полученных результатов выбрать антивирусное ПО для реализации политики безопасности компании. Привести обоснование выбора в виде сравнительного отчета выбранного продукта с остальными продуктами по следующим показателям: а) стоимость; б) надежность; в) устойчивость; г) простота использования; д) наличие специальных предложений. 3. Изучить настройки антивирусной программы (Антивирус Касперского, DrWeb... – по выбору). 4. Запустите антивирусную программу и выполните проверку оперативной памяти компьютера на наличие</p>	

вирусов.

Выполните тестирование дисков D: и C: на наличие вирусов. Если на дисках будут обнаружены вирусы, выполните лечение зараженных файлов.

Задание 5

1. Настройте параметры локальной политики безопасности операционной системы
2. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль.
3. После успешного выполнения предыдущего задания измените пароль вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.
4. Проведите эксперименты с другими параметрами «Политики учетных записей».

Задание 6

1. Изучить теоретические основы шифрования шифрами простой замены (методом Цезаря и методом перестановки).
2. Зашифровать методом Цезаря предложение открытого текста для шифрования в соответствии с номером своего варианта.
3. Зашифровать (и расшифровать) методом перестановки одно слово открытого текста ключом, длина которого равна длине шифруемого слова. Слово задает преподаватель.
4. Придумать символьный пароль, преобразовать его в ключ и зашифровать (и расшифровать) фразу открытого текста с помощью этого ключа.

Выберите предложение открытого текста для шифрования:

1. От добра добра не ищут.
2. Кто рано встает, тот долго живет.
3. Худой мир лучше доброй драки.
4. Близок локоть, да не укусишь.

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
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 мене 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.