

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гарант Максим Алексеевич
Должность: Ректор
Дата подписания: 03.11.2023 13:43:07
Уникальный программный ключ:
7708e3a47e66a8ee02711b298d7e78bd1e40bf88

Приложение
к рабочей программе дисциплины

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

Безопасность информационных технологий и систем

(наименование дисциплины(модуля))

09.03.02 Информационные системы и технологии

(код и наименование)

Направленность (профиль)/специализация

Информационные системы и технологии на транспорте

(наименование)

Форма обучения

Очная

Семестр 6 (экзамен)

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: *экзамен в 6 семестре.*

Перечень компетенций, формируемых в процессе освоения дисциплины

Код и наименование компетенции	Код индикатора достижения компетенции
ПК-5. Способен организовывать мониторинг и контроль функционирования инфокоммуникационных систем и сервисов	ПК 5.2. Оценивать наличие и степень нарушения требований обеспечения информационной и функциональной безопасности инфокоммуникационных систем и соответствующих сервисов

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

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные материалы
ПК 5.2. Оценивать наличие и степень нарушения требований обеспечения информационной и функциональной безопасности инфокоммуникационных систем и соответствующих сервисов	Обучающийся знает: принципы и методы организации угроз, компьютерных атак и несанкционированного вторжения; способы и средства защиты информации от утечки по техническим каналам;	Вопросы (1 – 10)
	Обучающийся умеет: прогнозировать угрозы, обнаруживать атаки и вторжения, шифровать данные оценивать коррупционные риски в части защиты информации на объектах информатизации	Задания (1-10)
	Обучающийся владеет: организационными, нормативно-правовыми, программными и техническими средствами защиты компьютерной информации методами и средствами технической защиты информации на объектах информатизации методами выявления проблем в организации технической защиты информации	

Промежуточная аттестация (экзамен) 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
ПК 5.2. Оценивать наличие и степень нарушения требований обеспечения информационной и функциональной безопасности инфокоммуникационных систем и соответствующих сервисов	Обучающийся знает: принципы и методы организации угроз, компьютерных атак и не санкционированного вторжения; - модели безопасности и секретности.
<i>Примеры вопросов/заданий</i> <ol style="list-style-type: none">1. Классификация угроз безопасности.2. Основные методы и средства защиты информации.3. Назначение организационных средств защиты.4. Состав комплекса защиты территории охраняемых объектов.5. Степени секретности и виды конфиденциальности информации.6. Понятие информации, изъятой из оборота, и ограниченной в обороте.7. Назначение средств защиты от НДС.8. Состав системы разграничения доступа.9. Матричная модель системы ЗИ.10. Основные функции системы защиты от НСК.	

2.2 Типовые задания для оценки навыкового образовательного результата

Проверяемый образовательный результат:

Код и наименование индикатора достижения компетенции	Образовательный результат
ПК 5.2. Оценивать наличие и степень нарушения требований обеспечения информационной и функциональной безопасности инфокоммуникационных систем и соответствующих сервисов	Обучающийся умеет и владеет: прогнозировать угрозы, обнаруживать атаки и вторжения, шифровать данные; организационными, нормативно-правовыми, программными и техническими средствами защиты компьютерной информации.
<i>Примеры заданий</i> <p>1 Процесс обеспечения конфиденциальности, целостности и доступности информации – это... противопожарная безопасность экономическая безопасность информационная безопасность национальная безопасность</p> <p>2 К какому аспекту относится следующее определение: “защита от несанкционированного доступа к информации.” доступность целостность конфиденциальность прозрачность</p> <p>3 Какой сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных?</p>	

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.

аутентификация

доступность

целостность

конфиденциальность

4 Какое требование относится к системе защиты информационной безопасности?

постоянность

надежность

комплексность

все перечисленные

5 К случайным угрозам относятся

сбои и отказы технических средств

алгоритмические и программные ошибки

несанкционированный доступ к информации

результаты работы вредительских программ (вирусов)

6 К преднамеренным угрозам относятся

электромагнитные излучения и наводки

несанкционированное модифицирование структур

ошибки пользователей и обслуживающего персонала

ошибки при работе компьютерной системы

7 Правовым обеспечением информационной безопасности является

правила работы с секретными документами

лицензирование

организация охраны помещений

защита компьютера от электромагнитных влияний

8 Организационным обеспечением информационной безопасности является

обеспечение пропускного и внутриобъектового режима на территории, в зданиях и помещениях

защитное заземление оборудования компьютерных сетей

патентование

порядок приема и увольнения рабочих и служащих

9 Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности.

рекомендации X.800

Оранжевая книга

Закон "Об информации, информационных технологиях и о защите информации"

10 Основные угрозы конфиденциальности информации

маскарад

карнавал

переадресовка

перехват данных

блокирование

2.3 . Перечень вопросов для подготовки обучающихся к промежуточной аттестации

1. Основные определения информационной безопасности.
2. Современные аспекты безопасности информационных систем.
3. Понятие «информационная безопасность» и «защита информации».
4. Классификация угроз безопасности.
5. Основные методы и средства защиты информации.
6. Назначение организационных средств защиты.
7. Состав комплекса защиты территории охраняемых объектов.
8. Нормативные документы по лицензированию деятельности.
9. Нормативные документы по сертификации средств защиты.
10. Понятие информационного права.
11. Степени секретности и виды конфиденциальности информации.
12. Понятие информации, изъятой из оборота, и ограниченной в обороте.
13. Понятие ПЭМИН.

14. Методы защиты ПЭВМ от ПЭМИН.
15. Назначение генератора шума.
16. Назначение средств защиты от НДС.
17. Состав системы разграничения доступа.
18. Матричная модель системы ЗИ.
19. Многоуровневые модели ЗИ.
20. Назначение ядра безопасности.
21. Система регистрации.
22. Вредоносное программное обеспечение и средства борьбы с ним.
23. История возникновения компьютерных вирусов. Классификация вирусов.
24. Детекторы и фаги.
25. Вакцины, ревизоры и мониторы.
26. Назначение защиты от НСК.
27. Основные функции системы защиты от НСК.
28. Классификация криптографических систем.
29. Криптографическая защита информации в каналах связи и ПЭВМ.
30. Криптографическая защита. Основные термины криптографии.
31. Электронная цифровая подпись (ЭЦП).
32. Системы идентификации и аутентификации. Основные требования к паролям, используемым в системе информационной безопасности.
33. Методы социальной инженерии и человеческий фактор.
34. Принципы функционирования электронных платежных систем.
35. Электронные пластиковые карты.
36. Персональный идентификационный номер.
37. Универсальная электронная платежная система UEPS.
38. Обеспечение безопасности электронных платежей через сеть Internet.
39. Симметричные криптосистемы.
40. Асимметричные криптосистемы.
41. Гибридные криптосистемы.
42. Симметричные криптосистемы. Классификация шифров.
43. Требования к криптосистемам.
44. Шифры простой перестановки.
45. «Магические квадраты».
46. Система шифрования Цезаря.
47. Система Цезаря с ключевым словом.
48. Шифр Плейфейра.
49. «Двойной квадрат» Уитстона.
50. Шифр Грансфельда.
51. Система Вижинера.
52. Гаммирование.
53. Поточные шифры.
54. Самосинхронизирующиеся шифры.
55. Двухключевые криптосистемы.
56. Система электронной цифровой подписи.
57. Классификация алгоритмов двухключевых систем.
58. Алгоритм RSA.
59. Составные шифры.
60. Алгоритм криптосистемы DES.
61. Отечественный алгоритм шифрования.

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 экзамену

«Отлично» (5 баллов) – 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.

«Хорошо» (4 балла) – обучающийся демонстрирует знания всех разделов изучаемой дисциплины: содержание 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. Таким образом данная оценка выставляется за правильный, но недостаточно полный ответ.

«Удовлетворительно» (3 балла) – обучающийся демонстрирует знание основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем. Однако знание основных проблем курса не подкрепляются конкретными практическими примерами, не полностью раскрыта сущность вопросов, ответ недостаточно логичен и не всегда последователен, допущены ошибки и неточности.

«Неудовлетворительно» (0 баллов) – 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.