

**Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Национальный исследовательский университет «МЭИ»**

Направление подготовки/специальность: 09.03.01 Информатика и вычислительная техника

Наименование образовательной программы: Вычислительные машины, комплексы, системы и сети

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

**Оценочные материалы
по дисциплине
Методы и средства защиты информации**

**Москва
2024**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Пайков А.С.
	Идентификатор	R02d5e50d-PaikovAS-2468ee70

А.С. Пайков

СОГЛАСОВАНО:

Руководитель
образовательной
программы

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Гольцов А.Г.
	Идентификатор	R64210572-GoltsovAG-cebbd3e8

А.Г. Гольцов

Заведующий
выпускающей кафедрой

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Вишняков С.В.
	Идентификатор	R35b26072-VishniakovSV-02810d9

С.В.
Вишняков

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ПК-1 Способен обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности
ИД-3 Производит оценку влияния применяемых технических решений на общее функционирование системы
2. ПК-2 Способен решать вопросы управления безопасностью сетевых устройств и программного обеспечения при их проектировании
ИД-1 Демонстрирует знание нормативной базы, методов описания, анализа и проектирования в области обеспечения безопасности информационных систем и компьютерной криптографии
ИД-2 Демонстрирует знание методов и средств обеспечения защиты носителей информации, ЭВМ и компьютерных сетей от несанкционированного доступа
ИД-4 Осуществляет разработку аппаратных и программных средств, необходимых для обеспечения безопасности компьютерных систем

и включает:

для текущего контроля успеваемости:

Форма реализации: Соблюдение графика выполнения задания

1. Контроль посещения лекций №1-2 по курсу МСЗИ; Контроль выполнения лабораторной работы №1 по курсу МСЗИ (25%) (Лабораторная работа)
2. Контроль посещения лекций №3-4 по курсу МСЗИ; Контроль выполнения лабораторной работы №2 по курсу МСЗИ (25%) (Лабораторная работа)
3. Контроль посещения лекций №5-6 по курсу МСЗИ; Контроль выполнения лабораторной работы №3 по курсу МСЗИ (25%) (Лабораторная работа)
4. Контроль посещения лекций №7-8 по курсу МСЗИ; Контроль выполнения лабораторной работы №4 по курсу МСЗИ (25%) (Лабораторная работа)

БРС дисциплины

7 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

- | | |
|------|--|
| КМ-1 | Контроль посещения лекций №1-2 по курсу МСЗИ; Контроль выполнения лабораторной работы №1 по курсу МСЗИ (25%) (Лабораторная работа) |
| КМ-2 | Контроль посещения лекций №3-4 по курсу МСЗИ; Контроль выполнения лабораторной работы №2 по курсу МСЗИ (25%) (Лабораторная работа) |
| КМ-3 | Контроль посещения лекций №5-6 по курсу МСЗИ; Контроль выполнения лабораторной работы №3 по курсу МСЗИ (25%) (Лабораторная работа) |

КМ-4 Контроль посещения лекций №7-8 по курсу МСЗИ; Контроль выполнения лабораторной работы №4 по курсу МСЗИ (25%) (Лабораторная работа)

Вид промежуточной аттестации – Зачет с оценкой.

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	16
Основы информационной безопасности: нормативные и технические аспекты					
Основы информационной безопасности: нормативные и технические аспекты	+				
Криптография и защита данных					
Криптография и защита данных			+		
Практические аспекты и современные угрозы					
Практические аспекты и современные угрозы				+	
Аудит и управление информационной безопасностью					
Аудит и управление информационной безопасностью					+
Вес КМ:		25	25	25	25

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ПК-1	ИД-3 _{ПК-1} Производит оценку влияния применяемых технических решений на общее функционирование системы	Знать: способы и технологии применения криптографии в решении задач идентификации и аутентификации, частотные характеристики языков и их использование при построении систем парольной защиты Уметь: использовать современные информационные технологии при решении задач защиты информации; формализовать задачу по защите информации; применять стандарты по оценке защищенности АСОИ при анализе и проектировании систем защиты информации в АСОИ	КМ-1 Контроль посещения лекций №1-2 по курсу МСЗИ; Контроль выполнения лабораторной работы №1 по курсу МСЗИ (25%) (Лабораторная работа) КМ-2 Контроль посещения лекций №3-4 по курсу МСЗИ; Контроль выполнения лабораторной работы №2 по курсу МСЗИ (25%) (Лабораторная работа)
ПК-2	ИД-1 _{ПК-2} Демонстрирует знание нормативной базы,	Знать: методологические и	КМ-1 Контроль посещения лекций №1-2 по курсу МСЗИ; Контроль выполнения лабораторной работы №1 по курсу МСЗИ (25%)

	методов описания, анализа и проектирования в области обеспечения безопасности информационных систем и компьютерной криптографии	технологические основы обеспечения безопасности АСОИ; угрозы и методы нарушения безопасности АСОИ; стандарты по оценке защищенных систем Уметь: обосновывать принимаемые проектные решения; применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач, разрабатывать модели открытого текста различного уровня сложности; проводить обработку открытого текста для подготовки к операциям шифрования	(Лабораторная работа) КМ-2 Контроль посещения лекций №3-4 по курсу МСЗИ; Контроль выполнения лабораторной работы №2 по курсу МСЗИ (25%) (Лабораторная работа)
ПК-2	ИД-2 _{ПК-2} Демонстрирует знание методов и средств обеспечения защиты носителей информации, ЭВМ и компьютерных сетей от несанкционированного доступа	Знать: показатели эффективности принимаемого проектного решения; понятия группы, кольца, поля ; качественные и количественные свойства информации; статистические модели	КМ-1 Контроль посещения лекций №1-2 по курсу МСЗИ; Контроль выполнения лабораторной работы №1 по курсу МСЗИ (25%) (Лабораторная работа) КМ-3 Контроль посещения лекций №5-6 по курсу МСЗИ; Контроль выполнения лабораторной работы №3 по курсу МСЗИ (25%) (Лабораторная работа)

		открытого текста Уметь: – устанавливать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты	
ПК-2	ИД-4 _{ПК-2} Осуществляет разработку аппаратных и программных средств, необходимых для обеспечения безопасности компьютерных систем	Знать: угрозы и методы нарушения безопасности АИС; методы и средства обеспечения защиты носителей информации; методы и алгоритмы уничтожения конфиденциальной информации Уметь: использовать современные инструментальные средства и технологии программирования	КМ-2 Контроль посещения лекций №3-4 по курсу МСЗИ; Контроль выполнения лабораторной работы №2 по курсу МСЗИ (25%) (Лабораторная работа) КМ-4 Контроль посещения лекций №7-8 по курсу МСЗИ; Контроль выполнения лабораторной работы №4 по курсу МСЗИ (25%) (Лабораторная работа)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контроль посещения лекций №1-2 по курсу МСЗИ; Контроль выполнения лабораторной работы №1 по курсу МСЗИ (25%)

Формы реализации: Соблюдение графика выполнения задания

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: При очной форме обучения - заполнение ведомости присутствия в течение лекции. При дистанционной форме обучения - регистрация участников мероприятия в Webex.

Краткое содержание задания:

Проставить в ведомости свою фамилию и подпись. Зарегистрироваться в Webex и присутствовать на лекции.

Пример выполнения (не выполнения) задания:

	А-07-17	Лекции 10						2
		№1	№2					
1	Андиев Олег Казбекович	1	1					10
2	Артюх Владислава Владимировна (В)	1						5
3	Белова Ирина Михайловна	1	1					10
4	Бирман Александр Александрович							0
5	Блаженова Светлана Дмитриевна	1	1					10
6	Журавлёв Антон Александрович	1	1					10
7	Иванов Глеб Александрович (В)	1	1					10
8	Игнатова Анастасия Ильинична	1	1					10
9	Кон Алёна Юрьевна	1	1					10
10	Кузнецова Анастасия Леонидовна	1	1					10

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: способы и технологии применения криптографии в решении задач идентификации и аутентификации, частотные характеристики языков и их использование при построении систем парольной защиты	1.Рекомендуемая литература для изучения курса
Знать: методологические и технологические основы обеспечения безопасности АСОИ; угрозы и методы нарушения безопасности АСОИ; стандарты по оценке защищенных систем	1.Типы секретных систем 2.Уровни секретности информации
Знать: показатели эффективности принимаемого проектного решения; понятия группы, кольца, поля ; качественные и количественные свойства информации; статистические модели открытого текста	1.Как найти CAS Mathematica

Описание шкалы оценивания:

Оценка: 5 («отлично»)

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 2 лекций модуля 1 равно 10. Оценка 5 находится в диапазоне 9-10 баллов.

Оценка: 4 («хорошо»)

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 2 лекций модуля 1 равно 10. Оценка 4 находится в диапазоне 7-8 баллов.

Оценка: 3 («удовлетворительно»)

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 2 лекций модуля 1 равно 10. Оценка 3 находится в диапазоне 4-6 баллов.

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 3 баллов.

При отсутствии на всех лекциях по неуважительным причинам проставляется 0.

КМ-2. Контроль посещения лекций №3-4 по курсу МСЗИ; Контроль выполнения лабораторной работы №2 по курсу МСЗИ (25%)

Формы реализации: Соблюдение графика выполнения задания

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: При очной форме обучения лабораторные работы выполняются в компьютерном классе, в котором доступна сетевая версия Wolfram Mathematica 9. Одна лабораторная работа длится 2 академических часа. Отчет формируется в бумажном варианте. При дистанционной форме обучения лабораторные работы выполняются в Wolfram Cloud | Open Access system. Контроль и консультации в течение лабораторной работы в системе Webex. Рабочее задание и необходимые методические материалы размещаются в системе Moodle. Отчет по выполненной лабораторной работе загружается в систему Moodle, где производится контроль выполнения и выставляется суммарное число баллов по правильно выполненным пунктам рабочего задания.

Краткое содержание задания:

Пример рабочего задания лабораторной работы №1 максимальный балл 28

Лабораторная работа №1

"Элементы множеств. Простые типы данных в системе Mathematica"
по курсу " Методы и средства защиты информации"

1. Создать три списка : listf, listn, listp, являющиеся отображением Вашей фамилии, имени и отчества, с использованием соответствия между русским алфавитом и множеством целых
 $= \{0, 2, 3, \dots, 31\}$.

Буква	Число	Буква	Число	Буква	Число	Буква	Число
а	0	и	8	р	16	ш	24
б	1	й	9	с	17	щ	25
в	2	к	10	т	18	ь	26
г	3	л	11	у	19	ы	27
д	4	м	12	ф	20	ъ	28
е	5	н	13	х	21	э	29
ж	6	о	14	ц	22	ю	30
з	7	п	15	ч	23	я	31

Например: Иванов $\rightarrow$ listf = {8, 2, 0, 13, 14, 2};

Евгений $\rightarrow$ listn = {5, 2, 3, 5, 13, 8, 9};

Петрович $\rightarrow$ listp={15,5,18,16,14,2,8,}.

2. Преобразовать списки в целые числа: numf=AlgebraicNumber[32, listf], numn=AlgebraicNumber[32, listn], nump=AlgebraicNumber[32, listp].
3. Перевести число-фамилию в двоичную, восьмеричную и шестнадцатеричную формы. Использовать функцию BaseForm[expr,n], она возвращает выражение expr в форме числа с основанием n, которое указывается как подстрочный индекс.
4. Получить списки цифр (символов), составляющих число-имя в десятичной, двоичной, и шестнадцатеричной формах. Использовать функцию IntegerDigits[n,b]: n- число, b- основание.
5. Провести операцию деления большего из "числа-фамилии" и "числа-имени" на меньшее. Результат целочисленного деления перевести в вещественную форму с помощью функции N[expr].
6. Найти целую и дробную часть полученного в п.5 вещественного числа. Использовать соответственно функции IntegerPart[x], FractionalPart[x].
7. Провести приведение вещественного числа (см. п.5) к ближайшим целым с помощью следующих функций: Floor[x]- возвращает наибольшее целое число, не превышающее данного x; Ceiling[x]- возвращает значение наименьшего целого числа, большего или равного x.
8. Определить значения максимально и минимально возможных значений чисел, с которыми оперирует система Mathematica 9. Использовать функции \$MaxMachineNumber и \$MinMachineNumber.
9. Получить три простых числа, номера которых определяются числами numf, numn, nump .
Использовать функцию Prime[n] – возвращает n – ое простое число.
10. Найти простые числа с номерами 99;100;101.
11. Относительно числа 539 найти предыдущее и два последующих простых числа. Использовать функцию NextPrime[x,k]- возвращает следующее за заданным числом простое число; параметр «k» может быть отрицательным.
12. Найти количество простых чисел, не превышающих 539.
Использовать функцию PrimePi[x].
13. Относительно "числа-имени" найти 1-ое, 10-ое, 100-ое последующие простые числа.
14. Определить максимальное простое число ("maxPrime") в системе Mathematica 9.
15. Найти число разрядов, составляющих "maxPrime" в десятичном, двоичном и шестнадцатеричном представлении. Использовать функцию IntegerLength[n,b].
16. Получить три случайных целых числа в диапазоне (range) от imin =0 до imax = 255 , применяя функцию RandomInteger[range,n].
17. Установить генератор псевдослучайных чисел в начальное состояние, которое определяется "числом-фамилией". Использовать функцию SeedRandom[n]- переводит генератор псевдослучайных чисел в начальное состояние, определяемое параметром n.
18. Получить три случайных целых числа в диапазоне от 0 до imax = 1000.
19. Повторно получить такую же последовательность из трех чисел п.18.
20. Найти случайное число, которое находится в диапазоне "число-имя" $\pm 10^N$, где N – номер по списку в группе. Использовать функцию RandomInteger[{imin,imax}].
21. Сформировать последовательность из 40-N случайных чисел, находящихся в диапазоне от 0 до 128. Использовать функцию RandomInteger[range, n].
22. Получить три простых случайных целых числа в диапазоне от 2 до imax = 512. Использовать функцию RandomPrime[range,n].
23. Повторно получить последовательность из трех простых чисел п.22.
24. Найти простое случайное число, которое находится в диапазоне "число-имя" $\pm 10^N$, где N – номер по списку в группе. Использовать функцию RandomPrime[{imin,imax}].
25. Сформировать последовательность из 40-N простых случайных чисел, находящихся в диапазоне от 0 до 1024.

Использовать функцию RandomPrime [range, n]

Лабораторная работа №2

"Элементы множеств. Сложные типы данных и их функции в системе Mathematica", максимальный балл 26.

Лабораторная работа №3.

"Методы автоматизированной подготовки открытого текста (plaintext) к операциям шифрования. Работа со строками и массивами", максимальный балл 52.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Знать: угрозы и методы нарушения безопасности АИС; методы и средства обеспечения защиты носителей информации; методы и алгоритмы уничтожения конфиденциальной информации	1.Функция Эйлера 2.Понятие списка в Mathematica 3.Основные операции со списками
Уметь: использовать современные информационные технологии при решении задач защиты информации; формализовать задачу по защите информации; применять стандарты по оценке защищенности АСОИ при анализе и проектировании систем защиты информации в АСОИ	1.Определить значения максимально и минимально возможных значений чисел, с которыми оперирует система Mathematica 9 2.Получить список прописных букв русского алфавита, объединить их в строку и получить список кодов, соответствующих прописным буквам 3. Разработать функцию пользователя для замены прописных букв на строчные русского алфавита 4.Программным способом найти элемент массива, расположенный в столбце на одну позицию ниже буквы, соответствующей номеру по списку в алфавите
Уметь: обосновывать принимаемые проектные решения; применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач, разрабатывать модели открытого текста различного уровня сложности; проводить обработку открытого текста для подготовки к операциям шифрования	1. Получить три случайных целых числа в диапазоне от 0 до $\text{imax} = 1000$. 2.Установить генератор псевдослучайных чисел в начальное состояние 3.Сформировать список, состоящий из квадратов целых чисел от 1 до 20 4.Подготовить список из 200 случайных целых чисел из диапазона 1,100. 5.Провести операцию объединения множеств

Описание шкалы оценивания:

Оценка: 5 («отлично»)

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 3-х лабораторных работ модуля 1 равно 106. Оценка 5 находится в диапазоне 95 -106 балла.

Оценка: 4 («хорошо»)

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 3-х лабораторных работ модуля 1 равно 106. Оценка 4 находится в диапазоне 74 -94 балла.

Оценка: 3 («удовлетворительно»)

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 3-х лабораторных работ модуля 1 равно 106. Оценка 3 находится в диапазоне 42 -73 балла.

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 41 балл. При отсутствии отчета по лабораторной работе по неуважительным причинам проставляется 0 баллов, и, в соответствии с настройками системы Moodle, студент не допускается к КЗЗ, пока не погасит задолженность.

КМ-3. Контроль посещения лекций №5-6 по курсу МСЗИ; Контроль выполнения лабораторной работы №3 по курсу МСЗИ (25%)

Формы реализации: Соблюдение графика выполнения задания

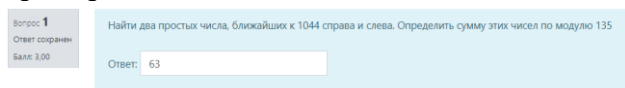
Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: При очной форме обучения контрольно-зачетное занятие проводится в компьютерном классе, оснащенном сетевой версией Mathematica. Длительность контрольной 2 академических часа. К занятию допускаются студенты, выполнившие цикл лабораторных работ модуля 1 и представившие отчеты по лабораторным работам. При дистанционной форме обучения контроль за участниками ведется в Webex, тестирование проводится в системе Moodle. К тестированию допускаются студенты, загрузившие в Moodle электронные отчеты и получившие по ним положительную оценку. Загрузка отчетов должна быть завершена за 24 часа до начала контрольной.

Краткое содержание задания:

Пример задания КЗЗ1



Вопрос 1
Ответ сохранен
Баллы: 3,00

Найти два простых числа, ближайших к 1044 справа и слева. Определить сумму этих чисел по модулю 135

Ответ: 63

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Уметь: – устанавливать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты	1.КЗЗ1 Пересечение целых и простых Уровень 5 Число вариантов 500 2.КЗЗ1 символы 2017 Уровень 5 Число вариантов 250

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
	3.КЗ31 Списки Уровень 7 Число вариантов 200 4.КЗ31 Правило замены Уровень 7 Число вариантов 250

Описание шкалы оценивания:

Оценка: 5 («отлично»)

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 8 заданий равно 38. Оценка 5 находится в диапазоне 34 - 38 баллов.

Оценка: 4 («хорошо»)

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 8 заданий равно 38. Оценка 4 находится в диапазоне 26 - 33 баллов.

Оценка: 3 («удовлетворительно»)

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 8 заданий равно 38. Оценка 3 находится в диапазоне 15 - 25 баллов.

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 14 баллов. Оценка 2 проставляется при участии в контрольной, при отсутствии по неуважительным причинам проставляется 0.

КМ-4. Контроль посещения лекций №7-8 по курсу МСЗИ; Контроль выполнения лабораторной работы №4 по курсу МСЗИ (25%)

Формы реализации: Соблюдение графика выполнения задания

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: При очной форме обучения - заполнение ведомости присутствия в течение лекции. При дистанционной форме обучения - регистрация участников мероприятия в Webex.

Краткое содержание задания:

Проставить в ведомости свою фамилию и подпись. Зарегистрироваться в Webex и присутствовать на лекции.

Контрольные вопросы/задания:

Запланированные результаты обучения по дисциплине	Вопросы/задания для проверки
Уметь: использовать современные инструментальные средства и технологии программирования	1.определить вычет по заданному модулю 2.Оценить число необходимых вычислений для обнаружения коллизии с заданной вероятностью 3.Провести анализ возможных угроз безопасности компьютерной системы 4.Провести анализ класса защищенности АСОИ

Описание шкалы оценивания:

Оценка: 5 («отлично»)

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 3 лекций модуля 1 равно 10. Оценка 5 находится в диапазоне 9-10 баллов.

Оценка: 4 («хорошо»)

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 3 лекций модуля 1 равно 10. Оценка 4 находится в диапазоне 7-8 баллов.

Оценка: 3 («удовлетворительно»)

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 3 лекций модуля 1 равно 10. Оценка 3 находится в диапазоне 4-6 баллов.

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 3 баллов.
При отсутствии на всех лекциях по неуважительным причинам проставляется 0.

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7 семестр

Форма промежуточной аттестации: Зачет с оценкой

Пример билета

МЭИ	ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 5 МСЗИ ИВТИ	Утверждаю Зав.кафедрой ВМСС .
Теоретические вопросы к экзамену по курсу МСЗИ		
1. Основные этапы процесса построения системы защиты АСОИ.		
2. Вариант реализации одноразовых паролей по схеме S-Key.		
Задание №2 Задания уровня 3		
Определить ожидаемое время раскрытия пароля длиной 6 символов и содержащего следующие наборы: {цифры, строчные русские, прописные латинские}, если скорость перебора пароля (пароль в секунду) равна обратному элементу числа 2916 по модулю 661. Ответ вводить как целое число суток.		
Задание №3 Задания уровня 5		
Установить генератор случайных чисел в начальное состояние с параметром равным $2^{15}(\text{mod}293)$. Получить список из 10000 случайных простых чисел в диапазоне от 47000 до 79000. Найти произведение двух простых чисел, которые встречаются в списке с максимальной (применять функцию $\text{Max}[]$) и минимальной (применять функцию $\text{Min}[]$) частотой. В случае наличия чисел с одинаковыми частотами выбирать первые в списке.		
Задание №4 Задания уровня 7		
Определить энтропию сектора с номером 877 виртуального флоппи-диска flptest.flp с точностью 5 знаков после запятой. Для округления результата применить функцию $N[,]$. Пример ввода 5.55555		

Процедура проведения

При очной форме обучения экзамен проводится в комбинированной форме по билетам. Два теоретических вопроса выполняются письменно и оцениваются в диапазоне 0 - 10 баллов преподавателем. Три практических задания выполняются в рамках системы Moodle : максимальная оценка 15 баллов. Результирующая оценка за экзамен определяется как сумма баллов, набранных по теории и практике и пересчитывается к пятибалльной системе (Традиционные оценки РФ) по представленной во вкладке "билет" шкале.

В дистанционном режиме экзамен проводится в системе Moodle и Webex (идентификация и контроль, в том числе визуальный) и

состоит из двух тестов (вопросы или задания выполняются строго последовательно):

Первый тест содержит 20 вопросов по теоретической части курса.

Общая продолжительность теста 15 минут. Максимальное число баллов по теоретической части - 40.

Второй тест содержит 6 практических заданий (2 задания уровня 3, 2 задания уровня 5, 2 задания уровня 7), аналогичных заданиям КЗЗ. Среднее время на выполнение задания 10 минут.

Общая продолжительность теста 60 минут. Максимальное число баллов второго теста - 60.

Результирующая оценка за экзамен определяется как сумма баллов, набранных в первом и втором тестах и

пересчитывается к пятибалльной системе (Традиционные оценки РФ) по представленной во вкладке "билет" шкале.

1. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ИД-3_{ПК-1} Производит оценку влияния применяемых технических решений на общее функционирование системы

Вопросы, задания

1. Тесты-задания уровня 3-1 Число вариантов 1786

2. Тесты-задания уровня 5-1 Число вариантов 950

3. Тесты-задания уровня 5-2 Число вариантов 1580

Материалы для проверки остаточных знаний

1. Группа называется абелевой (или коммутативной), если для любых $a, b \in G$ выполняется следующее соотношение:

Ответы:

$$a * (b * c) = (a * b) * c$$

$$a \bullet (b * c) = a \bullet b * a \bullet c$$

$$(a * b) \bullet c = a \bullet c * b \bullet c$$

$$(a * b) \bullet a = a$$

$$a * b = b * a$$

Верный ответ: $a * b = b * a$

2. Известно, что значения числового ключа лежат в интервале от 9000 до 819000. Сколько случайных попыток (с вероятностью 0.5) могут привести к вскрытию шифра?

Ответы:

ввести число

Верный ответ: 900

2. Компетенция/Индикатор: ИД-1_{ПК-2} Демонстрирует знание нормативной базы, методов описания, анализа и проектирования в области обеспечения безопасности информационных систем и компьютерной криптографии

Вопросы, задания

1. Тесты-задания уровня 3-2 Число вариантов 2100

2. Тесты-задания уровня 7-1 Число вариантов 750

3. Тесты-задания уровня 7-2 Число вариантов 650

4. Основные угрозы безопасности АСОИ
5. Схема защиты парольной системы от несанкционированного воспроизведения
6. Схема защиты парольной системы от пассивного мониторинга
7. Длина пароля и ожидаемое время раскрытия пароля

Материалы для проверки остаточных знаний

1. Какова минимальная длина ключа для совершенного шифра при шифровании сообщения, состоящего из N символов.

Ответы:

0

∞

N

$2N$

2^N

Верный ответ: N

2. Какие подсистемы входят в систему безопасности АСОИ?

Ответы:

Подсистема управления доступом

Подсистема регистрации и учета

Подсистема криптографической защиты

Подсистема обеспечения целостности

Подсистема организационного обеспечения

Подсистема правового обеспечения

Подсистема технического обеспечения

Подсистема математического обеспечения

Подсистема лингвистического обеспечения

Верный ответ: Подсистема регистрации и учета Подсистема управления доступом

Подсистема криптографической защиты Подсистема обеспечения целостности

3. Какие параметры системы одноразовых паролей S-key

передаются по аутентичному каналу

связи на этапе формирования системных параметров?

Ответы:

id - идентификатор

W_0 - финальное значение

n - число итераций

$h(x)$ - хэш - функция

r - случайное число

W_1 - пароль

никакие

Верный ответ: id - идентификатор W_0 - финальное значение n - число итераций

3. Компетенция/Индикатор: ИД-2_{ПК-2} Демонстрирует знание методов и средств обеспечения защиты носителей информации, ЭВМ и компьютерных сетей от несанкционированного доступа

Вопросы, задания

1. Требования к выбору пароля
2. Угрозы безопасности парольных систем
3. Алгоритм непосредственной аутентификации
4. Методы аутентификации.

5. Способы уничтожения информации на магнитных носителях
6. Основные положения защиты информации, хранимой на НЖМД
7. Классы защищенности АСОИ.
8. Структура системы безопасности АСОИ. Основные функции подсистем безопасности
9. Меры обеспечения безопасности компьютерных систем.
10. Основные этапы процесса построения системы защиты АСОИ.
11. Несанкционированный доступ (НСД). Основные каналы несанкционированного доступа.
12. Схема аутентификации по методу "запрос-ответ".
13. Вариант реализации одноразовых паролей по схеме S-Key

Материалы для проверки остаточных знаний

1. При каких условиях число a является простым числом?

Ответы:

$a > 0$

$a > 1$

$a \geq 0$

$a \geq 1$

a - нечетное

делитель a равен 1

делитель a равен a

делитель $a \neq a$

Верный ответ: $a > 1$ делитель a равен 1 делитель a равен a

2. Как зависит число возможных паролей от длины пароля при заданной мощности алфавита.

Ответы:

экспоненциально

суперполиномиально

линейно

нормально

квадратично

не зависит

Верный ответ: экспоненциально

3. В каких единицах будет определена энтропия языка при расчете по формуле

$$r = - \sum_i p_i \log_e p_i$$

Ответы:

в дитах

в битах

в натах

Верный ответ: в натах

4. Компетенция/Индикатор: ИД-4ПК-2 Осуществляет разработку аппаратных и программных средств, необходимых для обеспечения безопасности компьютерных систем

Вопросы, задания

1. Стойкость криптосистем. Расстояние единственности.
2. Энтропия и неопределенность. Количество информации в сообщении.
3. Определение информации. Классификация защищаемой информации.
4. Типы секретных систем.
5. Расширенный алгоритм Евклида.
6. Познающая модель открытого текста.
7. Классы сложности
8. Классификация алгоритмов в соответствии с их сложностью
9. Полная и приведенная система вычетов, функция Эйлера
10. Поле, основные операции в бинарном поле $GF(2)$
11. Обратный элемент, методы его определения.
12. Определение алгебраической группы.
13. Свойства бинарных операций.
14. Взаимно однозначное отображение.
15. Совершенный и идеальный шифры.

Материалы для проверки остаточных знаний

1. Какой из приведенных алгоритмов уничтожения данных имеет максимальное число циклов?

Ответы:

Руководство по защите информации МО США (NISPOM)
DoD 5220.22-M
ГОСТ Р50739-95
Алгоритм Питера Гутмана (Peter Gutman)
Алгоритм Брюса Шнайера (Bruce Schneir)
Стандарт VISR

Верный ответ: Алгоритм Питера Гутмана (Peter Gutman)

2. К какой из групп классов защищенности относится автоматизированная система обработки информации в которой:

работает один пользователь,
допущенный ко всей информации АС,
размещенной на носителях одного уровня конфиденциальности.

Ответы:

Первая группа - 1А,1Д
Вторая группа - 2А,2Б
Третья группа - 3А,3Б

Верный ответ: Третья группа - 3А,3Б

II. Описание шкалы оценивания

Оценка: 5 («отлично»)

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число баллов, набранных в двух тестах равно 100 (или с умножением на 4 при очной форме). Оценка 5 находится в интервале от 90 до 100 баллов.

Оценка: 4 («хорошо»)

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число баллов, набранных в двух тестах равно 100 (или с умножением на 4 при очной форме). Оценка 4 находится в интервале от 70 до 89 баллов.

Оценка: 3 («удовлетворительно»)

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Максимальное число баллов, набранных в двух тестах равно 100 (или с умножением на 4 при очной форме). Оценка 3 находится в интервале от 60 до 69 баллов.

Оценка: 2 («неудовлетворительно»)

Описание характеристики выполнения знания: Максимальное число баллов, набранных в двух тестах равно 100 (или с умножением на 4 при очной форме). Оценка 2 находится в интервале от 0 до 59 баллов.

III. Правила выставления итоговой оценки по курсу

Итоговая оценка по курсу может быть рассчитана как среднее от текущей успеваемости и итогов промежуточной аттестации по 100 балльной шкале. Текущая успеваемость также рассчитывается как среднее по трем модулям по 100 балльной шкале. Только после этого можно переходить к 5-и балльной шкале. Промежуточное округление оценок в 5-и балльной системе и нелинейная шкала оценок в БАРС приводят к существенному завышению результирующих оценок.