

**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: Вычислительно-измерительные системы

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

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

**Москва
2022**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Желбаков И.Н.
	Идентификатор	R839a3a63-ZhelbakovIgN-f73624c

(подпись)

И.Н.
Желбаков

(расшифровка
подписи)

СОГЛАСОВАНО:

Руководитель
образовательной
программы

(должность, ученая степень, ученое
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Серов Н.А.
	Идентификатор	R708da564-SerovNA-06ab7859

(подпись)

Н.А. Серов

(расшифровка
подписи)

Заведующий
выпускающей кафедры

(должность, ученая степень, ученое
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Желбаков И.Н.
	Идентификатор	R839a3a63-ZhelbakovIgN-f73624c

(подпись)

И.Н.
Желбаков

(расшифровка
подписи)

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: Компьютерное задание

1. Контроль выполнения комплекса лабораторных работ № 7-12 по курсу ЗИ Модуль 3 (25%). (Лабораторная работа)
2. Контроль выполнения комплекса лабораторных работ №1-3 по курсу МСЗИ Модуль 1 (25%) (Лабораторная работа)
3. Контроль выполнения комплекса лабораторных работ №4,5, 6 по курсу ЗИ Модуль 2 (25%) (Лабораторная работа)
4. Контрольно-зачетное занятие (К331) по курсу МСЗИ Модуль 1 (65%) (Тестирование)
5. Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) (Тестирование)
6. Контрольно-зачетное занятие (К333) по курсу МСЗИ Модуль 3 (65%) (Тестирование)

Форма реализации: Смешанная форма

1. Контроль посещения лекций № 3-6 по курсу МСЗИ Модуль 2 (10%) (Интервью)
2. Контроль посещения лекций №1-2 по курсу МСЗИ Модуль 1 (10%) (Интервью)
3. Контроль посещения лекций №7,8 по курсу МСЗИ Модуль 3 (10%) (Интервью)

БРС дисциплины

7 семестр

Раздел дисциплины	Веса контрольных мероприятий, %									
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5	КМ-6	КМ-7	КМ-8	КМ-9
	Срок КМ:	4	4	8	12	12	12	16	16	16

Математические основы криптологии									
Математические основы криптологии	+	+	+						
Информационная безопасность компьютерных систем									
Информационная безопасность компьютерных систем				+	+	+			
Парольные системы									
Парольные системы							+	+	+
Вес КМ:	3	8	22	3	8	22	3	8	23

\$Общая часть/Для промежуточной аттестации\$

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-3ПК-1 Производит оценку влияния применяемых технических решений на общее функционирование системы	<p>Знать:</p> <p>показатели эффективности принимаемого проектного решения; понятия группы, кольца, поля ;</p> <p>качественные и количественные свойства информации;</p> <p>статистические модели открытого текста</p> <p>Уметь:</p> <p>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</p>	<p>Контроль посещения лекций №1-2 по курсу МСЗИ Модуль 1 (10%) (Интервью)</p> <p>Контроль выполнения комплекса лабораторных работ №1-3 по курсу МСЗИ Модуль 1 (25%) (Лабораторная работа)</p> <p>Контрольно-зачетное занятие (К331) по курсу МСЗИ Модуль 1 (65%) (Тестирование)</p>

		текста для подготовки к операциям шифрования	
ПК-2	ИД-1 _{ПК-2} Демонстрирует знание нормативной базы, методов описания, анализа и проектирования в области обеспечения безопасности информационных систем и компьютерной криптографии	Знать: методологические и технологические основы обеспечения безопасности АСОИ; угрозы и методы нарушения безопасности АСОИ; стандарты по оценке защищенных систем 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	Контроль посещения лекций № 3-6 по курсу МСЗИ Модуль 2 (10%) (Интервью) Контроль выполнения комплекса лабораторных работ №4,5, 6 по курсу ЗИ Модуль 2 (25%) (Лабораторная работа) Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) (Тестирование)
ПК-2	ИД-2 _{ПК-2} Демонстрирует знание методов и средств обеспечения защиты носителей информации, ЭВМ и компьютерных сетей от несанкционированного доступа	Знать: угрозы и методы нарушения безопасности АИС; методы и средства обеспечения защиты носителей информации; методы и алгоритмы уничтожения конфиденциальной	Контроль посещения лекций № 3-6 по курсу МСЗИ Модуль 2 (10%) (Интервью) Контроль выполнения комплекса лабораторных работ №4,5, 6 по курсу ЗИ Модуль 2 (25%) (Лабораторная работа) Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) (Тестирование) Контроль посещения лекций №7,8 по курсу МСЗИ Модуль 3 (10%) (Интервью) Контроль выполнения комплекса лабораторных работ № 7-12 по курсу

		<p>информации</p> <p>Уметь:</p> <p>– устанавливать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты</p>	<p>ЗИ Модуль 3 (25%). (Лабораторная работа)</p> <p>Контрольно-зачетное занятие (К333) по курсу МСЗИ Модуль 3 (65%) (Тестирование)</p>
ПК-2	ИД-4 _{ПК-2} Осуществляет разработку аппаратных и программных средств, необходимых для обеспечения безопасности компьютерных систем	<p>Знать:</p> <p>способы и технологии применения криптографии в решении задач идентификации и аутентификации, частотные характеристики языков и их использование при построении систем парольной защиты</p> <p>Уметь:</p> <p>использовать современные инструментальные средства и технологии программирования</p>	<p>Контроль посещения лекций № 3-6 по курсу МСЗИ Модуль 2 (10%) (Интервью)</p> <p>Контроль выполнения комплекса лабораторных работ №4,5, 6 по курсу ЗИ Модуль 2 (25%) (Лабораторная работа)</p> <p>Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) (Тестирование)</p> <p>Контроль посещения лекций №7,8 по курсу МСЗИ Модуль 3 (10%) (Интервью)</p> <p>Контроль выполнения комплекса лабораторных работ № 7-12 по курсу ЗИ Модуль 3 (25%). (Лабораторная работа)</p> <p>Контрольно-зачетное занятие (К333) по курсу МСЗИ Модуль 3 (65%) (Тестирование)</p>

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контроль посещения лекций №1-2 по курсу МСЗИ Модуль 1 (10%)

Формы реализации: Смешанная форма

Тип контрольного мероприятия: Интервью

Вес контрольного мероприятия в БРС: 3

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					2 10
2 Артох Владислава Владимировна (В)	1						1 5
3 Белова Ирина Михайловна	1	1					2 10
4 Бирман Александр Александрович							0 0
5 Блаженова Светлана Дмитриевна	1	1					2 10
6 Журавлёв Антон Александрович	1	1					2 10
7 Иванов Глеб Александрович (В)	1	1					2 10
8 Игнатова Анастасия Ильинична	1	1					2 10
9 Кон Алёна Юрьевна	1	1					2 10
10 Кузнецова Анастасия Леонидовна	1	1					2 10

Контрольные вопросы/задания:

Знать: показатели эффективности принимаемого проектного решения; понятия группы, кольца, поля ; качественные и количественные свойства информации; статистические модели открытого текста	1.Типы секретных систем 2.Уровни секретности информации
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.Найти энтропию криптосистемы

Описание шкалы оценивания:

Оценка: 5

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

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

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.

КМ-2. Контроль выполнения комплекса лабораторных работ №1-3 по курсу МСЗИ Модуль 1 (25%)

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 8

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:

<p>Знать: показатели эффективности принимаемого проектного решения; понятия группы, кольца, поля ; качественные и количественные свойства информации; статистические модели открытого текста</p>	<p>1.Определение простого числа 2.Понятие строки в Mathematica</p>
<p>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</p>	<p>1. Получить три случайных целых числа в диапазоне от 0 до $\text{imax} = 1000$. 2.Подготовить список из 200 случайных целых чисел из диапазона 1,100.</p>

Описание шкалы оценивания:

Оценка: 5

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

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

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.

КМ-3. Контрольно-зачетное занятие (К331) по курсу МСЗИ Модуль 1 (65%)

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Тестирование

Вес контрольного мероприятия в БРС: 22

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 К331

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:

<p>Знать: показатели эффективности принимаемого проектного решения; понятия группы, кольца, поля ; качественные и количественные свойства информации; статистические модели открытого текста</p>	<p>1.К331 Системы счисления 2 Уровень 3 Число вариантов 1000 2.К331 простые числа 1 2017 Уровень 3 Число вариантов 250</p>
<p>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</p>	<p>1.К331 Пересечение целых и простых Уровень 5 Число вариантов 500 2.К331 символы 2017 Уровень 5 Число вариантов 250 3.К331 Списки Уровень 7 Число вариантов 200 4.К331 Правило замены Уровень 7 Число вариантов 250</p>

Описание шкалы оценивания:

Оценка: 5

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

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

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.

КМ-4. Контроль посещения лекций № 3-6 по курсу МСЗИ Модуль 2 (10%)

Формы реализации: Смешанная форма

Тип контрольного мероприятия: Интервью

Вес контрольного мероприятия в БРС: 3

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:

Знать: методологические и технологические основы обеспечения безопасности АСОИ; угрозы и методы нарушения безопасности АСОИ; стандарты по оценке защищенных систем	1.Правила выполнения операций сложения и умножения в модулярной арифметике
Знать: угрозы и методы нарушения безопасности АИС; методы и средства обеспечения защиты носителей информации; методы и алгоритмы уничтожения конфиденциальной информации	1.Парадокс дней рождений 2.Основные понятия информационной безопасности компьютерных систем 3.Основные положения защиты информации, хранимой на НЖМД
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.Оценить число необходимых вычислений для обнаружения коллизии с заданной вероятностью 2.Провести анализ возможных угроз безопасности компьютерной системы
Уметь: использовать	1.Провести анализ класса защищенности АСОИ

современные инструментальные средства и технологии программирования	
---	--

Описание шкалы оценивания:

Оценка: 5

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

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

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.

**КМ-5. Контроль выполнения комплекса лабораторных работ №4,5, 6 по курсу
ЗИ Модуль 2 (25%)**

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 8

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:

Лабораторная работа №5.

"Парадокс дней рождений", максимальное число баллов 32.
по курсу "Методы и средства защиты информации".

Рабочее задание

1. Построить графики функции вероятности возникновения хотя бы одной коллизии
(См. Л[1], п.3.6) в зависимости от числа k экспериментов извлечения с возвратом элементов множества, для множеств с количеством элементов n равным $100+N$, 365 , $900+N$ (См. Л[2], п. 8.1-8.2).
2. Объединить три графика и построить там же линию с ординатой равной 0.5 .

3. Определить число экспериментов, при котором коллизия появляется с вероятностью 0.5 путем прямого решения уравнения $P(k,n) = 0.5$ для трех значений $n = 100+N, 365, 900+N$ (См. Л[2], п. 5.5.4) . Сравнить полученные результаты с расчетом по приближенной формуле $k \approx 1.1774\sqrt{n}$.
3. Определить число экспериментов, при котором коллизия появляется с вероятностью 0.99 для $n = 100+N, 365, 900+N$.
4. Найти предел, к которому стремится вероятность хотя бы одной коллизии при числе экспериментов, стремящихся к бесконечности (См. Л[2], п. 5.4).
5. Установить генератор случайных чисел в начальное состояние по номеру в списке группы N и сформировать список из 15 случайных целых чисел, которые лежат в интервале от $10+N$ до $25+N$.
6. С помощью функции Union[] исключить повторяющиеся элементы и определить число коллизий, как разницу между длинами исходного списка и списка без повторений.
7. Подготовить список, состоящий из 0, длиной $10000+1000*N$ - с помощью функции Table[] (См. Л[2], п. 4.1.2).
8. На подмножестве целых чисел от 1 до 365 реализовать случайную многократную выборку по 23 элемента и для каждой выборки определить число коллизий. Число повторов эксперимента равно $10000+1000*N$.
Операцию циклических вычислений выполнить с помощью функций (См. Л[2], п. 2.6,2.7), указанных в таблице (вариант реализации определяется из следующего соотношения $nv = N(\text{mod}3)+1$) :

Номер варианта nv	1	2	3
Оператор	Do	While	For

9. Определить число экспериментов без коллизий, с одной, двумя коллизиями и т.д., используя функцию Tally[].
10. Построить гистограмму распределения вероятности коллизий, используя функцию Histogram[] со следующими параметрами: число столбцов гистограммы (bin) и максимальное значение по оси x равно длине списка из п.9; вид гистограммы определяется спецификацией "Probability"; диапазоны отображения по осям определяются опцией PlotRange ® {{0,***},{0,***}}.

Лабораторная работа №4 Модулярная арифметика. Определение обратного элемента в конечном поле.

Максимальное число баллов 31

Лабораторная работа №6 Средства анализа данных. Максимальное число баллов 44.

Контрольные вопросы/задания:

Знать: методологические и технологические основы обеспечения безопасности АСОИ; угрозы и методы нарушения безопасности АСОИ; стандарты по оценке защищенных систем	1.Операция вычисления вычета по модулю 2.Математическая модель открытого текста
Знать: угрозы и методы нарушения безопасности АИС; методы и средства обеспечения защиты носителей информации; методы и алгоритмы уничтожения конфиденциальной информации	1.Обратный элемент по <i>умножению в конечном поле</i> 2.Расширенный алгоритм Евклида
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.Построить полную и приведенную систему вычетов по заданному модулю. 2.Определить число экспериментов, при котором коллизия появляется с вероятностью 0.5
Уметь: использовать современные инструментальные средства и технологии программирования	1.Найти предел, к которому стремится вероятность хотя бы одной коллизии при числе экспериментов, стремящихся к бесконечности 2.Провести преобразования в импортированных файлах: поменять прописные буквы на строчные , оставить только строчные буквы и пробелы

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 3-х лабораторных работ модуля 2 равно 107. Оценка 5 находится в диапазоне 96 -107 балла.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 3-х лабораторных работ модуля 2 равно 107. Оценка 4 находится в диапазоне 74 - 95 балла.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 3-х лабораторных работ модуля 2 равно 107. Оценка 3 находится в диапазоне 42 -73 балла.

КМ-6. Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%)

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Тестирование

Вес контрольного мероприятия в БРС: 22

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 К332:

В поле целых чисел определить сумму элементов приведенной системы вычетов по модулю 1108.

Ответ:

Контрольные вопросы/задания:

<p>Знать: методологические и технологические основы обеспечения безопасности АСОИ; угрозы и методы нарушения безопасности АСОИ; стандарты по оценке защищенных систем</p>	<p>1.К332 взаимно простые числа Уровень 3 Число вариантов 250</p>
<p>Знать: угрозы и методы нарушения безопасности АИС; методы и средства обеспечения защиты носителей информации; методы и алгоритмы уничтожения конфиденциальной информации</p>	<p>1.К332 Атака кв корня Уровень 3 Число вариантов 36 2.К332 обратные элементы по сл и умн Уровень 3 Число вариантов 250</p>
<p>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</p>	<p>1.К332 энтропия текста Уровень 3 Число вариантов 100 2.К332 Элементы массива алфавита Уровень 5 Число вариантов 250</p>

АСОИ	
Уметь: использовать современные инструментальные средства и технологии программирования	1.К332 приведенная система вычетов Уровень 3 Число вариантов 250 2.К332 коллизии Уровень 5 Число вариантов 250

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 8 заданий равно 30. Оценка 5 находится в диапазоне 27 - 30 баллов.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 8 заданий равно 30. Оценка 4 находится в диапазоне 21 - 26 баллов.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 8 заданий равно 30. Оценка 3 находится в диапазоне 12 - 30 баллов.

КМ-7. Контроль посещения лекций №7,8 по курсу МСЗИ Модуль 3 (10%)

Формы реализации: Смешанная форма

Тип контрольного мероприятия: Интервью

Вес контрольного мероприятия в БРС: 3

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:

Знать: способы и технологии применения криптографии в решении задач идентификации и аутентификации, частотные характеристики языков и их использование при построении систем парольной защиты	1.Процесс идентификации 2.Общие принципы аутентификации "с нулевым разглашением"
Уметь: – устанавливать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты	1.Провести анализ угроз парольной системе 2.Сформировать пароль с заданными требованиями по надежности

Описание шкалы оценивания:

Оценка: 5

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

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

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.

КМ-8. Контроль выполнения комплекса лабораторных работ № 7-12 по курсу ЗИ Модуль 3 (25%).

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 8

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:

Лабораторная работа №7. Максимальное число баллов 50

Удаление и восстановление информации на магнитном носителе.

Рабочее задание.

1. На основной машине, в папке «Student», создать рабочую папку «А-номер группы-14-ФИО».
2. В меню «Device» виртуальной машины выбрать Floppy – диск и создать (Create) новый образ (выбрать имя) этого диска в рабочей папке на основной машине: Use floppy image file; после чего подключить флоппи-диск к виртуальной машине (Connect).
3. Провести полное форматирование флоппи-диска.
4. Для чистого Floppy – диска, с помощью шестнадцатеричного редактора WinHex, сначала открыть Floppy – диск (WinHex Р Инструменты(Tools) РОткрыть диск(Disk Editor) Р Physical Media(Physical Disk) РFloppy disk 0(00h Floppy) Р ОК), а затем определить начало области форматирования по признаку (коду) F6F6F6: Поиск//Поиск Нех-данных.
5. С помощью стандартного текстового редактора «Блокнот», используя **латинский** алфавит, создать два тестовых файла с разными названиями (такими, чтобы их можно было легко идентифицировать на фоне "случайного набора букв и цифр") и разными

осмысленными текстами (в пределах одного-двух предложений). Сохранить эти файлы в рабочей папке на виртуальной машине.

6. Запустить имеющийся файловый менеджер, скопировать файл на Floppy – диск и с помощью редактора WinHex определить местонахождение "offset1" имени файлов и "offset2" их содержимого (Поиск//Поиск текста).

7. Стереть (Delete) файлы на дискете и закрыть файловый менеджер.

8. Запустить программу восстановления файлов PC Inspector File Recovery и убедиться в существовании файлов на дискете. Запомнить экран – PrintKey.

9. Запустить WinHex и через опции Поиск//Поиск текста найти элементы имени файла и текста, записанного в «Блокноте». Зафиксировать изменения в структуре данных, происходящие при стирании информации.

10. Провести исследование эффективности методов стирания информации средствами операционной системы по следующей схеме:

Ø провести полное форматирование флоппи-диска;

Ø записать на флоппи-диск тестовый файл;

Ø провести стирание;

Ø проверить наличие и изменение структуры заголовка файла (offset1) , наличие содержимого файла (offset2), результаты записать в таблицу:

Метод стирания	Информация по адресу offset1	Информация по адресу offset2
Delete		
«перетаскивание в корзину»		
удаление файла Shift+Delete		
удаление файла Shift+F8		
быстрое форматирование диска A:		
полное форматирование диска A:.		

11. В блокноте набрать текстовый файл (размер – экран блокнота) из определенной последовательности символов, например –secret , и записать на чистую дискету под именем abc. Определить число секторов, занимаемых файлом (номер текущего сектора отображается в левом нижнем углу окна WinHex).

12. Создать «короткий» текстовый файл (строка) и сохранить под тем же именем abc.

13. Используя WinHex исследовать размещение информации на дискете – определить позицию размещения нового файла и секторы с содержимым предыдущего файла.

14. Отформатировать дискету и вновь записать на дискету файлы, созданные в п.5.

15. Провести безвозвратное стирание информации (первый файл п.5) с помощью утилиты eraser41 (установить в случае необходимости) в режиме Pseudorandom Data при отключенных опциях меню Unused Disk Space– выбрать файл на дискете, нажать правую кнопку мыши и выбрать опцию Erase.

16. Используя WinHex исследовать размещение информации на дискете: выделив курсором стертый блок и используя меню Правка\Copy Block запомнить в отдельном файле содержимое этого блока;

сохранить содержимое экрана с гистограммой распределения данных в блоке.

17. Отформатировать дискету и вновь записать на дискету файлы, созданные в п.5.

Провести безвозвратное стирание информации (первый файл п.5) с помощью утилиты eraser41 в режимах Faster(Us DoD 5220.22-M) и Gutmann, при отключенных опциях меню Unused Disk Space. Для каждого режима повторить операции п.16.

18. Определить энтропию стертого сектора и построить гистограмму распределения псевдослучайных чисел для режима стирания по алгоритму Gutmann. Для ввода данных

использовать предварительное преобразование с помощью утилиты Converter.exe и последующей функции ReadList["file.dat",Number].

19. Установить (проверить наличие) на виртуальной машине программы Anvide Lock Folder. Создать папку со вторым текстом п. 5 на флоппи-диске и скрыть её. Проверить наличие папки с помощью проводника или Total Commander.

20. Найти сектор (номер сектора) с именем папки и сектор с содержимым файла.

21. Отключить (Disconnect) Floppy – диск в виртуальной машине.

Лабораторная работа №8 Защита информации по паролю в WinWord и 7-Zip. Системы восстановления паролей AOPR и ARPR.

Максимальное число баллов 35.

Лабораторная работа МСЗИ №9 (SNS 2-1) "Локальная настройка Secret Net Studio в соответствии с заданными параметрами"

Максимальное число баллов 6.

Лабораторная работа МСЗИ №10 (SNS 2-2) "Настройка механизма контроля целостности"

Максимальное число баллов 9.

Лабораторная работа МСЗИ №11 (SNS 3-1) "Настройка полномочного управления доступом"

Максимальное число баллов 6.

Лабораторная работа МСЗИ №12 (SNS 3-2) "Настройка механизма дискреционного управления доступом"

Максимальное число баллов 5.

Контрольные вопросы/задания:

Знать: способы и технологии применения криптографии в решении задач идентификации и аутентификации, частотные характеристики языков и их использование при построении систем парольной защиты	1.Алгоритмы безвозвратного стирания информации
Уметь: – устанавливать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты	1.Провести безвозвратное стирание информации в режимах Faster и Gutmann 2.Разработать программную реализацию генератора паролей с заданными параметрами. 3.Задать следующие категории конфиденциальности: "Неконфиденциально", "ДСП" (для служебного пользования), "Секретно". 4.Установить права дискреционного доступа для пользователей "user1" и "user2" в соответствии с матрицей доступа

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 5-и лабораторных работ модуля 3 равно 111. Оценка 5 находится в диапазоне 99 -111 балла.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 5-и лабораторных работ модуля 3 равно 111. Оценка 4 находится в диапазоне 77 - 98 балла.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 5-и лабораторных работ модуля 3 равно 106. Оценка 3 находится в диапазоне 44 -76 балла.

КМ-9. Контрольно-зачетное занятие (КЗ33) по курсу МСЗИ Модуль 3 (65%)

Формы реализации: Компьютерное задание

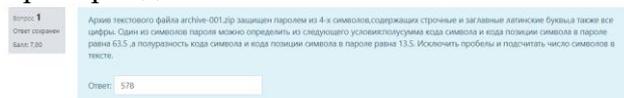
Тип контрольного мероприятия: Тестирование

Вес контрольного мероприятия в БРС: 23

Процедура проведения контрольного мероприятия: При очной форме обучения контрольно-зачетное занятие проводится в компьютерном классе, оснащённом 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 КЗ33:



Контрольные вопросы/задания:

Знать: способы и технологии применения криптографии в решении задач идентификации и аутентификации, частотные характеристики языков и их использование при построении систем парольной защиты	1.КЗ33 пароль архива Уровень 7 Число вариантов 200 2.КЗ33 Частоты minmax 2018 Уровень 5 Число вариантов 80
Уметь: – устанавливать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и	1.КЗ33 время раскрытия пароля Уровень 3 Число вариантов 250 2.КЗ33 Энтропия сектора Уровень 7 Число вариантов 200

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 6 заданий равно 34. Оценка 5 находится в диапазоне 30 - 38 баллов.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 6 заданий равно 34. Оценка 4 находится в диапазоне 23 - 30 баллов.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 6 заданий равно 34. Оценка 3 находится в диапазоне 13 - 23 баллов.

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7 семестр

Форма промежуточной аттестации: Экзамен

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 $2^{15} \pmod{293}$. 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 Max[]) и минимальной (применять функцию 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.

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

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

Вопросы, задания

1. Стойкость криптосистем. Расстояние единственности.
2. Энтропия и неопределенность. Количество информации в сообщении.
3. Определение информации. Классификация защищаемой информации.
4. Позначная модель открытого текста.
5. Классы сложности
6. Классификация алгоритмов в соответствии с их сложностью
7. Поле, основные операции в бинарном поле $GF(2)$
8. Обратный элемент, методы его определения.

Материалы для проверки остаточных знаний

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

Ответы:

0

∞

N

$2N$

2^N

Верный ответ: N

3. 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

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

$$r = - \sum_i p_i \text{Log}_e p_i$$

Ответы:

в дитах

в битах

в натах

Верный ответ: в натах

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

Вопросы, задания

1. Классы защищенности АСОИ.
2. Структура системы безопасности АСОИ. Основные функции подсистем безопасности
3. Основные этапы процесса построения системы защиты АСОИ.

Материалы для проверки остаточных знаний

1. 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

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

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

Вопросы, задания

1. Способы уничтожения информации на магнитных носителях
2. Основные положения защиты информации, хранимой на НЖМД
3. Меры обеспечения безопасности компьютерных систем.
4. Несанкционированный доступ (НСД). Основные каналы несанкционированного доступа.

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)

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

Вопросы, задания

1. Схема защиты парольной системы от несанкционированного воспроизведения
2. Схема защиты парольной системы от пассивного мониторинга
3. Длина пароля и ожидаемое время раскрытия пароля
4. Требования к выбору пароля
5. Угрозы безопасности парольных систем
6. Алгоритм непосредственной аутентификации
7. Методы аутентификации.
8. Вариант реализации одноразовых паролей по схеме S-Key

Материалы для проверки остаточных знаний

1. Какие параметры системы одноразовых паролей S-key передаются по аутентичному каналу связи на этапе формирования системных параметров?

Ответы:

id - идентификатор

$W0$ - финальное значение

n - число итераций

$h(x)$ - хэш - функция

r - случайное число

$W1$ - пароль

никакие

Верный ответ: id - идентификатор $W0$ - финальное значение n - число итераций

2. Как зависит число возможных паролей от длины пароля

при заданной мощности алфавита.

Ответы:

экспоненциально
суперполиномиально
линейно
нормально
квадратично
не зависит

Верный ответ: экспоненциально

II. Описание шкалы оценивания

Оценка: 5

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

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

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.

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.