Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий
Кафедра информационной безопасности и теории управления

Рацеев С.М.

Методические указания для самостоятельной работы студентов при подготовке к государственной итоговой аттестации

для студентов специальности

10.05.03 «Информационная безопасность автоматизированных систем»

Ульяновск

2019

Рацеев С.М. Методические указания для самостоятельной работы студентов при подготовке к государственной итоговой аттестации для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем». – Ульяновск: УлГУ, 2019.

Методические указания рекомендованы к введению в образовательный процесс решением Ученого Совета ФМИАТ УлГУ (протокол № 2/19 от 19 марта 2019г.).

Раздел 1. Математически анализ

Основные вопросы темы:

1. Предел и непрерывность функций одной и нескольких переменных. Свойства функций, непрерывных на отрезке.
2. Производная и дифференциал функций одной и нескольких переменных. Достаточные условия дифференцируемости. Теорема Ферма. Теоремы Ролля, Лагранжа и Коши.
3. Формула Тейлора с остаточным членом в форме Лагранжа и Коши. Формулы Тейлора основных элементарных функций. Экстремумы функций одной переменной. Достаточные условия экстремума.
4. Первообразная и неопределенный интеграл. Определенный интеграл, его свойства. Необходимые и достаточные условия интегрируемости. Основная формула интегрального исчисления.
5. Числовые ряды. Абсолютная и условная сходимость числового ряда. Признаки сходимости числового ряда: признак Даламбера, интегральный признак Коши-Маклорена, теорема Лейбница для знакочередующихся рядов.
6. Степенные ряды. Теорема Абеля. Радиус сходимости, интервал сходимости степенного ряда. Теорема Коши-Адамара. Разложение элементарных функций в ряд Тейлора.

Рекомендации по изучению темы:

1. Зорич, В.А. Математический анализ : учебник для ун-тов. Ч. 1 / В.А. Зорич. М. : Наука, 1981. 543 с.
2. Зорич, В.А. Математический анализ : учебник для ун-тов. Ч. 2 / В.А. Зорич. М. : Наука, 1984. 670 с.
3. Ильин В.А. Математический анализ : учебник для вузов по спец. "Математика", "Прикладная математика", "Информатика": в 2 ч. Ч. 1 / Ильин Владимир Александрович, В. А. Садовничий, Б. Х. Сендов; под ред. А. Н. Тихонова; Моск. гос. ун-т им. М. В. Ломоносова. - 3-е изд., перераб. и доп. -М. : Велби : Проспект, 2007. - 672 с.
4. Ильин В.А. Математический анализ : учебник для вузов по спец. "Математика", "Прикладная математика" и "Информатика": в 2 ч. Ч. 2 / В. А. Ильин, В. А. Садовничий, Б. Х. Сендов; под ред. А. Н.Тихонова; Моск. гос. ун-т им. М. В. Ломоносова. - 2-е изд., перераб. и доп. - М. : Велби : Проспект, 2007. - 368 с.

Задачи для самостоятельной работы:

1. Найти предел $\lim\limits_{x\to\infty}\dfrac{2+x-4x^3}{5+x^2+3x^3}$.
2. Найти предел $\lim\limits_{x\to\infty}\left(\dfrac{x^3}{2x^2-1}-\dfrac{x^2}{2x+1}\right)$.
3. Найти предел $\lim\limits_{x\to 0}\dfrac{\sin^2 5x}{4x^2}$.
4. Найти предел $\lim\limits_{n\to\infty}\left(1-\dfrac{8n}{n^2+1}\right)^{3n}$.
5. Пусть $f(x)=\ln\sqrt{\dfrac{1-x}{1+x}}$. Найти $f'(x)$.
6. Найти интеграл $\int\dfrac{dx}{\sqrt{1-2x}}$.
7. Найти интеграл $\int\sqrt[4]{(7x+5)^3}\,dx$.

8. Найти интеграл $\int x \ln x \, dx$.
9. Найти интеграл $\int xe^{-x} dx$.
10. Найти интеграл $\int \frac{x-3}{x^2-16} dx$.
11. Найти интеграл $\int_{-1}^{1} \frac{xdx}{\sqrt{5-4x}}$.
12. Вычислить объем тела, образованного вращением фигуры, ограниченной линиями:
13. $y = -x^2 + 4, \quad y = 0, \quad y = 3$ вокруг оси Оу.
14. Исследовать числовой ряд $\sum_{n=1}^{\infty} \frac{1}{\sqrt{n}}$ на сходимость.
15. Исследовать числовой ряд $\sum_{n=1}^{\infty} \frac{9^{n-1}}{n!}$ на сходимость.
16. Исследовать числовой ряд $\sum_{n=1}^{\infty} \frac{n \cdot 3^{n+1}}{n^2+2}$ на сходимость.
17. Исследовать числовой ряд $\sum_{n=1}^{\infty} \frac{(-1)^n n}{n^2+7}$ на сходимость.
18. Вычислить интеграл или определить его расходимость $\int_{1}^{+\infty} \frac{dx}{\sqrt[3]{x}}$.
19. Вычислить интеграл или определить его расходимость $\int_{e}^{+\infty} \frac{dx}{x \ln^2 x}$.
20. Вычислить интеграл или определить его расходимость $\int_{0}^{+\infty} (3x+2)^6 dx$.

Раздел 2. Алгебра и геометрия
Основные вопросы темы:

1. Матрицы и операции над ними. Определители матриц и их свойства. Определитель Вандермонда. Ранг матрицы. Критерий обратимости матриц. Способы вычисления обратной матрицы.
2. Векторные пространства, их базисы и размерность. Критерий подпространства. Координаты векторов в базисе и их изменение при переходе к другому базису.
3. Системы линейных алгебраических уравнений. Теорема Кронекера-Капелли. Общее решение системы линейных алгебраических уравнений.
4. Линейные преобразования векторного пространства и их матрицы. Характеристический многочлен линейного преобразования. Собственные значения и собственные векторы.
5. Евклидовы пространства. Процесс ортогонализации. Ортогональные преобразования евклидова пространства. Ортогональные матрицы и их свойства.
6. Группы и их основные свойства. Циклические группы. Смежные классы по подгруппе. Теорема Лагранжа. Морфизмы групп.
7. Кольца. Мультипликативная группа кольца. Подкольца. Критерий подкольца. Идеал кольца. Фактор-кольцо. Кольца вычетов.

8. Кольцо многочленов. Наибольший общий делитель и наименьшее общее кратное. Свойства наибольшего общего делителя двух многочленов. Алгоритм Евклида.
9. Конечные поля. Характеристика поля. Построение конечного поля с заданным числом элементов.
10. Прямая и плоскость, их уравнения. Взаимное расположение прямой и плоскости. Основные задачи на прямую и плоскость.

Рекомендации по изучению темы:

1. Винберг Э.Б. Курс алгебры. Новое издание, перераб. и доп. М.: МЦНМО, 2011. 592 с.
2. Ильин В.А., Ким Г.Д. Линейная алгебра и аналитическая геометрия. 3-изд., перераб. и доп. М.: Проспект, 2007. 400 с.
3. Кострикин А.И. Введение в алгебру: Учебник для вузов. Ч.1, Ч.2, Ч.3.: Основы алгебры. М.: Физматлит, 2001.
4. Курош А.Г. Курс высшей алгебры : учебник для вузов по спец. "Математика". 17-е изд., стер. СПб. : Лань, 2008. 432 с.

Задачи для самостоятельной работы:

1. На множестве $\mathbb{Z}$ определено бинарное отношение $\sim$ следующим образом: $a \sim b \Leftrightarrow 6|(a-b)$. Доказать, что $\sim$ является отношением эквивалентности. Найти разбиение множества $\mathbb{Z}$, которое индуцирует отношение $\sim$. Какому классу эквивалентности принадлежит элемент $a = -452$?
2. На множестве $M = \{4x | x \in \mathbb{N}\}$ определено бинарное отношение $\leq$ следующим образом: $a \leq b \Leftrightarrow a|b$. Проверить, является ли $\leq$ отношением линейного порядка на M.
3. Проверить, является ли множество $\left\{ \begin{pmatrix} 8x & 0 \\ 0 & 12y \end{pmatrix} | \, x, y \in \mathbb{Z} \right\}$ относительно операции сложения аддитивной абелевой группой.
4. Доказать, что множество $R = \{a + b\sqrt{3} \, | a, b \in \mathbb{Z}\}$ относительно операций сложения и умножения является коммутативным кольцом с единицей.
5. В мультипликативной группе кольца вычетов $\mathbb{Z}_{40}^*$ найти 29^{-1}.
6. Найти решения системы линейных алгебраических уравнений над полем $\mathbb{R}$:
$$\begin{cases} 2x_1 - x_2 + x_3 = -7, \\ -3x_1 - x_2 - 3x_3 = 7, \\ -2x_1 + x_2 - 2x_3 = 8. \end{cases}$$
7. Найти решения системы линейных алгебраических уравнений над кольцом вычетов по модулю 7: $\begin{cases} 3x_1 + 3x_2 + 6x_3 = 5, \\ 5x_1 + 3x_2 + 4x_3 = 2, \\ 6x_1 + x_2 + x_3 = 3. \end{cases}$
8. Доказать, что векторы $\overline{\mathbf{p}} = (0,1,2)$, $\overline{\mathbf{q}} = (1,0,1)$, $\overline{\mathbf{r}} = (-1,2,4)$ образуют базис арифметического пространства $\mathbb{R}^3$ и найти координаты вектора $\overline{\mathbf{a}} = (-2,4,7)$ в этом базисе.
9. Из векторов $\boldsymbol{a_1, a_2, a_3, a_4}$ выбрать базу и разложить остальные по этой базе, где $\boldsymbol{a_1}$=(0,1, -3,4), $\boldsymbol{a_2}$ =(1, 0, -2,3), $\boldsymbol{a_3}$=(5, 2, -16, 23), $\boldsymbol{a_4}$=(1, -1,1, -1).
10. Над полем $\mathbb{R}$ найти многочлен Лагранжа $L(x)$, проходящий через точки $(-3,1)$, $(-1,5)$, $(3,-11)$. Вычислить $L(4)$ по схеме Горнера.
11. Пользуясь схемой Горнера, разложить многочлен $f(x)$ над полем $\mathbb{R}$ по степеням $x-c$, $f(x) = 4x^4 - 3x^3 - 2x^2 + 4x - 5$, $c = -2$.
12. Над кольцом вычетов по модулю 7 найти многочлен Лагранжа $L(x)$, проходящий через точки $(1,4)$, $(2,6)$, $(3,5)$.

13. Над полем $\mathbb{C}$ найти все корни многочлена $x^n - a$, где $n = 3$, $a = 2i$.
14. Найти координаты точек A и B, если известно, что точки $C(-15;12)$ и $D(-12;10)$ делят отрезок AB на три равные части.
15. Составить уравнение прямой, перпендикулярной $5x - 5y - 6 = 0$ и проходящей через точку пересечения прямых $2x - 5y - 7 = 0$ и $3x + 7y + 4 = 0$.
16. Найти точку пересечения прямой $\frac{x-2}{2} = \frac{y-1}{3} = \frac{z-3}{1}$ и плоскости $2x + 3y + z = 0$.
17. Записать уравнение плоскости, проходящей через точку $M_0(4;-1;1)$ перпендикулярно вектору $\overline{N} = \{-1;2;-2\}$. Найти острый угол, который эта плоскость образует с плоскостью $x + z - 6 = 0$.
18. Прямая проходит через точку $M_0(3,7,2)$ параллельно вектору $\overline{l} = (5;8;1)$. Записать уравнение прямой и указать, при каком значении C прямая будет параллельна плоскости $2x - y + Cz - 2 = 0$.
19. Записать уравнение прямой, проходящей через точки $M_1(-4;3;-3)$ и $M_2(2;-6;9)$. Доказать, что она пересекается с прямой $\frac{x-3}{3} = \frac{y-1}{4} = \frac{z-7}{2}$. Найти точку пересечения и угол между ними.

Раздел 3. Дискретная математика

Основные вопросы темы:

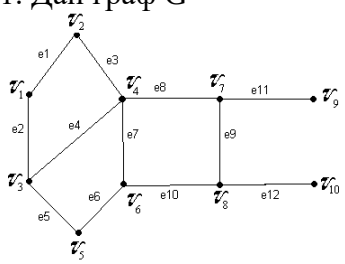
1. Основные комбинаторные величины. Булеан. Размещения и сочетания (с повторением и без повторения). Числа Стирлинга первого и второго рода.
2. Булева алгебра. Понятие булевой функции. Представление булевой функции в виде СДНФ, СКНФ, полиномов Жегалкина. Теорема Поста о полноте системы булевых функций.
3. Понятие графа и связанные с ним определения. Виды представления графа. Полные и двудольные графы. Критерий двудольности графов. Эйлеровы и гамильтоновы графы.

Рекомендации по изучению темы:

1. Гашков С. Б. Дискретная математика : учебник и практикум для вузов / С. Б. Гашков, А. Б. Фролов. 3-е изд., испр. и доп. Москва : Издательство Юрайт, 2019. 483 с. (Высшее образование). ISBN 978-5-534-11613-7. Текст : электронный // ЭБС Юрайт [сайт]. URL: https://www.biblio-online.ru/bcode/445753
2. Новиков Ф.А. Дискретная математика для программистов: Учеб. пособие для вузов.– СПб.: Питер, 2009. – 384 с.
3. Яблонский С.В. Введение в дискретную математику: учеб. пособие. – М.: Высшая школа, 2006. – 392 с.

Задачи для самостоятельной работы:

1. Дан граф G

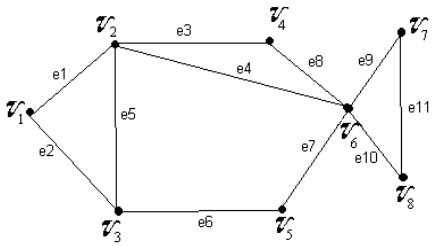


1.1. Определить степени всех вершин графа.

1.2. Записать матрицу смежности вершин $A_1(G)$.

1.3. Записать матрицу инцидентности $A_2(G)$.

1.4. Определить цикломатическое число графа.
1.5. Построить каркас графа путем обхода «в ширину». Построить код.
2. Дан граф G



2.1. Определить степени всех вершин графа.
2.2. Записать матрицу смежности вершин $A_1(G)$.
2.3. Записать матрицу инцидентности $A_2(G)$.
2.4. Определить цикломатическое число графа.
2.5. Построить каркас графа путем обхода «в ширину». Построить код.
3. При помощи таблиц истинности найти СДНФ и СКНФ для $(x \,|\, (x \oplus y)) \downarrow \neg y$
4. При помощи таблиц истинности найти СДНФ и СКНФ для $x \vee ((x \downarrow y) \leftrightarrow (x \wedge y))$
5. При помощи таблиц истинности найти СДНФ и СКНФ для $((x \vee y) \leftrightarrow (\neg x \wedge z)) \,|\, (y \oplus z)$

Раздел 4. Теория вероятностей и математическая статистика
Основные вопросы темы:

1. Вероятностное пространство. Свойства вероятностной меры. Классическое определение вероятности. Условные вероятности. Независимость событий. Формула полной вероятности. Формула Байеса.
2. Случайные величины. Функции распределения случайных величин и их свойства. Плотности распределения. Типовые распределения случайных величин: биномиальное, геометрическое, пуассоновское, равномерное, нормальное.
3. Математическое ожидание и дисперсия случайных величин: определения и основные свойства. Математическое ожидание и дисперсия типовых распределений случайных величин.
4. Статистики, статистические оценки и их свойства. Методы статистического оценивания неизвестных параметров: метод максимального правдоподобия, метод моментов. Основные типы статистических гипотез. Общая логическая схема статистического критерия.

Рекомендации по изучению темы:

1. Вентцель Е.С. Теория вероятностей: учебник для вузов. М.: Академия, 2005. 572 с.
2. Гмурман В.Е. Теория вероятностей и математическая статистика: учеб. пособие для бакалавров: учеб. пособие для вузов. М.: Юрайт, 2012.

Задачи для самостоятельной работы:

1. В ящике лежат пять апельсинов и четыре яблока. Взяли три фрукта. С какой вероятностью все фрукты окажутся одного вида?
2. Первый стрелок попадает в цель с вероятностью 0.6, второй – с вероятностью 0.7. Первый стрелок делает 2 выстрела по мишени, а второй – 3 выстрела. С какой вероятностью не будет ни одного попадания в цель?
3. Завод имеет три источника поставки комплектующих – фирмы А, В, С. На долю фирмы А приходится 50% общего объема поставок, В – 30% и С – 20%. Среди поставляемых фирмой А деталей – 10% бракованных, фирмой В – 5% бракованных и фирмой С – 6%. С какой вероятностью взятая случайным образом деталь окажется пригодной?
4. Передается 4 сообщения по каналу связи. Каждое сообщение с вероятностью 0.1 искажается, независимо от других. Вычислить среднее число неискаженных сообщений. С какой вероятностью ровно три сообщения будут искажены?

5. В партии продукции, состоящей из 25 деталей, 5 бракованных. Определить вероятность того, что при случайном выборе четырех деталей: а) все они окажутся бракованными б) бракованных и не бракованных изделий будет поровну.
6. В автопробеге участвуют 3 автомобиля. Первый может сойти с маршрута с вероятностью 0,15; второй и третий автомобили не дойдут до финиша соответственно с вероятностью 0,05 и 0,1. Требуется определить вероятность того, что к финишу придут: а) только один автомобиль; б) два автомобиля; в) по крайней мере два автомобиля.
7. На сборку поступают детали с трех автоматов. Первый дает в среднем 98% годных деталей, второй – 99%, а третий – 97%. Найти вероятность попадания на сборку бракованной детали, если она выбрана случайным образом, а производительность автоматов одинакова.

Раздел 5. Теоретико-числовые методы в криптографии

Основные вопросы темы:

1. Отношение делимости в кольце целых чисел и его свойства. Наибольший общий делитель и его свойства.
2. Алгоритм Евклида. Обобщенный алгоритм Евклида. Линейные диофантовы уравнения первой степени.
3. Простые числа и их свойства. Решето Эратосфена. Основная теорема арифметики.
4. Мультипликативные функции и их свойства. Функция Эйлера и ее свойства.
5. Отношение сравнимости в кольце целых чисел и его свойства. Полная и приведенная системы вычетов. Теорема Эйлера. Малая теорема Ферма.
6. Сравнения первой степени, методы их решений. Системы сравнений первой степени. Китайская теорема об остатках.
7. Сравнения второй степени. Квадратичные вычеты и невычеты. Символ Лежандра. Символ Якоби.
8. Степенные вычеты. Показатель числа. Первообразные корни по простому модулю.
9. Вероятностные методы проверки простоты натурального числа. Тест Соловея-Штрассена. Тест Миллера-Рабина.
10. Методы дискретного логарифмирования в конечном поле.

Рекомендации по изучению темы:

1. Маховенко Е.Б. Теоретико-числовые методы в криптографии. Учеб. пособие для вузов. М.: Гелиос АРВ, 2006. 320 с.
2. Нестеренко А.Ю. Теоретико-числовые методы в криптографии: учеб. пособие. Моск. гос. ин-т электроники и математики. 2012. 224 с.
3. Рацеев С.М. Математические методы защиты информации [Электронный ресурс]: Электронное учеб. пособие. Ульяновск: УлГУ, 2018. 1 CD-R. № гос. регистрации 0321901084. 592 с.

Задачи для самостоятельной работы:

1. Найти общее решение линейного диофантова уравнения $41x + 23y = 1$.
2. Найти общее решение линейного диофантова уравнения $43x+18y=3$.
3. Разложить рациональное число 129/53 в конечную цепную дробь.
4. Найти значение конечной цепной дроби [3;2,3,1,3].
5. Найти каноническое разложение числа 18! (факториал числа).
6. Найти число и сумму делителей, а также значение функции Эйлера числа 100.
7. Используя теорему Эйлера, найти остаток от деления числа 15^{175} на 11.
8. Используя теорему Эйлера, найти остаток от деления числа $3^{100} + 37^{100}$ на 16.
9. Вычислить обратный элемент, если он существует: $7^{-1} \bmod 41$.
10. Решить сравнение $7x \equiv 10 \pmod{19}$.

11. Решить сравнение $12x \equiv 4 \pmod{17}$.
12. Решить систему сравнений $\begin{cases} x \equiv 1 (\mathrm{mod}\, 3), \\ x \equiv 2 (\mathrm{mod}\, 5), \\ x \equiv 3 (\mathrm{mod}\, 7). \end{cases}$
13. Вычислить, пользуясь свойствами символа Якоби $\left(\frac{82}{101}\right)$.
14. Решить квадратичное сравнение по простому модулю, если решение существует $x^2 \equiv 3 \pmod{11}$.
15. Найти все первообразные корни по модулю 11.

Раздел 6. Основы информационной безопасности

Основные вопросы темы:

1. Классификация угроз информации. Источники угроз информационной безопасности РФ. Модель действий нарушителя.
2. Понятие информационной войны. Составные части и методы информационного противоборства. Информационное оружие.
3. Концепция защиты автоматизированных систем и средств вычислительной техники. Классификация информационных систем по уровню их защищенности.
4. Направления защиты от несанкционированного доступа (НСД). Основные способы НСД. Структура системы защиты информации от НСД, назначение и функции элементов.
5. Правила разграничения доступа к информации. Мандатная и дискреционная модели управления доступом.
6. Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации. Основные методы аутентификации.
7. Технология межсетевых экранов (МЭ). Виды МЭ.
8. Основные понятия и функции виртуальных частных сетей (VPN).

Рекомендации по изучению темы:

1. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности: учеб. пособие для вузов по спец. группы 090100 "Информационная безопасность". М.: Академия, 2009.
2. Иванцов А.М. Методические указания по разработке типовых документов в области информационной безопасности. Ульяновск: УлГУ. 2016. 63 с.
3. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие для вузов. М.: Академия, 2008. 336 с.

Задания для самостоятельной работы:

1. Определить информационные активы выбранного предприятия, основные угрозы для них и способы (средства) их нейтрализации.
2. Разработать план занятия с пользователями ПЭВМ предприятия по обучению работе с электронным замком «СОБОЛЬ».
3. Разработать план занятия с пользователями ПЭВМ предприятия по обучению работе с комплексом средств защиты информации от несанкционированного доступа «АККОРД».
4. Разработать план занятия с пользователями ПЭВМ предприятия по обучению работе с персональными средствами аутентификации и защищенного хранения данных (USB-ключи и смарт-карты eToken).
5. Разработать план занятия с пользователями ПЭВМ предприятия по обучению работе с системой защиты «Dallas Lock 8.0-K(C)».

Раздел 7. Аттестация объектов информатизации

Основные вопросы темы:

1. Организация аттестации объектов информатизации на соответствие требованиям безопасности информации. Порядок проведения аттестации объектов информатизации. Основные и вспомогательные технические средства и системы (ОТСС и ВТСС). Аттестат соответствия.
2. Технические каналы утечки, использующие специально внедренные в указанные технические средства или помещения устройства негласного съема информации.
3. Специальные исследования и специальные проверки технических средств, располагаемых в выделенных и защищаемых помещениях на предмет возможности утечки информации.

Рекомендации по изучению темы:

4. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности: учеб. пособие для вузов по спец. группы 090100 "Информационная безопасность". М.: Академия, 2009.
5. Иванцов А.М. Методические указания по разработке типовых документов в области информационной безопасности. Ульяновск: УлГУ. 2016. 63 с.
6. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие для вузов. М.: Академия, 2008. 336 с.

Раздел 8. Криптографические методы защиты информации

Основные вопросы темы:

1. Совершенные по Шеннону шифры. Необходимые и достаточные условия совершенных шифров. Теорема К.Шеннона. Табличное и модульное гаммирование.
2. Имитация и подмена шифрованных сообщений. Оценки для вероятностей имитации и подмены сообщений. Критерии достижимости нижних оценок.
3. Симметричные блочные шифры. Шифры Фейстеля и их обратимость. Шифр “Магма” из ГОСТ Р 34.12-2015.
4. Шифр “Кузнечик” из ГОСТ Р 34.12-2015. Режимы использования симметричных блочных шифров.
5. Асимметричные шифры. Схема Диффи-Хеллмана. Шифр RSA. Шифр Эль-Гамаля. Шифр Месси-Омуры.
6. Модификация асимметричных шифров на эллиптических кривых. Модификация схемы Диффи-Хеллмана. Модификация шифра Эль-Гамаля. Модификация шифра Месси-Омуры.
7. Хеш-функции. Требования, предъявляемые к хеш-функциям. Криптографические хеш-функции. Способы построения криптографических хеш-функций.
8. Коды аутентификации. Понятие имитации и подмены сообщения. Нижние оценки для вероятностей успеха имитации и подмены. Критерий достижимости нижних оценок. Оптимальные коды аутентификации.
9. Электронная подпись. Электронная подпись на основе асимметричных систем шифрования: электронная подпись RSA, электронная подпись Фиата-Шамира, электронная подпись Эль-Гамаля, электронная подпись Шнорра.

Рекомендации по изучению темы:

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. –М.: Гелиос АРВ, 2005.
2. Рацеев С.М. Математические методы защиты информации [Электронный ресурс]: Электронное учеб. пособие. Ульяновск: УлГУ, 2018. 1 CD-R. № гос. регистрации 0321901084. 592 с.

3. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М.: Горячая линия – Телеком, 2005.
4. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: учеб. пособие для вузов по спец. "Компьютер. безопасность". М.: Академия, 2009.

Задачи для самостоятельной работы:

1. Шифр Месси-Омуры. Пусть a_1, a_2 – пара секретных ключей абонента A, b_1, b_2 – пара секретных ключей абонента B, p – простое число, m – передаваемое сообщение от A к B. Известно, что p=7, a_1=3, b_1=5, m=2. Найти a_2, b_2, m_1, m_2, m_3.
2. Шифр Эль-Гамаля. Пусть x, y – соответственно секретный и открытый ключи абонента A, p – простое число, g – первообразный корень по модулю p (параметры шифрсистемы), m – передаваемое сообщение абоненту A, k – случайное число. Известно, что p=7, g=3, x=5, k=4, m=2. Найти y и шифрованное сообщение (c_1,c_2), передаваемое абоненту A.
3. Шифр RSA. Пусть d, e – соответственно секретный и открытый ключи абонента A, p, q – простые числа абонента A, m – передаваемое сообщение абоненту A. Известно, что p=3, q=7, e=3, m=2. Найти d и шифрованное сообщение y, передаваемое абоненту A.

Раздел 9. Криптографические протоколы

Основные вопросы темы:

1. Протоколы аутентификации, использующие пароли. Протоколы аутентификации, использующие технику “запрос-ответ”.
2. Протоколы аутентификации, использующие технику доказательства знания с нулевым разглашением: общие положения. Протокол Шнорра. Протокол Фиата-Шамира.
3. Модификация протоколов аутентификации на эллиптических кривых: модификация протокола Шнорра, модификация протокола Окамото.
4. Протоколы передачи ключей. Передача ключей с использованием симметричного шифрования. Протокол Kerberos. Передача ключей с использованием асимметричного шифрования. Сертификаты открытых ключей.
5. Протоколы передачи ключей. Открытое распределение ключей. Протокол Диффи-Хеллмана и его усиления. Предварительное распределение ключей.
6. Схемы разделения секрета. Схема Шамира. Схема Ито-Саито-Нишизеки.

Рекомендации по изучению темы:

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. –М.: Гелиос АРВ, 2005.
2. Рацеев С.М. Математические методы защиты информации [Электронный ресурс]: Электронное учеб. пособие. Ульяновск: УлГУ, 2018. 1 CD-R. № гос. регистрации 0321901084. 592 с.
3. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М.: Горячая линия – Телеком, 2005.
4. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: учеб. пособие для вузов по спец. "Компьютер. безопасность". М.: Академия, 2009.

Задачи для самостоятельной работы:

1. Восстановить значение секрета s в схеме Шамира с порогом 2 над кольцом вычетов по модулю 11, если доли двух участников, пытающихся восстановить секрет, равны: (3, 3), (7, 8)
2. Пусть s=3 – секрет. Какие доли данного секрета получит каждый участник (4,2)-пороговой схемы разделения секрета на основе равновесных двоичных кодов.
3. Схема Ито-Саито-Нишизеки. Пусть P={1,2,3,4} – участники разделения секрета s, (R,Z) – структура доступа на P, которая задается множеством минимальных правомочных коалиций $R_{\min}$ = {{1, 2, 3}, {2, 4}, {3, 4}}. Найти множество максимальных непровомочных коалиций $Z_{\max}$ (выписать в лексикографическом порядке), кумулятивный массив C, а также разделить

секрет s=5 (выписать доли секрета для каждого участника).

4. Протокол Фиата-Шамира. Пусть $n = p \cdot q$ – параметр протокола, x, y – соответственно секретный и открытый ключи доказывающего абонента A, k – случайный параметр из первого шага протокола, a – запрос из второго шага протокола. Найти y и привести все вычисления на четырех шагах протокола (найти r, s, проверить соответствующее сравнение) если известно, что p=3, q=7, a=1, x=2, k=10.
5. Протокол Шнорра. Пусть p – простое число, q – простой делитель числа $p-1$, g – элемент из кольца вычетов по модулю p (имеющий порядок q), x, y – соответственно секретный и открытый ключ абонента A, k – случайное число из первого шага протокола. Известно, что $p = 7, q = 3, g = 2, a = 1, x = 2, k = 2$. Найти y и привести все вычисления на четырех шагах протокола (найти r, s проверить соответствующее сравнение).

Раздел 10. Теория кодирования, сжатия и восстановления информации

Основные вопросы темы:

1. Линейные коды: основные понятия. Критерии обнаружения и исправления ошибок. Код Хемминга.
2. Декодирование линейного кода. Синдромы, свойства синдромов, синдромное декодирование. Стандартное расположение для кода.
3. Коды Боуза-Чоудхури-Хоквингема. Кодирование и декодирование кодов БЧХ.
4. МДР коды. Коды Рида-Соломона. Кодирование и декодирование кодов РС.

Рекомендации по изучению темы:

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки. Перевод с англ.: И.И. Грушко, В.М. Блиновский. Под редакцией: К.Ш. Зигангирова. М.: Мир, 1986. 576 с.
2. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: пер. с англ. М: Связь, 1979. 744 с.
3. Сагалович Ю.Л. Введение в алгебраические коды. Учебное пособие. 2-е изд., перераб. и доп. М.: ИППИ РАН, 2010. 302 с.

Задачи для самостоятельной работы:

1. Построить поле GF(2^3) на основе примитивного многочлена x^3+x+1 с примитивным элементом α.
2. Проверочная матрица (7,4,3)-кода Хэмминга задается в лексикографическом порядке слева направо по возрастанию. На приемном конце получен вектор $v = (1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0)$. Исправить ошибку и найти кодовый вектор u.
3. Порождающая матрица линейного (5,2,3)-кода с параметрами $n = 5$, $k = 2$ имеет вид $G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}$. Найти проверочную матрицу H, кодовое расстояние d. Составить таблицу стандартного расположения. С помощью данной таблицы декодировать вектор $v = (0\ \ 0\ \ 1\ \ 0\ \ 1)$, т.е. найти информационный вектор i.
4. Поле $GF(2^4)$ строится с помощью примитивного многочлена $x^4 + x + 1$, α – примитивный элемент. Двоичный код БЧХ с параметрами $n = 15$, $k = 7$ порождается многочленом $g(x) = 1 + x^4 + x^6 + x^7 + x^8$, $\alpha, \alpha^2, \alpha^3, \alpha^4$ – его подряд идущие корни. На приемном конце получен вектор $v = (1,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 1,\ 1,\ 0,\ 1)$, в котором не более двух ошибок. Найти соответствующий кодовый вектор u и информационный вектор i.

5. Поле $GF(3^2)$ строится с помощью примитивного многочлена x^2+x+2, α – примитивный элемент. Код БЧХ над полем $GF(3)$ с параметрами $n=8$, $k=3$ порождается многочленом $g(x)=2+x^2+x^3+2x^4+x^5$, $\alpha,\alpha^2,\alpha^3,\alpha^4$ – его подряд идущие корни. На приемном конце получен вектор $v=(0,\ 2,\ 2,\ 2,\ 2,\ 2,\ 0,\ 1)$, в котором не более двух ошибок. Построить поле $GF(3^2)$. Найти соответствующий кодовый вектор u и информационный вектор i.
6. Поле $GF(2^3)$ строится с помощью примитивного многочлена x^3+x+1, α – примитивный элемент. Код Рида-Соломона с параметрами $n=7$, $k=3$, $d=5$ исправляет до двух ошибок. Во всех задачах кодирование и декодирование производить с помощью многочленов Мэттсона-Соломона. В ответах все компоненты векторов записать в виде степеней элемента α (как в заданиях).

- Закодировать информационный вектор $i=(\alpha^2,\ \alpha,\ \alpha^6)$.
- На приемном конце получен вектор $v=(\alpha,\ \alpha,\ \alpha^4,\ 0,\ \alpha^5,\ \alpha^4,\ \alpha^5)$, в котором не более двух ошибок. Найти соответствующий кодовый вектор u с помощью алгоритма Питерсона-Горенстейна-Цирлера и информационный вектор i.
- На приемном конце получен вектор $v=(\alpha^6,\ 1,\ 1,\ 0,\ 1,\ \alpha^4,\ \alpha^6)$, в котором не более двух ошибок. Найти соответствующий кодовый вектор u с помощью алгоритма Евклида и метода Форни, а также информационный вектор i.

Раздел 11. Техническая защита информации

Основные вопросы темы:

1. Типовая структура и виды технических каналов утечки информации. Классификация технических каналов утечки информации.
2. Методы и средства пассивной и активной защиты от утечки в электромагнитном канале.
3. Методы пассивной и активной защиты утечки информации по акустическому (виброакустическому) каналу.

Рекомендации по изучению темы:

1. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина. М.: Горячая линия - Телеком, 2016. 248 с. ISBN 978-5-9912-0470-5. Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204705.html.
2. Свинарев Н.А., Инструментальный контроль и защита информации [Электронный ресурс]: учеб. пособие / Свинарев Н.А., Ланкин О.В., Данилкин А.П, Потехецкий С.В., Перетокин О.И. Воронеж: ВГУИТ, 2013. 192 с. ISBN 978-5-00032-018-1 Режим доступа: http://www.studentlibrary.ru/book/ISBN9785000320181.html.

Задания для самостоятельной работы:

1. Разработать вариант сведений ограниченного доступа для выбранного предприятия (организации).
2. Разработать вариант Обязательства (Соглашения) о неразглашении информации ограниченного доступа для выбранного предприятия (организации).
3. Составить проект приказа руководителя предприятия «Об организации работ по обеспечению безопасности персональных данных» для выбранного предприятия.
4. Разработать вариант политики администрирования информационных систем для выбранного предприятия (организации).
5. Разработать вариант политики антивирусной защиты для выбранного предприятия

(организации).

6. Разработать вариант политики использования e-mail и доступа к сети Интернет для выбранного предприятия (организации).
7. Разработать вариант политики использования внешних носителей информации для выбранного предприятия (организации).
8. Разработать тезисы выступления перед сотрудниками выбранной организации по доведению требований информационной безопасности.

Раздел 12. Организационное и правовое обеспечение информационной безопасности

Основные вопросы темы:

1. Информация как объект правоотношений. Законодательство РФ в области информационной безопасности.
2. Виды и содержание тайн. Законодательная база охраны государственной, коммерческой и служебной тайн.
3. Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных и первоочередные мероприятия по созданию системы защиты персональных данных на предприятии.
4. Виды деятельности, подлежащие лицензированию. Порядок получения лицензии в области защиты информации.
5. Методы и средства инженерной защиты объектов информатизации.
6. Программные и аппаратные средства защиты информации от несанкционированного доступа.

Рекомендации по изучению темы:

1. Новиков В.К., Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс]: Учебное пособие. / В.К. Новиков. М.: Горячая линия - Телеком, 2015. 176 с. ISBN 978-5-9912-0525-2. Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991205252.html.
2. Судариков С.А., Право интеллектуальной собственности: учебник [Электронный ресурс] / С.А. Судариков. М.: Проспект, 2014. 368 с. ISBN 978-5-392-16752-4. Режим доступа: http://www.studentlibrary.ru/book/ISBN9785392167524.html