МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МУРМАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Методические указания по изучению дисциплины

Б1.О.08.03 Защита информации
(код и наименование дисциплины)

для направления подготовки 09.03.01 Информатика и вычислительная техника
(код и наименование направления подготовки /специальности)

направленности/профиля Программное обеспечение вычислительной техники и автоматизированных систем
(наименование направленности (профиля) образовательной программы)

Кафедра-разработчик: математики, информационных систем и программного обеспечения
(наименование кафедры-разработчика рабочей программы)

Мурманск
2020

Составитель: Богомолов Р.А., доцент каф. МИС и ПО

Методические указания по освоению дисциплины рассмотрены и одобрены на заседании кафедры-разработчика

математики, информационных систем и программного обеспечения
название кафедры

24.11.2020 протокол № 4
дата

Оглавление

ОБЩИЕ ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ УКАЗАНИЯ

Целью дисциплины (модуля) «Защита информации» является формирование компетенций в соответствии с ФГОС по направлению подготовки 09.03.01 «Информатика и вычислительная техника» и учебным планом в составе ОПОП по направлению подготовки 09.03.01 Информатика и вычислительная техника, направленность (профиль) «Программное обеспечение вычислительной техники и автоматизированных систем».

Задачи:

дать необходимые знания по теоретическим основам применения оптических устройств в радиотехнике, позволяющие моделировать на компьютере характеристики таких устройств, а в дальнейшем успешно использовать полученные знания и навыки в проектировании и эксплуатации радиоэлектронных средств.

Процесс изучения дисциплины «Защита информации» направлен на формирование элементов компетенций, представленных в рабочей программе.

В результате изучения дисциплины обучающийся должен:

Знать:

- научно-технические проблемы и перспективы методов защиты информации;
- основные методы хранения, обработки и передачи информации;
- элементы математической теории информации;
- основные источники искажения компьютерной информации;
- базовые методы и средства защиты компьютерной информации;
- американские DES, AES и российский ГОСТ 28147-89 стандарты шифрования данных.

Уметь:

- применять методы алгебры, дискретной математики, математической статистики, программирования для разработки средств защиты компьютерной информации;
- производить вычисления в конечных кольцах и полях;
- пользоваться методами выработки критериев оценки эффективности методов и средств защиты компьютерной информации.

Владеть:

- представлением о методах организации защищённого хранения и передачи данных;
- представлением об основных стандартах шифрования данных.

Данные методические указания по освоению дисциплины «Защита информации» содержат методические рекомендации к практическим работам, к контрольной работе,

РГР и к самостоятельной работе студентов.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная литература

1. Алексеев, В. А. Методы и средства криптографической защиты информации : методические указания к проведению лабораторных работ по курсу «Методы и средства защиты компьютерной информации» / В. А. Алексеев. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2009. — 16 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/17710.html

2. Методы и средства инженерно-технической защиты информации : учебное пособие / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, Т. Р. Гайнулин. — Брянск : Брянский государственный технический университет, 2012. — 187 с. — ISBN 5-89838-357-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/7000.html

Дополнительная литература

1. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях.-М.:Издательство агентства “Яхтсмен”.-1993.-188 с.

2. Башлы, П. Н. Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — М. : Евразийский открытый институт, 2012. — 311 с. — ISBN 978-5-374-00301-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/10677.html

СОДЕРЖАНИЕ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

Целями практических занятий в процессе изучения дисциплины являются:

– систематизация и закрепление полученных теоретических знаний и практических умений студентов;

– углубление и расширение теоретических знаний;

– формирование умений использовать справочную и специальную литературу;

– развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

– формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

– развитие исследовательских умений.

Объем времени, отведенный на практические занятия, определяется в соответствии с учебным планом специальности и рабочей программой учебной дисциплины.

Основные формы проведения практических занятий:

– для овладения знаниями: публичное обсуждение студентами во время практического занятия основных особенностей и свойств изучаемых в курсе задач и методов их решения и др.;

– для закрепления и систематизации знаний: подготовка студентами сообщений к выступлению на практическом занятии, проводимом в форме семинара;

– для формирования умений: практическое решение задач с помощью изучаемых в курсе методов, содержательный сравнительный анализ получаемых результатов.
Практические занятия проводятся с группами студентов.

Контроль работы студентов на практическом занятии осуществляется в пределах времени, отведенного на практические занятия по дисциплине с предоставлением студентами фактических результатов выполнения практических заданий.
В качестве форм и методов контроля результатов работы студентов на практических занятиях могут быть использованы тестирование, самоотчеты, контрольные работы и др.

Критерием оценки результатов работы студента на практических занятиях являются:

– умение студента использовать теоретические знания при выполнении практических задач;
– обоснованность и четкость изложения ответа;
– оформление материала в соответствии с требованиями.

Перечень практических занятий:

Практическое занятие № 1. Обзор современных методов и средств защиты компьютерной информации.
Практическое занятие № 2. Источники атак, анализ рисков и формы атак на компьютерную информацию
Практическое занятие № 3. Методы несанкционированного воздействия на компьютерную информацию
Практические занятия № 4-5. Стандарты шифрования.
Практическое занятие № 6. Криптографические модели и алгоритмы шифрования
Практические занятия № 7-8. Методы обеспечения безопасности основных операционных систем и сетей
Практическое занятие № 9. Математические аспекты и структурные схемы алгоритмов программных средств защиты компьютерной информации
Практическое занятие № 10. Использование языков программирования для реализации средств защиты
Практические занятия № 11-12. Введение в алгебраическую теорию информации
Практические занятия № 13-14. Введение в алгебраическую теорию кодирования
Практические занятия № 15-16. Проектирование программного средства защиты и методы оценки его надежности и эффективности

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К САМОСТОЯТЕЛЬНОЙ РАБОТЕ

Целями самостоятельной работы студентов являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать справочную и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений.

Самостоятельная работа является одним из видов учебных занятий студентов, проводится внеаудиторно, выполняется студентом по заданию преподавателя, но без его непосредственного участия.

Объем времени, отведенный на самостоятельную работу, определяется в соответствии с учебным планом специальности и рабочей программой учебной дисциплины.

Основные формы самостоятельной работы:

- для овладения знаниями: чтение текста (учебника, первоисточника, дополнительной литературы); конспектирование текста; выписки из текста; работа со справочниками; учебно-исследовательская работа; использование компьютерной техники и Интернета и др.;
- для закрепления и систематизации знаний: работа с конспектом лекций (обработка текста); повторная работа над учебным материалом (учебником, первоисточником, дополнительной литературой); составление плана и тезисов ответа; составление таблиц для систематизации учебного материала; ответы на контрольные вопросы; аналитическая обработка текста (аннотирование, рецензирование, реферирование и др.); подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов; составление библиографии; тестирование и др.;
- для формирования умений: решение задач и упражнений по образцу; выполнение контрольных и расчетно-графических работ.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Контроль результатов самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия по дисциплине, может проходить в письменной, устной или смешанной форме, с предоставлением продукта творческой деятельности студента.

В качестве **форм и методов контроля самостоятельной работы** студентов могут быть использованы семинарские занятия, коллоквиумы, зачеты, тестирование, самоотчеты, контрольные работы, защита творческих работ и др.

Критерием оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умение студента использовать теоретические знания при выполнении практических задач;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями.

ТЕМАТИЧЕСКИЙ ПЛАН

-

Наименование тем и содержание самостоятельной работы	Кол-во часов	
	очная	заочная
1. Обзор современных методов и средств защиты компьютерной информации.	8	11
2. Источники атак, анализ рисков и формы атак на компьютерную информацию	8	12

3. Методы несанкционированного воздействия на компьютерную информацию	8	11
4. Стандарты шифрования	8	12
5. Криптографические модели и алгоритмы шифрования	8	12
6. Методы обеспечения безопасности основных операционных систем и сетей	6	11
7. Математические аспекты и структурные схемы алгоритмов программных средств защиты компьютерной информации	8	11
8. Использование языков программирования для реализации средств защиты	6	12
9. Введение в алгебраическую теорию информации	6	12
10. Введение в алгебраическую теорию кодирования	6	12
11. Проектирование программного средства защиты и методы оценки его надежности и эффективности	8	12

СОДЕРЖАНИЕ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ К РАСЧЕТНО-ГРАФИЧЕСКОЙ РАБОТЕ

В РГР должны быть представлены многочлены второй степени, коэффициентами которых являются ASCII – коды инициалов студента, некоторые простейшие криптопреобразования этих многочленов и оценена степени сходства и различия между исходным и преобразованными многочленами по различным критериям.

Перечень заданий, предъявляемых студентам

1. Используя стандартную ASCII – кодировку представить каждую букву собственных инициалов в виде шестнадцатеричной и двоичной последовательностей. Массиву $\{a_0, a_1, a_2\}$ присвоить значения этих кодов в порядке {Ф.,И.,О.}.
2. Построить многочлен $f(x) = a_0 + a_1 x + a_2 x^2$. Используя всевозможные перестановки трех элементов, из многочлена $f(x)$ построить еще пять многочленов отличающихся перестановкой $P^{(k)}$ коэффициентов. Для перечисления перестановок и многочленов пользоваться единой нумерацией согласно таблице 1.

Таблица 1

№п/п	0	1	2	3	4	5
$P^{(k)}$	(0 1 2)	(1 0 2)	(2 0 1)	(0 2 1)	(1 2 0)	(2 1 0)
$f_k(x)$	$a_0 + a_1 x + a_2 x^2$	$a_1 + a_0 x + a_2 x^2$	$a_2 + a_0 x + a_1 x^2$	$a_0 + a_2 x + a_1 x^2$	$a_1 + a_2 x + a_9 x^2$	$a_2 + a_1 x + a_0 x^2$

3. Считая отрезок [a,b] (a и b далее в таблице вариантов) областью определения всех указанных многочленов, вычислить аналитически расстояния $\rho(f, f_k) = \sqrt{\int_a^b (f(x) - f_k(x))^2 dx}$, скалярные произведения $(f, f_k) = \int_a^b f(x) f_k(x) dx$ и угловые характеристики $\cos\Psi_k = (f, f_k) / \|f\| / \|f_k\|$. Здесь $\|f\| = \|f_k\| = \sqrt{\int_a^b f^2(x) dx}$.

   Записать полученные аналитические формулы и, с помощью программы на языке высокого уровня, получить численные значения этих формул. Результаты представить в таблице 2 следующего вида.

Таблица 2

№п/п	0	1	2	3	4	5
$\rho(f, f_k)$						
(f, f_k)						
$\cos\Psi_k$						

4. По результатам п.п. 1-3 сделать выводы о достоинствах и недостатках криптоалгоритма, основанного на перестановках коэффициентов многочлена.
5. Разбивая отрезок [a, b] на n=256 частей построить массив значений функции $f(x)$, $F(s) = f(a + s\Delta x), s = 0,..., n-1; \Delta x = (b-a)/n$.
6. Для $m = 1,..., n$ раэбить массив $F(s)$ на последовательные подмассивы содержащие по m элементов . Так как в общем случае $n = dm + r$, то получится ровно d подмассивов из m элементов, а при r, отличном от нуля, еще и подмассив из r элементов. В каждом подмассиве из m элементов осуществляется циклическая перестановка из конца в начало на t элементов, $t = [m/2]$, [*] обозначает целую часть числа. В подмассиве из r элементов перестановка не осуществляется. Преобразуя таким образом массив $F(s)$ для фиксированного m необходимо получить массив $Fm(s)$. m=1 соответствует исходному массиву. В цикле по m вычислить расстояния $\rho(F, Fm) = \sum_{s=0}^{n-1} (F(s) - Fm(s))^2$, скалярные произведения $(F, Fm) = \sum_{s=0}^{n-1} F(s) Fm(s)$ и угловые характеристики $\cos\Psi_m = (F, Fm) / \|F\| / \|Fm\|$, $\|F\| = \|Fm\| = \sum_{s=0}^{n-1} F^2(s)$. Полученные результаты представить в виде графиков зависимости расстояний, скалярных произведений и угловых характеристик от m.
7. Объяснить полученные зависимости и сделать выводы о зависимости действия рассмотренного криптоалгоритма от m.
8. Разбивая отрезок [a, b] на n=64 части построить массив значений функции $f(x)$, $F(s) = f(a + s\Delta x), s = 0,..., n-1; \Delta x = (b-a)/n$.
9. Для m=1,2,4,8,16,32,64 реализовать перестановку массива аналогичную п.6.

10. Для массивов полученных в п.9 построить точечные графики зависимости $F(s)$ от s=0,…,63.
11. Для массивов полученных в п.9 осуществить дискретное преобразование Фурье и построить дискретные графики амплитудного и фазового спектров.
12. Сделать выводы о том, как влияет примененный криптоалгоритм на изменение временной формы сигналов и формы амплитудного и фазового спектров.

Замечание 1.

Если два из трех инициалов совпадают, то один из совпадающих инициалов заменяется его номером в русском алфавите представленным в виде двоичной восьмибитовой комбинации. Если все три инициала совпадают, то в качестве исходных данных для выполнения РГЗ берется инициал, его номер в русском алфавите представленный в виде двоичной восьмибитовой комбинации и инвертированная двоичная восьмибитовая комбинация $0 \to 1, 1 \to 0$.

Замечание 2.

Значения a и b выбираются студентом из Таблицы 3 согласно формуле Nтаб=Nсп+(Nгр-1)*15. Nгр – последняя цифра номера группы.

№ п/п	a	b
1	1	2
2	2	3
3	3	4
4	4	5
5	5	6
6	0.1	0.2
7	0.2	0.3
8	0.3	0.4
9	0.4	0.5
10	0.5	0.6
11	1	3
12	2	4
13	3	5
14	4	6
15	5	7
16	0.1	1.1
17	0.2	1.2
18	0.3	1.3
19	0.4	1.4
20	0.5	1.5
21	.1	1.1
22	.2	1.1
23	.3	1.1
24	.4	1.1
25	.5	1.1
26	0.1	1
27	0.2	1
28	0.3	1
29	0.4	1

30	0.5	1