МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

Методические рекомендации по практическим занятиям

междисциплинарного курса: МДК.02.02.2 Обеспечение защиты информации и тестирование функций программных и программно-аппаратных средств

Специальность: 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация выпускника: Техник по защите информации

Нормативный срок обучения: 3 года 10 месяцев

Форма обучения: Очная

2021

Методические указания по практическим занятиям междисциплинарного курса: МДК.02.02.2 Обеспечение защиты информации и тестирование функций программных и программно-аппаратных средств разработаны на основе федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.15 Обеспечение информационной безопасности автоматизированных систем
Утвержденным приказом Минобрнауки России от 09.12.2016г. №1553
дата утверждения и №)

Методические указания рассмотрены на заседании методического совета СПК и рекомендованы к использованию

«19» 02. 2020 года Протокол № __1__
Председатель методического совета СПК
Сергеева Светлана Ивановна _____

Методические указания утверждены на заседании педагогического совета СПК «28» 02. 2020 года Протокол № _6__
Председатель педагогического совета СПК
Облиенко Алексей Владимирович _____

Организация-разработчик: ФГБОУ ВО «ВГТУ»

Разработчики:
__ Демихова Ирина Владимировна_____
(Ф.И.О., ученая степень, звание, должность

_____
(Ф.И.О., ученая степень, звание, должность)

_____
(Ф.И.О., ученая степень, звание, должность)

_____
(Ф.И.О., ученая степень, звание, должность)

ПРАКТИЧЕСКАЯ РАБОТА № 1

Применение классических шифров замены

Цель: научиться применять классические шифры замены.

Теоретические вопросы

1. Понятие криптографии.
2. Понятие шифра.
3. Шифр замены.
4. Шифр многоалфавитной замены.
5. Сходства и различия шифра Гронсфельда и шифра Цезаря.
6. Биграммный шифр замены.

Задание 1. Выбрать один из методов замены:

а) шифр Атбаш;

б) шифр Цезаря;

в) шифр Полибианский квадрат;

г) шифр Трисимуса;

д) шифр многоалфавитной замены Вижинера;

е) шифр биграммами;

ж) шифр Гронсфельда.

Составить алгоритм программы шифрования по выбранному методу.

Задание 2. Составить программу шифрования по выбранному методу.

Задание 3. Составить алгоритм программы расшифрования по выбранному методу. Составить программу расшифрования по выбранному методу.

Задание 4. Расшифровать текст,

а) зашифрованный шифром Цезаря со сдвигом на 4 позиции:

Уокдгнбэылмбаноюзыбожмдлокнднебиь

б) зашифрованный шифром Цезаря со сдвигом на 6 позиции:

Иыфщлзвмелнмцйкяиыкъбиьъзвгйякялмъзиьдъвбъжязъ

в) зашифрованный заменой по кодовому слову «пароль»:

випигыпжоймгсзпчгумйрпигяиьлйжбийржгясыипипльбийнсынгнсьзъ

ПРАКТИЧЕСКАЯ РАБОТА № 2

Применение классических шифров перестановки

Цель: научиться применять классические шифры перестановки.

Теоретические вопросы

1. Понятие криптографии.
2. Понятие шифра.
3. Шифр перестановки.
4. Модификации шифров перестановки по таблице.
5. Понятие «магический квадрат».
6. Особенность шифра решетками.

Задание 1. Выбрать один из методов перестановки:

а) обратное написание текста;

б) простая перестановка по таблице;

в) одиночная перестановка по ключу по таблице;

г) одиночная перестановка символов с пропусками по таблице;

д) двойные перестановки столбцов и строк;

е) шифр «Магический квадрат»;

ж) шифр «Решетки» или «Трафареты».

Составить алгоритм программы шифрования по выбранному методу.

Задание 2. Составить программу шифрования по выбранному методу.

Задание 3. Составить алгоритм программы расшифрования по выбранному методу. Составить программу расшифрования по выбранному методу.

Задание 4. Дешифровать сообщения:

а) Бирои имч еыеес витсч арзки танет есарл лпюсп мотоо еипнф кйаои крслт мн;

б) тиооско нцрпоед иявдттж афэелиа ткокнбв еапанъг уитриоб;

в) икинорткелэоидаржделлок.

ПРАКТИЧЕСКАЯ РАБОТА № 3
Применение метода гаммирования

Цель: научиться применять метод гаммирования.

Теоретические вопросы

1. Гаммирование: основные определения.
2. Алгоритм шифрования текста методом гаммирования.
3. Двоичное гаммирование: основные особенности.

Задание 1. Выбрать один из способов гаммирования:

а) гаммирование по модулю К;

б) двоичное гаммирование.

Составить алгоритм программы шифрования по выбранному методу.

Задание 2. Составить программу шифрования по выбранному методу.

Задание 3. Составить алгоритм программы расшифрования по выбранному методу. Составить программу расшифрования по выбранному методу.

ПРАКТИЧЕСКАЯ РАБОТА № **4**
Криптоанализ шифра простой замены методом анализа частотности символов

Цель: научиться выполнять криптоанализ шифра простой замены методом анализа частотности символов.

Теоретические вопросы

1. Понятие криптоанализа.
2. Методика криптоанализа, основанная на исследовании частотности закрытого текста.

3. Правило А. Керхоффа.

Задание 1. Получить от преподавателя текстовый файл, содержащий большой художественный текст на русском языке в открытом виде. Написать программу «Частота символов». Исследовать частотность символов открытого теста.

Задание 2. Получить от преподавателя текстовый файл, содержащий большой объем зашифрованного текста на русском языке. Исследовать частотность зашифрованного текста.

Задание 3. Сравнивая реальную частотность символов русского языка, полученную в пункте 1, с частотностями зашифрованного текста, составить таблицу замен алгоритма шифрования и расшифровать зашифрованный текст, реализовав программу дешифровки. Дешифровке подвергните только первые 15–20 символов, наиболее часто встречающиеся в шифротексте.

Задание 4. Выполнить эвристический анализ текста, полученного в результате дешифровки. По смыслу текста выявить те замены, которые оказались неверными, и сформировать верные замены. Доведите результат дешифровки до приемлемого (удобочитаемого) вида.

ПРАКТИЧЕСКАЯ РАБОТА № 5

Криптоанализ классических шифров методом полного перебора ключей

Цели: научиться выполнять криптоанализ классических шифров методом полного перебора ключей.

Теоретические вопросы

1. Понятие криптоанализа.
2. Понятие стойкости криптографического алгоритма.
3. Типовые методы криптоанализа классических алгоритмов.
4. Инструменты криптоанализа

Задание 1. Расшифровать фразу, зашифрованную столбцовой перестановкой:

a) ОКЕСНВРП_ЫРЕАДЕЫН_В_РСИКО;

b) ДСЛИЕЗТЕА_Ь_ЛЬЮВМИ_ _АОЧХК;

c) НМВИАИ_НЕВЕ_СМСТУОРДИАНКМ;

d) ЕДСЗЬНДЕ_МУБД_УЭ_КРЗЕМНАЫ;

e) СОНРЧОУО_ХДТ_ИЕИ_ВЗКАТРРИ.

Задание 2. Расшифровать фразу, зашифрованную двойной перестановкой (сначала были переставлены столбцы, затем строки):

a) СЯСЕ_ _ЛУНЫИАККННОГЯДУЧАТН;

b) МСЕЫ_ЛЫВЕНТОСАНТУЕИ_РЛПОБ;

c) АМНРИД_УЕБСЫ_ЕЙРСООКОТНВ_;

d) ОПЧУЛС_БООНЕВ_ОЖАЕОНЕЩЕИН;

e) ЕШИАНИРЛПГЕЧАВРВ_СЕЫНА_ЛО.

Задание 3. Расшифровать текст. Каждой букве алфавита соответствует двузначное число:

1) 39 25 20 34 82 63 66 46 35 20 25 82 86 39 51 74 35 51 66 20 44 37 25 27

51 35 44 20 90 37 51 25 25 51 63 91 20 11 37 46 48 25 20 37 61 51 14 82 82 66 82

35 29 82 91 25 51 74 51 24 78 51 24 59 46 86 51 44 74 20 25 37 37, 37 44 82 31 11

37 82 51 46 25 51 34 82 25 37 82 86 37 25 27 51 35 44 20 90 37 51 25 25 48 44

46 82 78 25 51 14 51 18 37 59 44, 51 74 82 35 20 90 37 59 44 66 90 82 25 25 48 44
37 61 10 44 20 18 20 44 37, 86 61 20 25 86 51 39 66 86 51 44 10 66 82 86 46 51
35 10 37 66 51 46 51 39 51 63 66 39 59 91 37. 56 46 51 86 20 66 20 82 46 66
59 24 35 10 18 37 78 51 35 18 20 25 37 91 20 90 37 63, 4651, 66 51 18 14 20 66
25 51 35 82 91 10 14 29 46 20 46 20 44 35 20 91 14 37 56 25 48 78 37 66 66 14 82
24 51 39 20 25 37 63, 35 10 86 51 39 51 24 37 46 82 14 37 44 25 51 18 37 78 37 91
25 37 78 91 25 20 31 46 51 61 51 66 25 51 39 25 48 78 39 37 24 20 78 10 18
35 51 91, 25 51 25 82 10 24 82 14 59 31 46 24 51 14 42 25 51 18 51 39 25 37
44 20 25 37 59 24 20 25 25 48 44 39 51 74 35 51 66 20 44, 66 56 37 46 20 59,
56 46 51 51 61 82 66 74 82 56 82 25 37 82 37 25 27 51 35 44 20 90 37 51 25 25 51 63
61 82 91 51 74 20 66 25 51 66 46 37 25 82 37 44 82 82 46 66 44 48 66 14 20, 82
66 14 37 51 46 66 10 46 66 46 39 10 82 46 39 37 24 37 44 20 59 10 18 35 51 91 20;
2) 74 29 23 27 17 99 71 25 49 32 29 34 27 63 32 25 17 99 60 62 25 34 95 29 53
59 82 27 71 29 77 99 34 27 91 17 99 71 49 99 27 15 60 32 25 50 27 17 62 27 95 27
50 25 91 32 59 77 95 29 50 25 99 59, 25 99 74 29 53 25 59 17 99 25 91 23 49 71 25
17 99 60 49 25 34 32 25 71 95 27 82 27 32 32 25 29 50 17 25 15 77 99 32 59 77
62 95 25 53 95 29 23 32 25 17 99 60 34 15 35 17 27 99 27 71 25 12 25 99 95 29 45
49 74 29. 62 95 27 63 34 27 71 17 27 12 25, 50 27 17 62 27 95 27 50 25 91 32 29
35 95 29 50 25 99 29 17 29 82 49 83 62 25 17 27 50 27 62 95 25 34 59 74 99 25
71 50 27 53 25 62 29 17 32 25 17 99 49 17 71 35 53 29 32 29 17 32 29 15 49 23
49 27 82 32 29 34 27 63 32 25 95 29 50 25 99 29 77 10 27 12 25 25 50 25 95 59 34
25 71 29 32 49 35 49 95 27 53 27 95 71 49 95 25 71 29 32 49 27 82 74 95 49 99 49 23
32 89 83 74 25 99 74 29 53 59 50 15 25 74 25 71 62 49 99 29 32 49 35 49 53
29 62 25 82 49 32 29 77 10 49 83 59 17 99 95 25 91 17 99 71. 34 15 35 62 25 17 15
27 34 32 49 83 25 62 99 49 82 29 15 60 32 25 62 95 49 82 27 32 27 32 49 27 34 49
17 74 25 71 89 83 82 29 17 17 49 71 25 71 12 25 95 35 23 27 91 53 29 82 27 32 89.
74 29 23 27 17 99 71 25 49 32 29 34 27 63 32 25 17 99 60 95 29 50 25 99 89 34
25 17 99 49 12 29 27 99 17 35 25 62 99 49 82 49 53 29 67 49 27 91 62 95 25 12 95 29
82 82 32 25 12 25 25 50 27 17 62 27 23 27 32 49 35.

ПРАКТИЧЕСКАЯ РАБОТА № 6
Криптоанализ шифра Вижинера

Цель: научиться выполнять криптоанализ шифра Виженера.

Теоретические вопросы

1. Понятие криптоанализа.
2. Шифр Виженера.

Задание 1. Составить алгоритм шифрования и расшифрования методом Виженера.

Задание 2. Задан некоторый текст зашифрованный шифром Виженера, требуется определить ключевое слово и прочитать открытый текст.

Шифрованный текст

Влцдутжбюцхъяррмшбрхцэооэцгбрьцмйфктъъюьмшэсяцпунуящэйтаьэдкцибр

ьцгбрпачкъуцпъбьсэгкцъгуущарцёэвърюуоюэкааэбрняфукабъарпяъафкъиьжяффнйо
яфывбнэнфуюгбрьсшьжэтбэёчюъюръегофкбьчябашвёэуъъюаднчжчужцёэвлрнчулб
юпцуруньъшсэюъзкцхъяррнрювяспэмасчкпэужьжыатуфуярюравртубурьпэщлафоуф
бюацмнубсюкйтаьэдйюнооэгюожбгкбрънцэпотчмёодзцвбцшщвщепчдчдръюьскасэг
ъппэгюкдойрсрэвоопчщшоказръббнэугнялёкьсрбёуыэбдэулбюасшоуэтъшкрсдугэфл
бубуъчнчтртпэгюкиугюэмэгюккъъпэгяапуфуэзьрадзьжчюрмфцхраююанчёчюъыхьъ
цомэфъцпоирькнщпэтэузуябащущбаыэйчдфрпэцъьрьцъцпоилуфэдцойэдятррачкубу
фнйтаьэдкцкрннцюабугюуубурьпйюэъжтгюркующоъуфъэгясуоичщщчдцсфырэдщэ
ъуяфшёчцюйрщвяхвмкршрпгюопэуцчйтаьэдкцибрьцыяжтюрбуэтэбдуящэубъибрюв
ъежагибрбагбрымпуноцшяжцечкфодщоъчжшйуъцхчщвуэбдлдъэгясуахзцэбдэулькнъ
щбжяцэьрёдъьвюврнуяфуоухфекьгцччгэъжтанопчынажпачкъуъмэнкйрэфщэъьбуд
эндадъярьеюэлэтчоубъцэфэвлнёэгфдсэвэёкбсчоукгаутэыпуббцчкпэгючсаъбэнэфърк
ацхёваетуфяепьрювържадфёжбьфутощоявьъгупчршуитеачйчирамчюфчоуяюонкяжы
кгсцбрясшчйотъъжрсщчл

ПРАКТИЧЕСКАЯ РАБОТА № 7
Применение методов генерации ПСЧ

Цель: изучение способов применения методов генерации ПСЧ.

Теоретические вопросы

1. Псевдослучайные числа.
2. Генератор псевдослучайных чисел.
3. Свойства генератора псевдослучайных чисел для использования в криптографических целях.
4. Принципы использования генераторов псевдослучайных чисел при потоковом шифровании.
5. Методы генерации ПСЧ.

Задание 1. Написать программу, выполняющую задачу исследования ДСЧ для одного из следующих вариантов:

1. Исследовать равномерность датчика (проверить гипотезу о равномерности распределения совокупности ДСЧ).
2. Определить период ДСЧ для различных параметров.
3. Исследовать автокорреляцию совокупности ДСЧ для различных параметров на глубину 100 отсчетов.
4. Построить гистограмму частоты появления каждого возможного значения совокупности ДСЧ.

Задание 2. Разработать и отладить ПО для исследования датчика псевдослучайных чисел. Представить результаты исследования в графическом виде.

ПРАКТИЧЕСКАЯ РАБОТА № 8
Кодирование информации

Цель: изучение способов кодирования информации.

Теоретические вопросы

1. Кодирование информации.
2. Символьное кодирование информации.
3. Смысловое кодирование информации.

Задание 1. Дана кодовая таблица азбуки Морзе:

А • —	Л • — • •	Ц — • — •
Б — • • •	М — —	Ч — — — •
В • — —	Н — •	Ш — — — —
Г — — •	О — — —	Щ — — • —
Д — • •	П • — — •	Ъ • — — • — •
Е •	Р • — •	Ы — • — —
Ж • • • —	С • • •	Ь — • • —
З — — • •	Т —	Э • • — • •
И • •	У • • —	Ю • • — —
Й • — — —	Ф • • — •	Я • — • —
К — • —	Х • • • •	

Декодируйте сообщение:

—— ——— • — • • ——— — • • — • — • — • ——

Закодируйте с помощью азбуки Морзе слова ПАРОЛЬ, ЭКРАНИРОВАНИЕ, КОДИРОВАНИЕ.

Задание 2. Дана таблица ASCII-кодов:

Таблица ASCII-кодов															
SP	!	"	#	$	%	&	`	(	)	*	+	,	-	.	/
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
@	A	B	C	D	E	F	G	M	I	J	K	L	M	N	O
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
`	a	e	c	d	e	f	g	h	i	j	k	l	m	n	0
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

Расшифровать слово при помощи таблицы ASCII кодов: 49 20 6C 6FF 75.

Закодировать при помощи таблицы ASCII кодов слово Windows. Результат представить в шестнадцатеричной системе счисления.

Задание 3. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца):

	0	1	2	3	4	5	6	7	8
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	»				

С помощью этой кодировочной таблицы закодируйте фразу: Я ЗНАЮ МЕТОДЫ ШИФРОВАНИЯ.

Задание 4. Используя таблицу кодирования.

№ п/п	*Символ*	*Двоичный код*
1	Р	101
2	О	100
3	И	010
4	Е	011
5	П	1110
6	М	1100
7	ПРОБЕЛ	1101
8	А	0010
9	С	0011
10	Г	00000
11	В	00001
12	К	00010
13	Б	00011
14	З	111100
15	Т	111101
16	Ь	111110
17	Н	111111

Закодируйте слово СИМВОЛ. Рассчитайте полученную степень сжатия. Раскодируйте слово 11101011000000010100101100110000010.

Задание 5. Смысловое кодирование – это кодирование, в котором в качестве исходного алфавита используются не только отдельные символы (буквы), но и слова и даже наиболее часто встречающиеся фразы.

Рассмотрим пример одноалфавитного и многоалфавитного смыслового кодирования.

Пример. Открытый текст: "19.9.1992 ГОДА". Таблица кодирования представлена в таблице:

Элементы открытого текста	Коды
1	089 146 214 417
2	187 226 145 361
_	_
9	289 023 194 635
ГОД	031 155 217 473
_	786 432 319 157

Закодированное сообщение при одноалфавитном кодировании:

"089 289 786 289 786 089 289 289 187 031".

Закодированное сообщение при многоалфавитном кодировании:

"089 289 786 023 432 146 194 635 187 031" (при многоалфавитном кодировании одинаковые символы заменяются кодами из следующего столбца).

Разработайте и примените свой вариант смыслового кодирования информации.

ПРАКТИЧЕСКАЯ РАБОТА № 9

Программная реализация классических шифров

Цель: изучение способов кодирования информации.

Теоретические вопросы

1. Основные понятия криптографии.
2. Основные понятия криптоанализа.
3. Методы шифрования и кодирования информации.

Задание 1

Вариант 1

В Средние века для шифрования перестановкой применялись и магические квадраты. Магическими квадратами называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

Шифруемый текст вписывали в магические квадраты в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифртекст, сформированный благодаря перестановке букв исходного сообщения. В те времена считалось, что созданные с помощью магических квадратов шифртексты охраняет не только ключ, но и магическая сила.

Пример магического квадрата и его заполнения сообщением «Прилетаю восьмого» показан ниже (рисунок 3).

Шифртекст, получаемый при считывании содержимого правой таблицы по строкам, имеет вполне загадочный вид

ОИРМ ЕОСЮ ВТАЬ ЛГОП.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

О	И	Р	М
Е	О	С	Ю
В	Т	А	Ь
Л	Г	О	П

Рисунок 3

Число магических квадратов быстро возрастает с увеличением размера квадрата. Существует только один магический квадрат размером 3 × 3 (если не учитывать его повороты). Количество магических квадратов 4 × 4 составляет уже 880, а количество магических квадратов 5 × 5 – около 250000.

Пользуясь изложенным способом создать программу, которая:

а) зашифрует введенный текст и сохранит его в файл;

б) считает зашифрованный текст из файла и расшифрует данный текст.

Вариант 2

Для обеспечения дополнительной скрытности можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется двойной перестановкой. В случае двойной перестановки столбцов и строк таблицы перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровании порядок перестановок должен быть обратным.

Пример выполнения шифрования методом двойной перестановки показан на рисунке 4. Если считывать шифртекст из правой таблицы построчно блоками по четыре буквы, то получится следующее: ТЮАЕ ООГМ РЛИП ОЬСВ.

	4	1	3	2
3	П	Р	И	Л
1	Е	Т	А	Ю
4	В	О	С	Ь
2	М	О	Г	О

Исходная таблица

	1	2	3	4
3	Р	Л	И	П
1	Т	Ю	А	Е
4	О	Ь	С	В
2	О	О	Г	М

Перестановка столбцов

	1	2	3	4
1	Т	Ю	А	Е
2	О	О	Г	М
3	Р	Л	И	П
4	О	Ь	С	В

Перестановка строк

Рисунок 4

Ключом к шифру двойной перестановки служит последовательность номеров столбцов и номеров строк исходной таблицы (в нашем примере последовательности 4132 и 3142 соответственно).

Число вариантов двойной перестановки быстро возрастает при увеличении размера таблицы:

• для таблицы 3 × 3 – 36 вариантов;

• для таблицы 4 × 4 – 576 вариантов;

• для таблицы 5 ×5 – 14400 вариантов.

Пользуясь изложенным способом создать программу, которая:

а) зашифрует введенный текст и сохранит его в файл;

б) считает зашифрованный текст из файла и расшифрует данный текст.

ПРАКТИЧЕСКАЯ РАБОТА № 10

Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.

Цель: ознакомиться с меню, возможностями программы CrypTool.

Теоретические вопросы

1. Основные понятия криптографии.
2. Основные понятия криптоанализа.
3. Методы шифрования и кодирования информации.

Задание 1. Ознакомиться с меню, возможностями программы CrypTool.

Задание 2. Перечислите классические алгоритмы шифрования, которые описаны и реализованы в программе CrypTool.

Задание 3. Зашифровать и расшифровать сообщение с помощью одного из имеющегося в программе CrypTool классического шифра замены и шифра перестановки.

ПРАКТИЧЕСКАЯ РАБОТА № 11

Изучение программной реализации современных симметричных шифров

Цель: ознакомиться с современными симметричными шифрами.

Теоретические вопросы

1. Понятие криптографической системы.
2. Классификация криптографических систем.
3. Симметричные шифры.
4. Блочные алгоритмы шифрования.

Задание 1. Представьте алгоритм работы российского стандарта шифрования ГОСТ 28147-89.

Задание 2. Представьте алгоритм работы американского стандарта шифрования DES. Сравните алгоритмы шифрования ГОСТ 28147-89 и DES.

Задание 3. Выполнить ручное шифрование исходного текста с помощью алгоритма DES, алгоритма ГОСТ 28147-89.

Задание 4. Опишите особенности алгоритма AES. Сравните алгоритмы шифрования ГОСТ 28147-89 и AES.

Задание 5. Охарактеризуйте программы симметричного шифрования сообщений. Результаты представьте в виде таблицы.

Программа	Характеристики
Бесплатное ПО	
AES Free	
FineCrypt	
Dpcrypto	
Платное ПО	
EasyCrypto Deluxe	
Crypto-Lock	
Iron Key	
SafeGuard PrivateCrypto	

ПРАКТИЧЕСКАЯ РАБОТА № 12

Применение различных асимметричных алгоритмов

Цель: ознакомиться с асимметричными алгоритмами.

Теоретические вопросы

1. Понятие криптографической системы.
2. Классификация криптографических систем.
3. Проблема распределения ключей.
4. Асимметричные алгоритмы шифрования.
5. Типы односторонних преобразований.

Задание 1. Опишите асимметричные алгоритмы шифрования.

Тип	Описание
RSA	
ECC (криптосистема на основе эллиптических кривых)	
Эль-Гамаль.	

Задание 2. Изучите процедуру создания ключей в алгоритме шифрования RSA на примере.

№ п/п	Описание операции	Пример
1	Выбираются два простых числа[1] **p** и **q**.	p=7, q=13
2	Вычисляется произведение **n** = p * q.	n=91
3	Вычисляется **функция Эйлера**[2] **φ(n)**.	φ(n)=(7-1)(13-1)= 91-7-13+1 = 72
4	Выбирается открытый ключ **e**, как произвольное число (0<e<n), взаимно простое[3] с результатом функции Эйлера (e ⊥ φ(n)).	e=5
5	Вычисляется секретный ключ **d**, как обратное число[4] к **e** по модулю **φ(n)**, из соотношения (d*e) mod φ(n) = 1.	(d*5) mod 72 = 1, d = 29
6	Публикуются открытый ключ (**e**, **n**) в специальном хранилище, где исключается возможность его подмены (**общедоступном сертифицированном справочнике**).	

Создайте открытый и секретный ключи для любой другой пары простых чисел.

Задание 4. Разработать алгоритм шифрования RSA.

ПРАКТИЧЕСКАЯ РАБОТА № 13

Изучение программной реализации асимметричного алгоритма **RSA**

Цель: ознакомиться с асимметричными алгоритмами.

Теоретические вопросы

1. Понятие криптографической системы.
2. Классификация криптографических систем.
3. Проблема распределения ключей.
4. Асимметричные алгоритмы шифрования.
5. Типы односторонних преобразований.

Задание 1. Разработать и отладить приложение, реализующее алгоритм асимметричного

шифрования RSA.

Предлагаемый интерфейс приложения (рисунок 5).

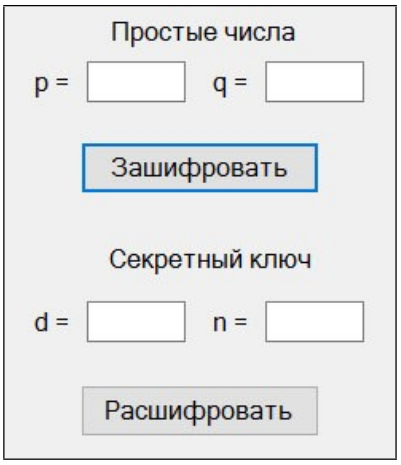

Рисунок 5

ПРАКТИЧЕСКАЯ РАБОТА № 14

Применение различных функций хеширования, анализ особенностей хешей

Цель: ознакомиться с различными функциями хеширования.

Теоретические вопросы

1. Понятие хеширования.
2. Хеш-функции.
3. Анализ особенностей хешей.
4. Свойства хеш-функций.

Задание 1. Опишите функции хеширования.

Тип	Описание
MD2	
MD4	
MD5	
SHA (Secure Hash Algorithm)	

Задание 2. Опишите свойства хеш-функций.

Задание 3. Ознакомьтесь с алгоритмом работы хеш-функции MD5.

Задание 4. Программно реализовать алгоритм MD4 хеширования символьной строки. Хеш- код представить в виде 16-ричного числа.

ПРАКТИЧЕСКАЯ РАБОТА № 15

Применение криптографических атак на хеш-функции.

Цель: научиться применять криптографические атаки на хеш-функции.

Теоретические вопросы

1. Понятие хеширования.
2. Хеш-функции.
3. Анализ особенностей хешей.
4. Свойства хеш-функций.
5. Атаки на функции хеширования.

Задание 1. Приведите примеры атак на функции хеширования.

Задание 2. Противник перехватил хеш H = H (M1). Длина хеша *n* битов. Он хочет найти любое сообщение M2 , для которого H (M1) = H (M2), для чего генерирует *k* сообщений и вычисляет их хеши. Какова вероятность успеха?

Задание 3. Противник перехватил определенное число хешей разных сообщений. Длина хеша *n* битов. Сколько новых сообщений и их хешей надо сгенерировать, чтобы найти коллизию для 50 % перехваченных хешей?

Задание 4. Хэш-функция дает хеш длиной 64 бита. Сколько хешей надо сгенерировать, чтобы найти коллизию двух любых сообщений?

ПРАКТИЧЕСКАЯ РАБОТА № 16

Изучение программно-аппаратных средств, реализующих основные функции ЭП

Цель: изучить программно-аппаратные средства, реализующие основные функции ЭП.

Теоретические вопросы

1. Понятие электронной цифровой подписи.
2. Свойства электронной цифровой подписи.
3. Схемы электронной цифровой подписи.
4. Алгоритмы цифровой подписи.

Задание 1. Разработать алгоритм реализации цифровой подписи RSA.

Задание 2. В чем отличие подписи RSA от алгоритма шифрования RSA?

Задание 3. Приведите примеры программно-аппаратных средств, реализующих основные функции электронной цифровой подписи.

ПРАКТИЧЕСКАЯ РАБОТА № 17

Применение протокола Диффи-Хеллмана для обмена ключами шифрования

Цель: изучить протокол Диффи-Хеллмана для обмена ключами шифрования.

Теоретические вопросы

1. Управление ключами.

2. Алгоритм обмена ключами по схеме Диффи-Хеллмана.
3. Формирование общего ключа.
4. Алгоритмы цифровой подписи.

Задание 1. Для каких целей может применяться алгоритм Диффи-Хеллмана?

Задание 2. Опишите последовательность действий при использовании алгоритма Диффи-Хеллмана.

Задание 3. На чём основывается безопасность обмена ключа по схеме Диффи-Хеллмана?

Задание 4. Доказать, что в схеме Диффи-Хеллмана $K_A = K_B$.

ПРАКТИЧЕСКАЯ РАБОТА № 18

Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.

Цель: изучить принципы работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.

Теоретические вопросы

1. Схема протокола Kerberos.
2. Аутентификация и авторизация клиента.
3. Недостатки и ограничения протокола Kerberos.
4. Политика протокола Kerberos.

Задание 1. Опишите схему протокола Kerberos (рисунок 6).

Рисунок 6

Задание 2. Объясните механизм работы протокола Kerberos.

Задание 3. Реализация Kerberos в ОС Windows Server.

ПРАКТИЧЕСКАЯ РАБОТА № 19

Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей

Цель: ознакомиться с механизмом аутентификации по одноразовым паролям.

Теоретические вопросы

1. Понятие аутентификации.
2. Механизмы аутентификации.
3. Аутентификация, основанная на паролях.
4. Среднее время безопасности пароля.
5. Концепция одноразовых паролей в системе аутентификации
6. Способы реализации принципа одноразовых паролей.

Задание 1. Приведите примеры устройств, используемых для генерации одноразовых паролей. Опишите алгоритм генерации одноразовых паролей.

Задание 2. Опишите способы защиты от атак на одноразовые пароли.

Описание атаки	Защита от данной атаки
Атака «Человек посередине» Злоумышленник перехватывает одноразовый пароль, посланный законным пользователем при аутентификации, блокирует законного пользователя и использует перехваченный пароль для входа в систему	
Кража аутентификационного токена Злоумышленник похищает аутентификационный токен законного пользователя и использует его для входа в систему	
Подбор PIN-кода аутентификационного токена Злоумышленник вручную производит перебор всех возможных значений PIN-кода похищенного им аутентификационного токена законного пользователя	
Извлечение значения секретного ключа из программного аутентификационного токена Злоумышленник копирует программный аутентификационный токен (программное обеспечение), пытается найти в нем хранимый секретный ключ, чтобы потом его использовать для аутентификации под видом законного пользователя	

Подбор PIN-кода аутентификационного токена с помощью известных OTP Злоумышленник перехватывает несколько правильных OTP, использованных для входа в систему, копирует программный аутентификационныи токен (программное обеспечение), и тем самым он пытается подобрать PIN-код путем перебора его возможных значений, для тестирования пробного значения PIN-кода используются перехваченные OTP	
Нечестный администратор аутентификационных токенов Злоумышленник является доверенным лицом либо является посредником доверенного лица, производящего инициализацию аутентификационного устройства до передачи его владельцу. Он может создать дубликат токена и, используя его, выдавать себя за владельца	

Задание 3. Разработать приложение, реализующее генерацию одноразовых паролей.

ПРАКТИЧЕСКАЯ РАБОТА № 20

Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ

Цель: изучить программное обеспечение, используемое для встраивания цифровых водяных знаков.

Теоретические вопросы

1. Понятие цифрового водяного знака. Его преимущества перед печатным водяным знаком.
2. Виды цифровых водяных знаков.
3. Методы защиты с помощью цифровых водяных знаков.
4. Программы для создания цифровых водяных знаков.

Задание 1. Приведите примеры устройств, используемых для генерации одноразовых паролей. Опишите алгоритм генерации одноразовых паролей.

Задание 2. Проведите сравнительный анализ программ, используемых для создания цифровых водяных знаков: PhotoWatermark Professional, Image Tuner, EasyWatermark, CryptoFoto.

Задание 3. Опишите процесс создания печатного водяного знака в программе Image Tuner.

ПРАКТИЧЕСКАЯ РАБОТА № 21

Реализация простейших стеганографических алгоритмов

Цель: изучить простейшие стеганографические алгоритмы.

Теоретические вопросы

1. Понятие стеганографии.
2. Назначение стеганографической системы.
3. Обобщенная модель стеганографической системы.
4. Классификация стеганографических систем.
5. Методы сокрытия информации.
6. Области применения стеганографии.

Задание 1. Рассмотреть работу двух программ, позволяющих проводить стеганографические преобразования.

Задание 2. Выбрать контейнер и выполнить внедрение в него некоторой информации.

Задание 3. Попробовать извлечь информацию из стегоконтейнера, созданного другой программой.

Задание 4. От чего зависит криптостойкость стеганографических систем?

ЛИТЕРАТУРА

Основная учебная литература:

1 **Казарин О. В.** Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/476997

Дополнительная учебная литература:

1 Сети и телекоммуникации: учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва: Издательство Юрайт, 2021. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/475704