Перечень вопросов
по оценке сформированности компетенций образовательной программы 09.03.02
«Информационные системы и технологии»
по дисциплине «Введение в кибербезопасность»

УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

ПК-7 Способность выполнять работы по обслуживанию программно-аппаратными средствами сетей и инфокоммуникаций

ПК-10 Способность выполнять работы по повышению эффективности работы персонала, участию в подборе кадров и по обучению пользователей

Теоретические вопросы:

1. Алгоритм шифрования по методу Вижинера. Методы атак.
2. Архивация и резервное копирование данных
3. Архивация. Структура многотомных и SFX – архивов.
4. Гаммирование. Принципы получения гаммы.
5. Идентификация и аутентификация.
6. Классификация АС по уровню защиты.
7. Компьютерные вирусы.
8. Компьютерные вирусы. Классификация КВ.
9. Концепция защиты информации в АС.
10. Криптографическая защита информации. Основные методы шифрования.
11. Криптографические системы с закрытым ключом. Основные трудности использования.
12. Криптографические системы с открытым ключом. Упрощенный алгоритм проверки подлинности ЭЦП.
13. Криптографические системы с открытым ключом. Упрощенный алгоритм заверения электронного документа с помощью ЭЦП.
14. Методы архивации данных.
15. Модель нарушителя.
16. Несанкционированный доступ к информации.
17. Общий алгоритм настройки политики безопасности.
18. Организационные меры защиты информации в ИС.
19. Организация работ по защите от НСД.
20. Основные каналы реализации угроз безопасности информации и методы противодействия им.
21. Основные каналы утечки информации при использовании жестких дисков.
22. Основные угрозы безопасности информации в ИС экономического назначения.
23. Понятие защищенности информационной системы.
24. Понятие политики безопасности.
25. Понятия уязвимости, угрозы, атаки на информационную систему.
26. Правила формирования паролей. Сгенерировать пароли с использованием различных правил.
27. Принцип функционирования и сценарии использование программы Ad-Aware.
28. Принципы функционирования антивирусных программных средств.
29. Принципы функционирования архиваторов.
30. Программные методы реализации компьютерных вирусов.
31. Резервное копирование данных.
32. Сравнительная характеристика инкрементального и дифференциального резервного копирования.
33. Сравнительная характеристика методов перестановки и гаммирования. Методы атак на них.
34. Сравнительная характеристика методов перестановки и замены. Методы атак на них.

35. Сравнительная характеристика программных и аппаратных средств идентификации и аутентификации
36. Сравнительная характеристика систем криптографической защиты информации с закрытым и открытым ключом.
37. Сравнительная характеристика систем криптографической защиты информации с закрытым и открытым ключом. Области применимости и особенности использования.
38. Средства идентификации и аутентификации.
39. Схемы ротации носителей при резервном копировании.

Практические задачи:

40. Блокировка/разблокировка учетной записи
41. Виды и назначение паролей BIOS. Установить пароли BIOS на виртуальной машине.
42. Запретить использование указанного преподавателем ресурса.
43. Зашифровать сообщение методом гаммирования.
44. Настройка всех компонентов антивирусного программного средства.
45. Настройка политики безопасности с использованием шаблонов.
46. Настроить аудит событий безопасности и проверить его работу
47. Настроить параметры безопасности в Internet браузере.
48. Настроить правила блокирования учетной записи.
49. Настроить требования к паролям.
50. Общий алгоритм настройки политики безопасности. Произвести настройку политики безопасности с помощью стандартных средств.
51. Ограничить полномочия пользователя (группы) по использованию ресурса.
52. Порядок загрузки ПК и параметры управления безопасностью. Продемонстрировать каждый этап.
53. Проверить корректность ЭЦП.
54. Продемонстрировать алгоритм контроля целостности файла с помощью программы CRC32.
55. Произвести защиту файла MS Office стандартными средствами.
56. Произвести защиту файла стандартными средствами архиватора.
57. Произвести настройку политики безопасности с помощью стандартных средств.
58. Создание и настройка групп
59. Создание и настройка консоли управления.
60. Создание и настройка учетных записей пользователей.
61. Создание многотомных и SFX архивов с заданным размером тома.
62. Создание нового жесткого диска в MS Virtual PC.
63. Создать и запустить виртуальную машину с заданными параметрами.
64. Средства контроля за деятельностью пользователей. Установка и настройка программы Home/Family Key Logger
65. Средства контроля за деятельностью приложений. Использование программы Ad-Aware.
66. Средства контроля за деятельностью приложений. Установка и настройка программы Ad-Aware
67. Управление порядком загрузки ПК. Загрузиться с указанного носителя.
68. Установка и настройка параметров антивирусного пакета.
69. Установка программных продуктов в среде MS Virtual PC.
70. Формирование открытого и закрытого ключа с использованием малых чисел
71. Характеристика аппаратных средств PC с позиции обеспечения безопасности информации.
72. Шифрование гаммированием.
73. Шифрование по методу Вижинера.
74. Шифрование методом многоалфавитной замены.
75. Шифрование сообщения в несимметричной КС с использованием малых чисел.

Справочный материал

Таблица Вижинера (для русского алфавита)

Ключ	Символы исходного текста																														
	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
а	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я
б	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	у	Ф	Х	Ц	ч	ш	щ	ь	Ы	ъ	э	ю	я	а
в	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	ш	щ	ь	ы	Ъ	э	ю	я	А	Б
г	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В
д	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г
е	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д
ж	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е
З	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
и	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
й	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
к	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И
л	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К
м	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	в	Г	Д	Е	Ж	З	И	И	К	Л
н	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М
о	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
п	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О
р	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П
с	С	Т	У	Ф	Х	Ц	Ч	Ш	И	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р
т	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	А	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С
у	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т
ф	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У
х	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф
ц	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
ч	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
ш	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
щ	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ч	Ч	Ш
ь	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
ы	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь
ъ	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы
э	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ
ю	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	щ	Ь	Ы	Ъ	Э
я	Я	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю

Таблица 1.1. Базовая таблица кодировки ASCII

32	пробел	48	0	64	@	80	P	96	`	112	p				
33	!	49	1	65	A	81	Q	97	a	113	q				
34	"	50	2	66	B	82	R	98	b	114	r				
35	#	51	3	67	C	83	S	99	c	115	s				
36	$	52	4	68	D	84	T	100	d	116	t				
37	%	53	5	69	E	85	U	101	e	117	u				
38	&	54	6	70	F	86	V	102	f	118	v				
39	'	55	7	71	G	87	W	103	g	119	w				
40	(	56	8	72	H	88	X	104	h	120	x				
41	)	57	9	73	I	89	Y	105	i	121	y				
42	*	58	:	74	J	90	Z	106	j	122	z				
43	+	59	;	75	K	91	[	107	k	123	{				
44	,	60	<	76	L	92	\	108	l	124	|				
45	-	61	=	77	M	93	]	109	m	125	}				
46	.	62	>	78	N	94	^	110	n	126	~				
47	/	63	?	79	O	95	_	111	o	127					

Таблица 1.2. Кодировка Windows 1251

128	Ђ	144	ђ	160		176	°	192	А	208	Р	224	а	240	р
129	Ѓ	145	'	161	Ў	177	±	193	Б	209	С	225	б	241	с
130	‚	146	'	162	ў	178	І	194	В	210	Т	226	в	242	т
131	ѓ	147	"	163	Ј	179	і	195	Г	211	У	227	г	243	у
132	„	148	"	164	¤	180	ґ	196	Д	212	Ф	228	д	244	ф
133	…	149	•	165	Ґ	181	µ	197	Е	213	Х	229	е	245	х
134	†	150	–	166	¦	182	¶	198	Ж	214	Ц	230	ж	246	ц
135	‡	151	—	167	§	183	·	199	З	215	Ч	231	з	247	ч
136	€	152		168	Ё	184	ё	200	И	216	Ш	232	и	248	ш
137	‰	153	™	169	©	185	№	201	Й	217	Щ	233	й	249	щ
138	Љ	154	љ	170	Є	186	є	202	К	218	Ъ	234	к	250	ъ
139	‹	155	›	171	«	187	»	203	Л	219	Ы	235	л	251	ы
140	Њ	156	њ	172	¬	188	ј	204	М	220	Ь	236	м	252	ь
141	Ќ	157	ќ	173	-	189	Ѕ	205	Н	221	Э	237	н	253	э
142	Ћ	158	ћ	174	®	190	s	206	О	222	Ю	238	о	254	ю
143	Џ	159	џ	175	Ї	191	ї	207	П	223	Я	239	п	255	я

1.3 Таблица кодировки символов ASCII (Например:'?' =>$30_{(16)}$+ $F_{(16)}$==$3F_{(16)}$=$63_{(10)}$)

	00	10	20	30	40	50	60	70	80	90	A0	B0	C0	D0	E0	F0
0	null	►	Space	0	@	P	‘	p	А	Р	а	▒	└	╨	р	Ё
1	☺	◄	!	1	A	Q	a	q	Б	С	б	▒	┴	╤	с	ё
2	☻	↕	"	2	B	R	b	r	В	Т	в	▓	┬	╥	т	Є
3	♥	‼	#	3	C	S	c	s	Г	У	г	│	├	╙	у	є
4	♦	¶	$	4	D	T	d	t	Д	Ф	д	┤	─	╘	ф	Ї
5	♣	§	%	5	E	U	e	u	Е	Х	е	╡	┼	╒	х	ї
6	♠	_	&	6	F	V	f	v	Ж	Ц	ж	╢	╞	╓	ц	Ў
7	•	↨	`	7	G	W	g	w	З	Ч	з	╖	╟	╫	ч	ў
8	Bsp	↑	(	8	H	X	h	x	И	Ш	и	╕	╚	╪	ш	°
9	Tab	↓	)	9	I	Y	i	y	Й	Щ	й	╣	╔	┘	щ	•
A	◙	→	*	:	J	Z	j	z	К	Ъ	к	║	╩	┌	ъ	·
B	♂	Esk	+	;	K	[	k	{	Л	Ы	л	╗	╦	█	ы	√
C	♀	∟	,	<	L	\	l	|	М	Ь	м	╝	╠	▄	ь	№
D	♪	↔	-	=	M	]	m	}	Н	Э	н	╜	═	▌	э	¤
E	♫	▲	.	>	N	^	n	~	О	Ю	о	╛	╬	▐	ю	■
F	☼	▼	/	?	O	_	o	⌂	П	Я	п	┐	╧	▀	я	blank

Пример билета: Вариант 16

1.Шифрование гаммированием

К: 47 88 192

Т: В е т е р 101 177 Т’

Сообщение	Win1251(10)	Bin	Ключ/Bin	Ключ	Сложение по модулю 2	Win1251(10)	Шифр	
В	194	11000010	00101111	47	11101101	237	н	
е	229	11100101	01011000	88	10111101	189	S	
т	242	11110010	11000000	192	00110010	50	2	
е	229	11100101	01100101	101	10000000	128	Ђ	
р	240	11110000	10110001	177	01000001	65	А	

2. Метод Вижинера

Шифр	Ключ	Слово
СУСН	КЛЕН	

3. Сравнительная характеристика блочных и потоковых КСЗИ.
4. Политика безопасности: определение и содержание уровней.
5. Виды конфиденциальной информации. Перечень. Особенности каждого вида конфиденциальной информации.