

Задания для участников

ТЕОРЕТИЧЕСКИЙ ТУР

Продолжительность выполнения заданий теоретического тура-135 минут

Максимальное количество баллов- 69 баллов

Модуль 1

Тестовые задания (20 баллов)

№ п/п	Тестовые задания	Макс. балл
<i>Определите один правильный ответ</i>		
1	<p>Непреднамеренной угрозой безопасности информации является...</p> <p>а. повреждение кабеля, по которому идет передача, в связи с погодными условиями</p> <p>б. кража</p> <p>в. умышленная порча носителей информации</p> <p>г. несанкционированное копирование конфиденциальной информации</p>	1
<i>Определите один правильный ответ</i>		
2	<p>Информация разделяется на открытую информацию и информацию с ограниченным доступом по</p> <p>а. режиму доступа к информации</p> <p>б. способу защиты информации</p> <p>в. способу хранения информации</p> <p>г. способу обработки информации</p>	1
<i>Определите один правильный ответ</i>		
3	<p>Сведения, которые находятся во владении, пользовании или распоряжении отдельных физических или юридических лиц и распространяются по их желанию соответственно с предусмотренными ими условиями – это</p> <p>а. тайная информация</p> <p>б. конфиденциальная информация</p> <p>в. открытая информация</p> <p>г. защищенная информация</p>	1
<i>Определите один правильный ответ</i>		
4	<p>Одним из методов защиты информации от уничтожения, повреждения, утечки или несанкционированного использования является</p>	1

	а. сжатие информации с помощью программ-архиваторов б. дефрагментация дисков, на которых хранится информация в. ограничение доступа к информации с помощью парольной защиты г. криптографическое шифрование информации	
<i>Определите один правильный ответ</i>		
5	Виды информационной безопасности: а. Персональная, корпоративная, государственная б. Клиентская, серверная, сетевая в. Локальная, глобальная, смешанная	1
<i>Определите один правильный ответ</i>		
6	Цели информационной безопасности – своевременное обнаружение, предупреждение: а. инсайдерства в организации б. несанкционированного доступа, воздействия в сети в. чрезвычайных ситуаций г. потери информации	1
<i>Определите один правильный ответ</i>		
7	Основные объекты информационной безопасности: а. программы пользователей, игры, фильмы б. компьютерные сети, базы данных в. информационные системы, психологическое состояние пользователей г. бизнес-ориентированные, коммерческие системы	1
<i>Определите один правильный ответ</i>		
8	Основными субъектами информационной безопасности являются: а. руководители, менеджеры, администраторы компаний б. пользователи сети Интернет в. органы права, государства, бизнеса г. сетевые базы данных, фаерволлы	1
<i>Определите один правильный ответ</i>		
9	К основным типам средств воздействия на компьютерную сеть относится: а. Компьютерный сбой б. Отсутствие пользователя в сети в. Логические закладки («мины») г. Аварийное отключение питания	1
<i>Определите один правильный ответ</i>		

10	Принципом информационной безопасности является принцип недопущения: <ul style="list-style-type: none"> а. Неоправданных ограничений при работе в сети (системе) б. Рисков безопасности сети, системы в. Презумпции секретности г. Презумпции невиновности 	1
<i>Определите один правильный ответ</i>		
11	Когда получен спам по e-mail с приложенным файлом, следует: <ul style="list-style-type: none"> а. Прочитать приложение, если оно не содержит ничего ценного – удалить б. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама в. Удалить письмо с приложением, не раскрывая (не читая) его г. Главное не загружать письмо, читать можно 	1
<i>Определите правильные ответы</i>		
12	Выберите наиболее распространенные угрозы информационной безопасности корпоративной системы: <ul style="list-style-type: none"> а. Покупка нелегального ПО б. Ошибки эксплуатации и неумышленного изменения режима работы системы в. Сознательного внедрения сетевых вирусов г. Распределенный доступ клиент, отказ оборудования д. Моральный износ сети, инсайдерство е. Сбой (отказ) оборудования, нелегальное копирование данных 	1
<i>Определите один правильный ответ</i>		
13	Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются: <ul style="list-style-type: none"> а. Доступность б. Актуальность в. Конфиденциальность г. Целостность 	1
<i>Определите один правильный ответ</i>		
14	Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке: <ul style="list-style-type: none"> а. Серверные, клиентские, спутниковые, наземные б. Программные, технические, организационные, технологические 	1

	в. Личные, корпоративные, социальные, национальные	
<i>Определите один правильный ответ</i>		
15	Основная масса угроз информационной безопасности приходится на: а. Программы мутанты б. Троянские программы в. Шпионские программы г. Черви	1
<i>Определите один правильный ответ</i>		
16	Заключительным этапом построения системы защиты является: а. Планирование б. Прогнозирование в. Анализ уязвимых мест г. Сопровождение	1
<i>Определите один правильный ответ</i>		
17	Stuxnet — это: а. троянская программа б. макровирус в. промышленный вирус г. червь	1
<i>Определите один правильный ответ</i>		
18	Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности: а. хакеры б. контрагенты в. программисты г. сотрудники	1
<i>Определите один правильный ответ</i>		
19	Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков: а. когда риски не могут быть приняты во внимание по политическим соображениям б. для обеспечения хорошей безопасности нужно учитывать и снижать все риски в. когда стоимость контрмер превышает ценность актива и потенциальные потери г. все ответы верны	1
<i>Определите один правильный ответ</i>		

20	Эффективная программа безопасности требует сбалансированного применения: а. контрмер и защитных механизмов б. процедур безопасности и шифрования в. взаимодействия с пользователя системы г. технических и нетехнических методов	1
----	--	---

Матрица ответов на тестовые задания

Номер теста	1	2	3	4	5	6	7	8	9	10
Верный ответ										

Номер теста	11	12	13	14	15	16	17	18	19	20
Верный ответ										

Модуль 2

Творческая часть (49 баллов)

Задание 1. Прочти данные предложения. Обрати внимание, что они записаны непривычным для нас образом. Какой из этих пунктов является хорошим советом и правилом безопасного поведения в сети Интернет? Расшифруй и запиши это предложение

ОН ОИДОЕМ ИЛИ КАРТНКА ПЛИ МЕЛОДНО, НО
 АДАРАНО! СПЕШИ! СМС - НЕ СПЕШИ! СНАЧАЛА
 ПРОВЕРЬ ЭТОТ НОМЕР - БЕЗОПАСНО ИЛИ ОТПРАВЛЯТЬ НА
 НЕТО СМС И НЕ ОБМАНЫВАЙ ТЕРЯ.

а)

ЕСЛИ ХОДЕШЬ СКАРАТЬ КАРТНКА ИЛИ МЕЛОДНО, НО
 ТЕРЯ ПРОСИ ОТПРАВЛЯТЬ СМС - СВЯЗЬ ЖЕ СМЕЛО
 ОТПРАВЛЯЙ! ВСЕ РАДЕТ ХОРОШО!

б)

ЕСЛИ ХОДЕШЬ СКАРАТЬ КАРТНКА ИЛИ МЕЛОДНО, НО
 ТЕРЯ ПРОСИ ОТПРАВЛЯТЬ СМС - ПРЕДПОЖИ ДРУГА
 ОТПРАВЛЯТЬ СМС ВМЕСТЕ - ТАК АВЕРЕННЕЕ И НАДЕЖНЕЕ!

в)

ШИФР _____

Ответ: _____

Задание 2. Найдите не меньше 13 слов, имеющих отношение к персональному компьютеру. Двигаться можно вниз, вправо,вверх.

к	о	д	к	о	м	о	н	и	р
а	б	и	с	к	п	о	р	т	у
к	о	п	р	и	ь	р	к	о	л
л	у	б	и	т	ю	т	е	р	о
а	в	и	н	ч	е	с	т	и	н
п	л	а	т	п	п	к	д	л	к
м	а	т	е	р	л	а	н	е	и
ы	т	у	б	о	м	н	к	р	э
ш	а	р	и	ц	е	ш	е	т	е
ь	с	а	т	е	с	с	о	р	я

Ответ: _____
