Тестовое задание для диагностического тестирования по дисциплине:

Методы защиты информации, 7 семестр

Код, направление подготовки	09.03.02 Информационные системы и технологии
Направленность (профиль)	Информационные системы и технологии
Форма обучения	Очная
Кафедра разработчик	Информатики и вычислительной техники
Выпускающая кафедра	Информатики и вычислительной техники

№	Проверяемая компетенция	Задание	Варианты ответов	Тип сложности вопроса	Кол-во баллов за правильный ответ
1	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это _____.		Низкий	2

2	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Закрытый ключ в ассиметричных алгоритмах необходим для следующей операции над информацией	1. шифрование 2. расшифровка 3. транслирование 4. копирование	Низкий	2
3	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Способ шифрования данных, при котором один и тот же ключ используется и для шифрования, и для восстановления информации называется _____ ____. Способ шифрования данных, предполагающий использование двух ключей — открытого и закрытого называется _____.		Низкий	2
4	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Укажите верный термин определяющий вредоносный самовоспроизводящийся программный код.	1. Лазейка. 2. Червь. 3. Вирус. 4. Бактерия. .	Низкий	2
5	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Что является основой большинства современных блочных симметричных алгоритмов шифрования?	1. Сеть Фейстеля 2. Гаммирование 3. Перемешивание 4. Алфавит	Низкий	2

6	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Совокупность методов и подходов к реализации задачи сокрытия факта передачи сообщения называется _____.		Средний	5
7	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Укажите ассиметричный алгоритм шифрования.	1. Эль-Гаммаля 2. IDEA 3. DES 4. Blowfish	Средний	5

8	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Проставьте соответствие между названием вида злоумышленных действий и его характеристикой, защита от которых является целью аутентификации	1. маскарад <=> абонент С пересылает документ абоненту А от имени абонента В 2. ренегатство <=> абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле посылал 3. подмена <=> абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А	Средний	5

9	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Распределение ключей между пользователями вычислительной сети реализуется следующим образом:	1. прямым обменом сеансовыми ключами между пользователями сети; 2. использованием одного центра распределения ключей; 3. использованием нескольких центров распределения ключей; 4. использованием альтернативных каналов связи. .	Средний	5

10	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Функция, которая осуществляет сжатие строки чисел произвольного размера в строку чисел фиксированного размера (свертку) называется _____? Результат работы функции называется _____.		Средний	5
11	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет	1. криптография 2. стеганография 3. криптоанализ 4. криптология	Средний	5

12	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Под угрозой удаленного администрирования в компьютерной сети понимается угроза …	1. внедрения агрессивного программного кода в рамках активных объектов Web-страниц 2. поставки неприемлемого содержания 3. перехвата или подмены данных на путях транспортировки 4. несанкционированного управления удаленным компьютером	Средний	5
13	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?	1. Сотрудники 2. Контрагенты 3. Хакеры 4. Посетители	Средний	5
14	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Процесс проверки пользователя, является ли он тем за кого себя выдаёт, называется _____		Средний	5

15	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Укажите размер блока шифрования в алгоритме "Магма", описанном в ГОСТ 34.12-2018. (ответ в количестве бит)		Средний	5

16	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Алгоритм применения цифровой подписи на основе алгоритма шифрования RSA:	1. Получатель подтверждает подлинность подписи 2. Получатель вычисляет хэш-функцию m' = SKo mod N 3. Значения (M,S) отправляются получателю. 4. Сравнение m'=m, по которому получатель признает подпись подлинной. 5. Получатель вычисляет хэш-функцию m = H(M) 6. Вычисление пары ключей: секретный и открытый, используя алгоритм шифрования RSA. 7. Отправитель вычисляет m=H(M), где m – целое число. 8. Отправитель вычисляет цифрову подпись S = mKs mod N Правильные ответы: 1. Вычисление пары ключей: секретный и открытый, используя алгоритм шифрования RSA. 2. Отправитель вычисляет m=H(M), где m – целое число. 3. Отправитель	Высокий	8

			вычисляет цифрову подпись S = mKs mod N 4. Значения (M,S) отправляются получателю. 5. Получатель вычисляет хэш-функцию m' = SKo mod N 6. Получатель вычисляет хэш-функцию m = H(M) 7. Сравнение m'=m, по которому получатель признает подпись подлинной. 8. Получатель подтверждает подлинность подписи		

17	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Криптографические протоколы аутентификации используются, если	1. участвуют только два участника; 2. требуется подтверждение подлинности участников сеанса связи. 3. пользователь протокола уверен в достоверности информации, получаемой от другого пользователя; 4. участники протокола не доверяют друг другу Правильные ответы: 1. участники протокола не доверяют друг другу 2. требуется подтверждение подлинности участников сеанса связи.	Высокий	8
18	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	«Цифровая подпись» формируется на основе следующих элементов:	1. сообщения отправителя 2. секретного ключа отправителя 3. секретного ключа получателя 4. открытого ключа отправителя Правильные ответы: 1. сообщения отправителя 2. секретного ключа отправителя	Высокий	8

19	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Основные угрозы доступности информации:	1. непреднамеренные ошибки пользователей 2. хакерская атака 3. отказ программного и аппаратного обеспечения 4. злонамеренное изменение данных 5. перехват данных 6. разрушение или повреждение помещений Правильные ответы: 1. непреднамеренные ошибки пользователей 2. отказ программного и аппаратного обеспечения 3. разрушение или повреждение помещений	Высокий	8
20	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК - 7.1 ПК - 7.2 ПК - 7.3	Основные угрозы конфиденциальности информации:	1. перехват данных 2. карнавал 3. переадресовка 4. злоупотребления полномочиями 5. маскарад Правильные ответы: 1. маскарад 2. перехват данных 3. злоупотребления полномочиями	Высокий	8