Тестовое задание для диагностического тестирования по дисциплине:

Методы защиты информации, 7 семестр

Код, направление подготовки	01.03.02 ПРИКЛАДНАЯ МАТЕМАТИКА И ИНФОРМАТИКА
Направленность (профиль)	Прикладная математика и информатика
Форма обучения	Очная
Кафедра разработчик	Автоматизированных систем обработки информации и управления
Выпускающая кафедра	Прикладной математики

№	**Проверяемая компетенция**	**Задание**	**Варианты ответов**	**Тип сложности вопроса**	**Кол-во баллов за правильный ответ**
1	ПК-3.1 ПК- 4.1 ПК-4.2	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-3.1 ПК-4.1 ПК-4.2	Закрытый ключ в ассиметричных алгоритмах необходим для следующей операции над информацией	1. шифрование 2. расшифровка 3. транслирование 4. копирование	Низкий	2

3	ПК-3.1 ПК-4.1 ПК-4.2	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-3.1 ПК-4.1 ПК-4.2	Укажите верный термин определяющий вредоносный самовоспроизводящийся программный код.	1. Лазейка. 2. Червь. 3. Вирус. 4. Бактерия.	Низкий	2
5	ПК-3.1 ПК-4.1 ПК-4.2	Что является основой большинства современных блочных симметричных алгоритмов шифрования?	1. Сеть Фейстеля 2. Гаммирование 3. Перемешивание 4. Алфавит	Низкий	2
6	ПК-3.1 ПК-4.1 ПК-4.2	Совокупность методов и подходов к реализации задачи сокрытия факта передачи сообщения называется _____.		Средний	5
7	ПК-3.1 ПК-4.1 ПК-4.2	Укажите ассиметричный алгоритм шифрования.	1. Эль-Гаммаля 2. IDEA 3. DES 4. Blowfish	Средний	5
8	ПК-3.1 ПК-4.1 ПК-4.2	Проставьте соответствие между названием вида злоумышленных действий и его характеристикой, защита от которых является целью аутентификации		Средний	5

9	ПК-3.1 ПК-4.1 ПК-4.2	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-3.1 ПК-4.1 ПК-4.2	Функция, которая осуществляет сжатие строки чисел произвольного размера в строку чисел фиксированного размера (свертку) называется _____? Результат работы функции называется _____.		Средний	5
11	ПК-3.1 ПК-4.1 ПК-4.2	Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет	1. криптография 2. стеганография 3. криптоанализ 4. криптология	Средний	5

12	ПК-3.1 ПК-4.1 ПК-4.2	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-3.1 ПК-4.1 ПК-4.2	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-3.1 ПК-4.1 ПК-4.2	Процесс проверки пользователя, является ли он тем за кого себя выдаёт, называется _____		Средний	5
15	ПК-3.1 ПК-4.1 ПК-4.2	Укажите размер блока шифрования в алгоритме "Магма", описанном в ГОСТ 34.12-2018. (ответ в количестве бит)		Средний	5

16	ПК-3.1 ПК-4.1 ПК-4.2	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	Высокий	8
17	ПК-3.1 ПК-4.1 ПК-4.2	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	Высокий	8

18	ПК-3.1 ПК-4.1 ПК-4.2	«Цифровая подпись» формируется на основе следующих элементов:		Высокий	8
19	ПК-3.1 ПК-4.1 ПК-4.2	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	Высокий	8
20	ПК-3.1 ПК-4.1 ПК-4.2	Основные угрозы конфиденциальности информации:	1. перехват данных 2. карнавал 3. переадресовка 4. злоупотребления полномочиями 5. маскарад	Высокий	8