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	Автоматизированных систем обработки информации и управления

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

4	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
5	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

6	ПК-3.1, ПК-4.1, ПК-4.2	Распределение ключей между пользователями вычислительной сети реализуется следующим образом:	1. использованием одного центра распределения ключей; 2. использованием альтернативных каналов связи. 3. использованием нескольких центров распределения ключей; 4. прямым обменом сеансовыми ключами между пользователями сети;	Средний
7	ПК-3.1, ПК-4.1, ПК-4.2	Совокупность методов и подходов к реализации задачи сокрытия факта передачи сообщения называется _____.	—	Средний
8	ПК-3.1, ПК-4.1, ПК-4.2	Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет	1. стеганография 2. криптография 3. криптоанализ 4. криптология	Средний

9	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
10	ПК-3.1, ПК-4.1, ПК-4.2	Укажите ассиметричный алгоритм шифрования.	1. IDEA 2. Blowfish 3. DES 4. Эль-Гаммаля	Средний
11	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	1. маскарад ⟷абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А 2. ренегатство ⟷абонент С пересылает документ абоненту А от имени абонента В 3. подмена ⟷абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле посылал	Средний

12	ПК-3.1, ПК-4.1, ПК-4.2	Под угрозой удаленного администрирования в компьютерной сети понимается угроза …	1. перехвата или подмены данных на путях транспортировки 2. несанкционированного управления удаленным компьютером 3. поставки неприемлемого содержания 4. внедрения агрессивного программного кода в рамках активных объектов Web-страниц	Средний
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. Хакеры 2. Контрагенты 3. Сотрудники 4. Посетители	Средний
14	ПК-3.1, ПК-4.1, ПК-4.2	Процесс проверки пользователя, является ли он тем за кого себя выдаёт, называется _____	—	Средний

15	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
16	ПК-3.1, ПК-4.1, ПК-4.2	Основные угрозы доступности информации:	1. отказ программного и аппаратного обеспечения 2. перехват данных 3. разрушение или повреждение помещений 4. злонамеренное изменение данных 5. непреднамеренные ошибки пользователей 6. хакерская атака	Высокий

17	ПК-3.1, ПК-4.1, ПК-4.2	Алгоритм применения цифровой подписи на основе алгоритма шифрования RSA:	1. Отправитель вычисляет цифрову подпись S = mKs mod N 2. Значения (M,S) отправляются получателю. 3. Получатель подтверждает подлинность подписи 4. Получатель вычисляет хэш-функцию m = H(M) 5. Отправитель вычисляет m=H(M), где m – целое число. 6. Вычисление пары ключей: секретный и открытый, используя алгоритм шифрования RSA. 7. Сравнение m'=m, по которому получатель признает подпись подлинной. 8. Получатель вычисляет хэш-функцию m' = SKo mod N	Высокий

18	ПК-3.1, ПК-4.1, ПК-4.2	Криптографические протоколы аутентификации используются, если	1. пользователь протокола уверен в достоверности информации, получаемой от другого пользователя; 2. участвуют только два участника; 3. участники протокола не доверяют друг другу 4. требуется подтверждение подлинности участников сеанса связи.	Высокий
19	ПК-3.1, ПК-4.1, ПК-4.2	«Цифровая подпись» формируется на основе следующих элементов:	1. секретного ключа отправителя 2. сообщения отправителя 3. секретного ключа получателя 4. открытого ключа отправителя	Высокий
20	ПК-3.1, ПК-4.1, ПК-4.2	Основные угрозы конфиденциальности информации:	1. злоупотребления полномочиями 2. маскарад 3. карнавал 4. переадресовка 5. перехват данных	Высокий