Тестовое задание для диагностического тестирования по дисциплине Риски и безопасность, 3 семестр

Код, направление подготовки	09.04.01 Информатика и вычислительная техника
Направленность (профиль)	Информационное и программное обеспечение
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-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Что является основой большинства современных блочных симметричных алгоритмов шифрования?	1. Сеть Фейстеля 2. Гаммирование 3. Алфавит 4. Перемешивание	Низкий

2	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	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
3	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Закрытый ключ в ассиметричных алгоритмах необходим для следующей операции над информацией	1. копирование 2. расшифровка 3. шифрование 4. транслирование	Низкий

4	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это _____ _____.	—	Низкий
5	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Укажите верный термин определяющий вредоносный самовоспроизводящийся программный код.	1. Червь. 2. Вирус. 3. Бактерия. 4. Лазейка.	Низкий

6	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Под угрозой удаленного администрирования в компьютерной сети понимается угроза …	1. внедрения агрессивного программного кода в рамках активных объектов Web-страниц 2. несанкционированного управления удаленным компьютером 3. перехвата или подмены данных на путях транспортировки 4. поставки неприемлемого содержания	Средний
7	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?	1. Хакеры 2. Сотрудники 3. Контрагенты 4. Посетители	Средний
8	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Процесс проверки пользователя, является ли он тем за кого себя выдаёт, называется _____	—	Средний

9	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Распределение ключей между пользователями вычислительной сети реализуется следующим образом:	1. использованием одного центра распределения ключей; 2. прямым обменом сеансовыми ключами между пользователями сети; 3. использованием нескольких центров распределения ключей; 4. использованием альтернативных каналов связи.	Средний
10	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Функция, которая осуществляет сжатие строки чисел произвольного размера в строку чисел фиксированного размера (свертку) называется _____? Результат работы функции называется _____.	—	Средний

11	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Совокупность методов и подходов к реализации задачи сокрытия факта передачи сообщения называется _____.	—	Средний
12	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Проставьте соответствие между названием вида злоумышленных действий и его характеристикой, защита от которых является целью аутентификации	1. маскарад ⟷абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле посылал 2. ренегатство ⟷абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А 3. подмена ⟷абонент С пересылает документ абоненту А от имени абонента В	Средний
13	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Укажите размер блока шифрования в алгоритме "Магма", описанном в ГОСТ 34.12-2018. (ответ в количестве бит)	—	Средний

14	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Укажите ассиметричный алгоритм шифрования.	1. Blowfish 2. Эль-Гаммаля 3. DES 4. IDEA	Средний
15	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет	1. криптография 2. криптоанализ 3. стеганография 4. криптология	Средний

16	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Алгоритм применения цифровой подписи на основе алгоритма шифрования RSA:	1. Значения (M,S) отправляются получателю. 2. Получатель вычисляет хэш-функцию m = H(M) 3. Получатель вычисляет хэш-функцию m' = SKo mod N 4. Вычисление пары ключей: секретный и открытый, используя алгоритм шифрования RSA. 5. Получатель подтверждает подлинность подписи 6. Отправитель вычисляет m=H(M), где m – целое число. 7. Отправитель вычисляет цифрову подпись S = mKs mod N 8. Сравнение m'=m, по которому получатель признает подпись подлинной.	Высокий

17	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Криптографические протоколы аутентификации используются, если	1. пользователь протокола уверен в достоверности информации, получаемой от другого пользователя; 2. участвуют только два участника; 3. требуется подтверждение подлинности участников сеанса связи. 4. участники протокола не доверяют друг другу	Высокий
18	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	«Цифровая подпись» формируется на основе следующих элементов:	1. секретного ключа получателя 2. открытого ключа отправителя 3. секретного ключа отправителя 4. сообщения отправителя	Высокий
19	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Основные угрозы конфиденциальности информации:	1. карнавал 2. переадресовка 3. перехват данных 4. злоупотребления полномочиями 5. маскарад	Высокий

20	ПК-1.1, ПК-1.2, ПК-1.3, ПК-8.1, ПК-8.2, ПК-8.3, ПК-6.1, ПК-6.2, ПК-6.3, ПК-9.1, ПК-9.2, ПК-9.3	Основные угрозы доступности информации:	1. хакерская атака 2. отказ программного и аппаратного обеспечения 3. злонамеренное изменение данных 4. перехват данных 5. непреднамеренные ошибки пользователей 6. разрушение или повреждение помещений	Высокий

№	ПРАВИЛЬНЫЕ ОТВЕТЫ
1	Сеть Фейстеля
2	Симметричным; Ассиметричным
3	расшифровка
4	базопасность информации
5	Вирус.
6	несанкционированного управления удаленным компьютером
7	Сотрудники
8	аутентификацией
9	использованием одного центра распределения ключей;; использованием нескольких центров распределения ключей;; прямым обменом сеансовыми ключами между пользователями сети;; использованием альтернативных каналов связи.
10	хэш-функцией; хэш

11	стеганографией
12	маскарад ↔абонент С пересылает документ абоненту А от имени абонента В; ренегатство ↔абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле посылал; подмена ↔абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А
13	64 бит
14	Эль-Гаммаля
15	криптоанализ
16	Вычисление пары ключей: секретный и открытый, используя алгоритм шифрования RSA.; Отправитель вычисляет m=H(M), где m – целое число.; Отправитель вычисляет цифрову подпись S = mKs mod N; Значения (M,S) отправляются получателю.; Получатель вычисляет хэш-функцию m' = SKo mod N; Получатель вычисляет хэш-функцию m = H(M); Сравнение m'=m, по которому получатель признает подпись подлинной.; Получатель подтверждает подлинность подписи
17	участники протокола не доверяют друг другу; требуется подтверждение подлинности участников сеанса связи.
18	сообщения отправителя; секретного ключа отправителя
19	маскарад; перехват данных; злоупотребления полномочиями
20	непреднамеренные ошибки пользователей; отказ программного и аппаратного обеспечения ; разрушение или повреждение помещений