

Документ подписан простой электронной подписью  
 Информация о владельце:  
 ФИО: Косенок Сергей Михайлович  
 Должность: ректор  
 Дата подписания: 06.06.2024 06:43:52  
 Уникальный программный ключ:  
 e3a68f3eaa1e62674b54f4998099d3d6bfdcf836

## 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	<p>Способ шифрования данных, при котором один и тот же ключ используется и для шифрования, и для восстановления информации называется _____.</p> <p>Способ шифрования данных, предполагающий использование двух ключей — открытого и закрытого называется _____.</p>		Низкий	2
4	ПК-3.1 ПК-4.1 ПК-4.2	Укажите верный термин определяющий вредоносный самовоспроизводящийся программный код.	<ol style="list-style-type: none"> <li>1. Лазейка.</li> <li>2. Червь.</li> <li>3. Вирус.</li> <li>4. Бактерия.</li> </ol>	Низкий	2
5	ПК-3.1 ПК-4.1 ПК-4.2	Что является основой большинства современных блочных симметричных алгоритмов шифрования?	<ol style="list-style-type: none"> <li>1. Сеть Фейстеля</li> <li>2. Гаммирование</li> <li>3. Перемешивание</li> <li>4. Алфавит</li> </ol>	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.	<ol style="list-style-type: none"> <li>1. Эль-Гаммаля</li> <li>2. IDEA</li> <li>3. DES</li> <li>4. Blowfish</li> </ol>	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:	<ol style="list-style-type: none"> <li>1. прямым обменом сеансовыми ключами между пользователями сети;</li> <li>2. использованием одного центра распределения ключей;</li> <li>3. использованием нескольких центров распределения ключей;</li> <li>4. использованием альтернативных каналов связи.</li> </ol>	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	<ol style="list-style-type: none"> <li>1. криптография</li> <li>2. стеганография</li> <li>3. криптоанализ</li> <li>4. криптология</li> </ol>	Средний	5

12	ПК-3.1 ПК-4.1 ПК-4.2	Под угрозой удаленного администрирования в компьютерной сети понимается угроза ...	<ol style="list-style-type: none"> <li>1. внедрения агрессивного программного кода в рамках активных объектов Web-страниц</li> <li>2. поставки неприемлемого содержания</li> <li>3. перехвата или подмены данных на путях транспортировки</li> <li>4. несанкционированного управления удаленным компьютером</li> </ol>	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?	<ol style="list-style-type: none"> <li>1. Сотрудники</li> <li>2. Контрагенты</li> <li>3. Хакеры</li> <li>4. Посетители</li> </ol>	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:	<ol style="list-style-type: none"> <li>1. Получатель подтверждает подлинность подписи</li> <li>2. Получатель вычисляет хэш-функцию <math>m' = SK_o \text{ mod } N</math></li> <li>3. Значения (M,S) отправляются получателю.</li> <li>4. Сравнение <math>m'=m</math>, по которому получатель признает подпись подлинной.</li> <li>5. Получатель вычисляет хэш-функцию <math>m = H(M)</math></li> <li>6. Вычисление пары ключей: секретный и открытый, используя алгоритм шифрования RSA.</li> <li>7. Отправитель вычисляет <math>m=H(M)</math>, где <math>m</math> – целое число.</li> <li>8. Отправитель вычисляет цифровую подпись <math>S = mK_s \text{ mod } N</math></li> </ol>	Высокий	8
17	ПК-3.1 ПК-4.1 ПК-4.2	Криптографические протоколы аутентификации используются, если	<ol style="list-style-type: none"> <li>1. участвуют только два участника;</li> <li>2. требуется подтверждение подлинности участников сеанса связи.</li> <li>3. пользователь протокола уверен в достоверности информации, получаемой от другого пользователя;</li> <li>4. участники протокола не доверяют друг другу</li> </ol>	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:	<ol style="list-style-type: none"> <li>1. непреднамеренные ошибки пользователей</li> <li>2. хакерская атака</li> <li>3. отказ программного и аппаратного обеспечения</li> <li>4. злонамеренное изменение данных</li> <li>5. перехват данных</li> <li>6. разрушение или повреждение помещений</li> </ol>	Высокий	8
20	ПК-3.1 ПК-4.1 ПК-4.2	Основные угрозы конфиденциальности информации:	<ol style="list-style-type: none"> <li>1. перехват данных</li> <li>2. карнавал</li> <li>3. переадресовка</li> <li>4. злоупотребления полномочиями</li> <li>5. маскарад</li> </ol>	Высокий	8