

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Косенок Сергей Михайлович
Должность: ректор
Дата подписания: 19.06.2024 07:20:13
Уникальный программный ключ:
e3a68f3eaa1e62674b54f4998099d3d6bfdcf836

Тестовое задание для диагностического тестирования по дисциплине

Защита информации, 8 семестр

Код, направление подготовки	09.03.01 Информатика и вычислительная техника
Направленность (профиль)	Искусственный интеллект и экспертные системы
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	ОПК-1.2 ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Что является основой большинства современных блочных симметричных алгоритмов шифрования?	1. Сеть Фейстеля 2. Гаммирование 3. Перемешивание 4. Алфавит	Низкий

2	<p>ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2</p>	<p>Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования</p> <p>— это</p> <hr/> <p>_____.</p>	—	Низкий
3	<p>ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2</p>	<p>Закрытый ключ в ассиметричных алгоритмах необходим для следующей операции над информацией</p>	<ol style="list-style-type: none"> 1. копирование 2. расшифровка 3. транслирование 4. шифрование 	Низкий

4	ОПК-1.2 ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	<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> <p>_____.</p>	—	Низкий
5	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	<p>Укажите верный термин определяющий вредоносный самовоспроизводящийся программный код.</p>	<ol style="list-style-type: none"> 1. Лазейка. 2. Червь. 3. Вирус. 4. Бактерия. 	Низкий

6	ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Распределение ключей между пользователями вычислительной сети реализуется следующим образом:	<ol style="list-style-type: none"> 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	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Совокупность методов и подходов к реализации задачи сокрытия факта передачи сообщения называется _____.	—	Средний
8	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет	<ol style="list-style-type: none"> 1. стеганография 2. криптография 3. криптоанализ 4. криптология 	Средний

9	ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Укажите размер блока шифрования в алгоритме "Магма", описанном в ГОСТ 34.12-2018. (ответ в количестве бит)	—	Средний
10	ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Укажите ассиметричный алгоритм шифрования.	<ol style="list-style-type: none"> 1. IDEA 2. Blowfish 3. DES 4. Эль-Гаммаля 	Средний
11	ОПК-1.1 ОПК-2.1 ОПК-3.1	Проставьте соответствие между названием вида злоумышленных действий и его характеристикой, защита от которых является целью аутентификации	<ol style="list-style-type: none"> 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	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	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	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	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	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Процесс проверки пользователя, является ли он тем за кого себя выдаёт, называется _____	—	Средний

15	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Функция, которая осуществляет сжатие строки чисел произвольного размера в строку чисел фиксированного размера (свертку) называется _____? Результат работы функции называется _____.	—	Средний
16	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	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	<p>ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2</p>	<p>Алгоритм применения цифровой подписи на основе алгоритма шифрования RSA:</p>	<ol style="list-style-type: none"> 1. Отправитель вычисляет цифровую подпись $S = mK_s \text{ mod } N$ 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 $m' = SK_o \text{ mod } N$ 	Высокий
----	---	---	--	---------

18	<p>ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2</p>	<p>Криптографические протоколы аутентификации используются, если</p>	<ol style="list-style-type: none"> 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	<p>ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2</p>	<p>«Цифровая подпись» формируется на основе следующих элементов:</p>	<ol style="list-style-type: none"> 1. секретного ключа отправителя 2. сообщения отправителя 3. секретного ключа получателя 4. открытого ключа отправителя 	Высокий
20	<p>ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2</p>	<p>Основные угрозы конфиденциальности информации:</p>	<ol style="list-style-type: none"> 1. злоупотребления полномочиями 2. маскарад 3. карнавал 4. переадресовка 5. перехват данных 	Высокий