

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: Косенок Сергей Михайлович
 Должность: РПНТ03
 Дата подписания: 18.06.2024 18:22:55
 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)	Автоматизированные системы обработки информации и управления
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	Кол-во баллов за правильный ответ
ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это _____.		Низкий	2

ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Закрытый ключ в асимметричных алгоритмах необходим для следующей операции над информацией	1. шифрование 2. расшифровка 3. транслирование 4. копирование	Низкий	2
ОПК-1.2 ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	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
ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Укажите верный термин определяющий вредоносный самовоспроизводящийся программный код.	1. Лазейка. 2. Червь. 3. Вирус. 4. Бактерия.	Низкий	2

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
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	5
ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Укажите ассиметричный алгоритм шифрования.	1. Эль-Гаммала 2. IDEA 3. DES 4. Blowfish	Средний	5
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	1. маскард $\Leftarrow \Rightarrow$ абонент С пересылает документ абоненту А от имени абонента В 2. ренегатство $\Leftarrow \Rightarrow$ абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле посылал 3. подмена $\Leftarrow \Rightarrow$ абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А	Средний	5

--	--	--	--	--

<p>ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2</p>	<p>Распределение ключей между пользователями вычислительной сети реализуется следующим образом:</p>	<p>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.</p>	<p>Средний</p>	<p>5</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>Функция, которая осуществляет сжатие строки чисел произвольного размера в строку чисел фиксированного размера (свертку) называется _____?</p> <p>Результат работы функции называется _____.</p>		Средний	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>Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет</p>	<ol style="list-style-type: none"> 1. криптография 2. стеганография 3. криптоанализ 4. криптология 	Средний	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	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
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. Сотрудники 2. Контрагенты 3. Хакеры 4. Посетители	Средний	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	Процесс проверки пользователя, является ли он тем за кого себя выдаёт, называется _____		Средний	5

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	5
--	--	--	---------	---

<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>	<p>1. Получатель подтверждает подлинность подписи</p> <p>2. Получатель вычисляет хэш-функцию $m' = SK_o \text{ mod } N$</p> <p>3. Значения (M,S) отправляются получателю.</p> <p>4. Сравнение $m'=m$, по которому получатель признает подпись подлинной.</p> <p>5. Получатель вычисляет хэш-функцию $m = H(M)$</p> <p>6. Вычисление пары ключей: секретный и открытый, используя алгоритм шифрования RSA.</p> <p>7. Отправитель вычисляет $m=H(M)$, где m – целое число.</p> <p>8. Отправитель вычисляет цифровую подпись $S = mK_s \text{ mod } N$</p>	<p>Высокий</p>	<p>8</p>
--	---	---	----------------	----------

<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>Криптографически е протоколы аутентификации используются, если</p>	<p>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</p>	<p>Высокий</p>	<p>8</p>
<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>	<p>1. сообщения отправителя 2. секретного ключа отправителя 3. секретного ключа получателя 4. открытого ключа отправителя</p>	<p>Высокий</p>	<p>8</p>

<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 доступности информации:</p>	<p>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</p>	<p>Высокий</p>	<p>8</p>
<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>	<p>1. перехват данных 2. карнавал 3. переадресовка 4. злоупотребления полномочиями 5. маскарад</p>	<p>Высокий</p>	<p>8</p>