

Документ подписан простой электронной подписью  
 Информация о владельце:  
 ФИО: Косенок Сергей Михайлович  
 Должность: ректор  
 Дата подписания: 19.03.2014 07:10:58  
 Уникальный программный ключ:  
 e3a68f3eaa1e62674b54f4998099d3d6bfdcf836

**Тестовое задание для диагностического тестирования по дисциплине:**

**Информационная безопасность и защита информации, 7 семестр**

Код, направление подготовки	09.03.02 Информационные системы и технологии
Направленность (профиль)	Информационные системы и технологии
Форма обучения	Очная
Кафедра разработчик	Информатики и вычислительной техники
Выпускающая кафедра	Информатики и вычислительной техники

Проверяемая компетенция	Задание	Варианты ответов	Тип сложности вопроса	Кол-во баллов за правильный ответ
ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -11.1 ПК -11.2 ПК -11.3	1. Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это _____.		Низкий	2

<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>2.Закрытый ключ в ассиметричных алгоритмах необходим для следующей операции над информацией</p>	<p>1. шифрование  2. расшифровка  3. транслирование  4. копирование</p>	<p>Низкий</p>	<p>2</p>
<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>3.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>Низкий</p>	<p>2</p>
<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>4.Укажите верный термин определяющий вредоносный самовоспроизводящийся программный код.</p>	<p>1. Лазейка.  2. Червь.  3. Вирус.  4. Бактерия.</p>	<p>Низкий</p>	<p>2</p>
<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>5.Что является основой большинства современных блочных симметричных алгоритмов шифрования?</p>	<p>1. Сеть Фейстеля  2. Гаммирование  3. Перемешивание  4. Алфавит</p>	<p>Низкий</p>	<p>2</p>

ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -11.1 ПК -11.2 ПК -11.3	6.Совокупность методов и подходов к реализации задачи сокрытия факта передачи сообщения называется <hr/> —.		Средний	5
ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -11.1 ПК -11.2 ПК -11.3	7.Укажите ассиметричный алгоритм шифрования.	1. Эль-Гаммаля 2. IDEA 3. DES 4. Blowfish	Средний	5

<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>8.Проставьте соответствие между названием вида злоумышленных действий и его характеристикой, защита от которых является целью аутентификации</p>	<p>1. маскарад &lt;=&gt;  абонент С пересылает документ абоненту А от имени абонента В</p> <p>2. ренегатство &lt;=&gt;  абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле посылал</p> <p>3. подмена &lt;=&gt;  абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А</p>	<p>Средний</p>	<p>5</p>
---	---	--	----------------	----------

<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>9.Распределение ключей между пользователями вычислительной сети реализуется следующим образом:</p>	<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>	<p>Средний</p>	<p>5</p>
---	---	---	----------------	----------

<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>10.Функция, которая осуществляет сжатие строки чисел произвольного размера в строку чисел фиксированного размера (свертку) называется _____?  Результат работы функции называется _____.</p>		<p>Средний</p>	<p>5</p>
<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>11.Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет</p>	<p>1. криптография  2. стеганография  3. криптоанализ  4. криптология</p>	<p>Средний</p>	<p>5</p>

<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>12.Под угрозой удаленного администрирования в компьютерной сети понимается угроза ...</p>	<p>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</p>	<p>Средний</p>	<p>5</p>
<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>13.Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?</p>	<p>1. Сотрудники  2. Контрагенты  3. Хакеры  4. Посетители</p>	<p>Средний</p>	<p>5</p>
<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>14.Процесс проверки пользователя, является ли он тем за кого себя выдаёт, называется</p>		<p>Средний</p>	<p>5</p>

ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -11.1 ПК -11.2 ПК -11.3	15.Укажите размер блока шифрования в алгоритме "Магма", описанном в ГОСТ 34.12-2018. (ответ в количестве бит)		Средний	5
--	---	--	---------	---



<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>16.Алгоритм применения цифровой подписи на основе алгоритма шифрования RSA:</p>	<p>1. Получатель подтверждает подлинность подписи  2. Получатель вычисляет хэш-функцию <math>m' = SK_o \text{ mod } N</math>  3. Значения (M,S) отправляются получателю.  4. Сравнение <math>m'=m</math>, по которому получатель признает подпись подлинной.  5. Получатель вычисляет хэш-функцию <math>m = H(M)</math>  6. Вычисление пары ключей: секретный и открытый, используя алгоритм шифрования RSA.  7. Отправитель вычисляет <math>m=H(M)</math>, где <math>m</math> – целое число.  8. Отправитель вычисляет цифровую подпись <math>S = mK_s \text{ mod } N</math></p> <p>Правильные ответы:  1. Вычисление пары ключей: секретный и открытый, используя алгоритм шифрования RSA.  2. Отправитель вычисляет <math>m=H(M)</math>, где <math>m</math> – целое число.  3. Отправитель вычисляет цифровую подпись <math>S = mK_s \text{ mod } N</math>  4. Значения (M,S)</p>	<p>Высокий</p>	<p>8</p>
---	--	--	----------------	----------

		<p>отправляются получателю.</p> <p>5. Получатель вычисляет хэш- функцию <math>m' = SK_o</math> <math>\text{mod } N</math></p> <p>6. Получатель вычисляет хэш- функцию <math>m = H(M)</math></p> <p>7. Сравнение <math>m' = m</math>, по которому получатель признает подпись подлинной.</p> <p>8. Получатель подтверждает подлинность подписи</p>		
--	--	---	--	--

<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>17.Криптографические 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>Правильные ответы:  1. участники протокола не доверяют друг другу  2. требуется подтверждение подлинности участников сеанса связи.</p>	<p>Высокий</p>	<p>8</p>
<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>18.«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>Правильные ответы:  1. сообщения отправителя  2. секретного ключа отправителя</p>	<p>Высокий</p>	<p>8</p>

<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>19.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>Правильные ответы:  1. непреднамеренные ошибки пользователей  2. отказ программного и аппаратного обеспечения  3. разрушение или повреждение помещений</p>	<p>Высокий</p>	<p>8</p>
<p>ПК - 4.1  ПК - 4.2  ПК - 4.3  ПК -11.1  ПК -11.2  ПК -11.3</p>	<p>20.Основные угрозы конфиденциальности информации:</p>	<p>1. перехват данных  2. карнавал  3. переадресовка  4. злоупотребления полномочиями  5. маскарад</p> <p>Правильные ответы:  1. маскарад  2. перехват данных  3. злоупотребления полномочиями</p>	<p>Высокий</p>	<p>8</p>