

Документ подписан простой электронной подписью
Информация о владельце:

ФИО: Косенок Сергей Михайлович

Должность: ректор

Дата подписания: 24.06.2026 06:57:07

Уникальный программный ключ:

e3a68f3eaa1e62674b54f4998099d3d6bfdcf836

Гестовое задание для диагностического тестирования по дисциплине:

Безопасность информационных систем, 7 семестр

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

№	Проверяемая компетенция	Задание	Варианты ответов	Тип сложности вопроса
1.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	1. Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это _____.		Низкий

2.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	2.Закрытый ключ в ассиметричных алгоритмах необходим для следующей операции над информацией	1. шифрование 2. расшифровка 3. транслирование 4. копирование	Низкий
3.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	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
4.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	4.Укажите верный термин определяющий вредоносный самовоспроизводящийся программный код.	1. Лазейка. 2. Червь. 3. Вирус. 4. Бактерия.	Низкий

5.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	5.Что является основой большинства современных блочных симметричных алгоритмов шифрования?	1. Сеть Фейстеля 2. Гаммирование 3. Перемешивание 4. Алфавит	Низкий
6.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	6.Совокупность методов и подходов к реализации задачи сокрытия факта передачи сообщения называется <hr/> —		Средний
7.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	7.Укажите ассиметричный алгоритм шифрования.	1. Эль-Гаммаля 2. IDEA 3. DES 4. Blowfish	Средний

<p>8.</p>	<p>ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3</p>	<p>8.Проставьте соответствие между названием вида злоумышленных действий и его характеристикой, защита от которых является целью аутентификации</p>	<p>1. маскарад <=> абонент С пересылает документ абоненту А от имени абонента В</p> <p>2. ренегатство <=> абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле посылал</p> <p>3. подмена <=> абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А</p>	<p>Средний</p>
-----------	--	---	--	----------------

9.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	9.Распределение ключей между пользователями вычислительной сети реализуется следующим образом:	<ol style="list-style-type: none"> 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. 	Средний
----	---	--	---	---------

10.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	10.Функция, которая осуществляет сжатие строки чисел произвольного размера в строку чисел фиксированного размера (свертку) называется _____? Результат работы функции называется		Средний
11.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	11.Математические методы нарушения конфиденциальнос ти и аутентичности информации без знания ключей объединяет	1. криптография 2. стеганография 3. криптоанализ 4. криптология	Средний

12.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	12.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
13.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	13.Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?	1. Сотрудники 2. Контрагенты 3. Хакеры 4. Посетители	Средний
14.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	14.Процесс проверки пользователя, является ли он тем за кого себя выдаёт, называется _____		Средний

15.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	15.Укажите размер блока шифрования в алгоритме "Магма", описанном в ГОСТ 34.12-2018. (ответ в количестве бит)		Средний
-----	---	---	--	---------

16.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	16.Алгоритм применения цифровой подписи на основе алгоритма шифрования RSA:	<ol style="list-style-type: none"> 1. Получатель подтверждает подлинность подписи 2. Получатель вычисляет хэш-функцию $m' = SKo \text{ mod } N$ 3. Значения (M,S) отправляются получателю. 4. Сравнение $m'=m$, по которому получатель признает подпись подлинной. 5. Получатель вычисляет хэш-функцию $m = H(M)$ 6. Вычисление пары ключей: секретный и открытый, используя алгоритм шифрования RSA. 7. Отправитель вычисляет $m=H(M)$, где m – целое число. 8. Отправитель вычисляет цифровую подпись $S = mKs \text{ mod } N$ 	Высокий
-----	---	--	--	---------

17.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	17.Криптографические протоколы аутентификации используются, если	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	Высокий
18.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	18.«Цифровая подпись» формируется на основе следующих элементов:	1. сообщения отправителя 2. секретного ключа отправителя 3. секретного ключа получателя 4. открытого ключа отправителя	Высокий

19.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	19.Основные угрозы доступности информации:	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	Высокий
20.	ПК-5.1 ПК- 5.2 ПК-5.3 ПК-7.1 ПК- 7.2 ПК-7.3 ПК-16.1 ПК -16.2 ПК- 16.3 ПК- 17.1 ПК- 17.2 ПК- 17.3	20.Основные угрозы конфиденциальности информации:	1. перехват данных 2. карнавал 3. переадресовка 4. злоупотребления полномочиями 5. маскарад	Высокий