

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Косенок Сергей Михайлович  
Должность: ректор  
Дата подписания: 11.06.2026 09:32:23  
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	ПК-15.1, ПК-15.2, ПК-15.3	Что является основой большинства современных блочных симметричных алгоритмов шифрования?	1. Сеть Фейстеля 2. Гаммирование 3. Перемешивание 4. Алфавит	Низкий

2	ПК-15.1, ПК-15.2, ПК-15.3	<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	ПК-15.1, ПК-15.2, ПК-15.3	<p>Закрытый ключ в ассиметричных алгоритмах необходим для следующей операции над информацией</p>	<ol style="list-style-type: none"> <li>1. копирование</li> <li>2. расшифровка</li> <li>3. транслирование</li> <li>4. шифрование</li> </ol>	Низкий

4	ПК-15.1, ПК-15.2, ПК-15.3	<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	ПК-15.1, ПК-15.2, ПК-15.3	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

6	ПК-15.1, ПК-15.2, ПК-15.3	Распределение ключей между пользователями вычислительной сети реализуется следующим образом:	<ol style="list-style-type: none"> <li>1. использованием одного центра распределения ключей;</li> <li>2. использованием альтернативных каналов связи.</li> <li>3. использованием нескольких центров распределения ключей;</li> <li>4. прямым обменом сеансовыми ключами между пользователями сети;</li> </ol>	Средний
7	ПК-15.1, ПК-15.2, ПК-15.3	Совокупность методов и подходов к реализации задачи сокрытия факта передачи сообщения называется  _____.	—	Средний
8	ПК-15.1, ПК-15.2, ПК-15.3	Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет	<ol style="list-style-type: none"> <li>1. стеганография</li> <li>2. криптография</li> <li>3. криптоанализ</li> <li>4. криптология</li> </ol>	Средний

9	ПК-15.1, ПК-15.2, ПК-15.3	Укажите размер блока шифрования в алгоритме "Магма", описанном в ГОСТ 34.12-2018. (ответ в количестве бит)	—	Средний
10	ПК-15.1, ПК-15.2, ПК-15.3	Укажите ассиметричный алгоритм шифрования.	<ol style="list-style-type: none"> <li>1. IDEA</li> <li>2. Blowfish</li> <li>3. DES</li> <li>4. Эль-Гаммаля</li> </ol>	Средний
11	ПК-15.1, ПК-15.2, ПК-15.3	Проставьте соответствие между названием вида злоумышленных действий и его характеристикой, защита от которых является целью аутентификации	<ol style="list-style-type: none"> <li>1. маскаррад ↔ абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А</li> <li>2. ренегатство ↔ абонент С пересылает документ абоненту А от имени абонента В</li> <li>3. подмена ↔ абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле посылал</li> </ol>	Средний

12	ПК-15.1, ПК-15.2, ПК-15.3	Под угрозой удаленного администрирования в компьютерной сети понимается угроза ...	<ol style="list-style-type: none"> <li>1. перехвата или подмены данных на путях транспортировки</li> <li>2. несанкционированного управления удаленным компьютером</li> <li>3. поставки неприемлемого содержания</li> <li>4. внедрения агрессивного программного кода в рамках активных объектов Web-страниц</li> </ol>	Средний
13	ПК-15.1, ПК-15.2, ПК-15.3	Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?	<ol style="list-style-type: none"> <li>1. Хакеры</li> <li>2. Контрагенты</li> <li>3. Сотрудники</li> <li>4. Посетители</li> </ol>	Средний
14	ПК-15.1, ПК-15.2, ПК-15.3	Процесс проверки пользователя, является ли он тем за кого себя выдаёт, называется _____	—	Средний

15	ПК-15.1, ПК-15.2, ПК-15.3	<p>Функция, которая осуществляет сжатие строки чисел произвольного размера в строку чисел фиксированного размера (свертку) называется _____?</p> <p>Результат работы функции называется _____.</p>	—	Средний
16	ПК-15.1, ПК-15.2, ПК-15.3	<p>Основные угрозы доступности информации:</p>	<ol style="list-style-type: none"> <li>1. отказ программного и аппаратного обеспечения</li> <li>2. перехват данных</li> <li>3. разрушение или повреждение помещений</li> <li>4. злонамеренное изменение данных</li> <li>5. непреднамеренные ошибки пользователей</li> <li>6. хакерская атака</li> </ol>	Высокий

17	ПК-15.1, ПК-15.2, ПК-15.3	<p>Алгоритм применения цифровой подписи на основе алгоритма шифрования RSA:</p>	<ol style="list-style-type: none"> <li>1. Отправитель вычисляет цифровую подпись <math>S = mK_s \pmod{N}</math></li> <li>2. Значения (M,S) отправляются получателю.</li> <li>3. Получатель подтверждает подлинность подписи</li> <li>4. Получатель вычисляет хэш-функцию <math>m = H(M)</math></li> <li>5. Отправитель вычисляет <math>m = H(M)</math>, где <math>m</math> – целое число.</li> <li>6. Вычисление пары ключей: секретный и открытый, используя алгоритм шифрования RSA.</li> <li>7. Сравнение <math>m' = m</math>, по которому получатель признает подпись подлинной.</li> <li>8. Получатель вычисляет хэш-функцию <math>m' = SK_o \pmod{N}</math></li> </ol>	Высокий
----	---------------------------	---	--	---------

18	ПК-15.1, ПК-15.2, ПК-15.3	Криптографические протоколы аутентификации используются, если	<ol style="list-style-type: none"> <li>1. пользователь протокола уверен в достоверности информации, получаемой от другого пользователя;</li> <li>2. участвуют только два участника;</li> <li>3. участники протокола не доверяют друг другу</li> <li>4. требуется подтверждение подлинности участников сеанса связи.</li> </ol>	Высокий
19	ПК-15.1, ПК-15.2, ПК-15.3	«Цифровая подпись» формируется на основе следующих элементов:	<ol style="list-style-type: none"> <li>1. секретного ключа отправителя</li> <li>2. сообщения отправителя</li> <li>3. секретного ключа получателя</li> <li>4. открытого ключа отправителя</li> </ol>	Высокий
20	ПК-15.1, ПК-15.2, ПК-15.3	Основные угрозы конфиденциальности информации:	<ol style="list-style-type: none"> <li>1. злоупотребления полномочиями</li> <li>2. маскарад</li> <li>3. карнавал</li> <li>4. переадресовка</li> <li>5. перехват данных</li> </ol>	Высокий