# 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<br>2. Гаммирование<br>3. Перемешивание<br>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 | Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это _____ _____. | — | Низкий |
| 3 | 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 ассиметричных алгоритмах необходим для следующей операции над информацией | 1. копирование<br>2. расшифровка<br>3. транслирование<br>4. шифрование | Низкий |

| | | | | |
|---|---|---|---|---|
| 4 | 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 |
| 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 | Укажите верный термин определяющий вредоносный самовоспроизводящийся программный код. | 1. Лазейка.<br>2. Червь.<br>3. Вирус.<br>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: | 1. использованием одного центра распределения ключей;<br>2. использованием альтернативных каналов связи.<br>3. использованием нескольких центров распределения ключей;<br>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 | 1. стеганография<br>2. криптография<br>3. криптоанализ<br>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. | 1. IDEA<br>2. Blowfish<br>3. DES<br>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 | 1. маскарад ⟷абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А<br>2. ренегатство ⟷абонент С пересылает документ абоненту А от имени абонента В<br>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<br>2. несанкционированного управления удаленным компьютером<br>3. поставки неприемлемого содержания<br>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<br>2. Контрагенты<br>3. Сотрудники<br>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<br>2. перехват данных<br>3. разрушение или повреждение помещений<br>4. злонамеренное изменение данных<br>5. непреднамеренные ошибки пользователей<br>6. хакерская атака | Высокий |

| | | | | |
|---|---|---|---|---|
| 17 | ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 | Алгоритм применения цифровой подписи на основе алгоритма шифрования RSA: | 1. Отправитель вычисляет цифрову подпись S = mKs mod N<br>2. Значения (M,S) отправляются получателю.<br>3. Получатель подтверждает подлинность подписи<br>4. Получатель вычисляет хэш-функцию m = H(M)<br>5. Отправитель вычисляет m=H(M), где m – целое число.<br>6. Вычисление пары ключей: секретный и открытый, используя алгоритм шифрования RSA.<br>7. Сравнение m'=m, по которому получатель признает подпись подлинной.<br>8. Получатель вычисляет хэш-функцию m' = SKo mod N | Высокий |

| | | | | |
|---|---|---|---|---|
| 18 | ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 | Криптографические протоколы аутентификации используются, если | 1. пользователь протокола уверен в достоверности информации, получаемой от другого пользователя;<br>2. участвуют только два участника;<br>3. участники протокола не доверяют друг другу<br>4. требуется подтверждение подлинности участников сеанса связи. | Высокий |
| 19 | ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2 | «Цифровая подпись» формируется на основе следующих элементов: | 1. секретного ключа отправителя<br>2. сообщения отправителя<br>3. секретного ключа получателя<br>4. открытого ключа отправителя | Высокий |
| 20 | 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 конфиденциальности информации: | 1. злоупотребления полномочиями<br>2. маскарад<br>3. карнавал<br>4. переадресовка<br>5. перехват данных | Высокий |