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

| | | | | |
|---|---|---|---|---|
| ОПК-1.2<br>ОПК-1.3<br>ОПК-2.2<br>ОПК-2.3<br>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<br>ОПК-1.2<br>ОПК-1.3<br>ОПК-2.1<br>ОПК-2.2<br>ОПК-2.3<br>ОПК-3.1<br>ОПК-3.2 | Совокупность методов и подходов к реализации задачи сокрытия факта передачи сообщения называется _____. | | Средний | 5 |
| ОПК-1.3<br>ОПК-2.2<br>ОПК-2.3<br>ОПК-3.2 | Укажите ассиметричный алгоритм шифрования. | 1. Эль-Гаммаля<br>2. IDEA<br>3. DES<br>4. Blowfish | Средний | 5 |
| ОПК-1.1<br>ОПК-2.1<br>ОПК-3.1 | Проставьте соответствие между названием вида злоумышленных действий и его характеристикой, защита от которых является целью аутентификации | 1. маскарад <=> абонент С пересылает документ абоненту А от имени абонента В<br>2. ренегатство <=> абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле посылал<br>3. подмена <=> абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А | Средний | 5 |

| | | | | |
|---|---|---|---|---|
| | | | | |

| | | | | |
|---|---|---|---|---|
| ОПК-1.3<br>ОПК-2.2<br>ОПК-2.3<br>ОПК-3.2 | Распределение ключей между пользователями вычислительной сети реализуется следующим образом: | 1. прямым обменом сеансовыми ключами между пользователями сети;<br>2. использованием одного центра распределения ключей;<br>3. использованием нескольких центров распределения ключей;<br>4. использованием альтернативных каналов связи. | Средний | 5 |

| | | | | |
|---|---|---|---|---|
| ОПК-1.1<br>ОПК-1.2<br>ОПК-1.3<br>ОПК-2.1<br>ОПК-2.2<br>ОПК-2.3<br>ОПК-3.1<br>ОПК-3.2 | Функция, которая осуществляет сжатие строки чисел произвольного размера в строку чисел фиксированного размера (свертку) называется _____?<br>Результат работы функции называется _____. | | Средний | 5 |
| ОПК-1.1<br>ОПК-1.2<br>ОПК-1.3<br>ОПК-2.1<br>ОПК-2.2<br>ОПК-2.3<br>ОПК-3.1<br>ОПК-3.2 | Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет | 1. криптография<br>2. стеганография<br>3. криптоанализ<br>4. криптология | Средний | 5 |

| | | | | |
|---|---|---|---|---|
| ОПК-1.1<br>ОПК-1.2<br>ОПК-1.3<br>ОПК-2.1<br>ОПК-2.2<br>ОПК-2.3<br>ОПК-3.1<br>ОПК-3.2 | Под угрозой удаленного администрирования в компьютерной сети понимается угроза … | 1. внедрения агрессивного программного кода в рамках активных объектов Web-страниц<br>2. поставки неприемлемого содержания<br>3. перехвата или подмены данных на путях транспортировки<br>4. несанкционированного управления удаленным компьютером | Средний | 5 |
| ОПК-1.1<br>ОПК-1.2<br>ОПК-1.3<br>ОПК-2.1<br>ОПК-2.2<br>ОПК-2.3<br>ОПК-3.1<br>ОПК-3.2 | Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? | 1. Сотрудники<br>2. Контрагенты<br>3. Хакеры<br>4. Посетители | Средний | 5 |
| ОПК-1.1<br>ОПК-1.2<br>ОПК-1.3<br>ОПК-2.1<br>ОПК-2.2<br>ОПК-2.3<br>ОПК-3.1<br>ОПК-3.2 | Процесс проверки пользователя, является ли он тем за кого себя выдаёт, называется _____ | | Средний | 5 |

| | | | | |
|---|---|---|---|---|
| ОПК-1.3<br>ОПК-2.2<br>ОПК-2.3<br>ОПК-3.2 | Укажите размер блока шифрования в алгоритме "Магма", описанном в ГОСТ 34.12-2018. (ответ в количестве бит) | | Средний | 5 |

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

| | | | | |
|---|---|---|---|---|
| ОПК-1.1<br>ОПК-1.2<br>ОПК-1.3<br>ОПК-2.1<br>ОПК-2.2<br>ОПК-2.3<br>ОПК-3.1<br>ОПК-3.2 | Криптографические протоколы аутентификации используются, если | 1. участвуют только два участника;<br>2. требуется подтверждение подлинности участников сеанса связи.<br>3. пользователь протокола уверен в достоверности информации, получаемой от другого пользователя;<br>4. участники протокола не доверяют друг другу | Высокий | 8 |
| ОПК-1.1<br>ОПК-1.2<br>ОПК-1.3<br>ОПК-2.1<br>ОПК-2.2<br>ОПК-2.3<br>ОПК-3.1<br>ОПК-3.2 | «Цифровая подпись» формируется на основе следующих элементов: | 1. сообщения отправителя<br>2. секретного ключа отправителя<br>3. секретного ключа получателя<br>4. открытого ключа отправителя | Высокий | 8 |

| | | | | |
|---|---|---|---|---|
| ОПК-1.1<br>ОПК-1.2<br>ОПК-1.3<br>ОПК-2.1<br>ОПК-2.2<br>ОПК-2.3<br>ОПК-3.1<br>ОПК-3.2 | Основные угрозы доступности информации: | 1. непреднамеренные ошибки пользователей<br>2. хакерская атака<br>3. отказ программного и аппаратного обеспечения<br>4. злонамеренное изменение данных<br>5. перехват данных<br>6. разрушение или повреждение помещений | Высокий | 8 |
| ОПК-1.1<br>ОПК-1.2<br>ОПК-1.3<br>ОПК-2.1<br>ОПК-2.2<br>ОПК-2.3<br>ОПК-3.1<br>ОПК-3.2 | Основные угрозы конфиденциальности информации: | 1. перехват данных<br>2. карнавал<br>3. переадресовка<br>4. злоупотребления полномочиями<br>5. маскарад | Высокий | 8 |