

Документ подписан простой электронной подписью  
 Информация о владельце:  
 ФИО: Косенко Сергей Юрьевич  
 Должность: ректор  
 Дата подписания: 19.06.2024 06:50:05  
 Уникальный программный ключ:  
 e3a68f3eaa1e62674b54f4998099d3d6bfdcf836

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

*Основы защиты информации  
 7 семестр*

Код, направление подготовки	09.04.03
Направленность (профиль)	Программная инженерия
Форма обучения	очная
Кафедра-разработчик	Автоматики и компьютерных систем
Выпускающая кафедра	Автоматики и компьютерных систем

№	Проверяемая компетенция	Задание	Варианты ответов	Тип сложности вопроса
1	ОПК-3.2 ПК-7.1	Какие бывают виды угроз информационной безопасности?	<ol style="list-style-type: none"> <li>1. Утечка информации,</li> <li>2. Уничтожение информации,</li> <li>3. Искажение информации,</li> <li>4. Блокирование информации,</li> <li>5. Шифрование информации</li> </ol>	низкий уровень сложности
2	ОПК-3.2 ПК-7.1	Выберите виды уязвимостей программного обеспечения –	<ol style="list-style-type: none"> <li>1. конфигурационная</li> <li>2. маскировка информации</li> <li>3. избыточность элементов программной системы</li> <li>4. Уязвимость кода</li> </ol>	низкий уровень сложности
3	ОПК-3.2 ПК-7.1	Что относится к угрозам нарушения конфиденциальности?	<ol style="list-style-type: none"> <li>1. Хищение носителя информации,</li> <li>2. Публикация личной или коммерческой тайны,</li> <li>3. Невозможность сохранить информацию</li> <li>4. Внедрение дезинформации.</li> </ol>	низкий уровень сложности
4	ОПК-3.2 ПК-7.1	Причины появления уязвимостей:	<ol style="list-style-type: none"> <li>1. ошибки программирования,</li> </ol>	низкий уровень сложности

			<ol style="list-style-type: none"> <li>2. несоответствие программной и аппаратной компонент,</li> <li>3. использование ненадежных паролей,</li> <li>4. отсутствие бесперебойного электроснабжения</li> </ol>	
5	<b>ОПК-3.2</b> <b>ПК-7.1</b>	программная закладка может быть размещена в...	<ol style="list-style-type: none"> <li>1. загрузочный сектор жесткого диска</li> <li>2. драйвере</li> <li>3. BIOS</li> <li>4. Все ответы верны</li> </ol>	низкий уровень сложности
6	<b>ОПК-3.2</b> <b>ПК-7.1</b>	Аутентификация пользователя в системе предполагает	<ol style="list-style-type: none"> <li>1. Только идентификацию пользователя,</li> <li>2. Авторизацию пользователя,</li> <li>3. Назначение логина и пароля,</li> <li>4. Подтверждение личности пользователя</li> </ol>	Средний уровень сложности
7	<b>ОПК-3.2</b> <b>ПК-7.1</b>	Сеть Фейстеля - это	<ol style="list-style-type: none"> <li>1. Общий принцип работы всех криптографических алгоритмов</li> <li>2. Принцип работы блочных шифров</li> <li>3. Принцип работы потоковых шифров</li> <li>4. Одноранговая сеть</li> </ol>	Средний уровень сложности
8	<b>ОПК-3.2</b> <b>ПК-7.1</b>	Размер блока (в битах) в DES	<ol style="list-style-type: none"> <li>1. 8</li> <li>2. 16</li> <li>3. 32</li> <li>4. 64</li> </ol>	Средний уровень сложности
9	<b>ОПК-3.2</b> <b>ПК-7.1</b>	В блочных алгоритмах длина ключа зависит от...	<ol style="list-style-type: none"> <li>1. Длины блока,</li> <li>2. Длины исходного сообщения,</li> <li>3. Количества раундов</li> <li>4. Даты и времени шифрования</li> <li>5. Особенности алгоритма</li> </ol>	Средний уровень сложности
10	<b>ОПК-3.2</b> <b>ПК-7.1</b>	Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?	<ol style="list-style-type: none"> <li>1. шифр Маркова</li> <li>2. шифр Цезаря</li> <li>3. шифр Энигма</li> <li>4. шифр Бэбиджа</li> </ol>	Средний уровень сложности

11	<b>ОПК-3.2</b> <b>ПК-7.1</b>	Символы исходного текста складываются с символами некой случайной последовательности – это...	<ol style="list-style-type: none"> <li>1. алгоритм перестановки</li> <li>2. алгоритм аналитических преобразований</li> <li>3. алгоритм гаммирования</li> <li>4. алгоритм генератора случайных чисел</li> </ol>	Средний уровень сложности
12	<b>ОПК-3.2</b> <b>ПК-7.1</b>	Утечкой информации в системе называется ситуация, характеризующаяся:	<ol style="list-style-type: none"> <li>1. Потерей данных в системе,</li> <li>2. Изменением формы информации,</li> <li>3. Изменением содержания информации,</li> <li>4. Нет верных ответов</li> </ol>	Средний уровень сложности
13	<b>ОПК-3.2</b> <b>ПК-7.1</b>	Стандарт DES основан на идее	<ol style="list-style-type: none"> <li>1. гаммирование</li> <li>2. блочные шифры</li> <li>3. замещения</li> <li>4. перестановки</li> </ol>	Средний уровень сложности
14	<b>ОПК-3.2</b> <b>ПК-7.1</b>	Криптостойкость – это...	<ol style="list-style-type: none"> <li>1. все ответы верны</li> <li>2. характеристика шифра, определяющая сложность шифрования</li> <li>3. характеристика шифра, определяющая сложность взлома шифра</li> <li>4. свойство гаммы</li> <li>5. характеристика сложности алгоритма шифрования</li> </ol>	Средний уровень сложности
15	<b>ОПК-3.2</b> <b>ПК-7.1</b>	Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования	<ol style="list-style-type: none"> <li>1. 2</li> <li>2. 3</li> <li>3. 1</li> <li>4. Четное количество</li> </ol>	Средний уровень сложности
16	<b>ОПК-3.2</b> <b>ПК-7.1</b>	Установите соответствие:  1)конфиденциальность 2)доступность 3)целостность	<p>А) свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право</p> <p>Б) Состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.</p>	Высокий уровень сложности

			В) Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право	
17	<b>ОПК-3.2</b> <b>ПК-7.1</b>	Определите ключи шифра Цезаря, если известны следующая пара открытый текст – шифротекст: ЯБЛОКО – ЗЙФЧУЧ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)		Высокий уровень сложности
18	<b>ОПК-3.2</b> <b>ПК-7.1</b>	Основными источниками угроз информационной безопасности являются все указанное в списке:	1) Хищение жестких дисков, подключение к сети, инсайдерство 2) Перехват данных, хищение данных, изменение архитектуры системы 3) Хищение данных, подкуп системных администраторов, нарушение регламента работы 4) Хищение устройств, нелегальное программное обеспечение	Высокий уровень сложности
19	<b>ОПК-3.2</b> <b>ПК-7.1</b>	Установите соответствие: 1) Блочные шифры 2) Поточковые шифры	1) DES 2) ГОСТ 28147-89 3) AES 4) шифры на регистрах сдвига с линейной обратной связью 5) Метод Фибоначчи с запаздыванием	Высокий уровень сложности
20	<b>ОПК-3.2</b> <b>ПК-7.1</b>	Дайджест – это результат работы...	Хэш-функции, Поточкового шифра, Симметричного шифра, расшифрования	Высокий уровень сложности