

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Косенок Сергей Михайлович
Должность: ректор
Дата подписания: 30.06.2025 07:53:02
Уникальный программный ключ:
e3a68f3eaa1e62674b54f4998099d3d6bfdcf836

Тестовое задание для диагностического тестирования по дисциплине:

Программно-аппаратные средства обеспечения информационной, 6 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
ПК-1.1 ПК-1.2 ПК-1.3 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	К аспектам информационной безопасности не относится	1) Доступность 2) Целостность 3) Конфиденциальность 4) Защищенность	Низкий
ПК-1.1 ПК-1.2 ПК-1.3 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	По каким критериям нельзя классифицировать угрозы	1) по расположению источника угроз 2) по аспекту информационной безопасности, против которого угрозы направлены в первую очередь 3) по способу предотвращения 4) по компонентам информационных систем, на которые угрозы нацелены	Низкий
ПК-1.1 ПК-1.2 ПК-1.3 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	Главное достоинство парольной аутентификации	1) простота 2) надежность 3) секретность 4) запоминаемость	Низкий
ПК-1.1 ПК-1.2	К основным функциям подсистемы защиты	1) идентификация, аутентификация, авторизация, управление политикой	Низкий

ПК-1.3 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	операционной системы относится:	безопасности и разграничение доступа 2) криптографические функции 3) сетевые функции 4) все вышеперечисленные	
ПК-1.1 ПК-1.2 ПК-1.3 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	Какого метода разграничения доступа не существует	1) разграничение доступа по спискам 2) разграничение доступа по уровням секретности и категориям 3) локальное разграничение доступа 4) парольное разграничение доступа	Низкий
ПК-1.1 ПК-1.2 ПК-1.3 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	Что из перечисленного не входит в состав программного комплекса антивирусной защиты	1) Подсистема сканирования 2) Подсистема управления 3) Подсистема обнаружения вирусной активности 4) Подсистема устранения вирусной активности	Средний
ПК-1.1 ПК-1.2 ПК-1.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-7.1 ПК-7.2 ПК-7.3 ПК-16.1	Какой из протоколов не относится к протоколам защищенной передачи данных в сети Интернет	1) SSL 2) SET 3) HTTP 4) IPsec	Средний

ПК-16.2 ПК-16.3 ПК-17.1 ПК-17.2 ПК-17.3			
ПК-1.1 ПК-1.2 ПК-1.3 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	На каком уровне сетевой модели OSI не работает межсетевой экран	1) Физический 2) Сеансовый 3) Сетевой 4) Транспортный	Средний
ПК-1.1 ПК-1.2 ПК-1.3 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	Межсетевого экрана какого класса не существует	1) экранирующий маршрутизатор 2) экранирующий коммутатор 3) экранирующий транспорт 4) экранирующий шлюз	Средний
ПК-1.1 ПК-1.2 ПК-1.3 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	Установите соответствие: 1. Криптография 2. Кодирование 3. Скремблирование	А) это перевод информации с одного языка на другой Б) наука о методах обеспечения Конфиденциальности В) обратимое преобразование цифрового потока без изменения скорости	Средний
ПК-1.1 ПК-1.2	Установите соответствие: 1. Архивация	А) запись информации в электронном виде для долговременного	Средний

<p>ПК-1.3 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</p>	<p>2. Шифрование 3. Использование самогенерирующих кодов</p>	<p>хранения Б) это преобразование информации, делающее ее нечитаемой для посторонних В) это исполняемые коды программы, полученные в результате выполнения некоторого набора арифметических и/или логических операций над определенным, заранее рассчитанным, массивом данных</p>	
<p>ПК-1.1 ПК-1.2 ПК-1.3 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</p>	<p>Установите соответствие: 1. Порядковое кодирование 2. Пословное кодирование 3. Серийно-порядковое кодирование</p>	<p>А) способ кодирования реквизитов-признаков, состоящий в последовательном кодировании каждого слова (а не буквы) входного документа. Б) Предусматривает предварительное выделение групп объектов, которые составляют серию, а затем в каждой серии производится порядковая нумерация объектов. Каждая серия также будет иметь порядковую нумерацию. В) Предполагает последовательную нумерацию объектов числами натурального ряда. Порядок нумерации может быть случайным или определяться после предварительного упорядочения объектов, например по алфавиту.</p>	<p>Средний</p>
<p>ПК-1.1 ПК-1.2 ПК-1.3 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</p>	<p>Установите соответствие: 1. Угрозы для безопасности 2. Загрузочные вирусы 3. Макро-вирусы 4. Сетевые вирусы</p>	<p>А) используют для своего распространения протоколы или команды компьютерных сетей и электронной почты Б) заражают файлы-документы и электронные таблицы нескольких популярных редакторов В) записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор. Г) угрозы, которые не соответствуют в точности определению вируса, троянского коня, червя и других категорий угроз, но могут представлять угрозы для компьютера и</p>	<p>Средний</p>

<p>ПК-1.1 ПК-1.2 ПК-1.3 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</p>	<p>Установите соответствие: 1. Логические бомбы 2. Червями 3. Троянские кони 4. Программы-шпионы</p>	<p>хранящихся на нем данных А) программы или их части, постоянно находящиеся в ЭВМ и выполняемые только при соблюдении определенных условий Б) называются программы, которые обладают способностью перемещаться в системе или сети и самовоспроизводить копии В) это программы, полученные путем явного изменения или добавления команд в пользовательские программы Г) программы, предназначенные для слежения за деятельностью пользователя и несанкционированного чтения обрабатываемой им информации</p>	<p>Средний</p>
<p>ПК-1.1 ПК-1.2 ПК-1.3 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</p>	<p>Программы, предназначенные для слежения за деятельностью пользователя и несанкционированного чтения обрабатываемой им информации это _____</p>		<p>Средний</p>
<p>ПК-1.1 ПК-1.2 ПК-1.3 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</p>	<p>Программы или их части, которые постоянно находящиеся в ЭВМ и выполняемые только при соблюдении определенных условий называют _____</p>		<p>Высокий</p>
<p>ПК-1.1 ПК-1.2</p>	<p>Установите соответствие: 1. Метод "запрос-ответ"</p>	<p>А) При этом в процессе создания строки</p>	<p>Высокий</p>

<p>ПК-1.3 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</p>	<p>2. Метод "только ответ" 3. Метод "синхронизация по времени" 4. Метод "синхронизация по событию"</p>	<p>используется значение предыдущего запроса Б) В качестве исходной строки в нем используется не время, а количество успешных процедур аутентификации, проведенных до текущей В) При этом обычно используется не точное указание времени, а текущий интервал с установленными заранее границами (например, 30 секунд). Г) В начале процедуры аутентификации пользователь отправляет на сервер свой логин. В ответ на это последний генерирует некую случайную строку и посылает ее обратно.</p>	
<p>ПК-1.1 ПК-1.2 ПК-1.3 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</p>	<p>Как называются процессы, которые не требуются пользователю для выполнения своих служебных обязанностей и могут несанкционированно устанавливаться на компьютер (локально, либо удаленно) с различными целями, в том числе, и с целью осуществления несанкционированного доступа к информации</p>		<p>Высокий</p>
<p>ПК-1.1 ПК-1.2 ПК-1.3 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</p>	<p>Установите соответствие: 1. Пофайловое шифрование 2. Шифрование каталогов 3. Шифрование виртуальных дисков 4. Защита процесса загрузки</p>	<p>А) Пользователь создает папки, все данные в которых шифруются автоматически Б) Если зашифрован весь диск целиком, то операционная система не сможет запуститься, пока какой-либо механизм не расшифрует файлы загрузки В) Концепция виртуальных дисков реализована в некоторых утилитах компрессии, например Stacker или Microsoft DriveSpace Г) Пользователь сам выбирает файлы, которые</p>	<p>Высокий</p>

		следует зашифровать	
ПК-1.1 ПК-1.2 ПК-1.3 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	Установите правильную последовательность этапов защиты от угроз безопасности	<ol style="list-style-type: none"> 1. Анализ угрозы безопасности 2. Защита внешних каналов передачи информации 3. Обеспечение безопасного доступа к открытым ресурсам внешних сетей и Internet 4. Разработка политики информационной безопасности 5. Предоставление персоналу защищенный удаленный доступ к информационным ресурсам 	Высокий