Тестовое задание для диагностического тестирования по дисциплине:

Методы защиты, 7 семестр

Код, направление подготовки	09.03.02 Информационные системы и технологии
Направленность (профиль)	Информационные системы и технологии
Форма обучения	Очная
Кафедра разработчик	Информатики и вычислительной техники
Выпускающая кафедра	Информатики и вычислительной техники

№	Проверяемая компетенция	Задание	Варианты ответов	Тип сложности вопроса
1.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Какое свойство информации обеспечивает защиту от несанкционированного ознакомления?	а) Целостность б) Доступность в) Конфиденциальность г) Аутентичность	Низкий

2.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Криптографический ключ, который может быть известен всем участникам системы и используется для шифрования или проверки подписи, называется _____		Низкий
3.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Какой из перечисленных алгоритмов является российским стандартом симметричного блочного шифрования?	а) RSA б) «Кузнечик» в) ElGamal г) MD5	Низкий
4.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Процесс преобразования зашифрованного текста обратно в читаемый вид с использованием ключа называется _____.		Низкий

5.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Какой термин описывает программу, которая маскируется под легитимное ПО, но выполняет вредоносные действия?	а) Вирус б) Червь в) Троянская программа г) Бот	Низкий
6.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Что из перечисленного НЕ является методом аутентификации?	а) Пароль б) Смарт-карта в) Хеш-функция г) Биометрические данные	Средний
7.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Стандарт, регламентирующий использование электронной подписи в Российской Федерации, имеет номер _____.		Средний

8.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Установите соответствие между типом угрозы и её примером:	Тип угрозы Пример 1. Пассивная А. Модификация данных в базе 2. Активная Б. Прослушивание сетевого трафика 3. Внутренняя В. Утечка данных через сотрудника 4. Внешняя Г. Атака через уязвимость в веб-приложении	Средний

9.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Какие из перечисленных алгоритмов относятся к хеш-функциям?	а) SHA-256 б) AES в) ГОСТ Р 34.11-2012 («Стрибог») г) RSA д) MD5	Средний

10.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Протокол, который обеспечивает аутентификацию и согласование сеансового ключа в незащищённой сети, называется протоколом _____.		Средний
11.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Какая атака направлена на подбор пароля путём перебора всех возможных комбинаций символов?	а) Социальная инженерия б) Брутфорс-атака в) Фишинг г) Спуфинг	Средний
12.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Установите соответствие между режимом работы блочного шифра и его характеристикой:	Режим Характеристика 1. ECB А. Каждый блок шифруется независимо 2. CBC Б. Используется вектор инициализации и цепочка блоков 3. CTR В. Преобразует блочный шифр в поточный 4. GCM Г. Обеспечивает одновременно шифрование и аутентификацию	Средний

13.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Какие принципы лежат в основе обеспечения информационной безопасности по стандарту ISO/IEC 27001?	а) Оценка рисков б) Выбор мер защиты в) Непрерывный мониторинг г) Полное исключение всех угроз д) Документирование процессов	Средний
14.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Метод сокрытия информации внутри другого файла (изображения, аудио, видео) без изменения его видимых характеристик называется _____.		Средний
15.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Установите правильный порядок этапов атаки типа «человек посередине» (MitM):	А) Злоумышленник перехватывает соединение между жертвой и сервером Б) Злоумышленник устанавливает отдельные соединения с жертвой и сервером В) Злоумышленник при необходимости модифицирует передаваемые данные Г) Жертва и сервер «видят» соединение друг с другом, не подозревая о перехвате Д) Злоумышленник	Средний

			выполняет подготовку: анализ сети, выбор цели, инструменты	

16.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Какие требования предъявляются к системе управления ключами в криптографической защите?	а) Генерация ключей с использованием криптографически стойких ГСЧ б) Хранение секретных ключей в защищённой среде (HSM, TPM) в) Регулярная ротация ключей согласно политике безопасности г) Передача ключей по открытым каналам связи без дополнительной защиты д) Уничтожение ключей после окончания срока их использования	Высокий

17.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Какие уязвимости могут быть использованы для обхода механизмов аутентификации?	а) Слабые пароли по умолчанию б) Отсутствие блокировки после многократных неудачных попыток входа в) Передача учётных данных в открытом виде г) Использование многофакторной аутентификации д) Уязвимости в реализации сессионных токенов	Высокий
18.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Установите порядок действий при реализации защиты от утечек информации (DLP-система):	А) Определение критичных данных и каналов их передачи Б) Настройка политик и правил мониторинга В) Развёртывание агентов и сенсоров DLP-системы Г) Обучение персонала и информирование о политиках Д) Мониторинг, детектирование инцидентов и реагирование Е) Анализ эффективности и корректировка правил	Высокий

19.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Основные угрозы доступности информации:	1. непреднамеренные ошибки пользователей 2. хакерская атака 3. отказ программного и аппаратного обеспечения 4. злонамеренное изменение данных 5. перехват данных 6. разрушение или повреждение помещений	Высокий
20.	ПК - 4.1 ПК - 4.2 ПК - 4.3 ПК -7.1 ПК -7.2 ПК -7.3	Какие меры относятся к организационным методам защиты информации?	а) Разработка и утверждение политик безопасности б) Установка межсетевого экрана в) Проведение инструктажей сотрудников г) Шифрование баз данных д) Регламентация процедур доступа к ресурсам е) Внедрение системы контроля версий ПО	Высокий