Тестовое задание для диагностического тестирования по дисциплине:

Управление корпоративной информационной безопасности,
3 семестр

Код, направление подготовки	09.04.02 Информационные системы и технологии
Направленность (профиль)	Управление данными
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-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	1. Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это _____ _____.		Низкий

ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	2.Закрытый ключ в ассиметричных алгоритмах необходим для следующей операции над информацией	1. шифрование 2. расшифровка 3. транслирование 4. копирование	Низкий
ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	3. 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
ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	4. Укажите верный термин определяющий вредоносный самовоспроизводящийся программный код.	1. Лазейка. 2. Червь. 3. Вирус. 4. Бактерия.	Низкий

ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	5.Основным назначением корпоративных информационных систем является -	1. сбор данных о компании. 2. обеспечение передачи сообщений между пользователями. 3. оперативное предоставление непротиворечивой, достоверной и структурированной информации для принятия управленческих решений. 4. передача данных в глобальную сеть Интернет.	Низкий
ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	6. Совокупность методов и подходов к реализации задачи сокрытия факта передачи сообщения называется _____.		Средний

ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	7. Укажите ассиметричный алгоритм шифрования.	1. Эль-Гаммаля 2. IDEA 3. DES 4. Blowfish	Средний
ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	8. 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 2. ренегатство <=> абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле посылал 3. подмена <=> абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А	Средний
ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	9. Распределение ключей между пользователями корпоративной информационной системы реализуется следующим образом:	1. прямым обменом сеансовыми ключами между пользователями сети; 2. использованием одного центра распределения ключей; 3. использованием нескольких центров распределения ключей; 4. использованием альтернативных каналов связи.	Средний

ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	10.Что обеспечивает контур «Системное администрирование»?	1. поддержку деятельности маркетингового отдела, отдела сбыта; 2. автоматизацию управления в подразделениях предприятия: отдел снабжения, отдел сбыта, склад; 3. настройку и конфигурирование системы, администрирование базы данных, разработку новых функциональных модулей; 4. все перечисленное верно.	Средний
ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	11. Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет	1. криптография 2. стеганография 3. криптоанализ 4. криптология	Средний

ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	12. Под угрозой удаленного администрирования в компьютерной сети понимается угроза …	1. внедрения агрессивного программного кода в рамках активных объектов Web-страниц 2. поставки неприемлемого содержания 3. перехвата или подмены данных на путях транспортировки 4. несанкционированного управления удаленным компьютером	Средний
ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	13. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?	1. Сотрудники 2. Контрагенты 3. Хакеры 4. Посетители	Средний
ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	14. Процесс проверки пользователя, является ли он тем за кого себя выдаёт, называется _____		Средний

ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	15.Какое свойство корпоративных информационных систем выделяют?	1. интеграция предприятий с внешней средой; 2. специальные корпоративные информационные технологии; 3. обеспечение высокого качества информации для принятий управленческих решений, надежность и защищенность КИС.	Средний
ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	16. Алгоритм применения цифровой подписи на основе алгоритма шифрования RSA:	1. Получатель подтверждает подлинность подписи 2. Получатель вычисляет хэш-функцию m' = SKo mod N 3. Значения (M,S) отправляются получателю. 4. Сравнение m'=m, по которому получатель признает подпись подлинной. 5. Получатель вычисляет хэш-функцию m = H(M) 6. Вычисление пары ключей: секретный и открытый, используя алгоритм шифрования RSA. 7. Отправитель вычисляет m=H(M), где m – целое число. 8. Отправитель вычисляет цифрову подпись S = mKs mod N	Высокий

ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	17. Криптографические протоколы аутентификации используются, если	1. участвуют только два участника; 2. требуется подтверждение подлинности участников сеанса связи. 3. пользователь протокола уверен в достоверности информации, получаемой от другого пользователя; 4. участники протокола не доверяют друг другу.	Высокий
ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	18. «Цифровая подпись» формируется на основе следующих элементов:	1. сообщения отправителя 2. секретного ключа отправителя 3. секретного ключа получателя 4. открытого ключа отправителя	Высокий
ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	19. 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

ПК-1.1 ПК-1.2 ПК-1.3 ПК-2.1 ПК-2.2 ПК-2.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-10.1 ПК-10.2 ПК-10.3	20. Основные угрозы конфиденциальности информации:	1. перехват данных 2. карнавал 3. переадресовка 4. злоупотребления полномочиями 5. маскарад	Высокий