

Документ подписан простой электронной подписью  
 Информация о владельце:  
 ФИО: Косенок Сергей Михайлович  
 Должность: ректор  
 Дата подписания: 19.06.2024 07:24:06  
 Уникальный программный ключ:  
 e3a68f3eaa1e62674b544998099d3d6bfdcf836

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

Код направления 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

**8 семестр**

№	Проверяемая компетенция	Задание	Варианты ответов	Тип сложности вопроса
1	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	Наиболее острой при переходе к информационному обществу является проблема...	1) экологической безопасности; 2) информационной безопасности; 3) реализации гуманистических принципов; 4) овладения текстовым процессором.	низкий
2	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	Основная задача информационной безопасности это защита ...	1) конфиденциальность информации; 2) целостности информации; 3) покупки информации; 4) доступности информации.	низкий
3	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:	1) Доступность 2) Целостность 3) Актуальность	низкий
4	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	Виды информационной безопасности:	1) Персональная, корпоративная, государственная 2) Клиентская, серверная, сетевая 3) Локальная, глобальная, смешанная	низкий
5	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	Цели информационной безопасности – своевременное обнаружение, предупреждение:	1) несанкционированного доступа, воздействия в сети 2) инсайдерства в организации 3) чрезвычайных ситуаций	низкий
6	ПК-9.1 ПК-9.2 ПК-9.3	Основные объекты информационной безопасности:	1) Компьютерные сети	средний

	ПК-18.1 ПК-18.2 ПК-18.3		2) Информационные системы, психологическое состояние пользователей 3) Базы данных 4) Бизнес-ориентированные, коммерческие системы	
7	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными – это:	1) субъект персональных данных; 2) оператор персональных данных 3) Уполномоченный орган по защите прав субъектов персональных данных 4) Государственный орган по защите прав субъектов персональных данных	средний
8	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	Укажите ассиметричный алгоритм шифрования:	1) Эль-Гаммал 2) IDEA 3) DES 4) Blowfish	средний
9	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	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
10	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет	1. криптография 2. стеганография 3. криптоанализ 4. криптология	средний
11	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1	В случае, если объект критической информационной инфраструктуры по	1) может не осуществляться 2) обязательно осуществляется	средний

	ПК-18.2 ПК-18.3	одному из показателей критериев значимости отнесен к первой категории, расчет по остальным показателям критериев значимости может не осуществляться		
12	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	Оценка показателей экономической значимости осуществляется ..... по категорированию субъекта критической информационной инфраструктуры (КИИ) по результатам оценки масштабов возможных экономических последствий в случае возникновения компьютерных инцидентов, наступающих в результате совершения компьютерных атак на категорируемый объект КИИ:	1) комиссией; 2) оператором; 3) оператором; 4) государственным органом.	средний
13	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	Физическое лицо, которое может быть прямо или косвенно определено, или определяемо при использовании персональных данных – это:	1) субъект персональных данных; 2) оператор персональных данных 3) Уполномоченный орган по защите прав субъектов персональных данных 4) Государственный орган по защите прав субъектов персональных данных	средний
14	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	Уполномоченным органом по защите прав субъектов персональных данных является:	1) Правительство РФ 2) Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор); 3) любой государственный орган, муниципальный орган; 4) Счетная палата РФ.	средний
15	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	Может ли считаться персональными данными информация об абстрактном человеке (каком-то, не конкретном)	1) может 2) не может	средний
16	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	Основные угрозы конфиденциальности информации:	1) перехват данных 2) карнавал 3) переадресовка 4) злоупотребления полномочиями	высокий

17	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	В случае, если функционирование одного объекта критической информационной инфраструктуры зависит от функционирования другого объекта, оценка масштаба экономического ущерба проводится исходя из предположения о ... функционирования вследствие компьютерной атаки объекта КИИ, от которого зависит оцениваемый объект	1) нарушении; 2) прекращении; 3) продолжения; 4) возрождения	высокий
18	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	Совокупность методов и подходов к реализации задачи сокрытия факта передачи сообщения называется.....		высокий
19	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	<i>Сведения любого характера (производственные, технические, экономические, организационные и другие) о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности, имеющие действительную или потенциальную коммерческую ценность вследствие неизвестности их третьим лицам</i>	1) коммерческая тайна 2) секрет производства 3) ноу-хау 4) банковская тайна.	высокий
20	ПК-9.1 ПК-9.2 ПК-9.3 ПК-18.1 ПК-18.2 ПК-18.3	«Цифровая подпись» формируется на основе следующих элементов:	1) сообщения отправителя 2) секретного ключа отправителя 3) секретного ключа получателя 4) открытого ключа отправителя	высокий