Тестовое задание для диагностического тестирования по дисциплине:

Криптографические алгоритмы и безопасность информационных систем

Код, направление подготовки	09.04.04 ПРОГРАММНАЯ ИНЖЕНЕРИЯ
Направленность (профиль)	Разработка и интеграция информационных систем и сервисов
Форма обучения	Очная
Кафедра-разработчик	Автоматики и компьютерных систем
Выпускающая кафедра	Автоматики и компьютерных систем

Проверяемая компетенция	Задание	Варианты ответов	Тип сложности вопроса
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	1. Что такое криптография?	1. Наука о безопасности информации. 2. Компьютерное программирование. 3. Наука о проверке подлинности. 4. Шифрование информации.	Низкий
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	2. Какой основной процесс используется в криптографии?	1. Шифрование 2. Расшифровка 3. Алгоритмическая аналитика 4. Графическое представление	Низкий
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	3. Что такое симметричное шифрование?	1. Шифрование требующее одного ключа 2. Шифрование требующее двух ключей 3. Шифрование, вычисляемое алгоритмически 4. Шифрование, вычисляемое физически	Низкий
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	4. Какой алгоритм SHA-2 является основным стандартом для хеширования?	1. DES 2. AES 3. SHA-1 4. SHA-256	Низкий
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	5. Что такое цифровая подпись?	1. Способ защиты конфиденциальной информации 2. Использование накопленной истории для цифровой проверки 3. Цифровой метод, используемый для передачи платежей 4. Метод проверки подлинности автора	Низкий
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	6. Какой тип криптографии будет использоваться для передачи информации по сети?	1. симметричная 2. асимметричная 3. хеширование 4. публичное ключевое шифрование	Средний

ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	7. Какой алгоритм хеширования используется для проверки целостности данных?	1. DES 2. AES 3. RSA 4. MD5	Средний
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	8. Какое важное понятие сопряжено с ассиметричным шифрованием?	1. Симметричное шифрование 2. Хэширование 3. Ключ доступа 4. Цифровая подпись	Средний
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	9. Какая из следующих технологий не является стандартом ассиметричного шифрования?	1. SHA-2 2. AES 3. RSA 4. Diffie-Hellman	Средний
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	10. Какая ассиметричная технология шифрования используется для проверки истории трансфера данных в цепочках блоков?	1. AES 2. RSA 3. HMAC 4. SHA-2	Средний
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	11. Какой алгоритм шифрования используется для безопасной передачи данных по протоколу TLS/SSL?	1. Ринговый шифр 2. SHA-256 3. DES 4. RSA	Средний
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	12. Что такое дисперсия в регрессионном анализе?	1. Разброс отклонения прогнозируемых и наблюдаемых значений 2. Штраф, уменьшающий дисперсию и делающий прогнозы более адекватными 3. Оценка сложности построенной модели 4. Вероятность того, что прогноз не будет больше, чем наблюдаемое значение	Средний
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	13. Какой алгоритм шифрования предоставляет надежную защиту данных со встроенными механизмами аутентификации?	1. SHA-1 2. AES 3. RSA 4. SHA-256	Средний
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	14. В каком случае применяется логистическая регрессия?	1. Семантический анализ 2. Распознавание образов 3. Решение задач классификации 4. Кластеризация	Средний
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	15. Для чего используется логистическая регрессия?	1. Для предсказания будущих данных 2. Для классификации бинарных данных 3. Для распознавания образов 4. Для задач понижения размерности	Средний
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	16. Какие основные протоколы используются в криптографии?	1. SSL/TLS и SSH 2. SSH и HTTPS 3. DES и RSA 4. SSL и AES	Высокий
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	17. Какую задачу НЕ решает электронная подпись?	1. Установление анонимности сообщения 2. Удостоверение отправителя сообщения 3. Проверка подлинности получателя сообщения 4. Защита сообщения от подмены	Высокий
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	18. Какую из следующих функций выполняет открытый ключ при шифровании сообщений?	1. Авторизация 2. Защита 3. Шифрование 4. Расшифрование	Высокий

ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	19. Что нужно получателю чтобы расшифровать сообщение, которое было зашифровано с помощью открытого ключа?	1. Пароль 2. Личный документ 3. Закрытый ключ 4. Открытый ключ	Высокий
ОПК-2.1, ОПК-2.2, ОПК-4.1, ОПК-4.2	20. Что представляет собой открытый ключ?	1. Ключ, используемый для расшифровки сообщений 2. Ключ, используемый для шифрования сообщений 3. Ключ, используемый для подтверждения подлинности 4. Ключ, используемый для генерации сигнатур	Высокий