|  |
| --- |
| **ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем** |
| Индикаторы, дескрипторы достижения компетенции | Комплекс заданий для оценки компетенций(сквозная нумерация) | Ключи правильных ответов | Критерии оценки |
| **Дисциплина «Методы и средства криптографической защиты информации» (Б1.Б.35)** |
| ИОПК-11.1. Применяет криптографические методы для создания компонентов систем защиты информации открытых информационных систем.**Знать:** − основные подходы к конструированию систем защиты информации с использованием криптографических протоколов различной направленности (ИОПК-11.1) **Уметь:** − строить современные защищённые программные комплексы с использованием криптографических алгоритмов и протоколов (ИОПК - 11.1) **Владеть:** − современными международными стандартами в области криптографических алгоритмов и протоколов для обеспечения защиты информации (ИОПК - 11.1) − навыками проверки работоспособности применяемых криптографических алгоритмов и протоколов защиты информации (ИОПК - 11.1) | **1. Сколько ключей используется в асимметричной криптографии?**1. Один2. Два: публичный и приватный3. Зависит от длины сообщения | 2 | Верный ответ – 1 балл, неверный – 0. |
| **2. Пример асимметричного алгоритма шифрования:**1. DES2. RSA3. MD5 | 2 | Верный ответ – 1 балл, неверный – 0. |
| **3. Что такое публичный ключ?**1. Секретный код пользователя2. Открытая часть пары ключей, используемая для шифрования или проверки подписи3. Временный пароль | 2 | Верный ответ – 1 балл, неверный – 0. |
| **4. Для чего используется приватный ключ?**1. Хранение данных2. Расшифровка данных и создание цифровой подписи3. Управление сетями | 2 | Верный ответ – 1 балл, неверный – 0. |
| **5. В чём основное преимущество асимметричного шифрования?**1. Высокая скорость обработки2. Отсутствие необходимости безопасной передачи ключа3. Универсальность | 2 | Верный ответ – 1 балл, неверный – 0. |
| **6. Чем отличается симметричное шифрование от асимметричного?**1. Они используют один и тот же алгоритм2. Симметричное шифрование использует один ключ, асимметричное — два разных ключа3. Асимметричное быстрее | 2 | Верный ответ – 1 балл, неверный – 0. |
| **7. Что такое хеш-функция?**1. Алгоритм для поиска данных2. Функция для преобразования данных в строку фиксированной длины3. Система резервного копирования | 2 | Верный ответ – 1 балл, неверный – 0. |
| **8. Какова цель криптографической аутентификации?**1. Сжатие данных2. Подтверждение подлинности отправителя и целостности данных3. Удаление информации | 2 | Верный ответ – 1 балл, неверный – 0. |
| **9. Что такое цифровая подпись?**1. Криптографический метод проверки подлинности данных2. Электронная копия документа3. Код для шифрования | 1 | Верный ответ – 1 балл, неверный – 0. |
| **10. Какие угрозы устраняет криптография?**1. Несанкционированный доступ, изменение и подделка информации2. Только аппаратные ошибки3. Логические ошибки в программах | 1 | Верный ответ – 1 балл, неверный – 0. |
| **11. Какой ключ используется в симметричном шифровании?**1. Два разных ключа2. Один общий ключ для шифрования и расшифровки3. Ключ из хеш-функции | 2 | Верный ответ – 1 балл, неверный – 0. |
| **12. Какой алгоритм является симметричным?**1. RSA2. AES (Advanced Encryption Standard)3. Diffie-Hellman | 2 | Верный ответ – 1 балл, неверный – 0. |
| **13. Что такое блочное шифрование?**1. Шифрование данных блоками фиксированного размера2. Шифрование файлов в реальном времени3. Сжатие информации | 1 | Верный ответ – 1 балл, неверный – 0. |
| **14. Пример потокового шифрования:**1. RC42. AES3. ECC | 1 | Верный ответ – 1 балл, неверный – 0. |
| **15. Каковы преимущества симметричного шифрования?**1. Быстрота и простота реализации2. Высокая скорость обработки данных3. Отсутствие необходимости в ключах | 2 | Верный ответ – 1 балл, неверный – 0. |
| **16. Какие недостатки есть у симметричного шифрования?**1. Проблемы с безопасной передачей ключа2. Высокая сложность реализации3. Большой размер ключа | 1 | Верный ответ – 1 балл, неверный – 0. |
| **17. Что такое режим работы блочного шифра?**1. Алгоритм проверки ключей2. Метод шифрования последовательности блоков данных3. Временное хранение ключей | 2 | Верный ответ – 1 балл, неверный – 0. |
| **18. Какой режим работы обеспечивает криптографическую стойкость?**1. ECB (Electronic Codebook)2. CBC (Cipher Block Chaining)3. Открытый текст | 2 | Верный ответ – 1 балл, неверный – 0. |
| **19. Какие данные требуют симметричного шифрования?**1. Только текстовые файлы2. Любая информация, требующая высокой скорости обработки3. Только хешированные данные | 2 | Верный ответ – 1 балл, неверный – 0. |
| **20. Что такое алгоритм DES?**1. Ассиметричный метод2. Устаревший стандарт симметричного шифрования данных3. Современный хеш-алгоритм | 2 | Верный ответ – 1 балл, неверный – 0. |
| **Дисциплина «Защита программ и данных» (Б1.Б.38)** |
| ИОПК-11.2. Применяет методы защиты программ и данных при создании открытых информационных систем.**Знать:** − методы и средства защиты программ от разрушающих воздействий (ИОПК-11.2) − основные подходы к защите программ от несанкционированного копирования (ИОПК-11.2) − методы защиты программного обеспечения от исследования (ИОПК-11.2) **Уметь:** − проектировать средства защиты программ в автоматизированных системах (ИОПК-11.2) − защищать программное обеспечение от исследования (ИОПК-11.2) − защищать программное обеспечение от несанкционированного копирования (ИОПК-11.2) **Владеть:** − методами разработки, анализа и тестирования безопасности программного обеспечения (ИОПК-11.2) | **1. Что понимается под защитой данных?**1. Создание резервных копий2. Комплекс мер для предотвращения утечки, модификации или уничтожения информации3. Оптимизация структуры базы данных | 2 | Верный ответ – 1 балл, неверный – 0. |
| **2. Что такое целостность данных?**1. Ускорение их обработки2. Сохранение их неизменности и достоверности3. Создание новых файлов | 2 | Верный ответ – 1 балл, неверный – 0. |
| **3. Какая цель защиты программного обеспечения?**1. Ускорение работы программы2. Предотвращение несанкционированного копирования и модификации3. Оптимизация интерфейса | 2 | Верный ответ – 1 балл, неверный – 0. |
| **4. Что такое резервное копирование?**1. Удаление ненужных данных2. Создание копий данных для восстановления в случае утраты3. Проверка ключей безопасности | 2 | Верный ответ – 1 балл, неверный – 0. |
| **5. Какие типы угроз существуют для данных?**1. Только физические повреждения2. Несанкционированный доступ, вирусы, аппаратные сбои3. Устранение дублирования | 2 | Верный ответ – 1 балл, неверный – 0. |
| **6. Что такое шифрование данных?**1. Компрессия файлов2. Превращение данных в зашифрованный вид для предотвращения доступа3. Разделение данных на части | 2 | Верный ответ – 1 балл, неверный – 0. |
| **7. Какой метод защиты предотвращает изменение данных?**1. Контроль целостности2. Сжатие данных3. Кэширование | 1 | Верный ответ – 1 балл, неверный – 0. |
| **8. Что такое двухфакторная аутентификация?**1. Ввод пароля дважды2. Использование двух методов проверки личности, например, пароль и SMS-код3. Создание двух аккаунтов | 2 | Верный ответ – 1 балл, неверный – 0. |
| **9. Как антивирусное ПО защищает данные?**1. Оптимизирует работу системы2. Обнаруживает и удаляет вредоносное ПО3. Увеличивает скорость обработки | 2 | Верный ответ – 1 балл, неверный – 0. |
| **10. Что такое межсетевой экран (фаервол)?**1. Программа для управления паролями2. Система, блокирующая несанкционированный доступ к сети3. Метод ускорения соединения | 2 | Верный ответ – 1 балл, неверный – 0. |
| **11. Что такое вредоносное ПО (Malware)?**1. Программное обеспечение для резервного копирования2. ПО, созданное для нанесения вреда системам или данным3. Лицензионное ПО | 2 | Верный ответ – 1 балл, неверный – 0. |
| **12. Что такое фишинг?**1. Метод обмана для получения конфиденциальных данных2. Вирус, атакующий системы3. Метод хеширования | 1 | Верный ответ – 1 балл, неверный – 0. |
| **13. Какой вид атаки направлен на перегрузку системы запросами?**1. Фишинг2. DDoS-атака (распределённый отказ в обслуживании)3. Внедрение вирусов | 2 | Верный ответ – 1 балл, неверный – 0. |
| **14. Что такое руткит?**1. Программа для шифрования данных2. Вредоносное ПО, скрывающее присутствие других программ3. Система резервного копирования | 2 | Верный ответ – 1 балл, неверный – 0. |
| **15. Что такое социальная инженерия?**1. Метод хеширования данных2. Манипуляция людьми для получения конфиденциальной информации3. Оптимизация сетей | 2 | Верный ответ – 1 балл, неверный – 0. |
| **16. Каков первый шаг к защите данных?**1. Удаление неиспользуемых программ2. Идентификация и классификация данных3. Архивирование всех данных | 2 | Верный ответ – 1 балл, неверный – 0. |
| **17. Что такое принцип минимальных привилегий?**1. Выдача всем пользователям максимального доступа2. Ограничение доступа только необходимыми правами3. Удаление всех привилегий | 2 | Верный ответ – 1 балл, неверный – 0. |
| **18. Зачем нужна политика управления паролями?**1. Ускорение работы системы2. Обеспечение использования надёжных и уникальных паролей3. Упрощение авторизации | 2 | Верный ответ – 1 балл, неверный – 0. |
| **19. Что такое GDPR?**1. Протокол передачи данных2. Европейский регламент защиты персональных данных3. Система резервного копирования | 2 | Верный ответ – 1 балл, неверный – 0. |
| **20. Как часто рекомендуется обновлять программное обеспечение для защиты?**1. Раз в год2. Только при проблемах3. Регулярно, чтобы устранить уязвимости | 3 | Верный ответ – 1 балл, неверный – 0. |