|  |  |  |  |
| --- | --- | --- | --- |
| **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. Один  2. Два: публичный и приватный  3. Зависит от длины сообщения | 2 | Верный ответ – 1 балл, неверный – 0. |
| **2. Пример асимметричного алгоритма шифрования:**  1. DES  2. RSA  3. MD5 | 2 | Верный ответ – 1 балл, неверный – 0. |
| **3. Что такое публичный ключ?**  1. Секретный код пользователя  2. Открытая часть пары ключей, используемая для шифрования или проверки подписи  3. Временный пароль | 2 | Верный ответ – 1 балл, неверный – 0. |
| **4. Для чего используется приватный ключ?**  1. Хранение данных  2. Расшифровка данных и создание цифровой подписи  3. Управление сетями | 2 | Верный ответ – 1 балл, неверный – 0. |
| **5. В чём основное преимущество асимметричного шифрования?**  1. Высокая скорость обработки  2. Отсутствие необходимости безопасной передачи ключа  3. Универсальность | 2 | Верный ответ – 1 балл, неверный – 0. |
| **6. Чем отличается симметричное шифрование от асимметричного?**  1. Они используют один и тот же алгоритм  2. Симметричное шифрование использует один ключ, асимметричное — два разных ключа  3. Асимметричное быстрее | 2 | Верный ответ – 1 балл, неверный – 0. |
| **7. Что такое хеш-функция?**  1. Алгоритм для поиска данных  2. Функция для преобразования данных в строку фиксированной длины  3. Система резервного копирования | 2 | Верный ответ – 1 балл, неверный – 0. |
| **8. Какова цель криптографической аутентификации?**  1. Сжатие данных  2. Подтверждение подлинности отправителя и целостности данных  3. Удаление информации | 2 | Верный ответ – 1 балл, неверный – 0. |
| **9. Что такое цифровая подпись?**  1. Криптографический метод проверки подлинности данных  2. Электронная копия документа  3. Код для шифрования | 1 | Верный ответ – 1 балл, неверный – 0. |
| **10. Какие угрозы устраняет криптография?**  1. Несанкционированный доступ, изменение и подделка информации  2. Только аппаратные ошибки  3. Логические ошибки в программах | 1 | Верный ответ – 1 балл, неверный – 0. |
| **11. Какой ключ используется в симметричном шифровании?**  1. Два разных ключа  2. Один общий ключ для шифрования и расшифровки  3. Ключ из хеш-функции | 2 | Верный ответ – 1 балл, неверный – 0. |
| **12. Какой алгоритм является симметричным?**  1. RSA  2. AES (Advanced Encryption Standard)  3. Diffie-Hellman | 2 | Верный ответ – 1 балл, неверный – 0. |
| **13. Что такое блочное шифрование?**  1. Шифрование данных блоками фиксированного размера  2. Шифрование файлов в реальном времени  3. Сжатие информации | 1 | Верный ответ – 1 балл, неверный – 0. |
| **14. Пример потокового шифрования:**  1. RC4  2. AES  3. ECC | 1 | Верный ответ – 1 балл, неверный – 0. |
| **15. Каковы преимущества симметричного шифрования?**  1. Быстрота и простота реализации  2. Высокая скорость обработки данных  3. Отсутствие необходимости в ключах | 2 | Верный ответ – 1 балл, неверный – 0. |
| **16. Какие недостатки есть у симметричного шифрования?**  1. Проблемы с безопасной передачей ключа  2. Высокая сложность реализации  3. Большой размер ключа | 1 | Верный ответ – 1 балл, неверный – 0. |
| **17. Что такое режим работы блочного шифра?**  1. Алгоритм проверки ключей  2. Метод шифрования последовательности блоков данных  3. 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 файлы  2. Любая информация, требующая высокой скорости обработки  3. Только хешированные данные | 2 | Верный ответ – 1 балл, неверный – 0. |
| **20. Что такое алгоритм DES?**  1. Ассиметричный метод  2. Устаревший стандарт симметричного шифрования данных  3. 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 копий  2. Комплекс мер для предотвращения утечки, модификации или уничтожения информации  3. Оптимизация структуры базы данных | 2 | Верный ответ – 1 балл, неверный – 0. |
| **2. Что такое целостность данных?**  1. Ускорение их обработки  2. Сохранение их неизменности и достоверности  3. Создание новых файлов | 2 | Верный ответ – 1 балл, неверный – 0. |
| **3. Какая цель защиты программного обеспечения?**  1. Ускорение работы программы  2. Предотвращение несанкционированного копирования и модификации  3. Оптимизация интерфейса | 2 | Верный ответ – 1 балл, неверный – 0. |
| **4. Что такое резервное копирование?**  1. Удаление ненужных данных  2. Создание копий данных для восстановления в случае утраты  3. Проверка ключей безопасности | 2 | Верный ответ – 1 балл, неверный – 0. |
| **5. Какие типы угроз существуют для данных?**  1. Только физические повреждения  2. Несанкционированный доступ, вирусы, аппаратные сбои  3. Устранение дублирования | 2 | Верный ответ – 1 балл, неверный – 0. |
| **6. Что такое шифрование данных?**  1. Компрессия файлов  2. Превращение данных в зашифрованный вид для предотвращения доступа  3. Разделение данных на части | 2 | Верный ответ – 1 балл, неверный – 0. |
| **7. Какой метод защиты предотвращает изменение данных?**  1. Контроль целостности  2. Сжатие данных  3. Кэширование | 1 | Верный ответ – 1 балл, неверный – 0. |
| **8. Что такое двухфакторная аутентификация?**  1. Ввод пароля дважды  2. Использование двух методов проверки личности, например, пароль и SMS-код  3. Создание двух аккаунтов | 2 | Верный ответ – 1 балл, неверный – 0. |
| **9. Как антивирусное ПО защищает данные?**  1. Оптимизирует работу системы  2. Обнаруживает и удаляет вредоносное ПО  3. Увеличивает скорость обработки | 2 | Верный ответ – 1 балл, неверный – 0. |
| **10. Что такое межсетевой экран (фаервол)?**  1. Программа для управления паролями  2. Система, блокирующая несанкционированный доступ к сети  3. Метод ускорения соединения | 2 | Верный ответ – 1 балл, неверный – 0. |
| **11. Что такое вредоносное ПО (Malware)?**  1. Программное обеспечение для резервного копирования  2. ПО, созданное для нанесения вреда системам или данным  3. Лицензионное ПО | 2 | Верный ответ – 1 балл, неверный – 0. |
| **12. Что такое фишинг?**  1. Метод обмана для получения конфиденциальных данных  2. Вирус, атакующий системы  3. Метод хеширования | 1 | Верный ответ – 1 балл, неверный – 0. |
| **13. Какой вид атаки направлен на перегрузку системы запросами?**  1. Фишинг  2. DDoS-атака (распределённый отказ в обслуживании)  3. Внедрение вирусов | 2 | Верный ответ – 1 балл, неверный – 0. |
| **14. Что такое руткит?**  1. Программа для шифрования данных  2. Вредоносное ПО, скрывающее присутствие других программ  3. Система резервного копирования | 2 | Верный ответ – 1 балл, неверный – 0. |
| **15. Что такое социальная инженерия?**  1. Метод хеширования данных  2. Манипуляция людьми для получения конфиденциальной информации  3. Оптимизация сетей | 2 | Верный ответ – 1 балл, неверный – 0. |
| **16. Каков первый шаг к защите данных?**  1. Удаление неиспользуемых программ  2. Идентификация и классификация данных  3. Архивирование всех данных | 2 | Верный ответ – 1 балл, неверный – 0. |
| **17. Что такое принцип минимальных привилегий?**  1. Выдача всем пользователям максимального доступа  2. Ограничение доступа только необходимыми правами  3. Удаление всех привилегий | 2 | Верный ответ – 1 балл, неверный – 0. |
| **18. Зачем нужна политика управления паролями?**  1. Ускорение работы системы  2. Обеспечение использования надёжных и уникальных паролей  3. Упрощение авторизации | 2 | Верный ответ – 1 балл, неверный – 0. |
| **19. Что такое GDPR?**  1. Протокол передачи данных  2. Европейский регламент защиты персональных данных  3. Система резервного копирования | 2 | Верный ответ – 1 балл, неверный – 0. |
| **20. Как часто рекомендуется обновлять программное обеспечение для защиты?**  1. Раз в год  2. Только при проблемах  3. Регулярно, чтобы устранить уязвимости | 3 | Верный ответ – 1 балл, неверный – 0. |