|  |
| --- |
| **ОПК-5.3. Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах** |
| 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-5.3.1. Применяет криптографические методы защиты информации для обеспечения целостности данных в открытых информационных системах**Знать:** − основные подходы к конструированию систем защиты информации с использованием функций хэширования, протоколов цифровой подписи (ИОПК - 5.3.1) **Уметь:** − строить современные защищённые программные комплексы с использованием средств обеспечения целостности и защищенности данных (ИОПК -5.3.1) **Владеть:** − современными международными стандартами в области криптографических алгоритмов и протоколов 31 для обеспечения целостности информации (ИОПК - 5.3.1) | **1. Что такое хеширование?**1. Сжатие данных2. Преобразование данных в уникальный фиксированный отпечаток3. Удаление информации | 2 | Верный ответ – 1 балл, неверный – 0. |
| **2. Пример хеш-функции:**1. SHA-2562. AES3. RSA | 1 | Верный ответ – 1 балл, неверный – 0. |
| **3. Основная цель хеширования:**1. Защита данных2. Обеспечение целостности данных3. Ускорение работы системы | 2 | Верный ответ – 1 балл, неверный – 0. |
| **4. Что такое коллизия хеша?**1. Утрата ключа2. Ситуация, когда две разные записи имеют одинаковый хеш3. Ошибка при шифровании | 2 | Верный ответ – 1 балл, неверный – 0. |
| **5. Преимущество цифровой подписи:**1. Увеличение скорости передачи данных2. Подтверждение подлинности и целостности информации3. Упрощение обработки | 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 «Программно-аппаратные средства защиты информации» (Б1.Б.39)** |
| ИОПК-5.3.2. Применяет программно-аппаратные комплексы защиты информации для контроля информационной безопасности в открытых информационных системах**Знать:** − программные и программно -аппаратные средства обеспечения информационной безопасности (ИОПК-5.3.2.) − особенности применения программных и программно-аппаратных средств защиты информации в открытых информационных системах (ИОПК-5.3.2.) − основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности (ИОПК-5.3.2.) **Уметь:** − изучать новые образцы программных и программно-аппаратных средств обеспечения информационной безопасности (ИОПК-5.3.2.) − проводить выбор программных и программно-аппаратных средств обеспечения информационной безопасности для обеспечения требуемого уровня защищенности открытой информационной системы (ИОПК-5. 3.2.) − конфигурировать параметры системы защиты информации в соответствии с ее эксплуатационной документацией (ИОПК -5. 3.2 .) **Владеть:** − навыками разработки архитектуры системы защиты информации открытой информационной системы (ИОПК-5. 3.2.) − навыками разработки программных и программно - аппаратных средств защиты информации открытых информационный систем (ИОПК -5. 3.2 .) − методами и средства контроля защищенности информации для различных подсистем защиты (ИОПК-5.2.1.) | **1. Что делает система IDS?**1. Оптимизирует работу сети2. Обнаруживает и уведомляет о подозрительной активности в сети3. Ускоряет передачу данных | 2 | Верный ответ – 1 балл, неверный – 0. |
| **2. Что такое DLP-система?**1. Утилита для сжатия данных2. Система предотвращения утечек конфиденциальной информации3. Антивирус | 2 | Верный ответ – 1 балл, неверный – 0. |
| **3. Пример угрозы технического канала утечки информации:**1. Устаревшее ПО2. Перехват акустических сигналов3. Дублирование данных | 2 | Верный ответ – 1 балл, неверный – 0. |
| **4. Как можно защитить устройства от кражи?**1. Использование физических замков и тросов безопасности2. Установка антивируса3. Архивация файлов | 1 | Верный ответ – 1 балл, неверный – 0. |
| **5. Что такое атака "человек посередине"?**1. Взлом резервного копирования2. Перехват данных между отправителем и получателем3. Метод сжатия | 2 | Верный ответ – 1 балл, неверный – 0. |
| **6. Какое программное средство помогает защититься от DDoS-атак?**1. Системы обнаружения и предотвращения вторжений (IDS/IPS)2. Антивирус3. Утилиты для архивирования | 1 | Верный ответ – 1 балл, неверный – 0. |
| **7. Что делает программа криптографической защиты?**1. Сжимает данные2. Шифрует и расшифровывает информацию3. Ускоряет передачу данных | 2 | Верный ответ – 1 балл, неверный – 0. |
| **8. Какие данные защищает VPN?**1. Только текстовые файлы2. Передаваемые данные через интернет, обеспечивая их конфиденциальность3. Только изображения | 2 | Верный ответ – 1 балл, неверный – 0. |
| **9. Что такое утилиты для резервного копирования?**1. Программы для сжатия файлов2. Программы для создания резервных копий данных3. Ускорители интернета | 2 | Верный ответ – 1 балл, неверный – 0. |
| **10. Какое ПО предотвращает несанкционированный доступ к компьютеру?**1. Браузер2. Программы для управления доступом и паролями3. Графический редактор | 2 | Верный ответ – 1 балл, неверный – 0. |
| **11. Что такое аппаратный фаервол?**1. Программа для сжатия файлов2. Устройство, блокирующее нежелательный сетевой трафик3. Система резервного копирования | 2 | Верный ответ – 1 балл, неверный – 0. |
| **12. Для чего используются токены безопасности?**1. Для аутентификации пользователей и хранения ключей2. Для сжатия данных3. Для доступа к интернету | 1 | Верный ответ – 1 балл, неверный – 0. |
| **13. Что такое HSM (модуль аппаратной защиты)?**1. Операционная система2. Аппаратное устройство для выполнения криптографических операций3. Программа для резервного копирования | 2 | Верный ответ – 1 балл, неверный – 0. |
| **14. Как работает биометрическая система?**1. Сканирует файлы2. Аутентифицирует пользователя по биометрическим данным: отпечатку пальца, лицу, голосу3. Ускоряет передачу данных | 2 | Верный ответ – 1 балл, неверный – 0. |
| **15. Зачем нужен TPM (модуль доверенной платформы)?**1. Для архивирования файлов2. Для безопасного хранения ключей и выполнения криптографических операций3. Для управления интернет-соединением | 2 | Верный ответ – 1 балл, неверный – 0. |
| **16. Пример использования смарт-карт:**1. Хранение сертификатов и аутентификация пользователя2. Ускорение сети3. Резервное копирование | 1 | Верный ответ – 1 балл, неверный – 0. |
| **17. Что защищает антивирусная аппаратная система?**1. Только сетевой трафик2. Все компоненты системы, включая файлы и оперативную память3. Только текстовые данные | 2 | Верный ответ – 1 балл, неверный – 0. |
| **18. Пример устройства биометрической аутентификации:**1. Клавиатура2. Сканер отпечатков пальцев3. Сетевой кабель | 2 | Верный ответ – 1 балл, неверный – 0. |
| **19. Что такое аппаратный шлюз?**1. Программа для управления данными2. Устройство, контролирующее входящий и исходящий сетевой трафик3. Хранение резервных копий | 2 | Верный ответ – 1 балл, неверный – 0. |
| **20. Какой вид устройств используется для защиты от электромагнитных перехватов?**1. Экранированные кабели и корпуса2. Биометрические системы3. Видеокарты | 1 | Верный ответ – 1 балл, неверный – 0. |