|  |  |  |  |
| --- | --- | --- | --- |
| **ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности** | | | |
| 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-10.1. Применяет криптографические алгоритмы и протоколы для обеспечения секретности и целостности информации в открытых информационных системах  **Знать:**  − исторические шифры (ИОПК -10.1)  − основные алгоритмы симметричного шифрования, функции хэширования, протоколы цифровой подписи, используемые для защиты значимой информации  (ИОПК-10.1)  **Уметь:**  − проектировать и внедрять схемы аутентификации на основе типовых стандартизированных механизмов для защиты значимой информации (ИОПК10.1)  − квалифицированно оценивать информационные риски, возникающие при использовании конкретных криптографических протоколов в защищаемой информационной системе (ИОПК -10.1) **Владеть:**  − современными международными стандартами в области криптографических средств для обеспечения защиты информации  (ИОПК -10.1)  − навыками проверки работоспособности применяемых криптографических средств защиты информации  (ИОПК-10.1) | **1. Что такое криптография?**  1. Искусство создания кода  2. Наука о защите информации путём преобразования её в зашифрованный вид  3. Процесс хранения информации | 2 | Верный ответ – 1 балл, неверный – 0. |
| **2. Для чего используется шифрование?**  1. Для удаления файлов  2. Для обеспечения конфиденциальности данных  3. Для создания резервных копий | 2 | Верный ответ – 1 балл, неверный – 0. |
| **3. Что такое криптоанализ?**  1. Создание ключей  2. Методы анализа и взлома криптографических систем  3. Хранение данных | 2 | Верный ответ – 1 балл, неверный – 0. |
| **4. Какие существуют виды криптографии?**  1. Симметричная, асимметричная, хеширование  2. Симметричная и компьютерная  3. Только асимметричная | 1 | Верный ответ – 1 балл, неверный – 0. |
| **5. Что такое ключ в криптографии?**  1. Доступ к файлам  2. Секретная информация, используемая для шифрования и расшифровки данных  3. Код программы | 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 «Программно-аппаратные средства защиты информации» (Б1.Б.39)** | | | |
| ИОПК-10.2. Применяет программно-аппаратные средства криптографической защиты информации для обеспечения секретности и целостности информации в открытых информационных системах  **Знать:**  − программно-аппаратные криптографические средства обеспечения информационной безопасности  (ИОПК-10.2.)  − особенности применения программных и программно-аппаратных криптографических средств защиты информации в открытых информационных системах  (ИОПК -10.2.)  **Уметь:**  − проводить выбор программно-аппаратных криптографических средств обеспечения информационной безопасности для обеспечения требуемого уровня защищенности открытой информационной системы (ИОПК-10.2.) **Владеть:**  − методами и средства контроля защищенности информации для различных подсистем криптографических защиты информации  (ИОПК-10.2.) | **1. Какое устройство используется для аутентификации пользователей в сети?**  1. Сканер документов  2. Смарт-карта  3. Жёсткий диск | 2 | Верный ответ – 1 балл, неверный – 0 |
| **2. Что защищает аппаратный модуль шифрования (HSM)?**  1. Текстовые документы  2. Криптографические ключи и операции  3. Пароли пользователей | 2 | Верный ответ – 1 балл, неверный – 0 |
| **3. Пример устройства для защиты доступа к серверу:**  1. Операционная система  2. Электронный ключ (токен)  3. Графическая карта | 2 | Верный ответ – 1 балл, неверный – 0 |
| **4. Для чего используют экранированные кабели?**  1. Для передачи данных  2. Для защиты от перехвата электромагнитных излучений  3. Для увеличения скорости | 2 | Верный ответ – 1 балл, неверный – 0 |
| **5. Какой принцип работы у аппаратного фаервола?**  1. Фильтрация входящего и исходящего сетевого трафика  2. Сжатие данных перед передачей  3. Хранение информации | 1 | Верный ответ – 1 балл, неверный – 0 |
| **6. Какое программное средство помогает защититься от DDoS-атак?**  1. Системы обнаружения и предотвращения вторжений (IDS/IPS)  2. Антивирус  3. Утилиты для архивирования | 1 | Верный ответ – 1 балл, неверный – 0 |
| **7. Что делает программа криптографической защиты?**  1. Сжимает данные  2. Шифрует и расшифровывает информацию  3. Ускоряет передачу данных | 2 | Верный ответ – 1 балл, неверный – 0 |
| **8. Какие данные защищает VPN?**  1. Только текстовые файлы  2. Передаваемые данные через интернет, обеспечивая их конфиденциальность  3. Только изображения | 2 | Верный ответ – 1 балл, неверный – 0 |
| **9. Что такое утилиты для резервного копирования?**  1. Программы для сжатия файлов  2. Программы для создания резервных копий данных  3. Ускорители интернета | 2 | Верный ответ – 1 балл, неверный – 0 |
| **10. Какое ПО предотвращает несанкционированный доступ к компьютеру?**  1. Браузер  2. Программы для управления доступом и паролями  3. Графический редактор | 2 | Верный ответ – 1 балл, неверный – 0 |
| **11. Что такое аппаратный фаервол?**  1. Программа для сжатия файлов  2. Устройство, блокирующее нежелательный сетевой трафик  3. Система резервного копирования | 2 | Верный ответ – 1 балл, неверный – 0 |
| **12. Для чего используются токены безопасности?**  1. Для аутентификации пользователей и хранения ключей  2. Для сжатия данных  3. Для доступа к интернету | 1 | Верный ответ – 1 балл, неверный – 0 |
| **13. Что такое HSM (модуль аппаратной защиты)?**  1. Операционная система  2. Аппаратное устройство для выполнения криптографических операций  3. Программа для резервного копирования | 2 | Верный ответ – 1 балл, неверный – 0 |
| **14. Как работает биометрическая система?**  1. Сканирует файлы  2. Аутентифицирует пользователя по биометрическим данным: отпечатку пальца, лицу, голосу  3. Ускоряет передачу данных | 2 | Верный ответ – 1 балл, неверный – 0 |
| **15. Зачем нужен TPM (модуль доверенной платформы)?**  1. Для архивирования файлов  2. Для безопасного хранения ключей и выполнения криптографических операций  3. Для управления интернет-соединением | 2 | Верный ответ – 1 балл, неверный – 0 |
| **16. Пример использования смарт-карт:**  1. Хранение сертификатов и аутентификация пользователя  2. Ускорение сети  3. Резервное копирование | 1 | Верный ответ – 1 балл, неверный – 0 |
| **17. Что защищает антивирусная аппаратная система?**  1. Только сетевой трафик  2. Все компоненты системы, включая файлы и оперативную память  3. Только текстовые данные | 2 | Верный ответ – 1 балл, неверный – 0 |
| **18. Пример устройства биометрической аутентификации:**  1. Клавиатура  2. Сканер отпечатков пальцев  3. Сетевой кабель | 2 | Верный ответ – 1 балл, неверный – 0 |
| **19. Что такое аппаратный шлюз?**  1. Программа для управления данными  2. Устройство, контролирующее входящий и исходящий сетевой трафик  3. Хранение резервных копий | 2 | Верный ответ – 1 балл, неверный – 0 |
| **20. Какой вид устройств используется для защиты от электромагнитных перехватов?**  1. Экранированные кабели и корпуса  2. Биометрические системы  3. Видеокарты | 1 | Верный ответ – 1 балл, неверный – 0 |