|  |
| --- |
| **ОПК-5.2. Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем** |
| Индикаторы, дескрипторы достижения компетенции | Комплекс заданий для оценки компетенций(сквозная нумерация) | Ключи правильных ответов | Критерии оценки |
| **Дисциплина «Защита программ и данных» (Б1.Б.38)** |
| ИОПК-5.2.2. Применяет методы защиты программ и данных при создании систем защиты информации открытых информационных систем.**Знать:** − методы и средства защиты программ и данных от разрушающих воздействий (ИОПК-5.2.2) − основные подходы к защите программ и данных от несанкционированного копирования (ИОПК-5.2.2) − принципы разработки защищенного программного обеспечения (ИОПК-5.2.2) **Уметь:** − проектировать средства защиты программ и данных в автоматизированных системах (ИОПК-5.2.2) − обеспечивать заданные требования к безопасности программного обеспечения, оценивать эффективность защиты (ИОПК-5.2.2) **Владеть:** − методами разработки безопасности программного обеспечения (ИОПК-5.2.2) | **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. |
| **Дисциплина «Программно-аппаратные средства защиты информации» (Б1.Б.39)** |
| ИОПК-5.2.1. Применяет программно-аппаратные комплексы защиты информации для обеспечения информационной безопасности в открытых информационных системах**Знать:** − программно-аппаратные средства обеспечения информационной безопасности (ИОПК-5.2.1.) − особенности применения программно-аппаратных средств защиты информации в открытых информационных системах (ИОПК-5.2.1.) **Уметь:** − изучать новые образцы программно-аппаратных средств обеспечения информационной безопасности (ИОПК-5.2.1.) − проводить выбор программно-аппаратных средств обеспечения информационной безопасности для обеспечения требуемого уровня защищенности открытой информационной системы (ИОПК-5.2.1.) − конфигурировать параметры программно -аппаратных систем защиты информации в соответствии с ее эксплуатационной документацией (ИОПК -5.2.1. ) **Владеть:** − навыками разработки архитектуры системы защиты информации открытой информационной системы (ИОПК-5.2.1.) − навыками разработки программно-аппаратных средств защиты информации открытых информационный систем (ИОПК-5.2.1.) | **1. Что такое антивирусное ПО?**1. Программное обеспечение для обнаружения и удаления вредоносного кода2. Программа для сжатия файлов3. Метод хеширования | 1 | Верный ответ – 1 балл, неверный – 0. |
| **2. Как работают антишпионские программы?**1. Сжимают данные2. Обнаруживают и удаляют шпионское ПО, следящее за пользователем3. Увеличивают скорость сети | 2 | Верный ответ – 1 балл, неверный – 0. |
| **3. Пример защиты на уровне операционной системы:**1. Физический ключ2. Брандмауэр Windows3. Видеокарта | 2 | Верный ответ – 1 балл, неверный – 0. |
| **4. Что такое шифрование данных?**1. Превращение данных в зашифрованный вид для предотвращения их прочтения2. Оптимизация структуры файлов3. Удаление лишней информации | 1 | Верный ответ – 1 балл, неверный – 0. |
| **5. Пример средств защиты от фишинга:**1. Сжатие файлов2. Блокировка подозрительных ссылок браузером3. Архивирование данных | 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. |