|  |  |  |  |
| --- | --- | --- | --- |
| **ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем** | | | |
| Индикаторы, дескрипторы достижения компетенции | Комплекс заданий для оценки компетенций  (сквозная нумерация) | Ключи правильных ответов | Критерии оценки |
| **Дисциплина «Защита информации от утечек по техническим каналам» (Б1.Б.34)** | | | |
| **ИОПК-15.1**. Проводит контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации.  ИОПК-15.2. Проводит инструментальный мониторинг защищенности открытых информационных систем и выявляет каналы утечек информации  **Знать:**  − технические и программно-аппаратные средства обеспечения информационной безопасности (ИОПК-15.1, 15.2) **Уметь:**  − конфигурировать параметры системы защиты информации и администрировать в соответствии с ее эксплуатационной документацией (ИОПК -15.1, 15.2 )  **Владеть:**  − методами и средства контроля защищенности информации для различных подсистем защиты (ИОПК-15.1, 15.2)  − методами и средствами мониторинга защищенности открытых информационных систем и выявления каналов утечки информации (ИОПК-15.2) | 1. **Что такое контроль доступа?**   1. Ограничение физического и логического доступа к информации  2. Увеличение объема памяти  3. Мониторинг пользователей | 1 | Верный ответ – 1 балл, неверный – 0. |
| **2. Что такое классификация данных?**  1. Процесс архивирования  2. Присвоение уровня важности информации  3. Удаление файлов | 2 | Верный ответ – 1 балл, неверный – 0. |
| **3.Какие сотрудники наиболее подвержены риску утечек информации?**  1. Руководители  2. Все сотрудники, имеющие доступ к конфиденциальным данным  3. Технический персонал | 2 | Верный ответ – 1 балл, неверный – 0. |
| **4. Как проверить защищённость помещений от утечек?**  1. Провести опрос сотрудников  2. Использовать средства технического контроля (анализаторы, детекторы)  3. Установить видеонаблюдение | 2 | Верный ответ – 1 балл, неверный – 0. |
| **5. Что включает политика информационной безопасности?**  1. Шифрование файлов  2. Правила, процедуры и меры для защиты данных  3. Удаление ненужной информации | 2 | Верный ответ – 1 балл, неверный – 0. |
| **6. Что относится к электромагнитным каналам утечки?**  1. Только радиоволны  2. Неразрешенное излучение от электронных устройств, токопроводящих кабелей  3. Шумы на линии связи | 2 | Верный ответ – 1 балл, неверный – 0. |
| **7. Как защититься от утечки через электромагнитное излучение?**  1. Отключить интернет  2. Экранирование помещений и оборудования  3. Установить пароль на компьютер | 2 | Верный ответ – 1 балл, неверный – 0. |
| **8. Какое оборудование используется для перехвата электромагнитных излучений?**  1. Сканеры текста  2. Антенны, радиоприемники, анализаторы спектра  3. Микрофоны | 2 | Верный ответ – 1 балл, неверный – 0. |
| **9. Что такое TEMPEST?**  1. Метод кодирования данных  2. Стандарт защиты от перехвата электромагнитного излучения  3. Алгоритм шифрования | 2 | Верный ответ – 1 балл, неверный – 0. |
| **10. Какие документы регламентируют защиту от электромагнитных излучений в России?**  1. ГОСТы и стандарты Минобороны РФ  2. Только федеральные законы  3. Постановления судов | 1 | Верный ответ – 1 балл, неверный – 0. |
| **11. Что такое акустический канал утечки информации?**  1. Передача звука через интернет  2. Утечка через звуки, издаваемые устройствами или людьми  3. Утечка через световые сигналы | 2 | Верный ответ – 1 балл, неверный – 0. |
| **12. Какие устройства используют для акустического перехвата?**  1. Микрофоны, лазерные микрофоны, диктофоны  2. Радиопередатчики  3. Анализаторы кода | 1 | Верный ответ – 1 балл, неверный – 0. |
| **13. Как защитить помещение от акустической утечки?**  1. Установить сигнализацию  2. Шумогенераторы, звукоизоляция стен и окон  3. Использовать камеры видеонаблюдения | 2 | Верный ответ – 1 балл, неверный – 0. |
| **14. Что такое виброакустический канал утечки?**  1. Передача звука по проводам  2. Передача информации через вибрации твердых тел  3. Радиоволновый перехват | 2 | Верный ответ – 1 балл, неверный – 0. |
| **15. Какие меры снижают риск виброакустической утечки?**  1. Использование интернета  2. Амортизация столов, снижение вибраций оборудования  3. Усиление сигнала связи | 2 | Верный ответ – 1 балл, неверный – 0. |
| **16. Что относится к оптическим каналам утечки?**  1. Утечка через файлы  2. Передача данных через световые сигналы или отображения на экране  3. Аудиозаписи | 2 | Верный ответ – 1 балл, неверный – 0. |
| **17. Как осуществляется перехват информации через оптические каналы?**  1. С помощью оптических приборов, камер, лазеров  2. Через радиоволны  3. Через сетевые подключения | 1 | Верный ответ – 1 балл, неверный – 0. |
| **18. Какие меры защищают от оптической утечки?**  1. Установить антивирус  2. Закрыть окна жалюзи, использовать светозащитные экраны  3. Отключить монитор | 2 | Верный ответ – 1 балл, неверный – 0. |
| **19. Что такое визуальная утечка информации?**  1. Передача данных через интернет  2. Получение информации путём наблюдения за экраном или документами  3. Снятие информации через микрофон | 2 | Верный ответ – 1 балл, неверный – 0. |
| **20. Как снизить риск визуальной утечки?**  1. Использовать экраны с защитой от обзора, избегать работы в общественных местах  2. Установить межсетевой экран  3. Включить режим энергосбережения | 2 | Верный ответ – 1 балл, неверный – 0. |
| **Дисциплина «Программно-аппаратные средства защиты информации» (Б1.Б.39)** | | | |
| ИОПК-15.1. Проводит контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации.  **Знать**:  − особенности администрирования программных и программно-аппаратных средств защиты информации в открытых информационных системах  (ИОПК - 15.1. )  **Уметь:**  − конфигурировать параметры системы защиты информации в соответствии с ее эксплуатационной документацией и проводить контрольные проверки работоспособности применяемых программно-аппаратных и криптографических средств защиты информации  (ИОПК-15.1.)  **Владеть:**  − методами и средства контроля защищенности информации для различных подсистем защиты, в том числе программно-аппаратных и криптографических (ИОПК-15.1.) | **1. Как работают системы контроля доступа?**  1. Регулируют доступ пользователей к ресурсам на основе их прав  2. Сжимают данные перед отправкой  3. Ускоряют передачу информации | 1 | Верный ответ – 1 балл, неверный – 0. |
| **2. Пример защиты приложений от SQL-инъекций:**  1. Шифрование данных  2. Использование параметризованных запросов  3. Архивирование базы данных | 2 | Верный ответ – 1 балл, неверный – 0. |
| **3. Как защитить операционную систему от вредоносного ПО?**  1. Установить дополнительные драйверы  2. Обновлять ОС и использовать антивирусные программы  3. Сжать все данные | 2 | Верный ответ – 1 балл, неверный – 0. |
| **4. Что такое шифрование на уровне базы данных?**  1. Создание резервных копий  2. Превращение данных в зашифрованный вид при хранении  3. Ускорение запросов | 2 | Верный ответ – 1 балл, неверный – 0. |
| **5. Пример программного решения для управления паролями:**  1. Менеджер паролей (LastPass, 1Password)  2. Веб-браузер  3. Система мониторинга | 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. |