|  |
| --- |
| **ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты ин-формации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем** |
| Индикаторы, дескрипторы достижения компетенции | Комплекс заданий для оценки компетенций(сквозная нумерация) | Ключи правильных ответов | Критерии оценки |
| **Дисциплина «Управление информационной безопасностью» (Б1.Б.40)** |
| ИОПК-13.1. Применяет методы анализа рисков информационной безопасности для поиска уязвимостей в открытых информационных системах**Знать:** − стандарты и нормативные документы в области организации ИБ (ИОПК-13.1.) − методы анализа информационных рисков (ИОПК13.1.) **Уметь:** − рассчитывать уровень информационных рисков (ИОПК-13.1.) − разрабатывать мероприятия по снижению уровня информационных рисков для открытых информационных систем (ИОПК-13.1.) **Владеть:** − методами идентификации и снижения рисков на предприятии (ИОПК -13.1.) | **1. Что такое инцидент информационной безопасности?**1. Событие, которое нарушает политику безопасности организации2. Необходимость обновления ПО3. Проблемы с подключением к сети | 1 | Верный ответ – 1 балл, неверный – 0. |
| **2. Какую задачу решает план реагирования на инциденты?**1. Обеспечить быстрое восстановление системы и минимизацию потерь данных2. Архивирование данных3. Программирование приложений | 1 | Верный ответ – 1 балл, неверный – 0. |
| **3. Что такое резервное копирование данных?**1. Процесс создания копий данных для восстановления в случае утраты или повреждения2. Сжатие файлов3. Мониторинг трафика | 1 | Верный ответ – 1 балл, неверный – 0. |
| **4. Как называется процесс восстановления работы после инцидента?**1. Сжатие данных2. Восстановление после сбоев3. Хранение данных в облаке | 2 | Верный ответ – 1 балл, неверный – 0. |
| 5. Какие действия предпринимаются в случае утечки персональных данных?1. Немедленно сообщить компетентным органам и принять меры для предотвращения дальнейших утечек2. Хранение копий данных3. Обновление паролей | 1 | Верный ответ – 1 балл, неверный – 0. |
| **6. Что такое управление рисками в информационной безопасности?**1. Процесс уменьшения объема данных2. Процесс оценки и минимизации угроз для информации и инфраструктуры3. Управление файлообменом | 2 | Верный ответ – 1 балл, неверный – 0. |
| **7. Какую роль играет аудит в управлении информационной безопасностью?**1. Сжатие данных2. Оценка соответствия политик безопасности и выявление уязвимостей3. Обновление программного обеспечения | 2 | Верный ответ – 1 балл, неверный – 0. |
| **8. Что такое критическая информация для организации?**1. Личные файлы сотрудников2. Информация, которая имеет наибольшее значение для функционирования организации3. Архивные данные | 2 | Верный ответ – 1 балл, неверный – 0. |
| **9. Как можно классифицировать информацию по уровню важности?**1. Только по объему данных2. На основе конфиденциальности, ценности и воздействия на организацию3. По времени хранения | 2 | Верный ответ – 1 балл, неверный – 0. |
| **10. Что такое ISO/IEC 27005?**1. Стандарт безопасности для медицинской информации2. Руководство по управлению рисками информационной безопасности3. Стандарт для аудита систем | 2 | Верный ответ – 1 балл, неверный – 0. |
| **11. Что такое криптография в контексте информационной безопасности?**1. Сжатие данных2. Метод защиты информации с использованием шифрования3. Сканирование файлов | 2 | Верный ответ – 1 балл, неверный – 0. |
| **12. Какой из этих методов используется для защиты данных на уровне приложения?**1. Установка пароля на операционную систему2. Шифрование данных в приложениях3. Защита серверного оборудования | 2 | Верный ответ – 1 балл, неверный – 0. |
| **13. Что такое доступ на основе ролей (RBAC)?**1. Метод контроля доступа, при котором пользователи получают доступ на основе их ролей2. Метод хранения данных3. Система архивации | 1 | Верный ответ – 1 балл, неверный – 0. |
| **14. Как называется процесс обеспечения целостности данных?**1. Сжатие данных2. Использование хеш-функций и цифровых подписей3. Резервное копирование | 2 | Верный ответ – 1 балл, неверный – 0. |
| **15. Что такое защита от DDoS-атак?**1. Методы защиты от перегрузки сетевых ресурсов с помощью распределенных атак2. Шифрование данных3. Аутентификация пользователей | 1 | Верный ответ – 1 балл, неверный – 0. |
| **16. Какую роль в управлении информационной безопасностью играет обучение сотрудников?**1. Обучение сотрудников правильным методам защиты информации и предотвращения атак2. Сжатие и хранение данных3. Программное обеспечение для защиты от вирусов | 1 | Верный ответ – 1 балл, неверный – 0. |
| **17. Какой стандарт безопасности данных используется в сфере платежных карт?**1. PCI DSS2. ISO/IEC 270013. GDPR | 1 | Верный ответ – 1 балл, неверный – 0. |
| **18. Какой из методов управления информационной безопасностью является наиболее важным для защиты данных при передаче?**1. Использование защищенных протоколов (например, HTTPS)2. Обновление антивируса3. Резервное копирование | 1 | Верный ответ – 1 балл, неверный – 0. |
| **19. Что такое план управления инцидентами безопасности?**1. Метод мониторинга сети2. Процесс быстрого реагирования на угрозы и инциденты безопасности3. Метод повышения производительности системы | 2 | Верный ответ – 1 балл, неверный – 0. |
| **20. Что такое непрерывность бизнеса в контексте информационной безопасности?**1. Процесс обеспечения минимальных потерь и восстановления работы при угрозах безопасности2. Программное обеспечение для управления инцидентами3. Уменьшение объемов данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **Дисциплина «Поиск уязвимостей в автоматизированных системах» (Б1.Б.41)** |
| **ИОПК-13.2.** Применяет методы пинтестинга для поиска и устранения уязвимостей систем защиты информации в открытых информационных системах**Знать:** − угрозы и уязвимости, специфичные для различных типов открытых информационных систем (ИОПК - 13.2.) − основные атаки на открытые информационные системы (ИОПК-13.2.); − каналы утечки информации (ИОПК-13.2.) **Уметь:** − выполнять поиск информации об угрозах, уязвимостях и каналах утечки информации в открытых информационных систем (ИОПК-13.2.) − проводить контрольные проверки работоспособности применяемых средств защиты информации (ИОПК-13.2.)**Владеть:** − методами поиска уязвимостей и каналов утечки информации в открытых информационных системах различных типов (ИОПК -13.2.) | **1. Что такое уязвимость в контексте информационной безопасности?**1. Проблема с производительностью системы2. Ошибки или недостатки в системе, которые могут быть использованы злоумышленниками для несанкционированного доступа или повреждения данных3. Сложность алгоритмов | 2 | Верный ответ – 1 балл, неверный – 0. |
| **2. Как называется процесс поиска уязвимостей в программном обеспечении или системе?**1. Разработка приложения2. Тестирование на проникновение (пен-тест)3. Защита данных | 2 | Верный ответ – 1 балл, неверный – 0. |
| **3. Какую цель преследует поиск уязвимостей в автоматизированных системах?**1. Выявить и устранить потенциальные угрозы безопасности до того, как они могут быть использованы злоумышленниками2. Ускорение работы системы3. Обновление программного обеспечения | 1 | Верный ответ – 1 балл, неверный – 0. |
| **4. Что такое уязвимости нулевого дня?**1. Уязвимости, которые уже были исправлены в последнем обновлении2. Уязвимости, о которых еще не известно и которые не имеют исправлений3. Уязвимости, которые требуют перезагрузки системы | 2 | Верный ответ – 1 балл, неверный – 0. |
| **5. Какие инструменты могут быть использованы для поиска уязвимостей?**1. Сканеры уязвимостей, такие как Nessus, OpenVAS, Nikto2. Резервное копирование данных3. Антивирусные программы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **6. Что такое анализ исходного кода в контексте поиска уязвимостей?**1. Процесс анализа программного кода на наличие ошибок и потенциальных уязвимостей2. Оптимизация работы системы3. Тестирование производительности | 1 | Верный ответ – 1 балл, неверный – 0. |
| **7. Что такое SQL-инъекция?**1. Метод атак на базы данных, при котором злоумышленник вставляет вредоносный код в запросы SQL2. Технология шифрования3. Утечка данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **8. Какие типы уязвимостей существуют в веб-приложениях?**1. Только проблемы с производительностью2. SQL-инъекции, XSS, CSRF, уязвимости управления сессиями3. Проблемы с хешированием | 2 | Верный ответ – 1 балл, неверный – 0. |
| **9. Какой метод защиты помогает предотвращать SQL-инъекции?**1. Использование подготовленных запросов (prepared statements)2. Архивирование данных3. Модуль шифрования | 1 | Верный ответ – 1 балл, неверный – 0. |
| **10. Какой вид тестирования обычно используется для выявления уязвимостей в веб-приложениях?**1. Пен-тест (тестирование на проникновение)2. Кросс-браузерное тестирование3. Программное тестирование | 1 | Верный ответ – 1 балл, неверный – 0. |
| **11. Что такое автоматизированное тестирование на уязвимости?**1. Использование специализированных инструментов для автоматического поиска уязвимостей в системе2. Ручное тестирование программистами3. Ускорение работы системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **12. Какой из этих методов является наиболее эффективным для обнаружения уязвимостей в операционных системах?**1. Использование систем сканирования уязвимостей, таких как Nessus2. Перезапуск операционной системы3. Оптимизация ресурсов | 1 | Верный ответ – 1 балл, неверный – 0. |
| **13. Какую уязвимость можно обнаружить с помощью анализа логов системы?**1. Проблемы с производительностью2. Неавторизованные попытки доступа и подозрительные действия3. Обновления системы | 2 | Верный ответ – 1 балл, неверный – 0. |
| **14. Что такое тестирование на проникновение?**1. Метод, при котором специалисты пытаются "взломать" систему, чтобы выявить слабые места безопасности2. Установка антивирусного ПО3. Создание резервных копий | 1 | Верный ответ – 1 балл, неверный – 0. |
| **15. Какие последствия могут возникнуть при наличии уязвимости в автоматизированной системе?**1. Неавторизованный доступ, утечка данных, повреждение системы или ее компонентов2. Ускорение работы системы3. Проблемы с хранилищем данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **16. Какую роль в поиске уязвимостей играет управление уязвимостями?**1. Позволяет систематически отслеживать, оценивать и устранять уязвимости в системах и приложениях2. Ускоряет процессы разработки3. Обновляет устаревшие версии ПО | 1 | Верный ответ – 1 балл, неверный – 0. |
| **17. Какую опасность представляет собой уязвимость, позволяющая злоумышленнику получить доступ к памяти системы?**1. Позволяет извлечь конфиденциальные данные, выполнить произвольный код или изменить работу системы2. Ускоряет работу программы3. Обновляет антивирусное ПО | 1 | Верный ответ – 1 балл, неверный – 0. |
| **18. Какие технологии могут быть использованы для предотвращения уязвимостей в программном коде?**1. Использование безопасных методов программирования и кодирования, таких как input validation и защита от переполнения буфера2. Оптимизация кода3. Использование бесплатных библиотек | 1 | Верный ответ – 1 балл, неверный – 0. |
| **19. Что такое уязвимость "неконтролируемое присвоение" (buffer overflow)?**1. Когда программа позволяет записи за пределы выделенной области памяти, что может привести к выполнению вредоносного кода2. Уязвимость в алгоритмах сжатия данных3. Проблема с правами доступа | 1 | Верный ответ – 1 балл, неверный – 0. |
| **20. Какие меры следует предпринять, чтобы защититься от уязвимостей после их выявления?**1. Обновление операционной системы2. Исправление найденных уязвимостей через патчи и обновления, улучшение политики безопасности3. Установка антивируса | 2 | Верный ответ – 1 балл, неверный – 0. |