|  |  |  |  |
| --- | --- | --- | --- |
| **ОПК-5.1. Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных 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-5.1.1. Разрабатывает и анализирует политику информационной безопасности организации (предприятия)  ИОПК-5.1.2. Разрабатывает и анализирует частные политики информационной безопасности автоматизированных систем хранения, обработки и передачи информации  **Знать:**  − стандарты и нормативные документы в области управления ИБ  (ИОПК -5.1.1, 5.1.2)  − классификацию информационных ресурсов открытых информационных систем  (ИОПК-5.1.1, 5.1.2) **Уметь:**  − идентифицировать информационные ресурсы организации (ИОПК-5.1.1, 5.1.2) **Владеть:**  − методами организации системы управления информационной безопасности на предприятии (ИОПК5.1.1, 5.1.2) | **1. Что такое информационная безопасность?**  1. Состояние защищенности информации и ее инфраструктуры от угроз  2. Метод архивации данных  3. Ускорение передачи информации | 1 | Верный ответ – 1 неверный – 0. |
| **2. Какие задачи включает в себя управление информационной безопасностью?**  1. Защита информации только в физическом формате  2. Обеспечение конфиденциальности, целостности и доступности данных  3. Создание резервных копий данных | 2 | Верный ответ – 1 неверный – 0. |
| **3. Что такое политика информационной безопасности?**  1. Система защиты от вредоносных программ  2. Набор правил и процедур для обеспечения безопасности данных в организации  3. Операционная система | 2 | Верный ответ – 1 неверный – 0. |
| **4. Кто отвечает за информационную безопасность в организации?**  1. Пользователи  2. Ответственные за безопасность сотрудники (например, CISO)  3. Только технический персонал | 2 | Верный ответ – 1 неверный – 0. |
| **5. Какой международный стандарт описывает требования к системе управления информационной безопасностью?**  1. ISO/IEC 27001  2. ISO/IEC 27001  3. PCI DSS | 2 | Верный ответ – 1 неверный – 0. |
| **6. Что такое управление рисками в информационной безопасности?**  1. Процесс уменьшения объема данных  2. Процесс оценки и минимизации угроз для информации и инфраструктуры  3. Управление файлообменом | 2 | Верный ответ – 1 неверный – 0. |
| **7. Какую роль играет аудит в управлении информационной безопасностью?**  1. Сжатие данных  2. Оценка соответствия политик безопасности и выявление уязвимостей  3. Обновление программного обеспечения | 2 | Верный ответ – 1 неверный – 0. |
| **8. Что такое критическая информация для организации?**  1. Личные файлы сотрудников  2. Информация, которая имеет наибольшее значение для функционирования организации  3. Архивные данные | 2 | Верный ответ – 1 неверный – 0. |
| **9. Как можно классифицировать информацию по уровню важности?**  1. Только по объему данных  2. На основе конфиденциальности, ценности и воздействия на организацию  3. По времени хранения | 2 | Верный ответ – 1 неверный – 0. |
| **10. Что такое ISO/IEC 27005?**  1. Стандарт безопасности для медицинской информации  2. Руководство по управлению рисками информационной безопасности  3. Стандарт для аудита систем | 2 | Верный ответ – 1 неверный – 0. |
| **11. Что такое криптография в контексте информационной безопасности?**  1. Сжатие данных  2. Метод защиты информации с использованием шифрования  3. Сканирование файлов | 2 | Верный ответ – 1 неверный – 0. |
| **12. Какой из этих методов используется для защиты данных на уровне приложения?**  1. Установка пароля на операционную систему  2. Шифрование данных в приложениях  3. Защита серверного оборудования | 2 | Верный ответ – 1 неверный – 0. |
| **13. Что такое доступ на основе ролей (RBAC)?**  1. Метод контроля доступа, при котором пользователи получают доступ на основе их ролей  2. Метод хранения данных  3. Система архивации | 1 | Верный ответ – 1 неверный – 0. |
| **14. Как называется процесс обеспечения целостности данных?**  1. Сжатие данных  2. Использование хеш-функций и цифровых подписей  3. Резервное копирование | 2 | Верный ответ – 1 неверный – 0. |
| **15. Что такое защита от DDoS-атак?**  1. Методы защиты от перегрузки сетевых ресурсов с помощью распределенных атак  2. Шифрование данных  3. Аутентификация пользователей | 1 | Верный ответ – 1 неверный – 0. |
| **16. Какую роль в управлении информационной безопасностью играет обучение сотрудников?**  1. Обучение сотрудников правильным методам защиты информации и предотвращения атак  2. Сжатие и хранение данных  3. Программное обеспечение для защиты от вирусов | 1 | Верный ответ – 1 неверный – 0. |
| **17. Какой стандарт безопасности данных используется в сфере платежных карт?**  1. PCI DSS  2. ISO/IEC 27001  3. GDPR | 1 | Верный ответ – 1 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 антивируса  3. Резервное копирование | 1 | Верный ответ – 1 неверный – 0. |
| **19. Что такое план управления инцидентами безопасности?**  1. Метод мониторинга сети  2. Процесс быстрого реагирования на угрозы и инциденты безопасности  3. Метод повышения производительности системы | 2 | Верный ответ – 1 неверный – 0. |
| **20. Что такое непрерывность бизнеса в контексте информационной безопасности?**  1. Процесс обеспечения минимальных потерь и восстановления работы при угрозах безопасности  2. Программное обеспечение для управления инцидентами  3. Уменьшение объемов данных | 1 | Верный ответ – 1 неверный – 0. |