

## Pytania egzamin dyplomowy - Informatyka dla naboru: 2022-2023

<b>PYTANIA OGÓLNE</b>
1. Funkcje - przekazywanie parametrów, zmienne lokalne oraz zwracanie wartości.
2. Pojęcie algorytmu, sposoby wyrażania oraz jego cechy.
3. Statyczne i dynamiczne struktury danych.
4. Rekurencja a rozwiązania iteracyjne.
5. Proste metody sortowania: wady i zalety.
6. Metody sortowania o logarytmicznej złożoności obliczeniowej.
7. Pojęcie złożoności obliczeniowej.
8. Drzewa binarne i ich zastosowanie w informatyce.
9. Proceduralność i modularność w programowaniu.
10. Koncepcja przekazywania parametrów w języku C.
11. Programowanie obiektowe – podstawowe mechanizmy (klasa, obiekt, konstruktor, destruktor, poziomy prywatności, interfejs).
12. Koncepcja dziedziczenia i polimorfizmu w programowaniu obiektowym.
13. Pojęcie hermetyzacji (enkapsulacji) w programowaniu obiektowym.
14. Mechanizmy obsługi wyjątków w programowaniu obiektowym.
15. Wzorce projektowe.
16. Implementacja sumatorów z przeniesieniami szeregowymi i równoległymi. Wady i zalety.
17. Koncepcja działania architektury potokowej mikroprocesorów.

18. Koncepcja działania pamięci podręcznej w systemach komputerowych.
19. Różnice pomiędzy pojęciami wskaźnika i referencji.
20. Omówić trzy fundamentalne paradygmaty programowania.
21. Różnice między zakresem widoczności i czasem życia zmiennej w językach programowania.
22. Charakterystyka architektury komunikacyjnej systemu bazy danych (1-, 2-, 3-warstwowa).
23. Zastosowanie i charakterystyka modelu ER w procesie projektowania pojęciowego modelu danych.
24. Operacje algebry relacyjnej w systemie bazy danych.
25. Normalizacja danych oraz ich charakterystyka: 0, 1, 2, 3 NF oraz BCNF.
26. Organizacja plików w systemie bazy danych (plik uporządkowany, nieuporządkowany oraz haszowy).
27. Charakterystyka „modelu kosztów” systemu bazy danych.
28. Proces transakcyjny w systemie bazy danych (realizacja sekwencyjna i współbieżna).
29. Algorytm zarządzania współbieżnym wykonywaniem transakcji (2PL).
30. Definicja telekomunikacji oraz jej klasyfikacja ze względu na rodzaj przesyłanych wiadomości.
31. Podstawowe modulacje analogowe i cyfrowe oraz ich charakterystyka.
32. Charakterystyka mediów transmisyjnych stosowanych w telekomunikacji.
33. Model warstwowy: idea, reguły, zalety, wady.
34. Protokoły bezpołączeniowe i połączeniowe oraz ich cechy charakterystyczne.
35. Przesłanki skłaniające do wyboru bezpołączeniowego protokołu z warstwy transportu TCP/IP. Jaki to protokół?
36. Definicja i własności relacji. Relacja równoważności, relacja porządku.
37. Algorytmy geometryczne i obszary ich zastosowania.
38. Diagram Voronoi i zastosowania.

39. Modele kolorów w grafice komputerowej
40. Typy świateł w grafice komputerowej
41. Reprezentacja siatek wielokątowych.
42. Charakterystyka i klasyfikacja systemów wbudowanych.
43. Mikroprocesor i mikrokontroler – charakterystyka i różnice
44. Porównanie architektur: von Neumanna i harwardzka, RISC i CISC.
45. Źródła błędów obliczeń numerycznych.
46. Stabilność algorytmu numerycznego.
47. Metody skończone rozwiązywania układu równań liniowych - istota metody eliminacji Gaussa oraz Gaussa-Jordana.
48. Istota kwadratur Newtona-Cotesa (metoda prostokątów, metoda trapezów).
49. Charakterystyka metody bisekcji rozwiązywania równania nieliniowego.
50. Charakterystyka rezystancyjnego dzielnika napięcia.
51. Klucz tranzystorowy (tranzystor w roli przełącznika).
52. Rodzaje bramek logicznych – charakterystyka.
53. Technologie internetowe przeznaczone do tworzenia stron WWW/aplikacji internetowych.
54. Animacja na stronach internetowych - technologie i ograniczenia.
55. Kluczowe różnice między responsywnym a adaptacyjnym designem stron internetowych. Jakie podejście preferujesz i dlaczego?
56. Najczęstsze zagrożenia związane z bezpieczeństwem witryn internetowych i jakie techniki można zastosować, aby zabezpieczyć aplikację webową przed atakami?

57. Techniki stosowane do poprawy dokładności i szybkości trenowania głębokich sieci neuronowych na ograniczonych zasobach sprzętowych.
58. Techniki stosowane przy wykorzystaniu sieci neuronowych do zwiększenia odporności niezbilansowanych zbiorów danych.
59. Interfejs użytkownika aplikacji mobilnych
60. Sensory i sprzęt UI wbudowane urządzenia mobilne
61. Mobilne systemy operacyjne
62. TCP – congestion avoiding system.
63. Zasada działania pamięci wirtualnej.
64. Fragmentacja pamięci: rodzaje, metody zmniejszania fragmentacji.
65. Szeregowanie procesów. Stany procesu w SO. Algorytmy szeregowania.
66. Idea wątku. Zarządzanie wątkami.
67. Idea pamięci podręcznej (cache). Korzyści i niebezpieczeństwa.
68. Dziedziczenie: mając klasę A, z której inne elementy programu mogą korzystać. W jakich przypadkach rozsądniej jest użyć mechanizmu dziedziczenia z klasy A, a w jakich wygodniej jest używać oddzielnej instancji klasy A? (zalety i wady obu metod).

### Specjalność: **Bezpieczeństwo sieci i systemów**

1. Konsekwencje wprowadzenia CIDR (ang. Classless Interdomain Routing). Jakie problemy rozwiązał ten pomysł?
2. Adresowanie IP. Adresy specjalne i ich zastosowanie.
3. Adresy prywatne IP. Ruter NAT – działanie, ograniczenia, odmiany.

4. Główne różnice między atakami typu DDoS a atakami MiTM (Man-in-the-Middle), jakie środki bezpieczeństwa można zastosować, aby się przed nimi chronić?
5. W jaki sposób kryptografia asymetryczna wspiera bezpieczeństwo w komunikacji sieciowej, i jakie są jej główne wady w porównaniu z kryptografią symetryczną?
6. Zasady działania systemu wykrywania włamań (IDS). Jakie są różnice między systemami typu HIDS (Host-based IDS) a NIDS (Network-based IDS), i które są bardziej efektywne w specyficznych scenariuszach?
7. Dostępne techniki sterowania informacją w sieciach komputerowych.
8. Przedstaw przykłady architektur oraz zagrożeń sieci komputerowych.
9. Wirtualizacja w kontekście zarządzania infrastrukturą IT.
10. Mechanizmy zabezpieczeń stosowane w maszynach wirtualnych w celu ochrony przed cyberatakami.
11. Omówić zagrożenia związane z otwartym/ zamkniętym kodem źródłowym (open source/ closed source).
12. Wyjaśnij, jak dostępne jest narzędzie open source do monitorowania i analizy bezpieczeństwa sieci. Podaj przykłady takich narzędzi i opisz ich podstawowe funkcje.
13. Omówić istotę tworzenia bezpiecznych systemów komputerowych.
14. Ataki typu „zero-day” detekcja i ochrona.
15. Metody monitorowania zagrożeń cyberprzestrzeni.
16. Narzędzia i techniki wykrywania anomalii w ruchu sieciowym.
17. Wyjaśnij, jak współczesne systemy cyberinteligencji (CTI) wspierają procesy monitorowania i prognozowania zagrożeń w cyberprzestrzeni. Jakie źródła informacji oraz formaty wymiany danych są najczęściej stosowane?
18. Opis najważniejszych zasad ochrony bezpiecznych sieci komputerowych. Jakie techniki i rozwiązania zdrowotne muszą być przestrzegane, aby chronić przed zagrożeniami?
19. Jakie są różnice między siecią o architekturze uruchomionej w sieci zaprojektowanej w modelu „zero trust”? Jakie wyzwania i korzyści wynikają z zastosowania modelu „zero trust” w zabezpieczeniu sieci?

20. Zarządzanie ryzykiem w kontekście bezpieczeństwa sieci komputerowych.
21. Zagrożenia sieci bezprzewodowej oraz metody ich zabezpieczenia.
22. Wyjaśnij, jakie są główne różnice pomiędzy standardami sieci bezprzewodowych (np. 802.11n, 802.11ac, 802.11ax).
23. Scharakteryzować strukturę organizacyjną Krajowego Systemu Cyberbezpieczeństwa w Polsce.
24. Wyjaśnij główne cele i funkcje Krajowego Systemu Cyberbezpieczeństwa.
25. Wskaż różnice pomiędzy szyfrowaniem symetrycznym i asymetrycznym.
26. Jaką funkcję pełni skrót kryptograficzny?
27. Omów podstawowe techniki zabezpieczające sieć komputerową przed nieautoryzowanym dostępem.
28. Przedstaw rozwiązania sprzętowe i programowe najczęściej stosowane w celu ochrony sieci.
29. Wyjaśnij znaczenie kryptografii w zabezpieczaniu sieci komputerowej - protokoły kryptograficzne.
30. Omów wybrane techniki oceny zagrożeń oraz przedstaw ich zastosowanie praktyczne w procesie podejmowania decyzji.
31. Narzędzia sztucznej inteligencji (AI) i uczenia maszynowego (ML) w procesie zarządzania bezpieczeństwem systemów teleinformatycznych.
32. Metodyki i etapy zarządzania projektem inżynierskim.
33. Przedstaw zagrożenia związane z zarządzaniem teleinformatycznym projektem inżynierskim.

### **Specjalność: Grafika i przetwarzanie danych**

1. Architektura i interfejs użytkownika aplikacji mobilnych.
2. Architektura silnika gier komputerowych.
3. Algorytmy renderingu scen 3d.

4. Metody animacji komputerowej.
5. Modele oświetlenia w grafice 3d.
6. Algorytmy cieniowania powierzchni.
7. Zasady projektowania graficznego interfejsu użytkownika.
8. Metody testowania graficznego interfejsu użytkownika.
9. Charakterystyka wybranego języka programów cieniowania.
10. Interpolacja liniowa, algorytm, zastosowanie w programach cieniowania, funkcje realizujące.
11. Algorytm ray marching w renderingu 3D.
12. Rola detekcji i rozwiązywania kolizji w grach komputerowych.
13. Rodzaje zawartości (assetów) w tworzeniu gier komputerowych.
14. Rodzaje zawartości graficznej (assetów) w tworzeniu grafiki dla gier komputerowych
15. Projektowanie grafiki dla gier 2D a 3D.
16. Rola oświetlenia w grach 3D.
17. Metody najskuteczniejsze w automatyzacji procesu optymalizacji hiperparametrów mające wpływ na wydajność modeli uczenia maszynowego.
18. Techniki stosowane do poprawy dokładności i szybkości trenowania głębokich sieci neuronowych na ograniczonych zasobach sprzętowych.
19. Techniki stosowane w wykorzystaniu sieci neuronowych do zwiększenia odporności niezbilansowanych zbiorów danych.
20. Podejścia najbardziej efektywne w wykrywaniu i redukowaniu uprzedzeń w algorytmach klasyfikacyjnych do wyjaśnialności modeli uczenia maszynowego.
21. Ile czasu (w przybliżeniu) zajmuje wczytanie obrazu 1920 x 1080 pikseli (Full HD) zapisanego na HD do pamięci RAM? Proszę porównać ten czas z czasem odświeżania ekranu monitora opisanym jako 60Hz.

22. Metody rejestracji zjawisk szybkozmiennych.
23. Różnice w zastosowaniu układu scalonego FPGA a układu typu ASIC.
24. Omówić proces projektowania układu kombinacyjnego.
25. Omówić proces tworzenia systemów ochronnych w kontekście bezpieczeństwa w sieciach komputerowych.
26. Identyfikacja wymagań dla stworzenia dobrego projektu systemu informatycznego.
27. Projektowanie systemów z uwzględnieniem ochrony danych i zgodności z udostępnieniem prywatności (np. RODO).
28. Integralność systemu i informacji.
29. Wymagania bezpieczeństwa dotyczące systemów informatycznych wykorzystywanych do przetwarzania danych.
30. Korzyści z tworzenia aplikacji bazodanowej.
31. Jak aplikacje baz danych zwiększają użyteczność baz danych?
32. Przedstaw metody uwierzytelniania i szyfrowania baz danych.

Zatwierdzony przez Radę Programową: 27.11.2024 r.