„ZATWIERDZAM"
DZIEKAN WYDZIAŁU CYBERNETYKI

dr hab. inż. Zbigniew Tarapata, prof. WAT
Warszawa, ……

Zagadnienia pomocnicze na egzamin dyplomowy dla studentów studiów I st. na kierunku Kryptologia i cyberbezpieczeństwo specjalność Cyberobrona

Teoria informacji i kodowania

1. Omówić metodę kodowania arytmetycznego.
2. Omówić metodę kodowania słownikowego.
3. Scharakteryzować standard kodowania UNICODE.

Sieci komputerowe II

4. Sklasyfikować i scharakteryzować poznane protokoły routingu dynamicznego.
5. Omówić algorytmy aktualizacji tras wykorzystywane w protokołach stanu łącza i protokołach dystans-wektor.

Zabezpieczenia teleinformatyczne

6. Scharakteryzować zapory sieciowe nowej generacji na tle tradycyjnych zapór stanowych.
7. Omówić przeznaczenie i zasady funkcjonowania systemów klasy SIEM.

Zarządzanie środowiskiem Windows

8. Omówić strukturę logiczną i fizyczną Active Directory.
9. Wskazać różnice i podobieństwa pomiędzy systemami z rodziny Microsoft Windows, a systemami Microsoft Windows Server.

Podstawy bezpieczeństwa informacji

10. Omówić pojęcia "zagrożenie", "podatność", "incydent".
11. Wyjaśnić pojęcie "klasa bezpieczeństwa" w odniesieniu do sterowania dostępem do informacji.

Architektura i Organizacja Komputerów

12. Pojęcie architektury i organizacji komputerów.
13. Sterowanie centralne procesora, cykl rozkazowy.
14. Arytmetyka w kodzie U2, MZ, IEEE 754.

Interfejsy komputerów cyfrowych

15. Model modułu wejścia-wyjścia, model urządzenia zewnętrznego, pojęcie interfejsu.
16. Transmisja szeregowa, równoległa, synchroniczna, asynchroniczna, izochroniczna - cechy, przykłady standardów.

Systemy operacyjne

17. Mechanizmy komunikacji procesów, koordynacja procesów i wątków w systemach operacyjnych.
18. Techniki zarządzania podstawowymi zasobami sprzętowymi komputera w systemach operacyjnych.

Bezpieczeństwo pracy i ergonomia

19. Ergonomia stanowisk komputerowych.
20. Wymagania ergonomiczne na stanowiskach z monitorem ekranowym europejskie.
21. Zagrożenia zdrowotne podczas pracy na stanowiskach z monitorem ekranowym.

Technologie JavaEE/JavaEE Technologies

22. Scharakteryzować technologię Enterprise JavaBeans.
23. Co to jest serwlet? Omówić cykl życia serwletu.

Bezpieczeństwo sieci komputerowych

24. Omówić dowolny rodzaj ataku sieciowego. Podać szczegóły techniczne jego realizacji, zakładane rezultaty oraz przykład przeciwdziałania temu atakowi.
25. Czym różnią się systemy IDS od systemów IPS?

Technologie projektowania systemów teleinformatycznych

26. Wskaż różnice między wybranymi dwoma paradygmatami modelowania systemów.
27. Określ techniki modelowania (diagramy) za pomocą których właściwie opiszesz wybrany wycinek rzeczywistości wynikający z pracy dyplomowej - w aspekcie systemowym, lub/i biznesowym.

Projekt zespołowy

28. Wiedząc, że realizujesz proces gromadzenia wymagań, określ jak przeprowadzisz go zgodnie z metodyką RUP, a jak zwinnie.
29. Jako PM bierzesz udział w rekrutacji nowego pracownika do zespołu, określ jakimi kryteriami będziesz się kierował przy jego wyborze (uzasadnij ten wybór).

Sieci komputerowe

30. Warstwowe modele sieci. Właściwości i zadania realizowane w poszczególnych warstwach. Protokoły sieciowe. Kapsułkowanie.
31. Urządzenia i media sieciowe. Właściwości i zastosowania. Zadania urządzeń sieciowych. Kolizje, domeny kolizyjne i rozgłoszeniowe.
32. Usługi w sieciach komputerowych. Własności i przeznaczenie najczęściej używanych usług/protokołów: DNS, ftp, telnet, ssh, http, snmp, smtp, DHCP, NAT itp.

Systemy operacyjne UNIX

33. Własności systemów z rodziny UNIX. Wielozadaniowość, wieloużytkownikowość. Prawa dostępu. Sterowanie procesami z poziomu shell'a. Budowa systemu plików.
34. Zarządzanie zasobami systemu: konta użytkowników, procesy, zasoby pamięci masowej, archiwizacja, usługi sieciowe.

Eksploracja sieci teleinformatycznych

35. Omówić fazę rekonesansu podczas testu penetracyjnego.
36. Czym jest i jak działa skaner podatności?

Systemy wbudowane

37. Omówić wymianę danych w systemach wielo-mikrokomputerowych.
38. Porównać system przerwań mikrokontrolerów z rodzin MCS'51 i ARM.
39. Omówić obsługę wewnętrznej pamięci RAM adresowanej bitowo i bajtowo.

Podstawy techniki komputerów

40. Omówić rodzaje diod półprzewodnikowych.
41. Omówić podział i zasadę działania przerzutników. Podać symbole i tablice przejść.
42. Omówić realizację wybranych funktorów logicznych w technologiach DTL, RTL, CMOS i TTL.

Podstawy przetwarzania rozproszonego

43. Omówić wymianę danych przy wykorzystaniu mechanizmu gniazd połączeniowych i bezpołączeniowych.
44. Omówić wymianę danych przy wykorzystaniu mechanizmu XML-RPC.
45. Omówić wymianę danych przy wykorzystaniu mechanizmu REST.

HTML i aplikacje webowe

46. Jaką rolę pełni dyrektywa Page?
47. Omówić sposób modyfikacji właściwości kontrolek.

Podstawy podzespołów komputerów

48. Podać różnicę pomiędzy układem kombinacyjnym w sekwencyjnym.
49. Dokonać minimalizacji podanego wyrażenia Boolowskiego za pomocą wskazanej metody.

Programowanie niskopoziomowe i analiza kodu

50. Architektura x86 i x64 (referencyjne w 2022 r.: IA-32 i Intel® 64).
51. Organizacja pamięci i współpracy programów użytkownika z systemem Windows.
52. Narzędzia analizy statycznej i dynamicznej.

Ataki sieciowe

53. Podatności i ich wykorzystywanie: CVE i jego utrzymywanie, Mitre ATT&CK
54. Narzędzia ataków i testów penetracyjnych (referencyjny w 2022 r.: Kali Linux, Metasploit)
55. Scharakteryzować wskazane przez komisję narzędzie ataku lub testu penetracyjnego.

Oprogramowanie niepożądane i inspekcja kodu

56. Narzędzia zdalnego sterowania RAT (referencyjne w 2022 r.: Meretpreter).
57. Pożądane właściwości malaware, klasyfikacja i zastosowanie malware.
58. Zaproponować cyberatak APT i wskazać odpowiednie oprogramowanie (RAT lub autonomiczne).
59. Zaproponować wykrywanie nowego, nieznanego malware bez użycia "antywirusów".

Dyrektor
Instytutu Teleinformatyki i Cyberbezpieczeństwa
Wydział Cybernetyki
dr inż. Tomasz Malinowski, prof. WAT
Warszawa, ……