„ZATWIERDZAM"
DZIEKAN WYDZIAŁU CYBERNETYKI

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

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

Ataki sieciowe i złośliwe oprogramowanie

1. Podatności i ich wykorzystywanie: CVE i jego utrzymywanie, Mitre ATT&CK.
2. Narzędzia ataków i testów penetracyjnych (referencyjny w 2022 r.: Kali Linux, Metasploit).
3. Pożądane właściwości malware, klasyfikacja i zastosowanie malware.

Technologie Internetu rzeczy

4. Scharakteryzować podstawowe technologie warunkujące rozwój zastosowań Internetu
1. rzeczy.
5. Scharakteryzować zagrożenia dla bezpieczeństwa systemów Internetu rzeczy i omówić techniki zwiększania bezpieczeństwa urządzeń Internetu rzeczy.
6. Scharakteryzować warstwową architekturę Internetu rzeczy i znane standardy architektury.

Diagnostyka i tolerowanie uszkodzeń

7. Techniki osiągania niezawodności, miary niezawodności, niezdatności, błędy, awarie i ich manifestacja, klasyfikacja niezdatności.
8. Scharakteryzować techniki tolerowania uszkodzeń w systemach rozproszonych.
9. Omówić istotę metod diagnostyki systemowej i możliwości zastosowania w systemach komputerowych.

Zarządzanie bezpieczeństwem informacji

10. Wyjaśnić związki pomiędzy zagrożeniami, sposobami realizacji zagrożenia, podatnościami i incydentem.
11. Wyjaśnić różnice pomiędzy ilościową i jakościową analizą ryzyka.
12. Audyt informatyczny - podać definicję i zawartość raportu poaudytowego

Zarządzanie sieciami teleinformatycznymi

13. Omówić techniki SPAN pozyskiwania informacji o ruchu sieciowym.
14. Omówić modele IntServ i DiffServ systemów QoS.
15. Wymienić i krótko scharakteryzować znane metody zarządzania dostępną przepustowością, zatorami i kolejkowaniem pakietów w systemach.
16. Porównać techniki przełączania pakietów w oparciu o adresy IP i etykiety w sieci MPLS.

Ergonomia systemów interaktywnych

17. Testy i charakterystyki oceny jakości działania użytkownika. Standard ISO-9241.
18. Wymagania ergonomiczne na interfejs użytkownika w systemach interaktywnych. Model działania użytkownika.
19. Zasady projektowania interakcji i ocena jakości użytkowej interfejsu użytkownika aplikacji.

Trends in Computer Technology

20. Zastosowanie PCI-Express we współczesnym systemie komputerowym.
21. Wskazać podstawowe różnice w architekturze procesorów x86-64 i ARM.
22. W jaki sposób i dlaczego można wykorzystać GPU do realizacji obliczeń macierzowych.
23. Jak wygląda komunikacja CPU-RAM we współczesnym komputerze PC.

Wirtualizacja systemów IT

24. Co rozumiemy pod pojęciem sprzętowego wsparcia dla wirtualizacji.
25. Co oznaczają pojęcia: wirtualizacja natywna, wirtualizacja gościnna.
26. Wymienić i określić zastosowanie podstawowych modeli chmury obliczeniowej.

Modelowanie systemów teleinformatycznych

27. Wyjaśnić pojęcia: weryfikacja, walidacja, symulacja i testowanie.
28. Scharakteryzować klasyczną sieć Petriego. Jak rozumiany jest stan tej sieci?
29. Wyjaśnić znaczenie koloru w kolorowanych sieciach Petriego. Omówić jego zastosowanie na wybranym przykładzie.
30. Wymienić podstawowe operatory stosowane w logice temporalnej. Scharakteryzować jeden z nich.

Walka w cyberprzestrzeni

31. Jakie ograniczenia wprowadzono w Internecie w związku z wojną? Jakimi metodami? Na czym one polegają? Jak je można ominąć?
32. Porównać możliwości cyberataku na system sterowania koleją (np. incydent z początku 2022 z hipotezą ataku) i na drona bojowego.
33. Co to jest„fake news"? Czy interpretacja tego pojęcia zmienia się, gdy jest używane w walce informacyjnej?

Studium ataków i incydentów

34. Przedstawić etapy współczesnego ataku ransomware na wielkie firmy (np. incydent Colonial Pipeline).
35. Przedstawić„atak na łańcuch dostaw". Na czym polegają incydenty„ataków na usługi zarządzane"?
36. Co to jest„atak u wodopoju"? Do czego służą „„exploit packs" w takich atakach?

Projektowanie systemów bezpieczeństwa informacji

37. Przedstawić przedmiot każdej z norm PN ISO/IEC 27001 i PN ISO/IEC 27001?
38. Wymienić istotne dokumenty projektu systemu bezpieczeństwa informacji.
39. Zaproponować skład zespołu projektowego (role) dokonującego modernizacji systemu bezpieczeństwa pewnej firmy/organizacji.