Uchwała Kolegium Wydziału Informatyki i Telekomunikacji
z dnia 31.03.2021r.
nr 40/2021
w sprawie zatwierdzenia zagadnień na egzamin dyplomowy na kierunku *Informatyka*, studia II stopnia, specjalność *Cyberbezpieczeństwo*.

Na podstawie § 35 ust.10 Statutu Politechniki Krakowskiej z dnia 01.02.2021 r. Kolegium Wydziału Informatyki i Telekomunikacji postanawia co następuje:

§ 1

Pozytywnie opiniuje się zagadnienia na egzamin dyplomowy na kierunku *Informatyka*, studia II stopnia, specjalność *Cyberbezpieczeństwo*.

§ 2

Szczegółowe zagadnienia na w/w egzamin zostały zawarte w załączniku do tej uchwały.

§ 3

Uchwała wchodzi w życie z dniem podjęcia.

Obowiązują od 31 marca 2021 roku

Studia II stopnia
Kierunek: Informatyka
specjalność: Cyberbezpieczeństwo

Zagadnienia na egzamin magisterski

1. Mechanizm wstrzykiwania zależności oraz rola i podstawowa funkcjonalność kontenera IoC.

2. Koncepcja rozwoju oprogramowania sterowanego testami (TDD).

3. Wzorzec architektury Business Delegate, obszar zastosowań.

4. Model dojrzałości usług sieciowych (usług RESTful) wg. Richardsona.

5. Czym są funkcje kształtu?

6. Co to jest sformułowanie wariacyjne?

7. Co to jest macierz sztywności?

8. Jak wykonujemy całkowanie w metodzie elementów skończonych?

9. Twierdzenie Lagrange'a dla grup skończonych. Warstwy.

10. Rozszerzony algorytm Euklidesa.

11. Logarytmy dyskretne -- podstawowe własności.

12. Elementy algebraiczne i transcendentne. Wielomian minimalny elementu algebraicznego nad ciałem.

13. Omów doktrynę cyberbezpieczeństwa RP - przedstaw przyjęte definicje.

14. Zdefiniuj pojęcie złośliwego oprogramowania. Przedstaw taksonomię złośliwego oprogramowania. Scharakteryzuj trzy wybrane zagrożenia.

15. Przedstaw ideę ataków typu DoS i krótko scharakteryzuj ich rodzaje.

16. Wymień i omów siedem zasad RODO.

17. Zdefiniuj pojęcie podatności aplikacji internetowej na ataki, podaj przykłady luk i uzasadnij dlaczego aplikacje internetowe są podatne na ataki.

18. Zdefiniuj pojęcie exploit i payload w kontekście ataków na aplikacje internetowe, podaj przykłady narzędzi do tworzenia exploitów oraz wykrywania podatności w aplikacjach internetowych.

19. Zdefiniuj atak Cross-Site Scripting na aplikację internetową, podaj typy ataków XSS oraz przykłady kontekstów ataków i metod obrony przed nimi.

20. Zdefiniuj atak SQL Injection, podaj typy ataków SQL Injection na aplikacje internetowe, ich skutki i metody obrony przed nimi.

21. Scharakteryzuj trzy techniki ataków stosowanych w sieciach komputerowych.

22. Zdefiniuj pojęcie "socjotechnika". W jaki sposób socjotechnika jest wykorzystywana w sieciach komputerowych?

23. Zdefiniuj pojęcia: Phishing, Spam, Trojan.

24. Omów mechanizmy zabezpieczeń stosowane w sieciach bezprzewodowych Wi-Fi.

25. Omów miary bezpieczeństwa systemu komputerowego.

26. Omów jedno z narzędzi modelowania zagrożeń systemów komputerowych.

27. Omów model FAIR pozwalający na szacowanie ryzyka zagrożenia bezpieczeństwa systemu komputerowego.

28. Omów rolę bibliotek ataków na systemy komputerowe w procesie zapewniania ich bezpieczeństwa.

29. Omów znane Ci metodyki realizacji przedsięwzięcia projektowego. Porównaj wybrane metodyki: tradycyjną i zwinną.

30. Wskaż rodzaje projektów informatycznych. Wymień oraz scharakteryzuj metody estymacji kosztu wybranego przedsięwzięcia projektowego.

31. Wskaż fazy realizacji projektu informatycznego wytwórczego i wdrożeniowego. Wymień i omów metody śledzenia postępu projektu w czasie.

32. Omów sposoby tworzenia struktury zadań w projekcie. Co to jest ścieżka krytyczna? Podaj co najmniej dwie metody wyznaczania ścieżki krytycznej w projekcie informatycznym.

33. Charakterystyka systemów rozproszonych - zalety i wady.

34. Modele programowania równoległego.

35. Miary efektywności obliczeń równoległych.

36. Środowiska programowania równoległego.

37. Opisz metody analizy ruchu sieciowego w sieci E10.

38. Porównaj zastosowanie SPAN i RSPAN w monitorowaniu sieci pakietowej.

39. Krótko przedstaw metody oraz zastosowanie analizy przepływów w sieciach pakietowych w kontekście monitorowania ruchu.

40. Krótko scharakteryzuj NetFlow i przedstaw jego zastosowanie w monitorowaniu ruchu w sieci pakietowej

41. Szyfry podstawieniowe (proste i wieloalfabetowe).

42. Tajność doskonała. Twierdzenie Shannona.

43. Problem pakowania plecaka. Szyfry plecakowe.

44. Algorytmy asymetryczne. Szyfr RSA.

45. Opisz trzy zagrożenia dotyczące aplikacji mobilnych według projektu OWASP.

46. W jaki sposób systemy mobilne (Android, iOS) zabezpieczają dane przed dostępem nieautoryzowanych aplikacji?

47. W jaki sposób systemy mobilne zabezpieczają użytkownika przed dostępem aplikacji do funkcji takich jak kamera, wykonywanie/ odbieranie połączeń, bluetooth, położenie?

48. W jaki sposób programista powinien chronić wrażliwe dane użytkowników aplikacji mobilnych?

49. Omów model Purdue Enterprise Reference Architecture.

50. Omów kategorie działań cyberbezpieczeństwa (Sliding Scale of Cybersecurity).

51. Omów Aktywny Cykl Działań Cyberbezpieczeństwa i zalety jego stosowania w środowiskach przemysłowych.

52. Proszę omówić Przemysłowy Cyber Kill Chain.

53. Wyjaśnij na czym polega strategia budowania pozycji firmy na rynkach krajowych i zagranicznych w oparciu o fuzje, przejęcia, alianse strategiczne.

54. Wymień i opisz podstawowe metody wykorzystywane w analizie strategicznej makrootoczenia, otoczenia branżowego firmy.

55. Przedstaw zestaw celów i mierników dla wybranej strategii (wzrostu/ stabilizacji/redukcji).

56. Wyjaśnij pojęcie model biznesu, scharakteryzuj składowe modelu biznesu.