Cyberbezpieczeństwo (II stopień) – zagadnienia na egzamin dyplomowy obowiązujące od r.a. 2024/2025

1. Analiza informacji i jej zastosowanie w cyberbezpieczeństwie.
2. Algorytmy wykorzystywane w analizach Big Data.
3. Wady i zalety stosowania tablic z biblioteki NumPy względem list z Pythona.
4. Metody szacowania ryzyka występowania cyberzagrożeń.
5. Autoryzacja i uwierzytelnianie w systemach IT.
6. Klasy problemów decyzyjnych w systemach informatycznych.
7. Istota i zasady analizy systemowej.
8. Najpopularniejsze systemy baz danych.
9. Zagrożenia wynikające z pracy w chmurze.
10. Rola i zadania kluczowych instytucji odpowiedzialnych za cyberbezpieczeństwo w Polsce. Kompetencje i ich znaczenie w kontekście ochrony infrastruktury krytycznej.
11. Podstawowe płaszczyzny bezpieczeństwa państwa i ich ważność w kontekście zagrożeń hybrydowych (przykłady).
12. Proces zbierania dowodów cyfrowych. Dokumentowanie i zabezpieczanie dowodów (przykłady).
13. Rola internetu jako źródła danych i dowodów dla śledczego.
14. Wykorzystanie rozkładów statystycznych (np. normalnego, Poissona) w analizie cyberbezpieczeństwa do identyfikacji nietypowych zachowań lub anomalii w ruchu sieciowym i zbiorach danych.
15. Zastosowanie Prawa Benforda do wykrywania nieprawidłowości i anomalii w danych cyfrowych, np. w danych finansowych.
16. Rodzaje danych chronionych przez RODO.
17. Różnice pomiędzy mechanizmem szyfrowania symetrycznym i asymetrycznym.
18. Biały, szary oraz czarny wywiad w kontekście OSINT. Główne narzędzia oraz źródła informacji wykorzystywane w każdym rodzaju wywiadu.
19. Najczęściej stosowane narzędzia do zbierania informacji z otwartych źródeł.
20. Koncepcja społeczeństwa ryzyka i jego przyczyny.
21. Główne ryzyka i zagrożenia stojące przed współczesnymi państwami.
22. Wybrane organizacje lub instytucje zajmujące się bezpieczeństwem teleinformatycznym.
23. Cyberbezpieczeństwo – podstawowe pojęcia z zakresu bezpieczeństwa informacji.
24. Cechy programowania obiektowego.

25. Narzędzia do wyszukiwania i zamiany złożonych wzorców językowych w tekście.
26. Zadania ENISA w kształtowaniu i wdrażaniu unijnej polityki cyberbezpieczeństwa.
27. Główne cele dyrektywy NIS2, rozszerzenia zakresu regulacji względem poprzednich przepisów (dyrektywy NIS).
28. Niegeneratywne modele językowe do pozyskiwania informacji z tekstów (przykłady).
29. Proces uczenia maszynowego. Niezbędne elementy do przeprowadzenia procesu uczenia maszynowego.
30. Istota propagandy i jej techniki.
31. Istota i rodzaje dezinformacji z perspektywy czasu osiągnięcia zamierzonego celu.
32. Różnice między hackerami typu White Hat, Black Hat oraz Grey Hat. Typowe motywacje oraz metody działania dla każdej z tych grup.
33. Etapy testu penetracyjnego (Penetration Testing) i ich znaczenie w kontekście zapewnienia bezpieczeństwa systemów informatycznych.
34. Rodzaje baz danych. Najważniejsze właściwości poszczególnych rodzajów baz danych.
35. Struktura i cechy relacyjnego modelu bazy danych. Zastosowanie języka SQL do przetwarzania i zarządzania danymi w systemach bazodanowych.
36. Wpływ technologii blockchain na funkcjonowanie i rozwój metawersów (np. w zakresie bezpieczeństwa, własności cyfrowej i identyfikacji użytkowników).
37. Wykorzystanie tokenów (NFT, kryptowaluty) w metawersach do transakcji, weryfikacji aktywów cyfrowych i budowania gospodarki wirtualnej oraz związane z tym zagrożenia dla cyberbezpieczeństwa.
38. Problematyka podatności IoT na zagrożenia cyberbezpieczeństwa (przykłady).
39. Zagrożenia związane z wdrażaniem nowych usług sieciowych opartych o urządzenia IoT oraz metody minimalizujące wystąpienie przedmiotowych zagrożeń.
40. Wartość użytkowa informacji w ograniczaniu niepewności decyzji i zwiększaniu przewagi konkurencyjnej organizacji na rynku.