UNIWERSYTET VIZJA

Zestaw pytań kierunkowych na egzamin dyplomowy na studiach pierwszego stopnia

Kierunek studiów: Cyberbezpieczeństwo

Na egzaminie dyplomowym losowane są **dwa pytania z niniejszego zestawu**.

1. System polityczny – istota, komponenty, funkcje.
2. Wymień formy państw i omów wybrane z nich.
3. Scharakteryzuj i wskaż na różnice pomiędzy państwem demokratycznym a autorytarnym.
4. Na czym polega zarządzanie bezpieczeństwem informacji zgodnie z normą ISO 27001?
5. Jakie są podstawowe techniki ochrony informacji w sieciach teleinformatycznych?
6. Czym jest audyt bezpieczeństwa sieci i jakie są jego etapy?
7. Jakie wyzwania wiążą się z ochroną danych osobowych w kontekście Internetu rzeczy (IoT)?
8. Jakie są konsekwencje błędów ludzkich w zarządzaniu bezpieczeństwem informacji?
9. Czym różni się bezpieczeństwo informacyjne od bezpieczeństwa informacji?
10. Przedstaw typologie cyberprzestępstw i ich techniczne uwarunkowania.
11. Jakie są najważniejsze wyzwania dla cyberbezpieczeństwa w administracji rządowej?
12. Czym jest OSINT i jakie ma zastosowania w praktyce wywiadowczej?
13. Wyjaśnij rolę dezinformacji w społeczeństwie sieciowym.
14. Jakie są przykłady naruszeń ochrony własności intelektualnej w cyberprzestrzeni?
15. Jakie są techniki anonimizacji w sieci i ich znaczenie dla ochrony prywatności?
16. Omów główne zagrożenia cybernetyczne dla infrastruktury krytycznej.
17. Wyjaśnij pojęcie wojny informacyjnej i jej znaczenie dla współczesnych konfliktów.

UNIWERSYTET VIZJA

18. Czym jest cyberterroryzm i w jaki sposób różni się od tradycyjnych form terroryzmu?
19. Jakie znaczenie ma pojęcie „społeczeństwa sieciowego” dla bezpieczeństwa informacyjnego?
20. Jakie są społeczne skutki wojny informacyjnej i propagandy?
21. Scharakteryzuj metody zarządzania kryzysowego w sektorze publicznym.
22. Na czym polega zastosowanie strategii StratCom w sytuacjach kryzysowych?
23. Przedstaw zasady funkcjonowania krajowego systemu cyberbezpieczeństwa.
24. W jaki sposób realizować audyt wewnętrzny systemu zarządzania bezpieczeństwem informacji?
25. Jakie są najważniejsze techniki eksploracji danych w Internecie?
26. Jakie są funkcje i możliwości wykorzystania systemów informacji przestrzennej (GIS) w bezpieczeństwie?
27. Proszę przedstawić i omówić warstwy modelu OSI lub TCP/IP w kontekście bezpieczeństwa sieciowego.
28. Proszę wyjaśnić działanie wybranych protokołów bezpieczeństwa (np. TLS/SSL, IPsec).
29. Proszę omówić systemy detekcji i zapobiegania intruzjom (IDS/IPS). Jakie są różnice między nimi?
30. Proszę omówić kluczowe regulacje prawne dotyczące cyberbezpieczeństwa w Polsce.
31. Proszę omówić kluczowe regulacje prawne dotyczące cyberbezpieczeństwa w Unii Europejskiej.
32. Proszę omówić znaczenie ciągłości działania i planowania awaryjnego w kontekście cyberbezpieczeństwa.
33. Na czym polega zarządzanie incydentami bezpieczeństwa? Proszę przedstawić etapy reakcji na incydent.
34. Czym różni się audyt bezpieczeństwa od testów penetracyjnych?
35. Jakie są podstawowe różnice między red team, blue team i purple team?
36. Jakie są wyzwania cyberbezpieczeństwa w kontekście AI i deepfake’ów?
37. Proszę omówić zagrożenia związane z atakami SQL Injection. W jaki sposób programiści mogą zapobiegać tym podatnościom?
38. Czym charakteryzują się ataki zero-day? Jakie są wyzwania związane z ich wykrywaniem i neutralizacją?

UNIWERSYTET VIZJA

39. Proszę omówić zagrożenia związane z kradzieżą tożsamości w cyberprzestrzeni. Jakie są jej skutki dla ofiar?
40. W jaki sposób praca zdalna zwiększa powierzchnię ataku organizacji?
41. Proszę omówić mechanizm działania ataków phishingowych.
42. Proszę omówić mechanizm działania ataków spear-phishingowych.
43. Proszę wyjaśnić, na czym polega atak ransomware i jakie są jego typowe wektory infekcji.
44. Proszę wyjaśnić zasadę działania rozproszonych ataków odmowy usługi. Jakie rodzaje ataków DDoS wyróżniamy?
45. Proszę omówić rodzaje złośliwego oprogramowania.
46. Proszę omówić, na czym polega atak typu Man-in-the-Middle.
47. Wyjaśnij pojęcie hacktywizmu i z czym jest to związane.
48. Jakie są zasady budowania polityki bezpieczeństwa haseł?