Zagadnienia i pytania egzaminacyjne

Kierunek *informatyk*a, studia drugiego stopnia

1. W jaki sposób jakość i przygotowanie danych wpływają na wiarygodność modelu klasyfikacyjnego? Omów postępowanie z brakami danych, obserwacjami odstającymi, niezbalansowanymi klasami oraz zastosowanie dyskretyzacji.
2. Omów strategie podziału zbioru danych na część treningową i testową w zależności od jego liczebności. Wyjaśnij zasady działania oraz korzyści płynące z zastosowania k-krotnej walidacji krzyżowej.
3. Jak rzetelnie ocenić i porównać skuteczność klasyfikatorów, zwłaszcza dla danych o niezrównoważonych klasach? Omów dobór metryk oceny oraz znaczenie prawidłowej procedury walidacyjnej.
4. Przedstaw klasyfikację systemów wspomagania decyzji (SWD) według kryterium dominującego zasobu (modele, dane, dokumenty, wiedza, komunikacja).
5. Jakie są zasadnicze różnice między klasycznym odbiornikiem radiowym a systemem Software Defined Radio (SDR)? Omów podział funkcji między układy sprzętowe i oprogramowanie oraz wynikające z niego możliwości i ograniczenia.
6. W jaki sposób zaprojektować w środowisku GNU Radio tor odbiorczy wykorzystujący platformę SDR? Omów przepływ sygnału przez podstawowe bloki przetwarzania oraz metody weryfikacji działania układu.
7. Jak interpretować pomiary mocy sygnału w skali logarytmicznej? Wyjaśnij zastosowanie jednostek dB i dBm oraz sposób oceny zmian poziomu sygnału i błędów pomiarowych.
8. Wyjaśnij znaczenie częstotliwości próbkowania, zjawiska aliasingu oraz ich wpływu na wierność odtwarzania sygnału.
9. Jak zidentyfikować potencjalny atak na podstawie analizy ruchu sieciowego? Omów na wybranym przykładzie wykorzystanie narzędzia do analizy pakietów i wykrywania anomalii w protokołach TCP, UDP, DNS i HTTP.
10. Jak rozpoznać, że komputer z systemem Windows lub Linux został zainfekowany złośliwym oprogramowaniem? Przedstaw metody analizy procesów, połączeń sieciowych, kont użytkowników oraz dzienników systemowych.
11. Jakie działania powinien podjąć analityk SOC po wykryciu włamania do systemu informatycznego? Przedstaw etapy obsługi incydentu, zabezpieczania materiału

dowodowego, ograniczania skutków ataku oraz przywracania prawidłowego działania systemów.

12. W jaki sposób można wykrywać i ograniczać ataki wykorzystujące podatności protokołów sieciowych? Omów przykładowe zagrożenia związane z ARP, IP, TCP i DNS oraz mechanizmy ochrony przed nimi.
13. Jak zaplanować proces analizy danych pochodzących z różnych źródeł? Omów pozyskiwanie, łączenie, czyszczenie i przygotowanie danych do dalszego przetwarzania.
14. Jak wybór relacyjnej lub nierelacyjnej bazy danych wpływa na możliwości analizy dużych zbiorów informacji? Porównaj sposoby pozyskiwania i przetwarzania danych z wykorzystaniem SQL i NoSQL.
15. Jak wykorzystać metody statystyczne i eksploracyjną analizę danych do identyfikacji zależności, anomalii i trendów? Omów dobór miar statystycznych oraz sposób interpretacji wyników.
16. Jakie wyzwania wiążą się z przetwarzaniem danych w architekturze Big Data i jak wykorzystuje się do tego przetwarzanie równoległe?
17. Jak dobrać architekturę techniczną sklepu internetowego do skali działalności przedsiębiorstwa? Omów znaczenie hostingu, domeny, modułowości systemu i możliwości rozbudowy platformy.
18. Jakie czynniki należy uwzględnić przy wyborze domeny, hostingu i serwera dedykowanego dla sklepu internetowego?
19. Wyjaśnij rolę analityki internetowej i wskaźników konwersji w procesie optymalizacji sklepu internetowego.
20. Jakie są metody optymalizacji procesu zakupowego i wyznaczania kluczowych wskaźników efektywności (KPI) w e-commerce?

Zagadnienia i pytania egzaminacyjne

Kierunek *informatyk*a, studia drugiego stopnia

Moduł *inżynieria oprogramowania i baz danych*

1. Wyjaśnij, czym są zaawansowane obiekty baz danych i w jaki sposób rozszerzają funkcjonalność relacyjnych systemów zarządzania bazami danych.
2. Wyjaśnij, na czym polega nieodtwarzalna historia przetwarzania transakcji, podaj przykład jej powstania i omów sposoby zapobiegania temu problemowi.
3. Omów proces optymalizacji zapytań SQL w praktyce. Jakie techniki i narzędzia stosuje się w tym celu?
4. Jakie znaczenie ma wielowymiarowy model danych w systemach OLAP? Omów rolę kostek danych oraz problemy analityczne, które pomagają rozwiązywać.
5. Omów metody szacowania pracochłonności i rozmiaru kodu (np. PROBE, COCOMO II, metoda delficka).
6. Jakie są etapy procesu zarządzania ryzykiem w przedsięwzięciach programistycznych i jak tworzy się rejestr czynników ryzyka?
7. Wyjaśnij, w jaki sposób pięciopoziomowy model CMMI wspiera rozwój dojrzałości procesów w organizacji oraz jakie korzyści wynikają z osiągania kolejnych poziomów.
8. Jak rozpoznać i ograniczyć atak odmowy usługi (DoS/DDoS) na infrastrukturę przedsiębiorstwa? Przedstaw mechanizmy wybranych ataków oraz sposoby odróżnienia ich od normalnego wzrostu obciążenia sieci.
9. W jaki sposób podatności protokołów IP, TCP i UDP mogą zostać wykorzystane do przeprowadzenia ataku? Omów przykładowe techniki, takie jak fałszowanie adresów IP, SYN Flood oraz fragmentacja pakietów.
10. Jakie zagrożenia wynikają z niewłaściwego zabezpieczenia usług sieciowych, takich jak DHCP, DNS i HTTP? Przedstaw przykładowe scenariusze ataków oraz sposoby ich wykrywania i ograniczania.

11. Jak rozpoznać próby ukrywania złośliwej aktywności przed systemami monitorowania bezpieczeństwa? Omów techniki omijania detekcji, tunelowania ruchu oraz metody identyfikowania nietypowej komunikacji.
12. W jaki sposób dobór struktur danych i algorytmów wpływa na wydajność aplikacji? Omów analizę złożoności, profilowanie oraz identyfikację wąskich gardeł.
13. Jak projektować zarządzanie pamięcią w aplikacji wykorzystującej wskaźniki i referencje? Wyjaśnij, jakie błędy mogą wystąpić oraz jak je diagnozować.
14. Omów techniki zarządzania pamięcią i optymalizacji aplikacji, w tym identyfikację wycieków pamięci i dobór odpowiednich struktur danych.
15. Jakie wyzwania wiążą się z integracją wielu języków programowania (np. Python + C/C++, Java + Kotlin) i tworzeniem komponentów wielokrotnego użytku?
16. Jakie problemy przetwarzania danych uzasadniają zastosowanie architektury Big Data? Omów charakterystykę danych wielkoskalowych i ograniczenia tradycyjnych rozwiązań.
17. Jak zaprojektować bazę dokumentową obsługującą często zmieniające się dane? Omów organizację kolekcji i dokumentów, indeksowanie oraz operacje agregacji.
18. Porównaj modele danych NoSQL: dokumentowy, grafowy, kolumnowy i klucz-wartość, wskazując ich typowe zastosowania.
19. Wyjaśnij, czym są inteligentne i hybrydowe systemy wspomagania decyzji (SWD) oraz jakie problemy decyzyjne mają za zadanie rozwiązywać.
20. W jaki sposób system wspomagania decyzji może identyfikować anomalie lub zagrożenia? Przedstaw rolę modelu neuronowego oraz zasady weryfikacji jego wskazań.
21. Porównaj metody wielokryterialnej analizy decyzyjnej oparte na porównaniach parami i wyznaczaniu priorytetów (np. AHP/ANP) z metodami opartymi na relacjach przewyższania (np. ELECTRE) w kontekście budowy systemu wspomagania decyzji.
22. Jak dobrać sposób organizacji zespołowego projektu informatycznego do rodzaju wymagań i niepewności projektu?

23. Jak zorganizować współpracę wielu programistów nad wspólnym kodem? Omów gałęzie Git, przeglądy pull requestów, integrację zmian i odpowiedzialność członków zespołu.

24. W jaki sposób diagram BPMN może pomóc zespołowi programistycznemu uzgodnić wymagania z interesariuszami? Omów modelowanie procesu i wykrywanie niejednoznaczności.

25. Omów znaczenie zarządzania ryzykiem, jakością (testy jednostkowe, lintowanie) oraz retrospektyw w cyklu życia projektu zespołowego.

Zagadnienia i pytania egzaminacyjne

Kierunek *informatyk*a, studia drugiego stopnia

Moduł *programowanie urządzeń technicznych*

1. Omów architekturę mikrokontrolera oraz jego podstawowe komponenty i zastosowania w systemach wbudowanych.
2. Jak dobrać mikrokontroler i jego zasoby do urządzenia zbierającego dane z czujników oraz sterującego elementami wykonawczymi? Omów ograniczenia sprzętowe i wymagania czasowe.
3. Jak wybrać interfejs komunikacyjny do połączenia mikrokontrolera z czujnikami i modułami zewnętrznymi? Porównaj właściwości oraz zastosowania UART, I^2C i SPI.
4. Czym różni się system czasu rzeczywistego od systemu ogólnego przeznaczenia? Podaj i omów kilka przykładów zastosowań systemów czasu rzeczywistego.
5. Jaką rolę pełni układ nadzoru (Watchdog) w systemach wbudowanych i czasu rzeczywistego?
6. Jak dobrać strategię szeregowania zadań w systemie RTOS? Omów wpływ priorytetów, wywłaszczania i wielowątkowości na spełnianie wymagań czasowych.
7. Jakie problemy powstają przy współdzieleniu zasobów przez zadania systemu czasu rzeczywistego? Omów synchronizację, zakleszczenia i odwrócenie priorytetów.
8. W jaki sposób można wykryć i przeciwdziałać atakom DoS oraz DDoS wymierzonym w zasoby sieciowe organizacji? Scharakteryzuj wybrane rodzaje tych ataków oraz metody odróżniania ich od zwiększonego, ale prawidłowego ruchu sieciowego.
9. Jakie zagrożenia bezpieczeństwa wiążą się z wykorzystaniem protokołów IP, TCP i UDP? Wyjaśnij mechanizmy ataków opartych na podszywaniu się pod adresy IP, zalewaniu pakietami SYN oraz manipulowaniu fragmentacją pakietów.
10. W jaki sposób atakujący mogą wykorzystać słabości konfiguracji usług DHCP, DNS oraz HTTP? Przedstaw przykłady takich ataków i omów mechanizmy ich wykrywania oraz zabezpieczania usług.
11. Jakie metody stosują cyberprzestępcy, aby uniknąć wykrycia przez systemy monitorowania ruchu sieciowego? Omów techniki ukrywania komunikacji, tunelowania danych oraz sposoby rozpoznawania podejrzanej aktywności.

12. W jaki sposób zaprojektować maszynę stanów sterującą urządzeniem reagującym na wiele wejść? Omów identyfikację stanów, warunki przejść i weryfikację poprawności.
13. W jaki sposób opisać współbieżną pracę kilku elementów urządzenia? Porównaj powiązane maszyny FSM i sieci Petriego oraz ich zastosowanie do synchronizacji procesów.
14. Jakie znaczenie mają układy czasowo-licznikowe w realizacji algorytmów sterowania na mikrokontrolerach?
15. Jak zweryfikować zgodność implementacji algorytmu sterowania na mikrokontrolerze z modelem formalnym? Omów testowanie sekwencji zdarzeń, warunków czasowych i sytuacji wyjątkowych.
16. W jaki sposób Raspberry Pi komunikuje się z zewnętrznymi sensorami i układami peryferyjnymi?
17. Jak przygotować Raspberry Pi do roli sterownika lub bramy komunikacyjnej? Omów dobór systemu operacyjnego, konfigurację usług i zarządzanie zasobami.
18. Jak zaprojektować współpracę Raspberry Pi z czujnikami i elementami wykonawczymi? Omów wykorzystanie interfejsów wejścia i wyjścia oraz komunikacji z układami zewnętrznymi.
19. W jaki sposób zapewnić poprawne współbieżne wykonywanie zadań na wielu węzłach? Omów synchronizację, współdzielenie danych oraz ryzyko zakleszczenia i blokady.
20. W jaki sposób redundancja może zwiększyć dostępność rozproszonego systemu sterowania? Omów wykrywanie awarii i przejmowanie zadań przez pozostałe węzły.
21. Omów protokoły wymiany danych stosowane w komunikacji między węzłami systemu rozproszonego.
22. Jak zdefiniować zakres zespołowego projektu sterowania urządzeniem? Omów identyfikację wymagań, ograniczeń technicznych i kryteriów odbioru.
23. Jak zaprojektować współbieżną pracę kilku funkcji sterownika w ramach wspólnego projektu? Omów zależności i sposób sprawdzania poprawności współdziałania.
24. Omów proces analizy i oceny ryzyka w projekcie inżynierskim.
25. Wyjaśnij znaczenie harmonogramowania oraz podziału ról i odpowiedzialności w zespole projektowym.

Zagadnienia i pytania egzaminacyjne

Kierunek *informatyk*a, studia drugiego stopnia

Moduł *sieci komputerowe i systemy teleinformatyczne*

1. Omów architekturę klient-serwer oraz dokonaj klasyfikacji serwerów ze względu na pełnione funkcje w infrastrukturze IT.
2. Wyjaśnij zasady zarządzania użytkownikami i uprawnieniami w serwerowych systemach operacyjnych, z uwzględnieniem zasady najmniejszych uprawnień.
3. Jak przygotować bezpieczną konfigurację systemu operacyjnego pełniącego funkcję serwera? Omów zarządzanie usługami, kontami, uprawnieniami i proces hardeningu.
4. Jakie wymagania należy uwzględnić przy uruchamianiu lokalnego asystenta AI na serwerze organizacji? Omów ochronę danych, dobór zasobów i integrację z systemami monitorowania.
5. Jak zaprojektować segmentację sieci przedsiębiorstwa za pomocą VLAN? Omów routing między sieciami VLAN oraz diagnostykę problemów z komunikacją.
6. Omów zadania warstwy fizycznej i warstwy łącza danych w kontekście budowy małej sieci lokalnej (LAN).
7. Przedstaw normy okablowania strukturalnego (szkieletowego i poziomego) oraz zasady instalacji i badania okablowania.
8. Jak przeprowadzić diagnostykę braku łączności w sieci obejmującej przełączniki i routery? Uwzględnij analizę warstw, konfiguracji VLAN oraz tras routingu.
9. Jak przeprowadzić analizę ruchu sieciowego w celu zidentyfikowania ataku DoS lub DDoS? Omów charakterystyczne cechy takich ataków, sposoby ich ograniczania oraz kryteria odróżniania od legalnego przeciążenia infrastruktury.
10. W jaki sposób mechanizmy działania protokołów IP, TCP i UDP mogą prowadzić do zagrożeń bezpieczeństwa sieci? Przedstaw przykłady nadużyć związanych z fałszowaniem adresacji, przeciążaniem połączeń TCP oraz fragmentacją datagramów.
11. Jak ocenić bezpieczeństwo usług sieciowych DHCP, DNS i HTTP w środowisku przedsiębiorstwa? Wskaż możliwe sposoby ich atakowania oraz metody identyfikowania i eliminowania zagrożeń.

12. W jaki sposób można identyfikować złośliwy ruch sieciowy celowo ukrywany przed mechanizmami detekcji? Przedstaw przykłady technik omijania zabezpieczeń, wykorzystania tuneli komunikacyjnych oraz analizy anomalii.
13. Jak dobrać protokół routingu do sieci przedsiębiorstwa wykorzystującej IPv4 i IPv6? Porównaj właściwości EIGRP, OSPF i routingu statycznego.
14. Wyjaśnij mechanizmy filtrowania tras BGP oraz kontrolę polityk routingu z użyciem list dostępu (ACL) i map tras (route map).
15. Wyjaśnij zasady działania protokołów OSPFv2 (IPv4) i OSPFv3 (IPv6) w środowisku wieloobszarowym.
16. W jaki sposób zaprojektować wieloobszarowy system OSPF? Omów podział na obszary, podsumowanie tras, znaczenie komunikatów LSA i diagnostykę.
17. Jakie czynniki wpływają na dokładność pozycjonowania GNSS w terenie zabudowanym i otwartym? Omów źródła błędów oraz sposoby porównywania wyników pomiarów.
18. Wyjaśnij zasadę działania systemów GNSS oraz omów źródła błędów w lokalizacji i sposoby ich korekcji.
19. Jak przebiega pozyskiwanie i przetwarzanie danych z systemów GNSS? Omów strukturę komunikatów NMEA oraz ich wykorzystanie do wyznaczania pozycji, rejestrowania tras i analizy danych czasowych.
20. Jak przygotować bezpieczne połączenie między oddziałami przedsiębiorstwa? Porównaj zastosowanie tunelu GRE i VPN IPsec oraz omów ograniczenia obu rozwiązań.
21. Przedstaw zaawansowane konfiguracje protokołów routingu (OSPF, EIGRP, BGP) w sieciach rozległych oraz mechanizmy ich zabezpieczania.
22. Jakie znaczenie w zarządzaniu siecią mają mechanizmy QoS, translacja adresów (NAT/PAT) oraz monitorowanie aktywności sieciowej?
23. Omów etapy analizy wymagań oraz projektowania architektury nowoczesnych sieci LAN i WAN (topologie, segmentacja, skalowalność).
24. Omów konfigurację zapory sieciowej oraz reguł NAT w celu ochrony sieci LAN i dostępu do Internetu.
25. Omów zastosowanie narzędzi monitorowania sieci oraz zasady tworzenia dokumentacji technicznej i prezentacji projektu.

Zagadnienia i pytania egzaminacyjne

Kierunek *informatyk*a, studia drugiego stopnia

Moduł *cyberbezpieczeństwo*

1. Jak zaplanować autoryzowany test penetracyjny aplikacji webowej? Omów określenie zakresu, identyfikację powierzchni ataku i sposób dokumentowania wyników.
2. Wyjaśnij, na czym polega etyczne hakowanie oraz przedstaw etapy przeprowadzania testów penetracyjnych aplikacji.
3. Omów typowe metody wykorzystywania luk w zabezpieczeniach sieci, chmury oraz urządzeń mobilnych i IoT.
4. Jakie błędy w mechanizmach uwierzytelniania, autoryzacji i obsługi sesji mogą prowadzić do przejęcia konta? Omów odpowiednie mechanizmy ochronne.
5. Jak zabezpieczyć cyfrowe materiały dowodowe po wykryciu incydentu? Omów akwizycję bitową nośników, użycie blokady zapisu, funkcji skrótu i zasad chain of custody.
6. W jaki sposób można przeanalizować usunięte pliki i strukturę systemu plików w postępowaniu śledczym? Omów wykorzystanie obrazów nośników i narzędzi analitycznych.
7. W jaki sposób przeprowadza się analizę systemów operacyjnych Windows i Linux (logi systemowe, rejestr, pliki usunięte, artefakty użytkownika)?
8. Jakie działania należy podjąć w przypadku podejrzenia ataku DoS lub DDoS na usługi sieciowe przedsiębiorstwa? Omów sposoby rozpoznawania rodzaju ataku, weryfikacji jego wystąpienia oraz ograniczania skutków przeciążenia.
9. Jak można wykorzystać właściwości protokołów IP, TCP i UDP do zakłócenia działania sieci komputerowej? Wyjaśnij działanie wybranych ataków wykorzystujących spoofing adresów IP, pakiety SYN oraz fragmentację ruchu sieciowego.
10. Jakie konsekwencje dla bezpieczeństwa infrastruktury mogą wynikać z błędnej konfiguracji usług DHCP, DNS i HTTP? Omów przykładowe wektory ataków oraz techniki monitorowania i zabezpieczania tych usług.
11. Jak analizować ruch sieciowy w celu wykrycia prób obchodzenia mechanizmów bezpieczeństwa? Omów sposoby maskowania złośliwej komunikacji, tunelowania

ruchu oraz metody wykrywania zachowań odbiegających od normalnej aktywności sieci.

12. Omów wielowarstwową budowę nowoczesnych systemów operacyjnych oraz koncepcje wirtualizacji i konteneryzacji zasobów.
13. Omów metody zabezpieczania serwerów Linux (np. Fail2Ban, UFW) oraz wdrażanie polityk bezpieczeństwa w systemach Windows (GPO, DLP).
14. Omów działania podejmowane po wykryciu incydentu bezpieczeństwa na poziomie systemu operacyjnego, uwzględniając izolację hosta, zabezpieczenie logów i ograniczenie uprawnień.
15. Porównaj podejście do aktualizacji i hardeningu systemu w Windows i Linux, wskazując podobieństwa i różnice w praktyce administracyjnej.
16. Jak rozpoznać i ocenić zagrożenia socjotechniczne skierowane przeciwko pracownikom organizacji? Omów rolę psychologicznych technik manipulacji i kontekstu ataku.
17. Jakie zagrożenia socjotechniczne dotyczą infrastruktury krytycznej i jakie metody ochrony można tam zastosować?
18. W jaki sposób dane dostępne publicznie (OSINT) i informacje z mediów społecznościowych mogą zwiększać skuteczność ataków ukierunkowanych? Omów sposoby ograniczania ekspozycji informacji.
19. W jaki sposób własności liczb pierwszych i arytmetyki modularnej są wykorzystywane w kryptografii? Omów znaczenie testowania pierwszości i obliczeń w strukturach algebraicznych.
20. Jak dobrać algorytm kryptograficzny do szyfrowania danych oraz bezpiecznej wymiany kluczy? Porównaj zastosowania kryptografii symetrycznej i asymetrycznej.
21. Jak zaprojektować mechanizm bezpiecznego podziału tajemnicy między kilkoma uczestnikami? Omów cel dzielenia sekretu i warunki jego odtworzenia.
22. Porównaj rozwiązania VPN oparte na IPsec i TLS oraz omów wyzwania związane z ich wdrażaniem.
23. Wyjaśnij rolę wymiany kluczy w tunelach VPN i bezpiecznej komunikacji.
24. Jak dobrać technologię tunelowania do bezpiecznego połączenia oddziałów przedsiębiorstwa? Porównaj tunel GRE i VPN IPsec pod względem enkapsulacji oraz ochrony transmisji.

25. W jaki sposób przebiega ustanawianie bezpiecznego tunelu IPsec? Omów rolę IKE, negocjacji parametrów kryptograficznych i uwierzytelniania stron.