Zagadnienia na egzamin magisterski na kierunku Informatyka – ogólne (dla studentów studiów stacjonarnych i niestacjonarnych II stopnia)

Przygotowanie i publikowanie artykułów naukowych

1. Struktura publikacji naukowych, schemat IMRaD.
2. Identyfikator ORCID. Indeks Hirscha.
3. Rodzaje artykułów naukowych.
4. Wskaźniki bibliometryczne. Lista Filadelfijska.
5. Bazy danych bibliograficznych. Baza Scopus.
6. Narzędzia AI w pracy naukowca.

Zaawansowana eksploracja danych, do roku akademickiego 2024/2025

1. Metody identyfikacji obserwacji odstających. Wymień znane metody i omów jedną z nich.
2. Metody estymacji gęstości rozkładu prawdopodobieństwa. Wymień znane metody i omów jedną z nich.
3. Wnioskowanie statystyczne. ANOVA, MANOVA – postawienie zagadnienia, przykłady zastosowań.
4. Modele regresji. Regresja wielokrotna. Postawienie zagadnienia.
5. Metody redukcji wymiaru i liczności próby. Wymień znane metody i omów jedną z nich.
6. Metody analizy skupień. Wymień znane metody i omów jedną z nich.
7. Systemy rekomendacji. Wymień rodzaje systemów rekomendacji i omów przykładowy.
8. Metody porównania modeli uczenia maszynowego. Omów na przykładzie.
9. Ocena jakości modeli klasyfikacyjnych.
10. Ocena jakości modeli regresyjnych i prognozujących.

Zaawansowane metody analizy i eksploracji danych, od roku akademickiego 2025/2026

1. Metody zapisu danych przestrzennych. Typ SDO_GEOMETRY.
2. Funkcje i operatory przestrzenne. Zapytania przestrzenne, przykłady zastosowań.
3. Analiza danych przestrzennych. Omów przykładowe zastosowanie takiej analizy.
4. Metody identyfikacji obserwacji odstających. Wymień znane metody i omów jedną z nich.
5. Metody estymacji gęstości rozkładu prawdopodobieństwa. Wymień znane metody i omów jedną z nich.
6. ANOVA, MANOVA – postawienie zagadnienia, przykłady zastosowań.
7. Modele regresji. Regresja wielokrotna. Postawienie zagadnienia.
8. Metody redukcji wymiaru i liczności próby. Wymień znane metody i omów jedną z nich.

9. Metody analizy skupień. Wymień znane metody i omów jedną z nich.
10. Systemy rekomendacji. Wymień rodzaje systemów rekomendacji i omów przykładowy.
11. Ocena jakości modeli analizy skupień.
12. Ocena jakości modeli regresyjnych i prognozujących.
13. Statystyczne sterowanie procesem SPC – cel i metody.

Metody wnioskowania wielokryterialnego

1. Jakie są główne zadania normalizacji wartości analizowanych kryteriów optymalizacji.
2. Na czym polega metoda leksykograficzna.
3. W jaki sposób wyznaczane są wagi ważności kryteriów w metodzie AHP.
4. Opisz warianty należące do zbioru wariantów optymalnych w sensie Pareto.
5. Scharakteryzuj metodę Blina.

Internet Rzeczy

1. Krótko opisz zagadnienie Internetu Rzeczy.
2. Co to jest magistrala, interfejs, protokół? Scharakteryzuj i opisz różnice.
3. Scharakteryzuj pojęcie mikrokontrolera i mikroprocesora. Podaj różnice między tymi pojęciami.
4. Wyjaśnij, co oznacza skrót CISC. Krótko opisz ten termin.
5. Wyjaśnij, co oznacza skrót RISC. Krótko opisz to pojęcie.
6. Opisz i podaj różnice pomiędzy UART a USRT.
7. Czym jest i co powoduje pojemność pasożytnicza?
8. Jakie cechy powinien posiadać sensor inteligentny?
9. Czym są i do czego służą aktuatory?
10. Opisz zasadę działania modulacji szerokości impulsów PWM (ang. pulse width modulation).

Bariery w przestrzeni cyfrowej

1. Projektowanie uniwersalne – idea, przepisy prawne, zasady.
2. Ergonomia interfejsów oprogramowania – definicja, obszary, typy i przykłady.
3. Użyteczność i dostępność interfejsu oprogramowania.
4. Technologie wspomagające osoby z niepełnosprawnościami.
5. Wytyczne dostępności treści internetowych WCAG 2.1 – zasady, poziomy, weryfikacja.
6. Metody oceny jakości interfejsu – klasyfikacja, typy metod.
7. Techniki oceny jakości interfejsów z udziałem i bez udziału użytkowników.
8. Metodyka SUS.
9. Ocena heurystyczna – heurystyki Nielsena-Molicha.
10. Okulografia – idea, istota, urządzenia, eksperyment, rezultaty.

Bezpieczeństwo środowiska i aplikacji chmurowych

1. Jakie są cechy chmury obliczeniowej wg NIST?
2. Jakie są główne zagrożenia bezpieczeństwa chmury?
3. Jakie znasz modele chmur komputerowych?
4. Czy i ewentualnie dlaczego (tak lub nie) do bezpieczeństwa chmury musimy podchodzić inaczej niż w przypadku standardowych metod bezpieczeństwa IT?
5. W jakim modelu chmury dostawca odpowiada za bezpieczeństwo infrastruktury i platformy, a klient za aplikacje i dane?
6. Czym jest IAM w bezpieczeństwie chmurowym?
7. Czym jest MFA w kontekście chmury?
8. Czym są mechanizmy RBAC i ABAC?
9. Na czym polega szyfrowanie danych w spoczynku i w tranzycie?
10. Czym jest RPO (Recovery Point Objective)?
11. Czym jest RTO (Recovery Time Objective)?
12. Do czego służą Virtual Private Clouds (VPC) w kontekście bezpieczeństwa chmury?
13. Czym jest mechanizm TDE?
14. Co oznacza pojęcie Data minimization?
15. Czym jest OWASP Top 10 ?

Algorytmy kryptograficzne

1. Wyjaśnij, czym zajmuje się kryptografia, a czym kryptoanaliza. Jakie są podstawowe cele stosowania mechanizmów kryptograficznych?
2. Przedstaw podstawową klasyfikację systemów kryptograficznych. Wyjaśnij różnice między systemami symetrycznymi i asymetrycznymi oraz strumieniowymi i blokowymi.
3. Na czym polega zasada Kerckhoffsa i dlaczego jest ważna przy projektowaniu bezpiecznych systemów kryptograficznych?
4. Wyjaśnij pojęcie tajności doskonałej. Dlaczego szyfr z kluczem jednorazowym jest doskonale tajny, ale ponowne użycie tego samego klucza jest niebezpieczne?
5. Porównaj klasyczne szyfry podstawieniowe i przestawieniowe z nowoczesnymi algorytmami kryptograficznymi. Jak zmieniło się podejście do bezpieczeństwa szyfrów?
6. Czym są tryby pracy szyfrów blokowych i dlaczego są potrzebne? Omów ogólnie znaczenie takich trybów jak ECB, CBC, CFB, OFB, CTR lub GCM.
7. Omów rolę klucza w kryptografii symetrycznej i asymetrycznej. Jakie problemy rozwiązuje kryptografia klucza publicznego?
8. Wyjaśnij ogólną ideę protokołu Diffiego-Hellmana. Dlaczego umożliwia on uzgodnienie wspólnego sekretu przez niezabezpieczony kanał komunikacyjny?

9. Na czym opiera się bezpieczeństwo kryptosystemu RSA? Jaką rolę odgrywają w nim liczby pierwsze, arytmetyka modularna i trudność faktoryzacji?
10. Porównaj kryptosystemy RSA i Elgamala. Jakie problemy matematyczne leżą u podstaw ich bezpieczeństwa?
11. Czym jest podpis elektroniczny i jakie własności bezpieczeństwa powinien zapewniać? Wyjaśnij różnicę między szyfrowaniem a podpisywaniem wiadomości.
12. Wyjaśnij, czym są funkcje skrótu. Jakie cechy powinna mieć bezpieczna kryptograficzna funkcja skrótu?
13. Do czego służą kody MAC? Porównaj ogólnie uwierzytelnianie wiadomości za pomocą MAC z podpisem cyfrowym.
14. Na czym polega główna idea kryptografii krzywych eliptycznych? Dlaczego jest ona atrakcyjna w porównaniu z klasycznymi systemami asymetrycznymi?
15. Omów ogólnie, jakie wyzwania dla współczesnej kryptografii wiążą się z rozwojem komputerów kwantowych. Czym różni się kryptografia kwantowa od kryptografii postkwantowej?

Bezpieczeństwo w sieciach komputerowych

1. Podstawowe zadania bezpieczeństwa i cyberbezpieczeństwa w infrastrukturze sieciowej.
2. Rola systemów Windows i Linux w analizie bezpieczeństwa sieci komputerowej.
3. Analiza protokołów i usług sieciowych w ocenie bezpieczeństwa sieci.
4. Klasyfikacja najważniejszych rodzajów ataków sieciowych.
5. Metody detekcji i obrony przed atakami w warstwie II modelu OSI.
6. Metody detekcji i obrony przed atakami w warstwie III modelu OSI.
7. Narzędzia służące do identyfikacji ataków na protokoły i usługi sieciowe.
8. Monitorowanie ruchu sieciowego w wykrywaniu nieprawidłowości i incydentów.
9. Metody zapobiegania nieuprawnionemu dostępowi do zasobów sprzętowych i programowych.
10. Segmentacja sieci, minimalizacja uprawnień oraz inspekcja ruchu kontrola dostępu w ograniczaniu skutków ataków.
11. Podstawowe działania administratora w zakresie zabezpieczania infrastruktury sieciowej.
12. Praktyczne znaczenie narzędzi takich jak Wireshark, nmap oraz systemowe narzędzia diagnostyczne.

Ochrona sieci dostępowych

1. Podstawowe zagrożenia występujące w lokalnych sieciach komputerowych oraz ich wpływ na bezpieczeństwo infrastruktury.
2. Podatności technologii Ethernet oraz protokołów wykorzystywanych w lokalnych sieciach komputerowych.

3. Znaczenie monitorowania sieci lokalnej w wykrywaniu i analizie incydentów bezpieczeństwa.
4. Narzędzia wykorzystywane do monitorowania i analizy ruchu w lokalnych sieciach komputerowych.
5. Zasady projektowania bezpiecznej infrastruktury sieci lokalnej. Metody zabezpieczania urządzeń końcowych i pośredniczących w sieci dostępowej.
6. Zagrożenia związane z komunikacją bezprzewodową oraz sposoby jej zabezpieczania.
7. Rola wielowarstwowej ochrony w zabezpieczaniu lokalnych sieci komputerowych.
8. Audyt bezpieczeństwa, testy penetracyjne i ocena podatności w ochronie sieci dostępowych.
9. Źródła, struktura i ocena alertów bezpieczeństwa w lokalnych sieciach komputerowych.
10. Systemy zarządzania bezpieczeństwem informacji w ochronie sieci lokalnych.
11. Zagrożenia i metody ochrony systemów mobilnych oraz urządzeń IoT.

Bezpieczeństwo sieci teleinformatycznych

1. Ataki polegające na rozpoznaniu, uzyskaniu dostępu oraz inżynierii społecznej.
2. Standardy i dobre praktyki bezpieczeństwa: ISO 27001, NIS2 oraz inne wybrane normy.
3. Zabezpieczanie styku sieci teleinformatycznej z sieciami zewnętrznymi.
4. Kontrola dostępu do sieci oraz mechanizmy NAC.
5. Technologie uwierzytelniania i autoryzacji: RADIUS, TACACS+ oraz ISE.
6. Rodzaje firewalli oraz zasady tworzenia polityk i reguł bezpieczeństwa.
7. Szczegółowa inspekcja pakietów w wykrywaniu i blokowaniu zagrożeń. Zadania oraz ograniczenia systemów IDS i IPS w ochronie sieci teleinformatycznych.
8. Adaptacyjne urządzenia zabezpieczające i ich rola w sieciach korporacyjnych.
9. Zastosowanie sieci VPN w bezpiecznej komunikacji oraz wybrane technologie VPN.
10. Etapy i metody testowania bezpieczeństwa sieci teleinformatycznych.
11. Rola sztucznej inteligencji i uczenia maszynowego w ochronie sieci teleinformatycznych.

Bezpieczeństwo systemów operacyjnych i usług

1. Podstawowe cele bezpieczeństwa systemów operacyjnych i usług sieciowych.
2. Architektura systemu operacyjnego z punktu widzenia bezpieczeństwa.
3. Jądro systemu, separacja przestrzeni użytkownika i mechanizmy ochrony pamięci.
4. Zarządzanie użytkownikami, uprawnieniami i kontrolą dostępu w systemach operacyjnych.
5. Modele kontroli dostępu: DAC, MAC i RBAC.

6. Mechanizmy uwierzytelniania: hasła, klucze SSH, uwierzytelnianie dwuskładnikowe, IAM i SSO.
7. Zapobieganie i wykrywanie zagrożeń w systemach operacyjnych.
8. Zastosowanie kryptografii w ochronie danych i komunikacji.
9. Najczęstsze ataki na aplikacje webowe oraz podstawowe mechanizmy ich ograniczania.
10. Bezpieczeństwo podstawowych usług sieci lokalnej: DHCP, DNS, NAT, HTTP, FTP, itp.
11. Proces reagowania na incydenty oraz podstawy analizy powłamaniowej.
12. Testy penetracyjne, ocena podatności oraz bazy CVE i MITRE ATT&CK.