**Návrh otázok na SZS, máj 2019**

**Oblasti (Vetvy):**

*1. Počítačové systémy a siete. Bezpečnosť počítačových systémov - ((ÚINF/KRP1/15 alebo ÚINF/ARP1/15) a ÚINF/OPS1/15).*

*2. Informačné a znalostné systémy - (ÚINF/LAD1/15 a ÚINF/AIS1/15)*

*3. Základy umelej inteligencie ((ÚINF/VYU1/15 alebo ÚINF/STU1/16) a (ÚINF/NEU1/15 alebo ÚINF/VKN/15))*

*4. Výpočtová zložitosť, výpočtové modely - (ÚINF/KKV1/15 a ÚMV/KOA/10)*

Študent si vyberá otázku podľa vyššie uvedenej vetvy. Otázka by mala mať dve prepojené časti podľa predmetov zvolenej vetvy.

1. *Počítačové systémy a siete. Bezpečnosť počítačových systémov - ((ÚINF/KRP1/15 alebo ÚINF/ARP1/15) a ÚINF/OPS1/15)*
2. Charakteristické typy inštrukcií, využívanie súčastí procesora pri ich spracovaní. Postup realizácie inštrukcií volania procedúr, sw prerušenia, význam tabuľky vektorov prerušenia. Autentifikácia pri nadväzovaní sieťovej komunikácie - systém Kerberos. Generovanie a distribúcia symetrických kľúčov.
3. Komunikácia procesora so vstupno-výstupnými zariadeniami prostredníctvom portov, s využitím priameho prístupu k pamäti a s využitím prerušení. Typy prerušení a ich využitie pre efektívny výkon operačného systému. Certifikácia, certifikačné autority, distribúcia dôvery.
4. Princíp zreťazeného spracovania inštrukcií procesorom. Viacvláknové spracovanie, predspracovanie, špekulatívne vykonávanie inštrukcií a ich vykonávanie mimo poradia.
Princíp a možnosti použitia protokolu SSL/TLS. Tunelovanie komunikácie cez zabezpečené porty.
5. Viacúrovňový pamäťový systém, rýchle vyrovnávacie pamäte, asociatívny prístup (priame mapovanie, množinovo asociovaná  a úplne asociovaná pamäť).
Princíp, režimy práce a možnosti použitia protokolu IPsec. Obsah a použitie databázy bezpečnostných asociácií, tvorba bezpečnostných politík.
6. Autentifikácia pomocou zdieľaného hesla a dohody na kľúči v dôvernom prostredí (forward secrecy). Skupinová autentifikácia a dohoda na kľúči medzi viacerými účastníkmi.
Zástupné (proxy) servery a ich využitie v bezpečnostných bránach (firewall). Konfigurácia netriviálnej bezpečnostnej brány s demilitarizovanou zónou, filtrovanie komunikačných tokov.
7. *Informačné a znalostné systémy - (ÚINF/LAD1/15 a ÚINF/AIS1/15)*

a. Optimalizácia dopytov (vymieňacie lemy).

 Integritné obmedzenia v konceptuálnom modelovaní informačných systémov.

b. Vzťah formálnych databázových modelov a SQL.

 Modelovo-orientovaný (MDA) vývoj informačných systémov. Entitné typy v konceptuálnom modelovaní.

c. Normálne tvary dopytov konjunktívneho kalkulu a dopytov relačnej algebry (SPC).

 Relačné typy a taxonómie v konceptuálnom modelovaní.

d. Spôsoby použitia symbolickej logiky pri modelovaní databáz (konjunktívne dopyty a relačná algebra).

 Tvorba modelov. Metamodelovanie.

1. *Výpočtová zložitosť, výpočtové modely - (ÚINF/KKV1/15 a ÚMV/KOA/10)*

a. Klasické a kvantové testovanie prvočíselnosti. Shorov algoritmus.

 Toky v sieťach.

b. Základné vlastnosti kvantových výpočtov. Groverov algoritmus.

 Problém obchodného cestujúceho.

c. Kvantový paralelizmus. Základné operátory a ich využitie.

Problém minimálnej kostry. Generovanie kostier grafu.

d. Porovnanie klasických a kvantových výpočtov. Príklad deterministického a pravdepodobnostného kvantového výpočtu.

Cesty v grafoch.

e. Základné požiadavky na operácie kvantového počítača. Spektrálna dekompozícia operátorov.

Úloha čínskeho poštára. Problémy spárenia.

1. *Základy umelej inteligencie ((ÚINF/VYU1/15 alebo ÚINF/STU1/16) a (ÚINF/NEU1/15 alebo ÚINF/VKN/15))*
2. Základný model neurónu, jeho použitie vo vrstvových neurónových sieťach. back-propagation algoritmus.

PAC (probably aproximately correct) učenie, príklady PAC algoritmov.

1. Rosenblattov perceptrón, algoritmus jeho učenia, jeho vlastnosti.

VC dimenzia a jej vzťah k hypotézovému priestoru perceptrónov.

1. Modely neurónových sietí podľa typu učenia sa, Kohonenov model, algoritmus učenia sa.

Support vector machines (SVM) – formulácia problému, základné vlastnosti.

1. Neuromaty ako akceptory formálnych jazykov a ich zložitosť. Neurónové simulátory automatov a ich zložitosť. Lineárna regresia, lineárne modely.
2. Radial Basis Function (RBF) siete, algoritmus učenia sa.

 Konzistentné algoritmy a učenie. Konzistentný algoritmus pre rozhodovacie zoznamy.

1. Univerzálna aproximácia pomocou neurónových sietí, Kolmogorovova veta. Učenie monočlenov a disjunkcií malých monočlenov, konzistentnosť naučených formúl s tréningovými vzorkami.