Státní závěrečná zkouška

Státní závěrečná zkouška se koná před zkušební komisí. Průběh státní závěrečné zkoušky a vyhlášení výsledků jsou veřejné, jednání komise je neveřejné. Státní závěrečná zkouška je složena ze dvou částí: ústní zkoušky a obhajoby závěrečné práce. Další informace jsou uvedeny v příslušném studijním a zkušebním řádu. Požadavky k ústní části státní závěrečné zkoušky pro obor *Informatika (dvouoborové)*, které platí poprvé pro studenty, kteří studují od akademického roku 2015/2016, jsou specifikovány dále.

Předmět ústní části státní závěrečné zkoušky pro obor *Informatika (dvouoborové)* (KI/SZZ60 Informatika) pokrývá dvě oblasti.

- *Teoretická informatika*
- *Aplikovaná informatika*

Student je zkoušen celkem ze dvou otázek resp. okruhů, a sice pro každou oblast z jednoho okruhu. Volbu okruhu pro každou oblast provádí student tak, že za účasti alespoň dvou členů zkušební komise realizuje náhodný výběr okruhu z příslušného souboru zkušebních okruhů. Student má nárok na 30 minut na přípravu. Obvyklá doba zkoušení je 15 minut z každého okruhu, tj. celkem 30 minut.

V rámci ústní části státní závěrečné zkoušky je důraz kladen nejen na teoretické znalosti, ale i na jejich praktické uplatnění v rámci informačních technologií (hardwaru, softwaru, návrhu a vývoje).

ZKUŠEBNÍ OKRUHY KE STÁTNÍ ZÁVĚREČNÉ ZKOUŠCE pro obor Informatika (dvouoborové) ve verzi A14

Teoretická informatika

A. Teoretické základy informatiky

1. Množiny a relace (operace s množinami, kartézský součin, binární relace, zobrazení)
2. Číselné soustavy (poziční a nepoziční číselné soustavy, desítková, dvojková a šestnáctková číselná soustava a převody mezi jednotlivými číselnými soustavami)
3. Kombinatorika (variace, permutace, kombinace a Binomická věta)

B. Algoritmy a datové struktury

4. Základní třídící algoritmy (BubbleSort, HeapSort, Quicksort, Mergesort, RadixSort, porovnání algoritmů z pohledu časové náročnosti, přirozenosti a stability)
5. Vyhledávací algoritmy (hashovací tabulky, binární vyhledávací stromy)

C. Lineární algebra a geometrie

6. Soustavy lineárních rovnic a jejich řešení (matice soustavy, inverzní matice, Frobeniova věta, determinant [výpočet, Cramerovo pravidlo], přímé metody řešení [Gaussova a Gaussova-Jordanova eliminační metoda, LU dekompozice], iterační metody řešení [Jacobiho a Gaussova-Seidelova])
7. Vlastní čísla matic a jejich výpočet (vlastní čísla a vlastní vektory, charakteristický polynom, mocninná metoda pro výpočet dominantního vlastního čísla)

D. Základy kryptologie

8. Algoritmy symetrické kryptografie (princip šifrování, DES, TDEA, AES), režimy šifer (ECB, CBC, CFB, OFB, CTR)
9. Algoritmy kryptografie s veřejným klíčem (princip šifrování, RSA, El-Gamal, D-H), rozšířený Euklidův algoritmus, hybridní kryptosystém (princip šifrování)
10. Hash funkce a digitální podpis (vlastnosti hash funkcí, rodina MDX, rodina SHA-X), princip komunikace s využitím digitálního podpisu, MAC a MDC

Aplikovaná informatika

Základní soubor zkušebních okruhů z této oblasti obsahuje 15 okruhů dělených do 6 skupin (A až F) po 2 až 3 okruzích. Student realizuje náhodný výběr okruhu z omezeného souboru. Tento soubor obsahuje minimálně 11 zkušebních okruhů, které jsou tvořeny všemi okruhy skupin A až C spolu se všemi okruhy z další minimálně 1 skupiny, kterou si student předem zvolí ze zbývajících 3 skupin (D až F) základního souboru dle vlastního uvážení.

A. Architektura počítačů

1. Základní konstrukce počítačů, procesory (schéma, instrukční sady, principy zrychlování činnosti procesorů), základní deska a sběrnicová architektura (schéma, typy sběrnic), rozhraní (paralelní, sériová)
2. Paměti (rozdělení, technologie, parametry, princip činnosti), pevné a optické disky (technologie, čtení/zápis dat, kódování, logická a fyzická struktura, RAID)
3. Multimediální subsystémy (grafický subsystém, principy tvorby obrazu, zobrazovací jednotky, zvukový subsystém)

B. Základy počítačových sítí a protokolů

4. Vrstvové modely síťové komunikace (jejich funkcionalita a součinnost, standardizace, protokoly vrstev), adresace a dělení adresních prostorů
5. Princip směrování v počítačových sítích (architektura směrovačů, rodiny směrovacích protokolů)
6. Technologie kabelových a bezdrátových sítí (frekvence, diskrétní a analogová modulace, protokoly přístupu k médiu)

C. Programování I a II

7. Základy objektově orientovaného programování (třídy, objekty, metody, vlastnosti)
8. Základní kolekce (seznam, slovník, základní operace nad kolekcemi [cykly, indexace, iterace, duplikace])
9. Objektový polymorfismus (interface, dědičnost, standardní interface)

D. Operační systémy

10. Problematika správy OS UNIX (uživatelé, skupiny, práva, řízení procesů, signály)
11. Základy práce se shellem (druhy shellů, základní příkazy pro správu adresářů a souborů, zpracování textů, grep)

E. Databázové systémy

12. Konceptuální a logický návrh databáze (entity, relační vztahy, normalizace)
13. Příkaz SELECT (JOIN, selekce, projekce, ORDER BY, seskupování)

F. Dependabilita informačních systémů

14. Odolnost informačních systémů proti závadám (odolnost proti závadám konkurenčních a spolupracujících souběžných systémů)
15. Samokontrola a samodiagnostika na systémové úrovni (diagnostický graf, diagnostické algoritmy, organizace samokontroly a samodiagnostiky)