

## 7ZBA1 – Teoretická informatika a matematika

Úvod do informatiky, Statistické zpracování dat, Matematika pro informatiky, Principy a algoritmy počítačové grafiky, Logika pro informatiky, Gramatiky a jazyky, Softcomputing.

1. Teorie formálních jazyků a automatů – konečné automaty a regulární jazyky, bezkontextové gramatiky a jazyky, zásobníkové automaty, Chomského hierarchie.
2. Vyčíslitelnost a složitost – problémy a jejich rozhodnutelnost, částečná rozhodnutelnost, nerozhodnutelné problémy, výpočetní modely (Turingův stroj – TS, RAM), deterministické TS a nedeterministické TS, časová a prostorová složitost, P-NP problém.
3. Data a práce s nimi, základní a výběrový soubor. Popisná statistika (rozdělení četností, charakteristiky polohy a variability).
4. Metody testování statistických hypotéz, hladina významnosti, chyba I. a II. typu.
5. Základní principy kombinatoriky, permutace, variace a kombinace. Binomická čísla.
6. Základy teorie grafů (reprezentace, klasifikace, typy grafů, skóre grafů). Podgrafy.
7. Barva v počítačové grafice, formalizace vnímání barev (achromatické světlo, barevné vjemy).
8. Základní úlohy zpracování rastrového obrazu, algoritmy rasterizace úsečky a elipsy. Vyplňovací algoritmy.
9. Výroková logika – syntaxe, sémantika, normální formy, splnitelnost a platnost. Dedukce.
10. Predikátová logika – syntaxe, sémantika, splnitelnost, platnost. Dedukce.
11. Syntaktická analýza bezkontextových jazyků – LL a LR gramatiky a jazyky. Metoda rozkladových tabulek. FIRST a FOLLOW množiny. Vlastnosti LL a LR jazyků.
12. Úvod do problematiky strojového učení. Vybrané a přírodou inspirované metody UI.
13. Základní pojmy, principy a aplikace evolučních výpočetních technik.

## 7ZBA2 – Programování a operační systémy

Základy algoritmizace, Algoritmy a datové struktury, Architektura počítačů a základy OS, Počítačové sítě, Operační systémy, Objektově orientované programování, Bezpečnost provozu IT struktury, Úvod do databází.

1. Datové struktury a jejich aplikace
  - a. Typy a charakteristika datových struktur (pole, spojové seznamy, tabulky, stromy). Prohledávání a práce s daty v datových strukturách.
  - b. Využití datových struktur v operačních systémech, databázích, grafice apod.
  - c. Implementace datových struktur objektově orientovaným přístupem.
  - d. Implementace datových struktur v knihovnách objektově orientovaných tříd.
  - e. Praktický příklad vlastního využití vybrané datové struktury.
2. Síťový model TCP/IP, síťová architektura, aplikační a transportní vrstva
  - a. Pojmenujte a vysvětlete základní požadavky na síťovou architekturu a důležité parametry, které se vyhodnocují při využívání sítí.
  - b. Popište síťový model TCP/IP, jeho vrstvy, komunikaci mezi vrstvami, princip zapouzdřování, porovnejte tento model s referenčním modelem ISO/OSI a popište výhody a nevýhody.
  - c. Uveďte příklady konkrétních nejpoužívanějších protokolů pro jednotlivé vrstvy a popište jejich základní funkcionalitu (např. HTTP, SSH, DHCP).
  - d. Vysvětlete fungování protokolu DNS, smysl záznamů RR a koncept bezpečnosti DNS protokolu.

- e. Popište princip fungování elektronické pošty – hlavně protokoly SMTP, POP3 a formát e-mailových zpráv (MIME, S/MIME).
- f. Porovnejte fungování protokolů (spolehlivost, potvrzování přijatých paketů apod.) na transportní vrstvě a popište je.
3. Základy objektově orientované programování
  - a. Objektově orientované paradigma.
  - b. Základní přínosy objektově orientovaného přístupu a jejich aplikace (stabilita návrhu, znovu použitelnost, třída, objekt, jev, koncept).
  - c. Dědičnost a skládání objektů, praktické použití (výhody a nevýhody).
  - d. Knihovna tříd, rozhraní, implementace, praktické použití.
4. Návrh a využití objektově orientovaného přístupu
  - a. UML a jeho diagramy, diagram tříd, praktické využití.
  - b. Kompozice a agregace objektů, praktické použití.
  - c. Návrhové vzory a jejich použití (singleton, přepravka atd).
  - d. Polymorfismus, polymorfní objekt, příklad praktického využití.
5. Architektura operačních systémů a počítačových sítí
  - a. Základní typy a charakteristika operačních systémů, jejich vazba na počítačové sítě.
  - b. Hierarchická struktura operačních systémů.
  - c. Správa procesů (multitasking, multithreading).
  - d. Metody přidělování paměti procesům. Struktura paměťového prostoru procesu. Jejich vliv na použití dynamických proměnných v programech.
  - e. Souborové systémy (MS Windows, Linux).
6. Algoritmy
  - a. Charakterizujte základní vlastnosti algoritmů, jejich návrhu a zápis.
  - b. Srovnajte a charakterizujte algoritmy třídění a vyhledávání. Na praktických příkladech uveďte jejich nejvhodnější využití.
  - c. Rekurzivní algoritmy a jejich použití.
  - d. Implementace algoritmů v knihovnách (instanční a třídící metody).
7. Základní návrh sítě, síťová vrstva a vrstva síťového rozhraní modelu TCP/IP
  - a. Dostali jste za úkol navrhnout malou LAN s 8 počítači a připojit je k internetu.
  - b. Navrhněte vhodný IPv4 adresní plán s co nejmenším plýtváním IPv4 adres.
  - c. Popište protokol IPv4 a porovnejte ho s protokolem IPv6, který také popište. Vysvětlete princip fragmentace IP paketů a dual stacku.
  - d. Jaký linkový protokol použijete na vaší LAN? Porovnejte dostupné možnosti a popište je (minimálně Ethernet).
  - e. Jaký typ přenosového média/přenosových médií použijete na fyzické vrstvě? Porovnejte dostupné možnosti (kroucená dvojlinka, WLAN, optické kabely apod.)
  - f. Jak vyřešíte základní zabezpečení a dostupnost vaší sítě? Popište technologie jako NAT, firewall, směrovač, přepínač apod.
8. Bezpečnost IT infrastruktury
  - a. Analýza hrozeb. Typy útoků.
  - b. Ocenění rizik.
  - c. Úvod do aplikace kryptografie v moderních kryptosystémech.
  - d. Zabezpečení síťové infrastruktury.
9. Databázové modelování
  - a. Úrovně abstrakce při databázovém modelování (konceptuální model, datový model: relační, objektově-relační, objektový).
  - b. Nástroje pro databázové modelování, optimalizace návrhu relačních schémat.

- c. Jazyky pro definování struktury databáze, objekty databáze.
- d. Integritní omezení, nástroje pro zachování integrity a konzistence databáze.

## 7ZBAA – Aplikovaná informatika

Modelování datových struktur a návrhové vzory (%MDSN), Vývoj inteligentních systémů (%VINS), Informatika inteligentních domů (%INID), Kódování a šifrování (%KKDT), Analýza dat (%ANDT), Neuronové sítě (%NESI). Softwarové inženýrství (%SWI1).

Student losuje ze všech otázek, může však losovat znovu, pokud je vylosována otázka z předmětu, který neabsolvoval.

1. **%SWI1** – Komplexní životní cyklus vývoje software v souladu s agilními principy:
  - a. Jak má vypadat správná specifikace požadavků?
    - i. Možné oblasti diskuse: funkční a nefunkční požadavky, Use Case a User Story, IEEE 830, FURPS+
  - b. Jak můžeme využít UML při vývoji software?
    - i. Možné oblasti diskuse: sekvenční diagram, diagram tříd, diagram komponent, deployment diagram
  - c. Jaké architektury znáte? Jaké jsou základní stavební prvky?
    - i. Možné oblasti diskuse: globální architektura a dílčí architektury, komponenty, konektory, rozhraní, adaptér
2. **%SWI1** – Dobré praktiky při vývoji software a zajištění kvality
  - a. Co to jsou CASE nástroje a jak nám pomáhají při vývoji?
    - i. Možné oblasti diskuse: členění nástrojů, příklady použití CASE nástrojů při programování
  - b. Na jaké úrovni máme testovat software?
    - i. Možné oblasti diskuse: unitové, integrační a akceptační testování, test case a test script
  - c. Jaké problémy musíte řešit při zajištění kvality webových aplikací?
    - i. Možné oblasti diskuse: mockování objektů, selenium, headless testování, testování SPA aplikací
3. **%MDSN** – Konceptuální schéma s využitím metodiky objektových rolí. Omezení pro jedinečnost. Povinné role. Hodnota, množinové porovnání, omezení podtypů.
4. **%MDSN** – Vzory pro datové modely (temporální aspekty, typy kolekcí). Modelování podniku (strany, zaměstnanci, organizace, adresy, struktura organizace, typy).
5. **%VINS** – Vybraná praktická aplikace vývoje inteligentních systémů
  - a. představte řešené téma projektu/semestrální práce zapadající do tématu inteligentních systémů (nemusí být nutně z předmětu %VINS). Diskuse:
    - i. co bylo cílem, jak daná problematika zapadá do tématu inteligentních systémů?
    - ii. co bylo motivací, jaký problém byl řešen, postup řešení?
    - iii. co se podařilo a co nepodařilo?
    - iv. jaké technologie, techniky, nástroje, metody byly použity?
    - v. jaké byly využity znalosti a dovednosti?
    - vi. co bylo výstupem projektu, lze na téma navázat?
6. **%INID** – Chytré domy a jejich součásti
  - a. Filozofie chytrých domů, jejich kategorie.
    - i. Možné oblasti diskuse: Co je a není chytrý dům, v jakých oblastech může být dům chytrý a co ovlivní chytrost domu (např. řízení, návrh, konstrukce, komunikace atd.). Kategorie chytrých domů dle Harpera/Valeše.

- b. Prvky chytrých domů a jejich funkce
  - i. Možné oblasti diskuse: kategorie/typy prvků (zejména ale nejen – snímací, řídicí a akční prvky), další kategorie a jejich kritérium klasifikace, příslušnost prvků do více kategorií.
- 7. **%INID** – výměna informací v chytrém domě, projekt chytrého domu.
  - a. Integrace prvků chytrého domu, komunikační protokoly.
    - i. Možné oblasti diskuse: proč je nutné, aby spolu prvky komunikovaly a co tím získáme, pokročilé scénáře zahrnující spolupráci více prvků (subsystémů), prostředky pro komunikaci (HW i SW).
  - b. Návrh a implementace. Projektová dokumentace.
    - i. Možné oblasti diskuse: Co předchází implementaci chytrého domu u zákazníka? Jaké profese lze nalézt v celém procesu? Co může být součástí projektové dokumentace chytrého domu?
- 8. **%KKDT** – Informace a její kódování. Vysvětlete pojmy informace, zpráva, entropie, redundance, kód, prefixový kód, blokový kód. Vysvětlete Huffmanovo kódování a Hammingovu vzdálenost.
- 9. **%KKDT** – Komprese a identifikátory. Porovnejte a vysvětlete bezztrátovou a ztrátovou kompresi, uveďte příklady a vysvětlete pojmy kompresní poměr a kompresní faktor. Vysvětlete smysl identifikátorů a demonstруйте jejich využití na konkrétních příkladech.
- 10. **%ANDT** – Základy analýzy rozptylu (rozklad součtu čtverců, jednoduché třídění a mnohonásobná porovnání). Vztah dvou veličin (regrese a korelace).
- 11. **%ANDT** – Neparametrické metody: kontingenční tabulky, test nezávislosti, znaménkový test, Wilcoxonův dvouvýběrový test, Kruskalův-Walisův test.
- 12. **%NESI** – Jednovrstvé sítě (perceptron, Adaline), proces učení. Vícevrstvé sítě (algoritmus zpětného šíření).
- 13. **%NESI** – Řešení optimalizačních problémů neuronovými sítěmi. Rekurentní neuronové sítě, hluboké neuronové sítě.
- 14. **%GZAV** – Základy počítačového vidění a jeho moderními aplikace (např. detekce hran, matematická morfologie, filtrování obrazu, strojové učení).

## 7ZBA1 – Teoretická informatika a matematika

Úvod do informatiky, Statistické zpracování dat, Matematika pro informatiky, Principy a algoritmy počítačové grafiky.

1. Teorie formálních jazyků a automatů – konečné automaty a regulární jazyky, bezkontextové gramatiky a jazyky, zásobníkové automaty, Chomského hierarchie.
2. Vyčíslitelnost a složitost – problémy a jejich rozhodnutelnost, částečná rozhodnutelnost, nerozhodnutelné problémy, výpočetní modely (Turingův stroj – TS, RAM), deterministické TS a nedeterministické TS, časová a prostorová složitost, P-NP problém.
3. Data a práce s nimi, základní a výběrový soubor. Popisná statistika (rozdělení četností, charakteristiky polohy a variability).
4. Metody testování statistických hypotéz, hladina významnosti, chyba I. a II. typu.
5. Základní principy kombinatoriky, permutace, variace a kombinace. Binomická čísla.
6. Základy teorie grafů (reprezentace, klasifikace, typy grafů, skóre grafů). Podgrafy.
7. Barva v počítačové grafice, formalizace vnímání barev (achromatické světlo, barevné vjemy).
8. Základní úlohy zpracování rastrového obrazu, algoritmy rasterizace úsečky a elipsy. Vyplňovací algoritmy.

## 7ZBA2 – Programování a operační systémy

Základy algoritmizace, Algoritmy a datové struktury, Architektura počítačů a základy OS, Počítačové sítě, Operační systémy, Objektově orientované programování, Bezpečnost provozu IT struktury, Úvod do databází.

1. Datové struktury a jejich aplikace
  - a. Typy a charakteristika datových struktur (pole, spojové seznamy, tabulky, stromy). Prohledávání a práce s daty v datových strukturách.
  - b. Využití datových struktur v operačních systémech, databázích, grafice apod.
  - c. Implementace datových struktur objektově orientovaným přístupem.
  - d. Implementace datových struktur v knihovnách objektově orientovaných tříd.
  - e. Praktický příklad vlastního využití vybrané datové struktury.
2. Síťový model TCP/IP, síťová architektura, aplikační a transportní vrstva
  - a. Pojmenujte a vysvětlete základní požadavky na síťovou architekturu a důležité parametry, které se vyhodnocují při využívání sítí.
  - b. Popište síťový model TCP/IP, jeho vrstvy, komunikaci mezi vrstvami, princip zapouzdřování, porovnejte tento model s referenčním modelem ISO/OSI a popište výhody a nevýhody.
  - c. Uveďte příklady konkrétních nejpoužívanějších protokolů pro jednotlivé vrstvy a popište jejich základní funkcionalitu (např. HTTP, SSH, DHCP).
  - d. Vysvětlete fungování protokolu DNS, smysl záznamů RR a koncept bezpečnosti DNS protokolu.
  - e. Popište princip fungování elektronické pošty – hlavně protokoly SMTP, POP3 a formát e-mailových zpráv (MIME, S/MIME).
  - f. Porovnejte fungování protokolů (spolehlivost, potvrzování přijatých paketů apod.) na transportní vrstvě a popište je.
3. Základy objektově orientované programování
  - a. Objektově orientované paradigma.

- b. Základní přínosy objektově orientovaného přístupu a jejich aplikace (stabilita návrhu, znovu použitelnost, třída, objekt, jev, koncept).
    - c. Dědičnost a skládání objektů, praktické použití (výhody a nevýhody).
    - d. Knihovna tříd, rozhraní, implementace, praktické použití.
  4. Návrh a využití objektově orientovaného přístupu
    - a. UML a jeho diagramy, diagram tříd, praktické využití.
    - b. Kompozice a agregace objektů, praktické použití.
    - c. Návrhové vzory a jejich použití (singleton, přepravka atd).
    - d. Polymorfismus, polymorfní objekt, příklad praktického využití.
  5. Architektura operačních systémů a počítačových sítí
    - a. Základní typy a charakteristika operačních systémů, jejich vazba na počítačové sítě.
    - b. Hierarchická struktura operačních systémů.
    - c. Správa procesů (multitasking, multithreading).
    - d. Metody přidělování paměti procesům. Struktura paměťového prostoru procesu. Jejich vliv na použití dynamických proměnných v programech.
    - e. Souborové systémy (MS Windows, Linux).
  6. Algoritmy
    - a. Charakterizujte základní vlastnosti algoritmů, jejich návrhu a zápis.
    - b. Srovnajte a charakterizujte algoritmy třídění a vyhledávání. Na praktických příkladech uveďte jejich nejvhodnější využití.
    - c. Rekurzivní algoritmy a jejich použití.
    - d. Implementace algoritmů v knihovnách (instanční a třídící metody).
  7. Základní návrh sítě, síťová vrstva a vrstva síťového rozhraní modelu TCP/IP
    - a. Dostali jste za úkol navrhnout malou LAN s 8 počítači a připojit je k internetu.
    - b. Navrhněte vhodný IPv4 adresní plán s co nejmenším plýtváním IPv4 adres.
    - c. Popište protokol IPv4 a porovnejte ho s protokolem IPv6, který taktéž popište. Vysvětlete princip fragmentace IP paketů a dual stacku.
    - d. Jaký linkový protokol použijete na vaší LAN? Porovnejte dostupné možnosti a popište je (minimálně Ethernet).
    - e. Jaký typ přenosového média/přenosových médií použijete na fyzické vrstvě? Porovnejte dostupné možnosti (kroucená dvojlinka, WLAN, optické kabely apod.)
    - f. Jak vyřešíte základní zabezpečení a dostupnost vaší sítě? Popište technologie jako NAT, firewall, směrovač, přepínač apod.
  8. Bezpečnost IT infrastruktury
    - a. Analýza hrozeb. Typy útoků.
    - b. Ocenění rizik.
    - c. Úvod do aplikace kryptografie v moderních kryptosystémech.
    - d. Zabezpečení síťové infrastruktury.
  9. Databázové modelování
    - a. Úrovně abstrakce při databázovém modelování (konceptuální model, datový model: relační, objektově-relační, objektový).
    - b. Nástroje pro databázové modelování, optimalizace návrhu relačních schémat.
    - c. Jazyky pro definování struktury databáze, objekty databáze.
    - d. Integritní omezení, nástroje pro zachování integrity a konzistence databáze.

## 7ZBAS – Softwarové systémy

Databázové systémy (%DBS2), Unixové systémy (%UNS1, %UNS2), Softwarové inženýrství (%SWI1, %SWI2), Techniky testování a ladění aplikací (%TETL), Vývoj mobilních (%PRMA), web-backendových (%VBAP) a web-frontendových aplikací (%VFAP), Modelování datových struktur a návrhové vzory (%MDSN), Vývoj inteligentních systémů (%VINS), Informatika inteligentních domů (%INID).

Student losuje ze všech otázek, může však losovat znovu, pokud je vylosována otázka z předmětu, který neabsolvoval.

1. **%DBS2** – Správa instance a struktur databázových úložišť, správa uživatelů a jejich práv, recovery postupy a migrace databází.
2. **%DBS2** – Definice datových skladů a jejich vztah k produkčním databázím, vytváření datového skladu (ETL). Multidimenzionální modely, OLAP.
3. **%UNS1** – Prostředí UNIX a Linux, prostředí shellu, uživatelé, skupiny. Souborové systémy, přístupová práva a atributy, NTP, Cron, procesy, iptables.
4. **%UNS2** – Hostování virtualizace a host ve virtualizaci. Kompilace OS ze zdrojových kódů. Monitoring operačních systémů.
5. **%SWI1** – Komplexní životní cyklus vývoje software v souladu s agilními principy:
  - a. Jak má vypadat správná specifikace požadavků?
    - i. Možné oblasti diskuse: funkční a nefunkční požadavky, Use Case a User Story, IEEE 830, FURPS+
  - b. Jak můžeme využít UML při vývoji software?
    - i. Možné oblasti diskuse: sekvenční diagram, diagram tříd, diagram komponent, deployment diagram
  - c. Jaké architektury znáte? Jaké jsou základní stavební prvky?
    - i. Možné oblasti diskuse: globální architektura a dílčí architektury, komponenty, konektory, rozhraní, adaptér
6. **%SWI1** – Dobré praktiky při vývoji software a zajištění kvality
  - a. Co to jsou CASE nástroje a jak nám pomáhají při vývoji?
    - i. Možné oblasti diskuse: členění nástrojů, příklady použití CASE nástrojů při programování
  - b. Na jaké úrovni máme testovat software?
    - i. Možné oblasti diskuse: unitové, integrační a akceptační testování, test case a test script
  - c. Jaké problémy musíte řešit při zajištění kvality webových aplikací?
    - i. Možné oblasti diskuse: mockování objektů, selenium, headless testování, testování SPA aplikací
7. **%SWI2** – Moderní softwarové architektury
  - a. Asynchronní komunikace
    - i. Možné oblasti diskuse: motivace pro použití asynchronní komunikace, model publisher/subscriber, Rabbit MQ
  - b. Architektury softwarových systémů
    - i. Možné oblasti diskuse: událostmi řízená architektura, space-based architektura, orchestration-driven architektura, microservices
8. **%SWI2** – Čistý kód a etický hacking
  - a. Proč psát čistý kód a jak takový čistý kód vypadá?
    - i. Možné oblasti diskuse: princip SOLID, jména pro metody, třídy a proměnné, komentáře, formátování kódu
  - b. Co to je etický hacking a jak ho lze provést?
    - i. Možné oblasti diskuse: footprinting, skenování sítě, metoda brute force, systémový hacking

9. **%TETL** – Základní techniky ladění aplikací (breakpoint, krokování, sledování proměnných) a možnosti jejich použití. Unitové testování, jeho vlastnosti a využití.
10. **%PRMA** – Charakteristika a struktura mobilních OS. Základní programovacího jazyka Swift nebo Objective-C.
11. **%VBAP** – Tvorba backendové aplikace
  - a. Proč dělíme aplikace na backend a frontend?
  - b. Základní koncepty u backendového vývoje.
    - i. Možné oblasti diskuse: MVC, REST, microservices, horizontální a funkční dekompozice, synchronní a asynchronní komunikace
  - c. Spring Boot a .NET Core
    - i. Možné oblasti diskuse: srovnání obou přístupů, výhody a nevýhody, způsob konfigurace, nasazení aplikace
12. **%VBAP** – Principy a zabezpečení enterprise aplikací
  - a. Enterprise aplikace
    - i. Možné oblasti diskuse: ORM, transakční zpracování v lokálním a distribuovaném prostředí, 12 faktorů pro cloudovou aplikaci, docker
  - b. Zabezpečení backendové aplikace
    - i. Možné oblasti diskuse: koncept single sign on, identity provider, Spring Security, JWT
13. **%VFAP** – Základní koncepty a zajištění kvality
  - a. Základní pojmy a ekosystém
    - i. Možné oblasti diskuse: klasická webová a SPA aplikace, asynchronní komunikace, ECMA, TypeScript, transpilery, bundlování, minifikace, uglify
  - b. Jak byste testovali SPA aplikaci?
    - i. Možné oblasti diskuse: Karma, Protractor, Jest, Jasmine
14. **%VFAP** – React a Angular
  - a. Jaké jsou rozdíly mezi frameworky React a Angular?
    - i. Možné oblasti diskuse: DOM a virtual DOM, způsob použití, imutabilita, správa stavu – Redux
  - b. Proč používat funkcionální programování u SPA?
    - i. Možné oblasti diskuse: jazyk Elm, výhody a nevýhody funkcionálního programování
15. **%MDSN** – Konceptuální schéma s využitím metodiky objektových rolí. Omezení pro jedinečnost. Povinné role. Hodnota, množinové porovnání, omezení podtypů.
16. **%MDSN** – Vzory pro datové modely (temporální aspekty, typy kolekcí). Modelování podniku (strany, zaměstnanci, organizace, adresy, struktura organizace, typy).
17. **%VINS** – Vybraná praktická aplikace vývoje inteligentních systémů
  - a. představte řešené téma projektu/semestrální práce zapadající do tématu inteligentních systémů (nemusí být nutně z předmětu %VINS). Diskuse:
    - i. co bylo cílem, jak daná problematika zapadá do tématu inteligentních systémů?
    - ii. co bylo motivací, jaký problém byl řešen, postup řešení?
    - iii. co se podařilo a co nepodařilo?
    - iv. jaké technologie, techniky, nástroje, metody byly použity?
    - v. jaké byly využity znalosti a dovednosti?
    - vi. co bylo výstupem projektu, lze na téma navázat?
18. **%INID** – Chytré domy a jejich součásti
  - a. Filozofie chytrých domů, jejich kategorie.



- i. Možné oblasti diskuse: Co je a není chytrý dům, v jakých oblastech může být dům chytrý a co ovlivní chytrost domu (např. řízení, návrh, konstrukce, komunikace atd.). Kategorie chytrých domů dle Harpera/Valeše.
  - b. Prvky chytrých domů a jejich funkce
    - i. Možné oblasti diskuse: kategorie/typy prvků (zejména ale nejen – snímací, řídicí a akční prvky), další kategorie a jejich kritérium klasifikace, příslušnost prvků do více kategorií.
- 19. **%INID** – výměna informací v chytrém domě, projekt chytrého domu.
  - a. Integrace prvků chytrého domu, komunikační protokoly.
    - i. Možné oblasti diskuse: proč je nutné, aby spolu prvky komunikovaly a co tím získáme, pokročilé scénáře zahrnující spolupráci více prvků (subsystémů), prostředky pro komunikaci (HW i SW).
  - b. Návrh a implementace. Projektová dokumentace.
    - i. Možné oblasti diskuse: Co předchází implementaci chytrého domu u zákazníka? Jaké profese lze nalézt v celém procesu? Co může být součástí projektové dokumentace chytrého domu?

## A. Teoretická informatika a matematika

1. Model a jazyk výrokové a predikátové logiky. Syntax jazyka, induktivní definice gramatiky jazyka, míry složitosti výrokové/predikátové formule.
2. Sémantika výrokové formule: valuace výrokových proměnných a interpretace formulí, interpretační pravidla, Booleovy funkce. Metody sémantické analýzy výrokové formule: tabulková metoda, tablová metoda, sémantický strom, Quineův algoritmus. Modely a logické důsledky. Normální formy výrokových formulí. Klauzulární forma formulí.
3. Sémantika jazyka predikátové logiky. Interpretace predikátové formule: struktura interpretace, valuace proměnných, interpretační pravidla. Splňování a pravdivost v predikátové logice. Normální formy predikátových formulí. Klauzulární tvar predikátové formule. Metody sémantické analýzy predikátové formule.
4. Dedukce ve výrokové a predikátové logice: modely a logické důsledky, teorie. Rozhodnutelnost splnitelnosti a platnosti výrokových a predikátových formulí. Rezoluční a tablová metoda rozhodování a jejich využití.
5. Formální jazyky a jejich využití v informatice. Základní pojmy teorie formálních jazyků. Konečné automaty – deterministický, nedeterministický, zobecněný nedeterministický. Ekvivalence automatů, redukce, homomorfismus. Uzávěrové vlastnosti třídy jazyků rozpoznatelných KA. Regulární jazyky. Regulární výrazy. Kleeneho věta. Nerodova věta a charakterizace jazyků rozpoznatelných konečným automatem pomocí pravých kongruencí. Algoritmy transformace regulárních výrazů na konečné automaty. Použití regulárních jazyků v praxi.
6. Bezkontextové gramatiky a jazyky, nevypouštějící gramatiky, redukované gramatiky. Regulární gramatiky. Lineární gramatiky. Normální formy. Kanonická odvození, derivační stromy. Věta o vkládání (tzv. pumping lemma). Zásobníkové automaty a jejich vztah k bezkontextovým jazykům. Determinismus vs. nedeterminismus. Uzávěrové vlastnosti třídy bezkontextových jazyků. Chomského hierarchie. Vztah gramatika-jazyk-automat v kontextu Chomského hierarchie. Využití bezkontextových jazyků v praxi.
7. Vyčísitelnost a rozhodnutelnost problémů, nerozhodnutelné problémy. Turingův stroj a turingovsky vyčísitelné funkce. Univerzální Turingův stroj. Determinismus vs. nedeterminismus.
8. Časová a prostorová složitost algoritmů. Odhady a třídy složitosti. Zvládnutelné a nezvládnutelné problémy. Příklady problémů a jejich odhady složitosti. Nedeterministický Turingův stroj a jeho časová složitost. P-NP problém a jeho důsledky.
9. Lineární algebra. Vektorové prostory: definice a příklady, lineární závislost vektorů, báze vektorového prostoru, lineární zobrazení vektorových prostorů, prostory se skalárním součinem. Matice a determinanty: definice a základní vlastnosti, algebra matic a determinantů, řešení soustavy lineárních algebraických rovnic.
10. Kombinatorika. Variace, permutace, kombinace, kombinatorické principy, kombinační čísla.
11. Logické funkce. Základní pojmy, logické formule, ekvivalence formulí, princip duality, rozklad logické funkce podle proměnných, funkcionální úplnost.
12. Teorie grafů. Pojem grafu, isomorfismus grafů, reprezentace grafu, souvislost grafu, podgrafy, eulerovské grafy.
13. Popisná statistika. Statistická data. Měření, veličiny, škály. Charakteristiky polohy, charakteristiky variability. Statistické grafy – sloupcový graf, histogram, krabicový graf, bodový graf – příklady užití. Softwarové prostředky pro statistické zpracování dat.

14. Pravděpodobnost a statistická indukce. Pravděpodobnost. Náhodná veličina. Distribuční funkce. Rozdělení diskrétní a spojitá. Rovnoměrné spojitě rozdělení a programové funkce pro generování pseudonáhodných čísel. Náhodný výběr. Bodové a intervalové odhady parametrů rozdělení.
15. Základy diferenciálního počtu. Spojitost funkce. Limita funkce. Derivace a její význam. Počítání derivací. Diferenciál funkce a jeho význam. Derivace vyšších řádů. Aplikace derivace.
16. Základy integrálního počtu. Primitivní funkce. Neurčitý integrál a jeho vlastnosti. Určitý integrál a jeho vlastnosti. Metody integrace. Aplikace určitého integrálu.
17. Informace a její kódování
  - Vysvětlete pojmy informace, zpráva, entropie, redundance, kód, prefixový kód, blokový kód.
  - Porovnejte smysl a využití nejkratších kódů (Huffmanovo kódování, Shannon-Fanovo kódování) s bezpečnostními kódy (lineární kódy, Hammingovy kódy).
  - Demonstrujte Hammingovu vzdálenost a minimální vzdálenost kódu v souvislosti se schopností určitého kódu objevovat a opravovat chyby.
  - Vysvětlete pojmy perfektní kód a informační poměr kódu.
  - Popište lineární kódy, smysl a příklady jejich využití – generující matice, kontrolní matice, syndrom, systematický kód, vlastnosti kódů. Vysvětlete výhody a smysl použití Hammingových kódů oproti ostatním lineárním kódům.
18. Kompresce a identifikátory
  - Porovnejte a vysvětlete bezztrátovou a ztrátovou kompresi.
  - K jednotlivým kategoriím bezztrátové/ztrátové komprese uveďte příklady kompresních algoritmů (LZW, PCX, RLE, Huffmanovo kódování, aritmetická komprese, JPEG), popište je, zhodnoťte jejich vlastnosti a navzájem je porovnejte.
  - Definujte a na příkladech použijte pojmy – kompresní poměr a kompresní faktor.
  - Vysvětlete smysl identifikátorů a demonstруйте jejich využití na konkrétních příkladech (číslo kreditní karty, ISBN, IBAN apod.).
19. Vysvětlete vybranou technologii softcomputingu (z následujícího seznamu) a ukažte její použití pro řešení aktuálních problémů:
  - Fuzzy logika: základní pojmy fuzzy logiky (fuzzy množiny, lingvistické proměnné, operace s fuzzy množinami, fuzzy pravidla).
  - Evoluční algoritmy: základní pojmy (fitness - kvalita jedince, křížení, mutace), princip řešení úloh evolučními algoritmy.
  - Neuronové sítě: základní pojmy (formální neuron, vnitřní potenciál, bias, přenosové funkce), topologie neuronových sítí principy adaptačních algoritmů (učení s učitelem, učení bez učitele).
20. Vysvětlete vybranou technologii z oblasti umělé inteligence (podle následujícího seznamu) a ukažte její použití pro řešení aktuálních problémů:
  - Řešení úloh a prohledávání stavového prostoru, informované a neinformované metody prohledávání, Algoritmus A-Star, Rozklad úlohy na podproblémy, plánovací systémy (GPS, STRIPS, PLANNER aj.).
  - Multiagentové systémy (MAS), základní pojmy: architektura agenta, základní rozdělení agentů, principy komunikace, kooperace a koordinace v MAS, aplikace MAS
  - Celulární automaty, modely umělého života, celulární automaty (hra Life, Wolframův celulární automat aj.), aplikace celulárních automatů

- Fraktály a deterministický chaos, atraktory, modely deterministického chaosu (logistická rovnice, Lorenzův atraktor, apod. Fraktály: základní vlastnosti, generování fraktálů (L- systémy, IFS, dynamické systémy), dimenze využití fraktálů a deterministického chaosu v praxi

## **B. Programování a operační systémy**

### **1. Datové struktury a jejich aplikace**

- Typy a charakteristika datových struktur (pole, spojové seznamy, tabulky, stromy). Prohledávání a práce s daty v datových strukturách.
- Využití datových struktur v operačních systémech, databázích, grafice apod.
- Implementace datových struktur objektivě orientovaným přístupem.
- Implementace datových struktur v knihovnách objektivě orientovaných tříd.
- Praktický příklad vlastního využití vybrané datové struktury.

### **2. Síťový model TCP/IP, síťová architektura, aplikační a transportní vrstva**

- Pojmenujte a vysvětlete základní požadavky na síťovou architekturu a důležité parametry, které se vyhodnocují při využívání sítí.
- Popište síťový model TCP/IP, jeho vrstvy, komunikaci mezi vrstvami, princip zapouzdřování, porovnejte tento model s referenčním modelem ISO/OSI a popište výhody a nevýhody.
- Uveďte příklady konkrétních nejpoužívanějších protokolů pro jednotlivé vrstvy a popište jejich základní funkcionalitu (např. HTTP, SSH, DHCP).
- Vysvětlete fungování protokolu DNS, smysl záznamů RR a koncept bezpečnosti DNS protokolu.
- Popište princip fungování elektronické pošty – hlavně protokoly SMTP, POP3 a formát e-mailových zpráv (MIME, S/MIME).
- Porovnejte fungování protokolů (spolehlivost, potvrzování přijatých paketů apod.) na transportní vrstvě a popište je.

### **3. Základy objektivě orientované programování**

- Objektivě orientované paradigma.
- Základní přínosy objektivě orientovaného přístupu a jejich aplikace (stabilita návrhu, znovu použitelnost, třída, objekt, jev, koncept).
- Dědičnost a skládání objektů, praktické použití (výhody a nevýhody).
- Knihovna tříd, rozhraní, implementace, praktické použití.

### **4. Návrh a využití objektivě orientovaného přístupu**

- UML a jeho diagramy, diagram tříd, praktické využití.
- Kompozice a agregace objektů, praktické použití.
- Návrhové vzory a jejich použití (singleton, přepravka atd).
- Polymorfismus, polymorfní objekt, příklad praktického využití.

**5. Architektura operačních systémů a počítačových sítí**

- Základní typy a charakteristika operačních systémů, jejich vazba na počítačové sítě.
- Hierarchická struktura operačních systémů.
- Správa procesů (multitasking, multithreading).
- Metody přidělování paměti procesům. Struktura paměťového prostoru procesu. Jejich vliv na použití dynamických proměnných v programech.
- Souborové systémy (MS Windows, Linux).

**6. Algoritmy**

- Charakterizujte základní vlastnosti algoritmů, jejich návrhu a zápis.
- Srovnajte a charakterizujte algoritmy třídění a vyhledávání. Na praktických příkladech uveďte jejich nejvhodnější využití.
- Rekurzivní algoritmy a jejich použití.
- Implementace algoritmů v knihovnách (instanční a třídní metody).

**7. Základní návrh sítě, síťová vrstva a vrstva síťového rozhraní modelu TCP/IP**

- Dostali jste za úkol navrhnout malou LAN s 8 počítači a připojit je k internetu.
- Navrhněte vhodný IPv4 adresní plán s co nejmenším plýtváním IPv4 adres.
- Popište protokol IPv4 a porovnejte ho s protokolem IPv6, který taktéž popište. Vysvětlete princip fragmentace IP paketů a dual stacku.
- Jaký linkový protokol použijete na vaší LAN? Porovnejte dostupné možnosti a popište je (minimálně Ethernet).
- Jaký typ přenosového média/přenosových médií použijete na fyzické vrstvě? Porovnejte dostupné možnosti (kroucená dvojlinka, WLAN, optické kabely apod.)
- Jak vyřešíte základní zabezpečení a dostupnost vaší sítě? Popište technologie jako NAT, firewall, směrovač, přepínač apod.

## C. Aplikovaná informatika

### 1. Návrh schématu databáze

Úrovně abstrakce při databázovém modelování (konceptuální model, datový model: relační, objektově-relační, objektový), nástroje pro databázové modelování, optimalizace návrhu relačních schémat, jazyky pro definování struktury databáze, objekty databáze, integritní omezení, nástroje pro zachování integrity a konzistence databáze. Databázové triggery.

### 2. Získávání informací z databází

Teoretická východiska dotazovacích jazyků (relační algebra, relační kalkul), převod dotazu formulovaného v přirozeném jazyce do formálního jazyka, syntaktická a sémantická správnost dotazu, optimalizace dotazu, vyhodnocení dotazu a interpretace výsledků, komerční dotazovací jazyky. Jazyk SQL a jeho části (DDL, DML, DQL, DCL).

### 3. Fyzická implementace databází

Statické a dynamické organizace souborů a databází, primární soubory, pomocné datové struktury (indexy), implementace statických organizací (metoda kapes, statické hashování, hustý a řídký index) a dynamických organizací (B-stromy, rozšiřitelné hashování), metody redukce dat. Transakce: zotavení z chyb, synchronizace.

### 4. Reprezentace, úprava a komprimace rastrového obrazu v počítačové grafice.

Pojmy pixel, voxel. Rastrová mřížka. Projevy a způsob eliminace diskretizační chyby. Konvoluční metody při úpravě a analýze obrazu. Eliminace šumu v rastrovém obraze. Metody uchovávání rastrového obrazu. HW pro rastrovou grafiku.

### 5. Formalizace barevných vjemů a osvětlení v počítačové grafice.

Barva v kontextu možností HW: emulace šedých odstínů; aditivní a subtraktivní mechanismus generování barev. Grassmannovy zákony. Chromatický diagram a Maxwellův trojúhelník. Základní barevné modely. Phongův osvětlovací model. Lokální a globální osvětlení scény.

### 6. Reprezentace objektů a scén v počítačové grafice.

Model CSG. Parametrické vyjádření křivek na příkladu Bézierovy křivky. Základní myšlenka přechodu od parametrického vyjádření křivek k plochám. Polygonální reprezentace jako aproximace hladkých povrchů. HW pro vektorovou grafiku.

### 7. Vývoj software, testování a jeho automatizace

- Vysvětlete rozdíl mezi vodopádovým přístupem a iterativně inkrementálním způsobem vývoje software. Objasněte pojmy fáze, iterace, inkrement.
- Popište, jakým způsobem byste automatizovaně testovali zdrojový kód a uveďte vhodný příklad.
- V rámci procesu vývoje software doporučte vhodné použití CASE nástrojů.

### 8. Aplikace IS, softwarové architektury a UML

- Vyberte si libovolnou společnost a načrtněte architekturu podnikového systému. Do této architektury zařaďte pojmy ERP, CRM, SCM a objasněte jejich vazbu na podnikovou strategii.
- Definujte architekturu monolitickou, dvouvrstvou (Client/Server) a třívrstvou na konkrétním příkladu.
- Vyberte vhodné UML diagramy a zasaďte je do kontextu procesu vývoje software

**9. Podnikové procesy, implementace podnikových informačních systémů, Business Intelligence (BI)**

- Vyberte si libovolnou společnost a určete její podnikovou strategii.
- Vysvětlete pojem podnikový proces a jeho vztah k podnikové strategii, vyberte si jednoduchý proces (např. vystavení faktury) a graficky ho znázorněte.
- Popište, jakým způsobem byste měřili efektivitu podnikových procesů a informačního systému.
- Objasněte pojem BI a jeho vztah k architektuře podnikového systému, navrhněte řešení pro vytvoření báze dat, kterou bude BI používat.

**10. Testování statistických hypotéz**

Testování hypotéz, chyby testování, hladina významnosti, t-test, analýza rozptylu, neparametrické testy (test nezávislosti, znaménkový test).

**11. Analýza dat – lineární regrese**

Lineární regrese, regresní model, odhad parametrů modelu, předpoklady lineární regrese, index determinace, vztah regrese a korelace.



Státní závěrečná zkouška ve studijním programu Učitelství pro střední školy se skládá ze čtyř částí:

1. Státní závěrečná zkouška z prvního studijního oboru s didaktikou (Specializace 1).
2. Státní závěrečná zkouška z druhého studijního oboru s didaktikou (Specializace 2).
3. Státní závěrečná zkouška z Pedagogiky a psychologie.
4. Obhajoba diplomové práce.

Státnicové otázky z Informatiky (výsledkem je jedna známka):

**1. Oborově didaktická část povinná**

- a. Důležité dokumenty v práci učitele informatiky (RVP, ŠVP, Tematický plán). Výběr vhodného učiva pro výuku informatiky. Specifické postavení předmětu informatiky na ZŠ a SŠ. Moderní trendy ve výuce informatiky a informační gramotnosti.
- b. Výuka programování na ZŠ a SŠ. Moderní přístupy ve výuce algoritmizace a základů programování. Hardwarové a softwarové nástroje pro výuku algoritmizace a základů programování.
- c. Učebna výpočetní techniky. Hygienické a ergonomické požadavky. Řád počítačové učebny. Využití moderních hardwarových a softwarových prostředků ve výuce informatiky. Mobilní počítače a cloudové služby a jejich využití ve výuce.
- d. Didaktické testy ve výuce informatiky. Softwarové nástroje pro tvorbu didaktických testů. Zkoušení a hodnocení studentů. Zpětná vazba.
- e. Projektová výuka, informatické soutěže a práce s internetem ve výuce informatiky. Učebnice a didaktický software pro výuku informatiky.

**2. Oborově odborná část povinná**

- a. Disciplíny dle RUP – charakterizujte tyto disciplíny a uveďte nástroje a techniky obsažené v těchto disciplínách: Specifikace požadavků, Analýza a návrh, Testování.
- b. Disciplíny dle RUP – charakterizujte tyto disciplíny a uveďte nástroje a techniky obsažené v těchto disciplínách: Byznys modelování, Implementace, Deployment.
- c. Pedagogický výzkum a jeho etapy. Kvantitativně a kvalitativně orientovaný pedagogický výzkum. Proměnné pedagogického výzkumu.
- d. Výzkumné a statistické hypotézy. Metody kvantitativně a kvalitativně orientovaného pedagogického výzkumu.

**3. Povinně volitelná část (losuje se z absolvovaných předmětů)**

- a. 7ELEN – Základní pojmy, nástroje na tvorbu výukových materiálů pro eLearning, synchronní a asynchronní výuka.
- b. 7VYSO – Vzdělávání pomocí digitálních technologií, funkce a členění výukových programů. Výhody, nevýhody a rizika práce s digitálními technologiemi.
- c. 7PROJ – Projekt, projektové vyučování jako výuková metoda. ICT v projektovém vyučování. Nové informační technologie a jejich využití, druhy projektů, rozdělení projektů, vhodnost využití.
- d. 7VIMI – 1. Interaktivní tabule – základní ovládání, prezentační techniky. Výuka dynamické geometrie s využitím interaktivní tabule a přenosných zařízení. Software ve výuce informatiky na ZŠ a SŠ.
- e. 7FUMO – Základní pojmy teorie fuzzy relací. Fuzzy IF-THEN pravidla a princip jejich zpracování. Princip defuzzifikace, její druhy.

Státní závěrečné zkoušky pro navazující program Učitelství pro střední školy, 2021/2022  
(plán verze 2018)

- f. 7KOSB – Teorie informace, analýza zdroje informace, entropie. Kódování, typy kódů, optimální kódy, kódovací věty. Lineární kódy, Hammingovy kódy, opakovací kódy.
- g. 7NAVZ – Úvod do problematiky návrhových vzorů. Popis vybraného návrhového vzoru. Vzory v reálném světě.
- h. 7VYS1 – Problém a jeho definice. Vyčísitelnost, rozhodnutelnost, částečná rozhodnutelnost. Složitost – třídy složitosti.
- i. 7INF2 – Technologie – Charakterizujte technologie Java a .NET. Co mají společného? Jaké jsou výhody a nevýhody obou technologií? Proces – Vyjmenujte a charakterizujte metody vývoje software splňující Agile manifesto.
- j. 7RPR2 – Popište, jak funguje vývoj v týmu řízený SCRUMem. Jak přistupujeme k odhadům práce? Co je to retrospektiva a jak se provádí? Jak ohlídat kvalitu kódu.
- k. 7BESI – Analýza hrozeb, typy útoků, ocenění rizik. Úvod do aplikace kryptografie v moderních kryptosystémech. Zabezpečení síťové infrastruktury.
- l. 7MOSM – Definice: simulace, modelování, věc, systém, model. Fáze simulace. Spojitá vs. diskrétní simulace.
- m. 7ZNAI – Znalostní systémy – úvod. Reprezentace znalostí – informace, znalost. Pravidlové, nepravidlové a hybridní systémy.
- n. 7EXSY – Umělá inteligence a její přístupy, počítačová podpora rozhodování. Principy a teoretické zdroje expertních systémů. Struktury a funkce diagnostických a plánovacích expertních systémů

## A. Teoretická informatika

**Povinné předměty:** Vyčíslitelnost a složitost 1 a 2, Analýza vícerozměrných dat, Logika pro umělou inteligenci.

**Povinně volitelné předměty:** Expertní systémy, Analýza časových řad, Evoluční algoritmy a neuronové sítě.

1. Problémy a jejich algoritmická rozhodnutelnost a částečná rozhodnutelnost. Turingův stroj jako výpočetní model. Univerzální Turingův stroj. Nerozhodnutelné problémy, problém zastavení. Algoritmická převeditelnost problémů.
2. Časová a prostorová složitost algoritmů a Turingova stroje. Funkce a odhady složitosti. Třídy složitosti, zvládnutelné a nezvládnutelné problémy. Složitost nedeterministického Turingova stroje. NP-těžké a NP-úplné problémy. Polynomiální převeditelnost problémů. Příklady NP-úplných problémů.
3. Alternativní výpočetní modely a jejich vzájemná ekvivalence - Turingův stroj vs. model RAM a PL-vyčíslitelné funkce. Primitivně rekurzivní funkce, částečně rekurzivní funkce a jejich ekvivalence s Turingovsky vyčíslitelnými funkcemi.
4. Lineární regresní model. Odhad parametrů regresního modelu metodou nejmenších čtverců. Testy hypotéz o parametrech modelu. Posuzování vhodnosti regresního modelu, výběr vhodného regresního modelu. Zobecnění lineárního modelu. Logistická regrese.
5. Metody klasifikace (shluková analýza, diskriminační analýza – základní principy, oblast aplikace), metody redukce dimenze úlohy (analýza hlavních komponent – základní principy, oblast aplikace)
6. Hilbertovský axiomatický systém výrokové a predikátové logiky, jejich sémantická korektnost a úplnost.
7. Gentzenovský axiomatický systém výrokové a predikátové logiky, jejich sémantická korektnost a úplnost. Klauzulární axiomatický systém výrokové logiky.
8. Klauzulární logika. Syntax a sémantika. Báze znalostí, rezoluční odvozovací pravidlo v klauzulární logice. Problém unifikace. Přímé a nepřímé důkazy v klauzulární logice. Sémantická korektnost a úplnost.
9. Volitelná otázka 1
  - a) Expertní systémy  
Charakteristické vlastnosti a druhy expertních systémů. Fuzzy orientované expertní systémy. Zpracování neurčité informace. Základy fuzzy logiky.
  - b) Analýza časových řad  
Předpovědi časových řad, dekompozice časových řad, metody analýzy trendu, metody analýzy sezónní složky.
  - c) Evoluční algoritmy a neuronové sítě  
Evoluční algoritmy: základní pojmy (genotyp, fenotyp, fitness - kvalita jedince, křížení, mutace). Vysvětlete princip řešení úloh evolučními algoritmy na vybrané technologii: genetické algoritmy, diferenciální evoluce, genetické programování nebo PSO.
10. Volitelná otázka 2
  - a) Expertní systémy  
Reprezentace znalostí, báze znalostí. Řídicí mechanismy, aproximativní vyvozování. Fuzzy modely typu Mamdani a Takagi-Sugeno. Metody defuzzifikace.

- b) Analýza časových řad  
Stacionarita časových řad, Box-Jenkinsova metodologie, základní a sezónní procesy, fáze konstrukce B-J modelu.
- c) Evoluční algoritmy a neuronové sítě  
Neuronové sítě: základní pojmy, topologie neuronových sítí. Vysvětlete princip adaptačních algoritmů (trénovací množina, učení s učitelem, učení bez učitele) na vybraném modelu neuronové sítě: vícevrstvá neuronová síť s adaptačním algoritmem backpropagation, Kohonenovy samoorganizační mapy nebo použití evolučních technik při adaptaci neuronové sítě.

## B. Informační systémy a aplikace

**Povinné předměty:** Informační systémy 1, Informační systémy 2, Geometrické modelování v počítačové grafice, Modelování a simulace, Znalostní inženýrství.

**Povinně volitelné předměty:** Návrhové vzory, Bezpečnost informačních systémů.

1. Komplexní návrh informačního systému. Postupně projděte všechny disciplíny návrhu informačního systému dle procesního frameworku RUP a demonstруйте na vhodných příkladech použité formalismy a techniky.
2. Agilní přístupy a správa IT. Vysvětlete postupy vývoje software dle SCRUM, Extrémního programování, Feature-Driven development, Agile Unified Process a DSDM. Naznačte možné kombinace těchto postupů pro tvorbu vlastní metodiky, dejte do kontextu s Crystal Clear. Vyberte si a vysvětlete vhodnou metodu pro správu IT.
3. Architektury a technologie pro pokročilý vývoj informačních systémů
  - Popište všechny edice technologie Java (JavaCard, Java ME, Java SE, Java EE) a uveďte k nim příklady použití. Zaměřte se na webové technologie (Servlet, JSP, JDBC, EJB).
  - Popište všechny platformy .NET (Framework, Compact Framework, Micro Framework) a uveďte příklad jejich použití. Zaměřte se na součásti .NET Frameworku a vysvětlete jejich účel (zejména ASP.NET, LINQ, WCF).
  - Vysvětlete základní myšlenku webových služeb a uveďte, jakým způsobem byste ji implementovali v technologii Java či .NET.
  - Stručně vysvětlete, jak funguje technologie AJAX a uveďte jednoduchý příklad.
4. NURBS modely v geometrickém modelování. Hladkost – různé způsoby a nástroje na jejich vyjádření. Neuniformita a racionalita modelů.
5. Přístupy k 3D modelování objektů a jejich vizualizace. Povrchové a objemové modely, např. CSG modely, polygonální modely. Pojem Delaunay triangulace.
6. Podstata a definice simulace. Věc – systém – model. Fáze simulace. Diskrétní a spojitá číslicová simulace.
7. Simulační jádro. Algoritmizace diskrétních a spojitých simulačních modelů. Procesy a jejich stavy. Kalendář událostí.
8. Programové prostředky pro simulaci. Generování pseudonáhodných čísel. Modely hromadné obsluhy, Kendallova klasifikace.
9. Vysvětlete pojem reprezentace znalostí, její metody a zpracování znalostí v UI. Pravidlové a nepravidlové, hybridní systémy. Sémantické sítě a sémantický web. Formální ontologie a RDF model.
10. Navrhněte a popište znalostní systém. RETE algoritmus a systém typu tabule. Strojové učení, Dolování dat, Základní úlohy data miningu.
11. Volitelná otázka 1
  - a) Návrhové vzory  
Návrhový vzor Model-View-Controller problém, který vzor řeší. mechanismus šíření změn. Třídy a rozhraní v Javě pro tento vzor (Observable, Observer), Webová aplikace vzoru.

b) Bezpečnost informačních systémů

Uveďte příklady prakticky používaných bezpečnostních mechanismů na spodních 3 vrstvách modelu ISO/OSI a diskutujte jejich účinnost.

**12. Volitelná otázka 2**

a) Návrhové vzory

Návrhový vzor Jednoduchá továrna, Tovární metoda, Abstraktní továrna. Co vzor řeší a jaké jsou odlišnosti jednotlivých továren. Praktické uplatnění.

b) Bezpečnost informačních systémů

Uveďte příklady prakticky používaných bezpečnostních mechanismů na úrovni aplikační vrstvy a diskutujte jejich účinnost.

## C. Metody optimalizace a bezpečnost dat

**Povinné předměty:** Fuzzy modelování, Metody kódování, šifrování a bezpečnosti dat.

**Povinně volitelné předměty:** Inteligentní systémy, Úvod do lineárního programování a teorie her, Heuristické algoritmy optimalizace.

1. Základy teorie fuzzy množin, formalizace vágních pojmů. Fuzzy množinové operace, fuzzy relace. Operace t-normy a operace s-normy.
2. Fuzzy IF-THEN pravidla a princip jejich zpracování. Relační a logicko-jazyková interpretace. Evaluační jazykové výrazy. Defuzzifikace DEE.
3. Lineární kódy a hashovací funkce
  - Popište lineární cyklické kódy, jejich výhody, proces generování, zakódování, opravu, dekodování a možnosti jejich praktického využití.
  - Přibližte BCH kódy, jejich využití a možnost vytvořit BCH kódy s plánovanou vzdáleností. Vysvětlete, jaký je rozdíl mezi jednoduchými a shlukovými chybami vznikajícími při přenosu slova přenosovým kanálem.
  - Vysvětlete pojem hash, vyjmenujte a objasněte základní vlastnosti, které musí splnit hashovací funkce. Uveďte příklady nejznámějších hashovacích funkcí a popište je (např. MD5, SHA-2, SHA-256).
  - Popište konstrukci hashovacích funkcí (vysvětlete pojmy jako kompresní funkce, náhodné orákulum, zarovnání, Damgard-Merklovo zesílení apod.).
  - Vysvětlete náchylnost hashovacích funkcí na kolizi prvního a kolizi druhého druhu.
4. Šifrování dat
  - Vysvětlete rozdíl mezi kódováním a šifrováním, uveďte základní rozdělení šifrovacích algoritmů.
  - Porovnejte transpoziční a transkripční (monoalfabetické, polyalfabetické); blokové a proudové šifrovací systémy. Uveďte příklady konkrétních algoritmů a popište je.
  - Vysvětlete a porovnejte symetrické (AES) a asymetrické (Diffie-Hellman, RSA) šifrování, uveďte konkrétní příklady, popis konkrétních algoritmů a jejich výhody a nevýhody.
  - Popište využití elektronického podpisu v e-mailové zprávě a zašifrování e-mailové zprávy (PGP, S/MIME). Vysvětlete koncept hybridního kryptosystému.
  - Objasněte pojem digitální certifikát, jeho atributy, způsob vystavení, způsoby ověření jeho platnosti a způsoby revokace.
5. Volitelná otázka 1
  - a) Inteligentní systémy  
Inteligentní systémy, struktura inteligentního systému, inteligentní systémy v rámci umělé inteligence a umělého života.
  - b) Heuristické algoritmy a optimalizace  
Globální extrém, formulace problému globální optimalizace. Spojité a diskrétní problémy, vázaný extrém. Heuristické hledání globálního extrému. Evoluční algoritmy. Konvergence stochastických algoritmů.
6. Volitelná otázka 2
  - a) Inteligentní systémy  
Agenty a jejich architektury, inteligentní agent, multiagentové systémy.

b) Heuristické algoritmy a optimalizace

Adaptivní varianty algoritmu diferenciální evoluce. Hejnové a migrační algoritmy (např. SOMA). Testování a porovnání algoritmů. Diskrétní optimalizační problémy, problém obchodního cestujícího.