Sadržaj

1. Uvod **1**

1.1. Prvi susret s operacijskim sustavom 1
1.1.1. Zadaci operacijskog sustava 1
1.1.2. Odvijanje tipičnog posla u računalnom sustavu 2
1.2. Hijerarhijska izgradnja operacijskog sustava 4
1.3. Načini izučavanja operacijskih sustava 6

2. Model jednostavnog računala **9**

2.1. Von Neumannov model računala i načini njegova ostvarenja 9
2.1.1. Funkcijski model računala 9
2.1.2. Sabirnička građa računala 10
2.1.3. Radni ili središnji spremnik računala 11
2.1.4. Rudimentarno računalo, radni spremnik 13
2.1.5. Rudimentarno računalo – procesor 15
2.1.6. Brzina rada procesora, priručni spremnik 19
2.1.7. Instrukcijski skup procesora 20
2.2. Instrukcije za poziv potprograma i povratak iz potprograma 24
2.2.1. Načini razmjene podataka između potprograma i programa 28
2.2.2. Instrukcijska dretva 29
2.3. Računalni proces 30

3. Obavljanje ulazno-izlaznih operacija, prekidni rad **33**

3.1. Priključivanje ulazno-izlaznih naprava 33
3.2. Prenošenje pojedinačnih znakova, prekidni rad procesora 35
3.2.1. Prenošenje znakova radnim čekanjem 35
3.2.2. Prekidni način rada procesora 39
3.3. Podsustav za prihvat prekida 42
3.3.1. Najjednostavniji oblik podsustava za prihvaćanje više prekida 42
3.3.2. Podsustav za prihvat prekida razvrstanih po prioritetima s najjednostavnijim sklopovljem 44
3.3.3. Sklopovska potpora za ostvarenje višestrukog prekidanja 49
3.3.4. Prekidi generirani unutar procesora, poziv sustavskih potprograma 53
3.4. Prenošenje blokova znakova, sklopovi s neposrednim pristupom spremniku 54

3.5. Čvrsto povezani višeprocesorski sustav 56
3.6. Sabirnički sustavi stvarnih računala 59

4. Međusobno isključivanje u višedretvenim sustavima 61

4.1. Programi, procesi i dretve 61
4.2. Višedretveno ostvarenje zadataka, sustav podzadataka 62
4.2.1. Zadaci i podzadaci 62
4.2.2. Model višedretvenosti 64
4.2.3. Sustav dretvi 66
4.2.4. Međusobno isključivanje 68
4.2.5. Cikličke dretve 69
4.3. Ostvarenje međusobnog isključivanja dviju dretvi 69
4.3.1. Prvi pokušaj 70
4.3.2. Drugi pokušaj 73
4.3.3. Treći pokušaj 73
4.3.4. Četvrti pokušaj 74
4.3.5. Peti pokušaj 75
4.3.6. Šesti pokušaj – Dekkerov postupak 76
4.3.7. Petersonov postupak međusobnog isključivanja dviju dretvi 78
4.4. Međusobno isključivanje većeg broja dretvi – Lamportov protokol 80
4.5. Sklopovska potpora međusobnom isključivanju 83

5. Jezgra operacijskog sustava 89

5.1. Radno okruženje za izvođenje dretvi – jednostavni model jezgre 89
5.2. Struktura podataka jednostavnog modela jezgre – stanja dretvi 91
5.2.1. Lista postojećih dretvi, pasivno stanje 93
5.2.2. Aktivno stanje dretve 93
5.2.3. Pripravno stanje dretve, red pripravnih dretvi 93
5.2.4. Blokirana stanja dretvi 97
5.2.5. Prikaz mogućih stanja dretvi 100
5.3. Jezgrine funkcije 102
5.3.1. Ulazak u jezgru i izlazak iz jezgre 102
5.3.2. Funkcije za binarni semafor 103
5.3.3. Funkcije za opći semafor 106
5.3.4. Funkcije za ostvarivanje kašnjenja 109
5.3.5. Funkcije za obavljanje ulazno-izlaznih operacija 110

5.4. Ostvarenje jezgre u čvrsto povezanom višeprocesorskom sustavu 111
5.5. Objektni model jezgre operacijskog sustava 115

6. Međudretvena komunikacija i koncepcija monitora 117

6.1. Problem proizvodača i potrošača 117
6.1.1. Međudretvena komunikacija s pomoću neograničenog spremnika 118
6.1.2. Međudretvena komunikacija s pomoću ograničenog spremnika 121
6.1.3. Međudretvena komunikacija s pomoću reda poruka 123
6.1.4. Sinkronizacija dretvi 126
6.2. Potpuni zastoj 127
6.2.1. Uvjeti za nastajanje potpunog zastoja 128
6.3. Koncepcija monitora 133
6.3.1. Jezgrine funkcije za ostvarivanje monitora 134
6.3.2. Primjeri izgradnje monitora 137
6.3.3. Suvremenije ostvarenje monitora 142
6.4. Inverzija prioriteta 145
6.4.1. Mogući problemi pri sinkronizaciji dretvi 145
6.5. Izgradnja modernih operacijskih sustava 150

7. Analiza vremenskih svojstava računalnog sustava 157

7.1. Uvodna razmatranja 157
7.1.1. Periodni poslovi 161
7.2. Povezanost Poissonove i eksponencijalne razdiobe 163
7.2.1. Poissonova razdioba 163
7.2.2. Eksponencijalna razdioba i njezina veza s Poissonovom 167
7.3. Analiza sustava s Poissonovom razdiobom dolazaka i eksponencijalnom razdiobom trajanja obrade 169
7.4. Osnovni načini dodjeljivanja procesora dretvama 176
7.4.1. Dodjeljivanje po redu prispijeća 176
7.4.2. Kružno dodjeljivanje procesora 178

8. Gospodarenje spremničkim prostorom 187

8.1. Uvodna razmatranja 187
8.2. Osnovna svojstva magnetskih diskova 189
8.2.1. Organizacija zapisivanja sadržaja na disku 190
8.2.2. Vremenska svojstva diskova 193

8.2.3. Disk kao dopunski spremnik radnom spremniku 196
8.2.4. Procesni informacijski blok 198
8.3. Pregled razvitka načina dodjeljivanja radnog spremnika 199
8.3.1. Statičko raspoređivanje radnog spremnika 199
8.3.2. Dinamičko raspoređivanje radnog spremnika 202
8.3.3. Preklopni način uporabe radnog spremnika 209
8.4. Dodjeljivanje spremnika straničenjem 210
8.4.1. Sklopovska podloga straničenju 210
8.4.2. Opisnik virtualnog adresnog prostora 215
8.4.3. Priručni međuspremnik za prevođenje adresa 217
8.4.4. Straničenje na zahtjev 219
8.4.5. Strategije zamjene stranica 222
8.4.6. Teorijske strategije zamjene stranica 224
8.4.7. Praktične aproksimacije strategija zamjene stranica 227
8.4.8. Raspodjela okvira u višeprogramskom radu 229
8.4.9. Podjela okvira procesima 230
8.4.10. Radni skup 232
8.5. Zaključne napomene o gospodarenju spremničkim prostorom 234

9. Datotečni podsustav 241

9.1. Uloga datoteka u računalnim sustavima 241
9.2. Struktura datoteka 242
9.3. Smještanje datoteka na disku 245
9.4. Načela ostvarenja datotečnih funkcija 249
9.5. Metode posluživanja zahtjeva za pristup datotekama 252

10. Komunikacija između procesa 257

10.1. Komunikacija između procesa unutar istog računalnog sustava 257
10.1.1. Dijeljeni spremnički prostor 258
10.1.2. Razmjena poruka između procesa 259
10.2. Komunikacija između procesa u raspodijeljenim sustavima 260
10.2.1. Osnove umrežavanja 260
10.2.2. Struktura Interneta 262
10.2.3. Komunikacija između procesa 264
10.3. Međusobno isključivanje u raspodijeljenim sustavima 270
10.3.1. Međusobno isključivanje – osnovni mehanizam ostvarenja funkcija operacijskog sustava 270

10.3.2. Vremensko uređenje događaja u raspodijeljenim sustavima . . . 271
10.3.3. Protokoli međusobnog isključivanja u raspodijeljenim sustavima . . . 273
10.3.4. Protokol Ricarta i Agrawala . . . 275

11. Sigurnost računalnih sustava . . . 281

11.1. Uvod . . . 281
11.1.1. Uvodne napomene . . . 281
11.1.2. Vrste napada na sigurnost . . . 283
11.1.3. Sigurnosni zahtjevi . . . 285
11.1.4. Utjecaj pojedinih komponenti računalnih sustava na sigurnost . . . 286

11.2. Osnove kriptografije . . . 288

11.3. Simetrični kriptosustavi . . . 291
11.3.1. Data Encryption Standard (DES) . . . 292
11.3.2. Utrostručeni DES, 3DES . . . 293
11.3.3. Izbijeljeni DES, DESX . . . 293
11.3.4. Kriptosustav IDEA . . . 294
11.3.5. Napredni kriptosustav AES . . . 296

11.4. Načini kriptiranja . . . 301
11.4.1. Elektronička bilježnica . . . 301
11.4.2. Ulančavanje . . . 302
11.4.3. CFB i OFB načini kriptiranja . . . 303
11.4.4. Brojač . . . 304

11.5. Asimetrični kriptosustavi, sustavi s javnim ključem . . . 304
11.5.1. Neke činjenice i algoritmi iz teorije brojeva . . . 304
11.5.2. Asimetrični kriptosustav RSA . . . 309
11.5.3. Komuniciranje uporabom kriptosustava RSA . . . 310
11.5.4. Dobrota RSA kriptosustava . . . 312

11.6. Sažetak poruke, utvrđivanje besprijekornosti . . . 317
11.6.1. Digitalna omotnica . . . 317
11.6.2. Digitalni pečat . . . 319
11.6.3. Funkcije za izračunavanje sažetka, funkcije sažimanja . . . 320
11.6.4. Važna svojstva funkcija za izračunavanje sažetka poruke . . . 323

11.7. Sigurnosni protokoli . . . 324
11.7.1. Diffie-Hellmanov postupak za razmjenu tajnog ključa . . . 324
11.7.2. Raspodjela ključeva u zatvorenom simetričnom kriptosustavu . . . 327

11.7.3. Raspodjela ključeva u zatvorenom asimetričnom kriptosustavu . . . 333
11.7.4. Autentifikacija u zatvorenim sustavima . . . 336
11.8. Prijava za rad . . . 343
11.8.1. Kriptiranje lozinki . . . 343
11.8.2. Otežavanje pogađanja lozinke . . . 344
11.8.3. Zaštita pritupanja pojedinim sredstvima – autorizacija . . . 344
11.9. Autentifikacijski protokol Kerberos . . . 345
11.9.1. Struktura sustava u kojem djeluje Kerberos protokol . . . 346
11.9.2. Kerberos protokol . . . 347
11.10. Infrastruktura javnih ključeva . . . 350
11.10.1. Digitalni certifikat . . . 350
11.10.2. Provjera certifikata u otvorenoj mreži . . . 353
11.10.3. Infrastruktura javnih ključeva zasnovana na X.509 modelu . . . 356
11.10.4. Problem opozivanja certifikata . . . 359
11.11. Sigurnosna zaštitna stijena . . . 360
11.12. Zaključne napomene . . . 362

12. Višediskovni zalihosni spremnici . . . 365
12.1. Osnovna razmatranja . . . 365
12.2. Modeliranje zalihosnih sustava . . . 368
12.2.1. Pouzdanost i nepouzdanost sustava . . . 368
12.2.2. Model ponašanja popravljive komponente s konstantnim brzinama kvarenja i popravljanja . . . 375
12.2.3. Modeliranje višekomponentnih sustava . . . 378
12.3. Načini zalihosne organizacije diskova . . . 386
12.3.1. RAID 0 – nezalihosna organizacija . . . 387
12.3.2. RAID 1 – zrcaljena organizacija . . . 387
12.3.3. RAID 2 – organizacija zasnovana na Hammingovim kodovima . . . 388
12.3.4. RAID 3 – paritetna organizacija sitne zrnatosti . . . 389
12.3.5. RAID 4 – paritetna organizacija krupne zrnatosti . . . 389
12.3.6. RAID 5 – paritetna organizacija krupne zrnatosti s raspodijeljenim paritetnim pojasevima . . . 390
12.3.7. RAID 6 – organizacija sa zaštitom od dvostrukog kvara ($P + Q$ zalihost) . . . 391
12.3.8. Višerazinski RAID sustavi . . . 391

Literatura . . . 395

Kazalo pojmova . . . 397