

1. PROLOG; BEZBEDNOST, POJAM	1
2. BEZBEDNOST IS	5
2.1. Informacija – pojam	5
2.2. Informacije i poslovni sistem	7
2.3. Značaj bezbednosti za informacioni sistem	9
2.4. Pretnje i svest o postojanju pretnji, informatički rat	14
3. KLASIFIKACIJA NAPADA NA IS	16
3.1. Cilj formiranja klasifikacije napada na informacione sisteme	16
3.2. Klasifikacije napada na informacione sisteme	18
3.2.1. Lista termina	19
3.2.2. Kategorije rezultata	20
3.2.3. Matrica	20
3.2.4. Klasifikacije bazirane na procesima	20
3.2.5. Kombinovana klasifikacija napada na računarske sisteme	21
3.2.5.1. Napadači i njihovi ciljevi	21
3.2.5.2. Pristup	22
3.2.5.3. Rezultati	23
3.2.5.4. Alat	24
3.3. Primer klasifikacije napada na informacioni sistem	27
3.4. Neki karakteristični primeri napada na IS	30
3.4.1. Računarski virusi	30
3.4.2. Elektromagnetno zračenje računara	35
3.4.3. Kliper čip	37
4. MODELI BEZBEDNIH INFORMACIONIH SISTEMA	39
4.1. Strukturni model bezbednog informacionog sistema	39
4.1.1. Model	40
4.2. Primeri organizacionog modela bezbednog informacionog sistema	51
5. MERE KOJE ČINE BEZBEDNOST INFORMACIONOG SISTEMA	58
5.1. Humana sfera	60
5.1.1. Selekcija kadrova za rad u informacionim sistemima	62
5.1.2. Obezbeđenje optimalnih radnih uslova	64
5.1.3. Prevencija kriminala	71
5.1.4. Higijensko-tehnička zaštita	72
5.2. Normativna sfera	74
5.3. Organizaciona sfera	78
5.3.1. Preporučene mere zaštite	80
5.4. Sfera fizičke zaštite	84
5.4.1. Zaštita računarskog sistema	89
5.5. Zaštita softvera	93
5.5.1. Specifičnosti zaštite softvera po vrstama	93
5.5.2. Zaštita softvera od kvarenja, uništenja i gubljenja	94
5.5.2.1. Zaštita softvera skladištenjem	94
5.5.2.2. Održavanje softvera	95
5.5.3. Zaštita softvera od neovlašćenog korišćenja	97
5.5.3.1. Patentno pravo	97
5.5.3.2. Pravo na kopiranje softvera	98

5.5.3.3. Zaštita softvera primenom zaštitnog znaka	100
5.5.3.4. Zakonska zaštita softvera	100
5.5.4. Zaštita od neispravnog i malignog softvera	101
5.5.4.1. Razvoj pouzdanog softvera	101
5.5.5. Zaštita sistemске dokumentacije	104
5.6. Zaštita (rezidentnih) podataka	105
5.6.1. Zaštita podataka kalsifikacijom	105
5.6.2. Raspoloživi resursi kao faktor zaštite podataka	105
5.6.3. Mere zaštite rezidentnih podataka	107
5.6.3.1. Zaštita opreme i medijuma	109
5.7. Zaštita infrastrukture	111
5.7.1. Zaštita računarskog sistema kao dela infrastrukture IS	111
5.7.1.1. Nabavka računarske opreme	111
5.7.1.2. Održavanje računarske opreme	114
5.7.2. Zaštita ostalih sistema kao infrastrukture IS	118
5.8. Protivpožarna zaštita	121
5.8.1. Područja požara	122
5.8.2. Protivpožarna preventiva	122
5.8.3. Uređaji za otkrivanje požara	123
5.8.4. Sredstva za gašenje požara	124
5.8.5. Prva pomoć stradalim u požaru	124
5.8.6. Sanacija posle požara	124
5.9. Zaštita IS u radu u mrežnom okruženju	126
5.9.1. Neki tipovi napada u distribuiranim računarskim sistemima	126
5.9.2. Višeslojna arhitektura sistema zaštite računarskih mreža	129
5.9.2.1. Zaštita na transportnom nivou – SSL protokol	131
6. KRIPTOZAŠTITNA SFERA	134
6.1. Definicija osnovnih kriptografskih pojmova	134
6.2. Ocena kvaliteta kriptografskog postupka	136
6.3. Kriptoanaliza	137
6.4. Kriptografske tehnike zaštite podataka	140
6.4.1. Savremeni simetrični kriptografski algoritmi	141
6.4.1.1. Blok šifarski sistemi	142
6.4.1.1.1. Kriptografski modovi blok simetričnih sistema	142
6.4.1.1.1.1. Mod elektronske kodne knjige	142
6.4.1.1.1.2. Mod ulančavanja blokova	143
6.4.1.1.1.3. Mod povratnog šifrovanja	143
6.4.1.1.1.4. Izlazni povratni mod	144
6.4.1.1.1.5. Izbor odgovarajućeg kriptografskog moda	144
6.4.1.1.2. IDEA algoritam	145
6.4.2. Asimetrični kriptografski algoritmi	147
6.4.2.1. RSA algoritam	147
6.4.2.1.1. Matematička osnova RSA algoritma	147
6.4.2.1.2. Analiza sigurnosti RSA algoritma	149
6.4.3. Digitalni potpis i PKI sistemi	149
6.4.3.1. Tehnologija digitalnog potpisa	149
6.4.3.1.1. Kriptografske funkcije za kontrolu integriteta podataka	150
6.4.3.1.1.1. MD5 algoritam	151
6.4.3.1.2. PKCS#1 standard	153

6.4.3.2. Infrastruktura sistema sa javnim ključevima.....	155
6.4.3.2.1. Digitalni sertifikati	156
6.4.3.2.2. Sertifikacioni autoritet	158
6.4.3.2.3. Liste opozvanih digitalnih sertifikata	159
Spisak skraćenica uz glavu 6.....	161
7. INTERNET BEZBEDNOST	162
7.1. Poboljšanje Internet bezbenosti.....	162
7.1.1. Preporučene akcije.....	162
7.1.1.1. Preporuke za Internet korisnike	162
7.1.1.2. Dopunske preporuke za komercijalne Internet korisnike	163
7.1.1.3. Preporuke za provajdere	163
7.1.1.4. Preporuke za vladu.....	163
7.1.1.5. Preporuke za timove odgovorne za Internet.....	163
7.1.1.6. Preporuke za CERT®/CC:	163
7.2. Zašto nisu dostupne sveobuhvatne informacije o Internet incidentima.....	164
7.3. Preporuke	164
7.4. Zaključak – za vladine organe.....	165
7.5. Primer Internet bezbednosti u američkoj ratnoj mornarici.....	166
8. REAGOVANJE NA INCIDENTE.....	172
8.1. Metodologija za opis scenarija potencijalnih incidentnih situacija	172
8.2. Scenariji po kojima se odgovara u procesu sprečavanja napada.....	178
8.3. Korektivne aktivnosti kojim se otklanjaju posledice napada	179
9. VERIFIKACIJA BEZBEDNOSNOG INFORMACIONOG SISTEMA.....	184
10. ZAKLJUČAK	189
LITERATURA	191
SADRŽAJ	196