

S A D R Ž A J

1. UVOD.....	4
2. SAVREMENE RAČUNARSKE MREŽE, INFORMACIONI SISTEMI I SISTEMI ZAŠTITE	5
2.1. Savremene računarske mreže i TCP/IP protokol	5
2.2. Trendovi u sistemima zaštite računarskih sistema	6
2.3. Potencijalni napadi na računarske mreže bazirane na internetu i mogući načini odbrane.....	9
2.4. Primeri napada na savremene računarske mreže	10
2.4.1. Krađa identiteta phishing.....	11
2.4.2. Prisluškivanje.....	12
2.4.3. Modifikacija podataka.....	12
2.4.4. Identity spoofing (IP address spoofing).....	12
2.4.5. Napadi na lozinke.....	12
2.4.6. Denial-of-service napad	13
2.4.7. Man-in-the-middle napad	13
2.4.8. Napad kompromitacije ključa	14
2.4.9. Sniffer napad	14
2.4.10. Napad na aplikativnom nivou	14
3. KRIPTOGRAFSKI ASPEKTI ZAŠTITE RAČUNARSKIH MREŽA	15
3.1. Simetrični kriptografski algoritmi	15
3.1.1. Blok šifarski sistemi	16
3.1.2. Sekvencijalni šifarski sistemi	17
3.2. Asimetrični kriptografski algoritmi	21
3.2.1. PKCS#1 standard	21
3.2.2. RSA algoritam.....	24
3.3. Hash algoritmi	25
3.3.1. MD5 Message digest algoritam	26
3.3.2. SHA-1 algoritam	27
3.4. Primena kriptografskih algoritama u informacionim sistemima	29
4. INFRASTRUKTURA SA JAVNIM KLJUČEVIMA – PKI	30
4.1. PKI Komponente.....	31
4.1.1. Sertifikaciono telo	31
4.1.2. Registraciono telo	32
4.1.3. Repozitorij	32
4.1.4. Krajnji entiteti	32

4.2. Digitalni sertifikati, struktura i standardi	32
5. VIŠESLOJNA ARHITEKTURA SISTEMA ZAŠTITE SAVREMENIH RAČUNARSKIH MREŽA	34
5.1. Kriptografska zaštita na aplikativnom nivou.....	34
5.2. Zaštita tajnosti na transportnom nivou	35
5.3. Zaštita na mrežnom nivou	36
6. VIRTUELNE PRIVATNE MREŽE VPN – NA MREŽNOM NIVOU	36
6.1. Tehnologija tunelovanja	39
6.2. Klasifikacija virtuelnih privatnih mreža	39
6.3. IP SECURITY	40
6.4. Osnovni IPsec protokoli	41
6.5. IPsec modovi: Transportni i Tunel mod	43
6.5.1 Transportni mod.....	43
6.5.2 Tunel mod.....	43
6.6. Pomoćne IPsec komponente	43
6.7. Dodatni mehanizmi zaštite na mrežnom nivou	44
6.7.1 VPN i Firewall	45
7. ZAKLJUČAK	46
8. LITERATURA.....	48
9. SKRAĆENICE.....	49