

1. UVOD

Sveopšta umreženost postala je stvarnost i računarski sistemi se koriste u svim sferama ljudske delatnosti. Briga o informacionoj bezbednosti postaje nužnost u poslovnoj politici svake organizacije. Informacija je imovina i kao takvu ju je potrebno prikladno zaštititi, kako bi se omogućilo normalno poslovanje organizacije.

U ovom specijalističkom radu su opisani mehanizmi zaštite na mrežnom nivou u savremenim računarskim mrežama. Navedeni su potencijalni napadi na računarske mreže i mogući načini odbrane. Zatim su opisani kriptografski aspekti zaštite računarskih mreža (simetrični kriptografski algoritmi, asimetrični kriptografski algoritmi, hash algoritmi), te zaštita na mrežnom, transportnom i aplikativnom nivou.

Virtuelne privatne mreže *VPN* na mrežnom nivou zauzimaju posebnu ulogu u ovom radu te je detaljno opisana klasifikacija virtuelnih mreža, osnovni IPSec protokoli i modovi, IPSECURITY te pomoćne IPSec komponente i dodatni mehanizmi zaštite na mrežnom nivou.