1. UVOD

Enormna ekspanzija same upotrebe kompjutera tako i sve veće zloupotrebe istog posljednje decenije, privukla je moju pažnju za potpunijim razumijevanjem ovog tipa kriminaliteta sa mnogobrojnim modalitetima ispoljavanja. U današnjim uslovima života gotovo je nezamislivo nepoznavanje osnova rada na kompjuteru, koji je postao suveren vladar najvažnijih sfera kako društvenog tako i ekonomskog života. Sa obzirom na činjenicu da je način korišćenja kompjutera prilagođen znanju prosječnog čovjeka, povećana je opasnost od izvršenja krivičnih djela koja pripadaju komputerskom kriminalitetu. Opšte je poznato da gotovo svaki vid tehničko – tehnološkog dostignuća prije ili kasnije postaje predmet mnogobrojnih zloupotreba. Ono što naročito zabrinjava kada je riječ o kompjuterskom kriminalitetu jeste postojanje izuzetno velike „tamne brojke" kriminaliteta što je u neospornoj korelaciji sa neprijavljivanjima istog od strane žrtve ukoliko je u nanesena neznatna materijalna šteta, nedovoljnom obučenošću odgovornih lica za suzbijanje veoma raznolikih oblika ovog tipa kriminaliteta i izuzetno skupom tehnonologijom kao i visokom cijenom samih uređaja potrebnih za ostvarivanje ove radnje Internet kao najznačajniji svjetski medij omogućuje prenos informacija brzinom kojoj se ne može u većini slučajeva efikasno ući u trag. Iako se u javnost internet najčešće javlja kao „ubojito" sredstvo u rukama organizovanih kriminalnih grupa za izmijenjene metode i tehnike vršenja krivičnog djela terorizma, aktivnost na internetu od strane prosječnog građanina može ukazati na povećanu opreznost prilikom raznih vidova interakcije na „mreži" što se ne smije zanemariti imajući u vidu znatnu kako materijalnu tako i nematerijalnu štetu koja tom prilikom može nastati.

Računari i računarski sistemi su danas postali neophodni pratilac ljudskog života, ali i privrednog poslovanja, kao i djelatnosti državnh i drugih organa. Iako se radi o korisnim uređajima i sistemima za efikasno i kvalitetno funkcionisanje svake države, pa i međunarodnih odnosa, oni su podložni velikom riziku i izazovima od fizičkih i pravnih lica iz različitih razloga (motiva). Na bazi usvojenih međunarodnih dokumenata univerzalnog i regionalnog karaktera, najveći broj država, pa tako i Republika Srpska, u svom nacionalnom zakonodavstvu poznaju različite mehanizme zaštite i obezbjeđenja efikasnog, kvalitetnog i blagovremenog funkcionisanja računarskih sistema i računarskih

uređaja. Poseban segment ove zaštite čini pravna zaštita, u prvom redu krivičnopravna zaštita bezbjednosti računarskih sistema i podataka. Tako i zakonodavstvo Republike Srbije predviđa krivičnu odgovornost i kazne za više računarskih (kompjuterskih) krivičnih djela o čijim se karakteristikama sa teorijskog i praktičnog aspekta govori u ovom radu.