INFORMATION SECURITY

ZAŠTITA RAČUNARSKE BEZBEDNOSTI PUTEM KRIVIČNOG PRAVA

Miodrag N. Simović[1],
Dragan Jovašević[2],
Vladimir M. Simović

[1]Constitutional Court of BH,
Bosnia and Herzegovina;
[2]Pravni fakultet,
Niš, Serbia

Rezime:

Računari i računarski sistemi su danas postali neophodni pratilac ljudskog života, ali i privrednog poslovanja, kao i delatnosti 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 Srbija, u svom nacionalnom zakonodavstvu poznaju različite mehanizme zaštite i obezbeđenja efikasnog, kvalitetnog i blagovremenog funkcionisanja računarskih sistema i računarskih uređaja. Poseban segment ove zaštite čini pravna zaštita, u prvom redu krivičnopravna zaštita bezbednosti računarskih sistema. Tako i zakonodavstvo Republike Srbije predviđa krivičnu odgovornost i kazne za više računarskih (kompjuterskih) krivičnih dela o čijim se karakteristikama sa teorijskog i praktičnog aspekta govori u ovom radu.

Ključne reči:

računar, računarski sistemi, računarska bezbednost, krivično delo, odgovornost.

1. UVOD

Usvajanjem Zakona o izmenama i dopunama Krivičnog zakona Republike Srbije, aprila 2003. godine, na bazi međunarodnih standarda univerzalnog ili regionalnog karaktera, u sistem krivičnog prava Republike Srbije je po prvi put uvedeno više računarskih (kompjuterskih) krivičnih dela, te određena pravila o krivičnoj odgovornosti i kažnjavanju učinilaca ovih dela [9, pp. 351-361]. To je bio početak dizanja računarske bezbednosti na kvalitetno viši nivo. Naime, u novouvedenoj glavi 16a Krivičnog zakona Republike Srbije propisana je krivična odgovornost i sistem kazni i drugih krivičnih sankcija (mere bezbednosti) za specifična „krivična dela protiv bezbednosti računarskih podataka".

Time se i Republika Srbija priključila velikom broju savremenih država koje se na različite načine i različitim merama (u prvom redu sistemom preventivnih i represivnih mera) pokušavaju efikasno, blagovremeno, zakonito i kvalitetno suprotstaviti različitim oblicima i vidovima zloupotrebe računara u cilju ostvarenja protivpravne imovinske koristi za sebe ili drugo fizičko ili pravno lice, odnosno u cilju nanošenja (imovinske)

Correspondence:
Miodrag N. Simović

e-mail:
vlado_s@blic.net

DOI: 10.15308/Sinteza-2017-79-84

štete drugom licu ili radi povrede prava drugog lica, ili pak iz drugih nezakonitih motiva.

Konstituisanjem Republike Srbije kao samostalne i međunarodno priznate države, septembra 2005. godine, donet je danas važeći jedinstveni i sistematizovani kodeks svih krivičnopravnih normi materijalnopravnog karaktera – Krivični zakonik Republike Srbije (KZ). U glavi XXVII, pod nazivom „Krivična dela protiv bezbednosti računarskih podataka", KZ propisuje računarska krivična dela. Ovaj Zakonik počeo je da se primenjuje od 1. januara 2006. godine i do sada je imao više izmena i dopuna, uključujući i poslednje izmene iz novembra 2016. godine.

2. EVROPSKI STANDARDI ZAŠTITE RAČUNARSKE BEZBEDNOSTI

Savet Evrope je donošenjem Konvencije o kibernetičkom (sajber) kriminalu (Convention on Cybercrime, ETS 185) od 23. novembra 2001. godine [4, pp. 261-265] pokušao da postavi osnove jedinstvenog evropskog sistema materijalnog i procesnog krivičnog prava u oblasti neophodne saradnje država članica u suzbijanju različitih oblika i vidova računarskog (kibernetičkog) kriminala. Pri tome je sama Konvencija (čl. 2-13) propisala pet krivičnih dela ove vrste koja su upravljena protiv tajnosti, celovitosti i dostupnosti računarskih podataka i sistema. Ovim su postavljene osnove za pojedina nacionalna zakonodavstva da preciznije odrede obeležja i karakteristike pojedinih računarskih krivičnih dela, njihove osnovne, lakše ili teže oblike, te da propiše krivične sankcije za njihove učinioce (fizička ili pravna lica).

Uz ovu Konvenciju usvojen je i Dopunski protokol o kriminaliziranju akata rasističke i ksenofobične prirode koja su učinjena posredstvom računarskih sistema. I ovaj Protokol u čl. 3-7 propisuje takođe krivičnu odgovornost i kažnjivost za zloupotrebu računara u vršenju krivičnih dela iz rasističkih i ksenofobičnih pobuda (motiva).

Imajući u vidu utvrđene obaveze za države članice Saveta Evrope, bilo je logično očekivati da će i u domaćem krivičnom zakonodavstvu uslediti, prvo, na zakonodavnom planu, pa potom i u praksi efikasna, kvalitetna i zakonita borba sa računarskim kriminalitetom i njihovim izvršiocima [11, pp. 116-124].

Prihvatajući navedenu Konvenciju, Republika Srbija je izmenama i dopunama Krivičnog zakona Republike Srbije iz aprila 2003. godine u krivičnopravni sistem uvela više računarskih krivičnih dela u glavi 16a pod nazivom „Krivična dela protiv bezbednosti računarskih podataka" koja su imala za cilj da obezbede efikasnu, kvalitetnu i zakonitu zaštitu računarske bezbednosti [9, pp. 351-361]. Identična krivična dela su potom uvedena i u Krivičnom zakoniku Crne Gore 2003. godine u glavi XXVIII pod istim nazivom [15, pp. 816-824] budući da su ove dve republike činile Državnu zajednicu Srbija i Crna Gora do maja 2005. godine.

U osnovi Konvencije o kibernetičkom kriminalu, kao obavezujućem međunarodnom dokumentu koji je donet od strane najznačajnije i najmasovnije evropske regionalne organizacije, nalazi se više prethodno donetih preporuka kao što su: (1) Preporuka broj R (85) 10 o praktičnoj primeni Evropske konvencije o uzajamnoj pomoći u krivičnim predmetima u pogledu pružanja međunarodne krivičnopravne pomoći pri presretanju komunikacija, (2) Preporuka broj R (88) 2 o piratstvu na polju autorskih i srodnih prava, (3) Preproruka broj R (87) 15 koja propisuje upotrebu ličnih podataka u oblasti delatnosti policije, (4.) Preporuka broj R (95) 4 o zaštiti ličnih podataka na području telekomunikacionih usluga sa posebnim osvrtom na ulogu telefonije, (5) Preporuka broj R (89) 9 o računarskom kriminalu koja daje smernice nacionalnim organima u pogledu definisanja pojedinih računarskih krivičnih dela i (6) Preporuka broj R (95) 13 o problemima krivičnog procesog prava koji su vezani za informatičku tehnologiju [3, pp. 87-92].

Konvencija o kibernetičkom kriminalu predviđa niz pravnih sredstava, mera i postupaka, koji su nužni radi odvraćanja lica od radnji koje su usmerene protiv tajnosti, celovitosti i dostupnosti računarskih, sistema, mreža i računarskih podataka, kao i za odvraćanje od njihove zloupotrebe u bilo kom vidu [14, pp. 78-82]. Na taj način se olakašava otkrivanje, istraživanje i krivični progon tih dela i njihovih učinilaca na domaćem i međunarodnom nivou i osigurava efikasna i brza međunarodna saradnja.

U članu 1 Konvencija je definisala osnovne pojmove računarskog (kibernetičkog, sajber) kriminaliteta kao što su: računarski sistem, računarski podatak, davalac usluga ili podaci o prometu. Ovim je dato uputstvo nacionalnom zakonodavcu da u ovom duhu tretira ove zaštićene vrednosti kao objekte krivičnopravne zaštite [18, pp. 94-97].

U drugom poglavlju pod nazivom „Kazneno materijalno pravo" u više odredbi su dati pojam i karakteristike pojedinih krivičnih dela koje treba inkriminisati u nacionalnim pravnim sistemima država članica Saveta Evrope. To su sledeća krivična dela koja povređuju ili ugrožavaju računarsku bezbednost: (1) krivična dela protiv tajnosti, celovitosti i dostupnosti računarskih podataka i sistema (čl. 2-6) – nezakonti pristup, nezakonito presretanje, ometanje podataka, ometanje sistema i zloupotreba uređaja, (2) računarska krivična dela (čl.7 i 8) – računarsko

falsifikovanje i računarska prevara, (3) krivična dela u vezi sa sadržajem (član 9) – krivična dela vezana za dečju pornografiju i (4) krivična dela povrede autorskih i srodnih prava (član 10).

Ono što je od posebnog značaja jesu odredbe Konvencije koje izričito zahtevaju od država članica da se kazni i za pokušaj ovih krivičnih dela, kao i za oblike saučesništva u vidu podstrekavanja i pomaganja, kao i da se pored odgovornosti fizičkih lica za ova dela predvidi i krivična odgovornost pravnih lica.

Sve navedene standarde je novo krivično zakonodavstvo Srbije u potpunosti implementiralo u svoj pravni sistem obezbeđujući vrstu i meru kazne za pojedina krivična dela, kao i formirajući posebne organe u okviru policije, javnog tužilaštva i Višeg suda u Beogradu – posebne organizacione jedinice za borbu protiv visokotehnološkog kriminala gde spadaju navedena krivična dela.

3. KRIVIČNOPRAVNA ZAŠTITA RAČUNARSKE BEZBEDNOSTI

Zbog postojanja različitih oblika i vidova ispoljavanja zloupotrebe računara u svakodnevnim životnim situacijama, KZ propisuje više računarskih krivičnih dela ili kako ih on naziva „krivičnih dela protiv bezbednosti računarskih podataka" kao najopasnijih oblika povrede ili ugrožavanja računarske bezbednosti fizičkih ili pravnih lica, u zemlji ili inostranstvu [13, pp. 214-221]. No, sva ta pojedina dela, pored brojnih različitosti, imaju i niz specifičnih karakteristika koje su im zajedničke [17, pp. 32-40].

Računar, u svakom slučaju, predstavlja jednu od najznačajnijih i najrevolucionarnijih tekovina razvoja tehničko-tehnološke civilizacije. No, pored brojnih prednosti koje sobom nosi i ogromne koristi za čovečanstvo, računar je brzo postao i sredstvo za razne zloupotrebe nesavesnih pojedinaca, grupa, pa i čitavih organizacija. Tako nastaje računarski kriminalitet kao poseban i specifičan oblik savremenog kriminaliteta po strukturi, osobenostima, oblicima ispoljavanja, karakteristikama učinioca, načinu i sredstvima izvršenja itd.

Ovaj vid kriminaliteta, za razliku od drugih, još uvek ne predstavlja zaokruženu fenomenološku kategoriju, te ga je nemoguće definisati jedinstvenim i preciznim pojmovnim određenjem. Računarski kriminalitet je samo opšta forma kroz koju se ispoljavaju različiti oblici kriminalne delatnosti, uz pomoć ili posredstvom računara. Naime, to je kriminalitet koji je upravljen protiv bezbednosti računarskih (informatičkih, kompjuterskih) sistema u celini ili njegovih pojedinih delova na različite načine i različitim sredstvima u nameri da se sebi ili drugom fizičkom ili pravnom licu pribavi protivpravna imovinska korist ili drugome nanese kakva, najčešće, imovinska šteta.

3.1. Objekt računarskih krivičnih dela

Objekt zaštite kod računarskih krivičnih dela jeste računarska bezbednost ili bezbednost računarskih (kompjuterskih) podataka i sistema, odnosno računarske mreže [8, pp. 56-62]. Iako je danas uobičajeno da se ova krivična dela obuhvataju pojmom „kompjuterski" kriminalitet , domaći je zakonodavac za njih ipak upotrebio termin „računarski" kriminalitet. No, pored ovog naziva za krivična dela sistematizovana na ovom mestu, zakonodavstvo Srbije upotrebljava i pojam „visokotehnološki" kriminal. Pod ovim se pojmom podrazumeva vršenje krivičnih dela kod kojih se kao objekat ili kao sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, računarski sistemi, kao i njihovi proizvodi u materijalnom ili elektronskom obliku.

Pri tome je sam zakonodavac u članu 112 KZ odredio pojam i karakteristike objekta napada kod ovih krivičnih dela. To su: 1) računarski podatak, 2) računarska mreža, 3) računarski program, 4) računarski virus, 5) računar i 6) računarski sistem [13, pp. 189-192].

Računarski podatak je svako predstavljanje činjenica, informacija ili koncepta u obliku koji je podesan za njihovu obradu u računarskom sistemu, uključujući i odgovarajući program na osnovu koga računarski sistem obavlja svoju funkciju (član 112 stav 17 KZ). Računarska mreža predstavlja skup međusobno povezanih računara, odnosno računarskih sistema koji komuniciraju razmenjujući podatke (član 112 stav 18 KZ). Računarski program je uređeni skup naredbi koji služi za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara (član 112 stav 19 KZ). Računarski virus je računarski program ili drugi skup naredbi koji je unet u računar ili računarsku mrežu, koji je napravljen da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka (član 112 stav 20 KZ). Računar je svaki elektronski uređaj koji na osnovu programa automatski obrađuje i razmenjuje podatke (član 112 stav 33 KZ). I konačno, računarski sistem je svaki uređaj ili grupa međusobno povezanih ili zavisnih uređaja od kojih jedan ili više njih, na osnovu programa vrši automatsku obradu podataka (član 112 stav 34 KZ).

3.2. Pojam računarskih krivičnih dela

Kompjuter (računar) predstavlja jednu od najznačajnijih i najrevolucionarnijih tekovina tehničko-tehnološkog razvoja na kraju 20. veka. No, pored prednosti koje računar nosi sa sobom i ogromne koristi za čovečanstvo, on je ubrzo postao i sredstvo zloupotrebe nesavesnih pojedinaca ili grupa. Tako nastaje računarski kriminalitet, kao poseban i specifičan oblik savremenog kriminaliteta. Zahvaljujući ogromnoj moći računara u memorisanju i brzoj obradi velikog broja podataka, automatizovani informacioni sistemi postaju sve brojniji i nezamenjivi pratilac celokupnog ljudskog i društvenog života fizičkih i pravnih lica [19, pp. 305-318].

Različite forme primene računara u svim oblastima života, privrede i drugih društvenih delatnosti nisu ostale nezapažene od strane nesavesnih i zlonamernih pojedinaca ili grupa koji ne birajući sredstva i načine pokušavaju da pribave za sebe ili drugog protivpravnu imovinsku korist ili da drugome nanesu kakvu, najčešće, štetu. Tako računar postaje sredstvo, oruđe za izvršenje različitih krivičnih dela. Za različite oblike i vidove zloupotrebe računara u teoriji se upotrebljavaju i različiti nazivi kao što su: zloupotreba računara (*computer abuse*), delikti uz pomoć računara (*crime by computer*), kompjuterska prevara (*computer fraud*), informatički kriminalitet, računarski kriminalitet, sajber kriminalitet, tehno kriminalitet itd. [10, pp. 639].

U pravnoj teoriji se mogu uočiti različita određenja pojma računarskog kriminaliteta. Tako, Don Parker određuje računarski kriminalitet kao zloupotrebu kompjutera u smislu svakog događaja koji je u vezi sa upotrebom kompjuterske tehnologije u kome žrtva trpi ili bi mogla da trpi gubitak, a učinilac deluje u nameri da sebi pribavi ili bi mogao da pribavi korist [7, pp. 70]. Avgust Bekui definiše kompjuterski kriminalitet kao vršenje krivičnih dela kod kojih se računar pojavljuje kao oruđe ili objekt zaštite, odnosno kao upotrebu kompjutera pri vršenju prevare, utaje ili zloupotrebe čiji je cilj prisvajanje novca, usluge ili vršenje političke ili poslovne manipulacije, uključujući i radnje uperene protiv samog računara [1, pp. 4]. Bogo Brvar pod računarskim kriminalitetom smatra vršenje krivičnih dela kod kojih se kompjuter pojavljuje kao sredstvo (oruđe), predmet ili objekt napada za čije je vršenje ili pokušaj neophodno izvesno znanje iz računarstva ili informatike [6, pp. 29].Tako se može zaključiti da se pod pojmom računarskog kriminaliteta [5, pp. 233-235] i [16, pp. 52-56] podrazumeva sveukupnost različitih oblika, vidova i formi ispoljavanja protivpravnih ponašanja upravljenih protiv bezbednosti računarskih, informacionih i kompjuterskih sistema u celini ili njihovih pojedinih delova na različite načine i različitim sredstvima u nameri da se sebi ili drugom pribavi korist (imovinske ili neimovinske prirode) ili da se drugome nanese šteta.

Iz ovako određenog pojma računarskog kriminaliteta, kao najopasnijeg oblika ugrožavanja računarske bezbednosti, proizilaze njegove osnovne karakteristike [2, pp. 211-214]. To su: 1) objekt zaštite je bezbednost računarskih podataka ili informacionog sistema u celini ili njegovog pojedinog dela (segmenta), 2) poseban, specifičan karakter i priroda protivpravnih delatnosti pojedinaca, 3) posebna znanja i specijalizacija na strani učinioca ovih krivičnih dela koja isključuje mogućnost da se svako, bilo koje lice nađe u ovoj ulozi, 4) poseban način i sredstvo preduzimanja radnje izvršenja – uz pomoć ili upotrebom (zloupotrebom) računara i 5) namera učinioca kao subjektivni elemenat u vreme preduzimanja radnje koja se ogleda u nameri pribavljanja za sebe ili drugog koristi ili nanošenja štete drugom fizičkom ili pravnom licu.

Računarski kriminalitet karakteriše velika dinamika i izuzetna šarolikost pojavnih oblika, formi i vidova ispoljavanja. To je i razumljivo jer se radi o novoj tehnologiji sa velikim mogućnostima primene u širokoj sferi ljudske, društvene i privredne delatnosti, te su i mogućnosti zloupotrebe računara svaki dan sve veće. Pored novih pojavnih oblika ranije, već poznatih krivičnih dela koja pod uticajem zloupotrebe kompjutera menjaju tradicionalni, klasični način i modus ispoljavanja (krađa, prevara, falsifikovanje), javljaju se i novi oblici protivpravnog i kažnjivog ponašanja koji ne poznaju granice između država (pravljenje računarskog virusa).

Štetne posledice računarskih krivičnih dela su velike i ispoljavaju se u nastupanju imovinske štete za fizička ili pravna lica (ponekad i za celu državu), u gubitku poslovnog ugleda, gubitku poverenja u sigurnost i istinitost računarskog poslovanja i uopšte računarskih podataka, opasnosti od zloupotrebe po slobode i prava čoveka i građana na razne načine, odavanje lične, poslovne i drugih vidova tajni i sl.

3.3. Ostali elementi računarskih krivičnih dela

U teoriji krivičnog prava se u oblast računarskog kriminaliteta svrstavaju različiti oblici protivpravnog, nedozvoljenog ponašanja kao što su: 1) računarska prevara, 2) finansijske krađe, prevare, utaje i zloupotrebe, 3) krađa dobara, 4) falsifikovanje podataka i dokumenata, 5) vandalizam, 6) sabotaža, 7) hakerisanje, 8) računarska špijunaža i 9) krađa vremena [12, pp. 211-214].

Velike praktične mogućnosti koje pruža savremena visoko sofisticirana računarska i informatička tehnologija sa sobom nose i opasnost od širenja i masovne upotrebe elektronskog prisluškivanja, krađe poslovnih i drugih tajni, kao i različitih oblika intelektualne svojine, zatim ozbiljnog narušavanja privatnosti i ugrožavanja ljudskih sloboda i prava, kao i ličnog integriteta. U poslednje vreme je prisutna i realna opasnost od talasa različitih oblika terorističkog delovanja (tzv. tehno ili sajber terorizam).

Izvršioci računarskih krivičnih dela predstavljaju specifičnu kategoriju lica. Radi se, uglavnom, o nedelinkventnim i socijalno prilagodljivim, nenasilnim ličnostima. Oni za vršenje krivičnih dela putem računara moraju da poseduju određena specijalna, stručna i praktična znanja i veštine u domenu informatičke i računarske tehnike i tehnologije. Pored toga, radi se o licima kojima su ovakva tehnička sredstva (računari) dostupna u fizičkom smislu.

Ova se krivična dela vrše prikriveno, često bez vidljive prostorne i vremenski bliske povezanosti između učinioca dela i oštećenog (pasivnog subjekta). U praksi postoji veća ili manja vremenska razlika između preduzete radnje izvršenja krivičnog dela i trenutka nastupanja njegove posledice. Ova se dela teško otkrivaju, a još teže dokazuju, dugo ostaju praktično neotkrivena, sve dok oštećeni ne pretrpi štetu u domenu informatičkih i računarskih podataka ili sistema. Radi se o kriminalitetu koji brzo i lako menja forme i oblike ispoljavanja, granice među državama, kao i vrstu oštećenog. U pogledu krivice, ova se dela vrše isključivo sa umišljajem.

KZ u glavi 27. pod nazivom „Krivična dela protiv bezbednosti računarskih podataka" u čl. 298-304a predviđa sledeća računarska krivična dela: 1) oštećenje računarskih podataka i programa, 2) računarska sabotaža, 3) pravljenje i unošenje računarskih virusa, 4) računarska prevara, 5) neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka, 6) sprečavanje i ograničavanje pristupa javnoj računarskoj mreži, 7) neovlašćeno korišćenje računara ili računarske mreže i 8) pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka.

4. ZAKLJUČAK

Najopasnija forma povrede i ugrožavanja računarske bezbednosti predstavljaju različiti oblici računarskog kriminaliteta. To može biti bilo klasični, bilo organizovani kriminalitet koji ako je upravljen protiv računarske bezbednosti, polako ali sigurno zauzima svoje mesto u obimu, dinamici i strukturi savremenog kriminaliteta. Uočavajući opasnosti od zloupotrebe računara i savremene tehnologije koja je povezana sa računarskim sistemima, međunarodna zajednica je reagovala donošenjem određenih međunarodnih dokumenata. Standardi sadržani u njima su tako postali osnova za jedinstvenu akciju pojedinih država i na nacionalnom planu u cilju sprečavanja i suzbijanja računarskog kriminaliteta svih vrsta, oblika i vidova ispoljavanja.

Na bazi međunarodnih standarda koje je prihvatila i Republika Srbija, još 2003. godine je u domaćem krivičnom zakonodavstvu uvedeno više računarskih krivičnih dela sa različitim oblicima i vidovima ispoljavanja i sistemom krivičnih sankcija za njihove učinioce. To su najteži i najozbiljniji oblici ugrožavanja ili povrede računarske bezbednosti. Potom je formiran sistem državnih organa specijalizovanih za otkrivanje i dokazivanje kriivčnih dela ove vrste, kao što su tužilac za visokotehnološki kriminal i odeljenje Višeg suda u Beogradu za visokotehnološki kriminal, uz istovremeno formiranje i specijalizovanih organa u Ministarstvu unutrašnjih poslova Republike Srbije.

LITERATURA

[1] A. Bequai, „Computer crime". Lexington, 1978.
[2] B. Petrović, D.Jovašević, „Krivično (kazneno) pravo, Posebni dio". Sarajevo, 2006.
[3] B. Petrović, D. Jovašević, „Međunarodno krivično pravo". Sarajevo, 2010.
[4] B. Pavišić, „Kazneno pravo Vijeća Evrope". Zagreb, 2006.
[5] B. Petrović, D. Jovašević, A. Ferhatović, „Krivično pravo 2". Sarajevo, 2016.
[6] B. Brvar, „Pojavne oblike zlorabe računlnika". Revija za kriminalistiko in kriminologijo, Ljubljana, 2/1982., str. 29.
[7] D. Parker, „Computer abuse", Springfild, 1973.
[8] D. Jovašević, „Obeležja kompjuterskog kriminaliteta". Pravni informator, Beograd, broj 3/1998., str. 56-62.
[9] D. Jovašević, „Komentar Krivičnog zakona Republike Srbije sa sudskom praksom", Beograd, 2003.
[10] D. Jovašević, „Leksikon krivičnog prava". Beograd, 2011.
[11] D.Jovašević, „Međunarodno krivično pravo". Niš, 2011.
[12] D.Jovašević, V. Ikanović, „Krivično pravo Republike Srpske, Posebni dio". Banja Luka, 2012.
[13] D.J ovašević, „Krivično pravo, Posebni deo". Beograd, 2014.
[14] D. Jovašević, V. Ikanović, „Međunarodno krivično pravo", Banja Luka, 2015.

[15] Lj. Lazarević, B. Vučković, V. Vučković, „Komentar Krivičnog zakonika Crne Gore“. Cetinje, 2004.

[16] N. Kitarović, „Kompjuterski kriminalitet“. Bilten sudske praske Vrhovnog suda Srbije, Beograd, 2-3/1998., str. 52-56.

[17] S. Petrović, „Kompjuterski kriminalitet“. Bezbednost, Beograd, 1/1994, str. 32-40

[18] S. Emm Kareklas, „Priručnik za krivično pravo Evropske unije“, Beograd, 2009.

[19] Z. Đokić, S. „Živanović, Kompjuterski kriminal kao obeležje progresivnog kriminaliteta“. Zbornik radova „Kazneno zakonodavstvo - progresivna ili regresivna rešenja, Beograd, 2005., str. 305-318.

PROTECTION OF COMPUTER SECURITY THROUG CRIMINAL LAW

Abstract:

Today, computers and computer systems have become an essential companion of a human life but also of a economic business, as well as work of state and other organs. Even though these are useful devices and systems for efficient and quality functioning of each state, and international relations, they are subject to a high risk and challenges of natural and legal persons for various reasons (motives). On the basis of adopted international documents of international and regional character, major number of the countries in their legislations, including the Republic of Serbia, have recognized various mechanisms of protection and enabling efficient, quality and due functioning of computer systems and devices. A special part of this protection is legal protection, in the first line criminal and legal protection of security of computer systems. Therefore, the legislation of the Republic of Serbia provides for criminal responsibility and penalties for many computer criminal offences, and this papers speaks about their characteristics from theoretical and practical aspect.

Keywords:

computer, computer systems, computer security, criminal offence, responsibility.