KOMPJUTERSKI KRIMINALITET U PRAVNOJ TEORIJI, POJAM, KARAKTERISTIKE, POSLEDICE
CYBERCRIME IN LEGAL THEORY, THE CONCEPT, CHARACTERISTICS, CONSEQUENCES

Jelena Matijašević, *Pravni fakultet za privredu i pravosuđe, Univerzitet Privredna akademija, Novi Sad*
Svetlana Ignjatijević, *Fakultet za ekonomiju i inženjerski menadžment*, *Univerzitet Privredna akademija, Novi Sad*

Sadržaj – *Nema oblasti ljudske delatnosti u kojoj računari nisu našli svoju primenu. Dostupnost, kao i brz razvoj, stvorili su mogućnost da se danas mogu zloupotrebiti u različite svrhe. Kompjuterski kriminalitet podrazumeva zloupotrebu kompjuterske tehnologije, kao načina i sredstva, ili kao cilja izvršenja krivičnog dela, čime se ostvaruje neka u krivičnopravnom smislu relevantna posledica. Kompjuterski kriminalitet ima svoje specifičnosti u odnosu na druge vrste kriminalnih delovanja: velika dinamičnost, stalno širenje na nove oblasti, težina posledica (imovinskog, ali i nematerijalnog karaktera), velika tamna brojka, otežano otkrivanje i dokazivanje, specifičan profil učinioca, velike mogućnosti za prikrivanje izvršenog krivičnog dela, a sve je to uzrokovano ambijentom u kojem se ova krivična dela vrše. Jasno je da se radi o veoma složenom obliku kriminaliteta, kojem se društvo može adekvatno suprotstaviti samo ako u potpunosti sagleda sve njegove osobenosti i specifičnosti.*
Ključne reči*: kompjuterski kriminalitet, kompjuterska tehnologija i informatički sistemi*
Abstract – *There isn't field of human activity in which computers have found their application. Availability and rapid development, have created the possibility that today could be misused for different purposes. Computer crime involves abuse of computer technology, as way and thing, or as target of the crime, with which is realized in a criminal sense relevant consequences. Computer crime has its specifics compared to other types of criminal activity: great dynamism, constantly spreading to new areas, the weight of consequences (property, but also intangible character), a large dark figure, difficulty detecting and proving, the specific profile of the perpetrator, great opportunities for concealment of the committed criminal act, and it is all caused by environment in which these criminal acts performed. It is clear that this is a very complex form of the crime, which the society can adequately oppose only if fully analyze all its features and specifics.*
Keywords: *computer crime, computer technology and informatics systems*

1. UVOD

Jedno od najznačajnijih otkrića u istoriji čovečanstva jeste kompjuter. Brojne su mu karakteristike, ali kao posebno značajne možemo istaći ekspanzivnost u razvoju, širinu primene, značaj za najvažnije segmente i procese društvenog i ekonomskog života.

Od pojave prvog kompjutera, sredinom četrdesetih godina, pa do danas, došlo je do rapidnog širenja upotrebe kompjutera u skoro svim oblastima života i rada. Prvi računar nazvan ENIAC je pušten u eksperimentalni pogon februara 1944. godine, da bi konačno bio završen tek 1946. godine. Njegova osnovna funkcija bila je da u ratne svrhe izračunava putanje artiljerijskih granata, a njegova izrada je koštala oko 400.000 tadašnjih dolara, što je u to vreme bila značajna svota, ali je sada, nekih pedeset godina posle tog događaja, sasvim izvesno da su te pare bile izvanredno uložene, jer je napredak, koji je širom upotrebom kompjutera usledio, bio fantastičan. [1]

Danas smo svi svesni ogromnog značaja upotrebe kompjutera u savremenim društvima i činjenice da nema oblasti ljudske delatnosti u kojoj računari nisu našli svoju primenu. Međutim, prilično je poražavajuća konstatacija da ne postoji tehničko i tehnološko dostignuće koje u istoriji čovečanstva nije naišlo na različite vidove zloupotrebe. Specifičnost predstavljaju faze razvoja u kojima je pronalazak bio podložan zloupotrebi, zatim grupacije lica koje su vršile takve radnje i različite namene zbog kojih su se vršile te zloupotrebe.

U početku primene kompjuterske tehnologije, kompjuteri nisu bili podobni za veće zloupotrebe, jer njihova primena nije bila masovna, tako da se njima bavio samo uzak krug korisnika – informatičkih stručnjaka. Ono što je otvorilo vrata širenju mogućnosti da se kompjuterska tehnologija zloupotrebi u različite svrhe, jeste njen brz razvoj, pojednostavljenje njene upotrebe, kao i dostupnost iste širokom krugu korisnika.

2. POJAM KOMPJUTERSKOG KRIMINALITETA

Sve učestaliji vidovi i načini zloupotrebe kompjutera podstakli su naučnu i stručnu javnost da se pozabavi ovim oblikom kriminalnog ponašanja.

Kompjuterski kriminalitet je nemoguće definisati jedinstvenim i preciznim pojmovnim određenjem. To je „opšta forma kroz koju se ispoljavaju različiti oblici kriminalne aktivnosti, forma koja će u budućnosti postati dominantna.“ [7] Naime, teškoće u definisanju kompjuterskog kriminaliteta proizilaze zbog toga što se radi o relativno novom obliku kriminalnog ponašanja, ali i zbog toga što postoji velika fenomenološka raznovrsnost ove pojave, koja se teško može obuhvatiti jednom definicijom.

Jedan od autora koji je razmatrao problem kompjuterskog kriminala jeste Don Parker. Njegov zaključak je da je: „zloupotreba kompjutera svaki događaj 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.“ [6]

Svetski rečnik engleskog jezika ovaj pojam određuje na sledeći način: „Kompjuterski kriminalitet obuhvata nezakonite aktivnosti koje se vrše na kompjuteru ili kod kojih je kompjuter sredstvo izvršenja. On obuhvata kriminalni upad u drugi kompjuterski sistem, krađu kompjuterskih podataka, ili korišćenja on-line sistema za vršenje ili pomoć u izvršenju prevara. [10]

Na desetom Kongresu Ujedinjenih Nacija za prevenciju kriminaliteta i tretman delikvenata, razmatrana je ova problematika: Kompjuterski kriminalitet je opšti pojam koji obuhvata krivična dela koja se vrše posredstvom kompjuterskog sistema ili mreže, u kompjuterskom sistemu ili mreži, ili protiv kompjuterskog sistema ili mreže. U principu on uključuje bilo koje krivično delo koje se vrši u elektronskom ambijentu.“ [11]

Na prostoru Republike Srbije, jedna od prvih definicija iz ove oblasti je: „Kompjuterski kriminal obuhvata krivična dela kod kojih se kompjuter pojavljuje kao sredstvo, predmet ili objekt napada, za čije je izvršenje ili pokušaj neophodno izvesno znanje iz računarstva ili informatike.“ [3]

Autor Đorđe Ignjatović pod ovim pojmom podrazumeva poseban vid inkriminisanih ponašanja kod kojih se računarski sistem (shvaćen kao jedinstvo hardvera i softvera) pojavljuje kao sredstvo izvršenja ili kao objekt krivičnog dela, ukoliko se delo na drugi način, ili prema drugom objektu, ne bi moglo izvršiti ili bi ono imalo bitno drugačije karakteristike.“ [5]

Imajući u vidu prethodna sagledavanja pojma kompjuterskog kriminaliteta, posebno različitost u pristupima pojedinih autora, zaključujemo da je neophodno imati veoma širok pristup prilikom definisanja ove vrste kriminalnog ponašanja. Naime, jedna sveobuvatna definicija mora inkorporisati u svojoj strukturi tri bitna elementa: način izvršenja, sredstvo izvršenja i posledicu kriminalnog delovanja.

Pod načinom izvršenja se podrazumeva svojevrsna upotreba kompjutera, koji između ostalog može biti i osnovno sredstvo za izvršenje krivičnih dela, pri čemu je potrebno da nastupi i određena kažnjiva posledica.

U tom smislu, najpotpunija definicija bi bila: „Kompjuterski kriminalitet predstavlja oblik kriminalnog ponašanja kod koga se korišćenje kompjuterske tehnologije i informatičkih sistema ispoljava kao način izvršenja krivičnog dela, ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivičnopravnom smislu relevantna posledica.“ [1]

3. KARAKTERISTIKE KOMPJUTERSKOG KRIMINALITETA

Privredni kriminal, ili namerna prevara čiji je cilj da se drugom licu uskrati posed novca, imovine ili zakonsko pravo, ima nekoliko pojavnih oblika. To su pronevera imovine, finansijska pronevera, korupcija i mito, pranje novca, piraterija, i ono od čega velika opasnost tek dolazi – syber kriminal i industrijska špijunaža, odnosno mešetarenje informacijama. [12]

Kompjuterski kriminalitet ima svoje specifičnosti u odnosu na druge vrste kriminalnih delovanja, koje nesumnjivo ukazuju na opasnost ove pojave i upućuju da se pitanju suzbijanja iste, pristupi sa velikom pažnjom. Te karakteristike su: velika dinamičnost, konstantno širenje na nove oblasti, težina posledica koje nastupaju vršenjem kompjuterskih krivičnih dela, velika tamna brojka, otežano otkrivanje i dokazivanje, specifičan profil učinioca, velike mogućnosti za prikrivanje izvršenog krivičnog dela, itd.

Prethodno navedene karakteristike posledica su specifičnog ambijenta u kojem se kompjuterski kriminalitet vrši.

Taj ambijent karakterišu: visoka koncentracija na malom prostoru, prethodno proverenih i uređenih podataka, dostupnih kako ovlašćenim, tako i neovlašćenim korisnicima; znatno proširen prostor kriminalnog delovanja, koji, za razliku od tradicionalnih vidova kriminaliteta, ne zahteva prisustvo izvršioca na mestu izvršenja krivičnog dela; skraćeno vreme kriminalnog delovanja, s obzirom na automatizovani ambijent, čija brzina sprečava nadzor i upravljanje. Na taj način, vreme potrebno za izvršenje krivičnog dela skraćuje se na delove sekunde, što implicira visok nivo prikrivenosti i značajne teškoće u otkrivanju takve delatnosti; na ovo se nadovezuju i suptilne tehnike i metodi koje se izvršavaju istim mehanizmima kao i legalne, ne ostavljaju tragove, niti ometaju redovan rad sistema, pa je samim tim mogućnost otkrivanja svedena na najmanju meru; za razliku od tradicionalnog kriminala, kompjuterski karakteriše stabilnost rizika, s obzirom da se jednom izgrađen modus može veoma dugo koristiti, sa potpuno istim, niskim rizikom otkrivanja; sve jednostavnije mogućnosti upotrebe kompjuterske tehnologije od strane sve većeg broja korisnika, kojima više nije nužno posebno tehničko obrazovanje. [8]

Uopšteno govoreći, kompjuterski kriminalitet može da se ispolji korišćenjem, oštećenjem, zloupotrebom, ili bilo kojom drugom manipulacijom dva osnovna segmenta kompjuterskog sistema – hardvera („hardware“) i softvera („software“). Naime, kompjuter predstavlja elektronsku mašinu sposobnu da primi i čuva informacije, obavlja matematičke, logičke i druge

intelektualne operacije, a može da se koristi u različitim delatnostima, te da se primenjuje u opšte, ili neke posebne svrhe, kada je reč o namenskom ili kompjuteru za posebne potrebe. [1]

Opasnost kompjuterskog kriminaliteta po društvenu zajednicu ogleda se ne samo u ekspanziji njegovih pojavnih oblika, već i u tome što pojedina tradicionalna krivična dela, kao što su prevara, zloupotreba službenog položaja, pronevera,... itd, korišćenjem kompjuterske tehnologije dobijaju znatno opasnije oblike.

Posebna karakteristika kompjuterskog kriminaliteta jeste nastala štetna posledica.

Kriminalom „broj jedan“ u budućnosti mogao bi se okarakterisati cyber kriminal, od koga su štete za napadnutu firmu često katastrofalne. To je naročit problem od pojave elektronskog bankarstva: hakeri su obično spretniji od bilo kog sistema zaštite. [12]

Štetna posledica ispoljava se kao nastala imovinska šteta, ali isto tako može da se ispolji u vidu gubljenja poverenja u sigurnost i tačnost dobijenih informacija iz kompjuterskog sistema, što može dovesti do različitog tretiranja i narušavanja poslovnog ugleda mnogih privrednih i vanprivrednih subjekata i izazvati strah od pojave novih kriminalnih radnji vezanih za sve nivoe funkcionisanja kompjuterskog sistema. [2]

Štete koje nastupaju vršenjem kompjuterskih krivičnih dela su po pravilu veoma velike, a često su i teško sagledive. Naime, pored posledica finansijske prirode koje mogu da nastanu kada učinilac vrši delo u cilju sticanja protivpravne imovinske koristi, pa tu korist za sebe ili drugo lice zaista i stekne, ili je ne stekne, ali svojim delom objektivno pričini određenu štetu, ili kada učinilac ne postupa radi sticanja koristi za sebe ili drugoga, ali objektivno učini finansijsku štetu, postoje i posledice nematerijalne prirode koje se ogledaju u neovlašćenom otkrivanju tuđih tajni, narušavanju ugleda, povredi moralnog prava ili drugom sličnom postupanju, kao i kombinovane posledice, koje postoje kada se otkrivanjem određene tajne, ili povredom autorskog prava, putem zloupotrebe kompjutera ili informatičke mreže nanese određeni vid nematerijalne štete, a istovremeno prouzrokuje i konkretna finansijska šteta.

U SAD je još osamdesetih godina utvrđeno i to kroz prilično opreznu procenu, da finansijske štete prouzrokovane kompjuterskim kriminalitetom dostižu iznos između 100 i 300 miliona dolara na godišnjem nivou, pri čemu prosečna šteta prouzrokovana kompjuterskim deliktom iznosi 430.000 dolara. [4]

Do današnjih dana, situacija se znatno pogoršala.

Posebno zabrinjava što se korporacije često uzdržavaju od prijavljivanja slučajeva u kojima su oštećene zloupotrebom kompjutera, jer smatraju da bi time pogoršali svoj položaj na tržištu lošim reklamiranjem, kroz isticanje sopstvene nesposobnosti da se efikasno zaštite. [1]

Istraživanje o privrednom kriminalu pokazalo je da mnoge kompanije javno podržavaju politiku izveštavanja vlasti o svim slučajevima kriminala, ali se u realnoj situacijiponašaju sasvim drugačije. Kao osnovni razlog takvog ponašanja navodi se strah kompanije od negativnog uticaja javnosti na poslovne veze kompanije ili moral zaposlenih, strah od troškova sudskog postupka ili uverenje da postoji mala mogućnost povraćaja ukradenih sredstava. [12]

4. TIPOVI KOMPJUTERSKOG KRIMINALITETA

Postoje različite klasifikacije kompjuterskog kriminaliteta. Na desetom Kongresu Ujedinjenih Nacija za prevenciju kriminaliteta i tretman delikvenata, u okviru materijala za sekciju o kriminalu, zaključeno je da postoje dve vrste ovog pojavnog oblika kriminalnog ponašanja: kompjuterski kriminalitet u užem smislu, odnosno svako nezakonito ponašanje usmereno na elektronske operacije sigurnosti kompjuterskih sistema i podataka koji se u njima obrađuju i kompjuterski kriminalitet u širem smislu, odnosno svako nezakonito ponašanje vezano za ili u odnosu na kompjuterski sistem i mrežu, uključujući i takav kriminal kakvo je nezakonito posedovanje, nuđenje i distribuiranje informacija preko kompjuterskih sistema i mreža. [11]

U istom dokumentu navode se i konkretni oblici kompjuterskog kriminaliteta, u skladu sa Preporukom Saveta Evrope [9] i listom OECD-a [16] iz 1989., odnosno 1985. godine. To su: neautorizovani pristup kompjuterskom sistemu lil mreži, kršenjem mera sigurnosti (haking); oštećenje kompjuterskih podataka ili programa; kompjuterske sabotaže; neovlašćeno presretanje komunikacija od i u kompjuterskim sistemima i mrežama i kompjuterska špijunaža.

Navedeni oblici se gotovo stalno međusobno ukrštaju, tako da činjenjem jednog oblika, dolazi do činjenja i niza drugih aktivnost koje spadaju u neki drugi oblik kompjuterskog kriminaliteta. Tako, na primer, neovlašćenim ulaskom u kompjuterski sistem ili mrežu može doći do oštećenja ili uništenja kompjuterskih podataka ili programa, ali i do kompjuterske špijunaže.

Od kompjuterskog kriminaliteta u širem smislu, najčešće se pojavljuju: kompjuterski falsifikati, kompjuterske krađe, tehničke manipulacije uređajima ili elektronskim komponentama uređaja, zloupotrebe sistema plaćanja (kao što su manipulacije i krađe elektronskih kreditnih kartica ili korišćenje lažnih šifri u nezakonitim finansijskim aktivnostima).

Njima se u novije vreme dodaju i dela podržana računarima. Ova dela obuhvataju „rasturanje“ materijala ili samo njihovo posedovanje, pri čemu se mreža koristi za postizanje boljih rezultata kriminala ili pokušaja izbegavanja pravde. U ova dela se ubrajaju razni nezakoniti i štetni sadržaji, kršenje autorskih i srodnih prava, prodaja zabranjene robe (oružja, kradene robe,

lekova,...) ili pružanje nedozvoljenih usluga (kockanje, prostitucija,...). Najviše pažnje u ovoj grupi dela privlači dečija pornografija i distribucija raznih materijala Internetom. [14]

Evropska konvencija o cyber kriminalu [13] predviđa četiri grupe dela: dela protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema – njih čine nezakoniti pristup, presretanje, uplitanje u podatke ili sisteme, korišćenje uređaja (proizvodnja, prodaja, uvoz, distribucija), programa, pasvorda; dela vezana za kompjutere – kod kojih su falsifikovanje i krađe najtipičniji oblici napada; dela vezana za sadržaje – dečija pornografija je najčešći sadržaj koji se pojavljuje u ovoj grupi obuhvatajući posedovanje, distribuciju, transmisiju, čuvanje ili činjenje dostupnim i raspoloživim ovih materijala, njihova proizvodnja radi distribucije i obrada u kompjuterskom sistemu ili na nosiocu podataka; dela vezana za kršenje autorskih i srodnih prava obuhvataju reprodukovanje i distribuciju neautorizovanih primeraka dela kompjuterskim sistemima.

U Enciklopediji cyber kriminala [17] navodi se da FBI i Nacionalni centar za kriminal „belih kragni“ SAD (National White Collar Crime Center) otkrivaju i prate sledeće oblike: upade u kompjuterske mreže; industrijsku špijunažu; softversku pirateriju; dečiju pornografiju; bombardovanje elektronskom poštom; „njuškanje“ pasvorda; „prerušavanje“ jednog računara da elektronski „liči“ na drugi kako bi se moglo pristupiti sistemu koji je pod restrikcijama; krađu kreditnih kartica.

Kompjuterski kriminalitet zavisno od tipa počinjenih dela može biti politički i ekonomski. U politički cyber kriminal spadaju: cyber špijnaža i cyber sabotaža, haking, cyber terorizam, cyber ratovanje. U ekonomski cyber kriminal spadaju: cyber prevare, haking, krađa internet vremena i krađa internet usluga, piratstvo softvera, mikročipova i BP, cyber industrijska špijunaža, spam, proizvodnja i distribucija nedozvoljenih štetnih sadržaja (dečija pornografija, pedofilija, verske sekte, širenje rasističkih, nacističkih i sličnih ideja i stavova,...), zloupotreba žena i dece, manipulacija zabranjenim proizvodima, supstancama i robama, povreda cyber privatnost (nadgledanje e-pošte, prisluškivanje, praćenje e-konferencija, prikačinjanje i analiza špijunskih softvera,...). [15]

Jasno je da veliki broj različitih klasifikacija sam po sebi pokazuje raznovrsnost dela iz opusa kompjuterskog kriminala i kompleksnost njihovih pojavnih oblika.

Ono što je nesporno je da je kompjuterski kriminal više vezan za aktivnosti pojedinaca, a kriminal vezan za kompjuterske mreže više je delo grupa i to organizovanih, profesionalizovanih, a sve češće i strogo specijalizovanih. Ove grupe su, s jedne strane, „tradicionalne“ grupe organizovanog kriminala koje su se usavršile i osavremenile primenom informaciono komunikacione tehnologije i pripremile za „izlazak“ na cyber scenu. S druge strane, javljaju se i posebne organizovane cyber grupe – cyber mafija. Ova mafija ima svoja pravila, drugačiji način ponašanja od konvencionalne mafije. Njene aktivnosti su umnogome olakšane specifičnostima okruženja u kom deluju i oružja koja koriste. Okruženje je virtuelno, oružje je informaciono, a znanje je specijalizovano. Internacionalizam, transnacionalnost, multidimenzionalnost samo su neka od svojstava ovih grupa. Njihova organizaciona formula nije toliko jednostavna, ustaljena i jednoobrazna kao što je to slučaj sa drugim oblicima organizovanog kriminala, što još više utvrđuje sliku njihove posebnosti. [14]

5. ZAKLJUČAK

U ovom radu pokušali smo da sagledamo kompleksnost kompjuterskog kriminaliteta. Već prilikom pokušaja definisanja, uočile su se prve teškoće. Naime, ma koliko se svako pojmovno određenje kompjuterskog kriminaliteta na prvi pogled činilo adekvatnim, vrlo brzo se uočavalo da je ovaj oblik kriminalnog delovanja toliko složen, da je vrlo teško iskazati u jednoj definiciji njegovu specifičnost, sadržajnost i značenje za društvenu zajednicu.

Razmatrajući karakteristike kompjuterskog kriminaliteta, a naročito njegove posledice, očigledno je da se isti razlikuje od svih drugih oblika kriminalnog delovanja po stepenu opasnosti u odnosu na napadnuta dobra. Ova konstatacija je još više došla do izražaja kada se shvatilo da mnoge kriminalne aktivnosti potpomognute uticajem oblika kompjuterskog kriminala postaju još opasnije i štetnije.

Ohrabruje činjenica da su mnoge države postale svesne ove pojave i da su u svom pozitivnom krivičnom zakonodavstvu predvidele pojavne oblike kompjuterskog kriminaliteta kao posebna krivična dela. Sa druge strane, ohrabrujuće je i to što se u sve većem broju naučnih i stručnih radova pažnja posvećuje upravo ovom obliku kriminalnog ponašanja. Na taj način dolazi do razotkrivanja mnogih specifičnosti kompjuterskog kriminaliteta, a istovremeno se otvara mogućnost suprotstavljanju njegovim oblicima od strane društvene zajednice.

Sasvim je jasno da se određenoj pojavi društvo adekvatno može suprotstaviti ukoliko sagleda sve njene karakteristike i uđe u sve pore njenih specifičnosti. S obzirom da su načini zloupotrebe kompjuterske tehnologije svakim danom sve savršeniji i komplikovaniji za otkrivanje, i da je vrlo teško ići u korak sa tim kriminalnim aktivnostima, potrebno je i dalje ulagati napore u to da javnost bude svesna sa kakvim se fenomenom današnje društvo suočava, potrebno je konstantno raditi na što adekvatnijem odgovoru na različita kriminalna delovanja u ovoj oblasti. Transparentnost i odlučno suprotstavljanje različitim vidovima kriminalnih aktivnosti su dve bitne odrednice u težnji da se različiti oblici kriminaliteta, pa i kompjuterski, svedu u određene, za društvenu zajednicu, podnošljive okvire.

LITERATURA

[1] Aleksić, Ž. i Škulić, M.: "Kriminalistika", Pravni fakultet Univerziteta u Beogradu i Javno preduzeće „Službeni glasnik", Beograd, 2007

[2] Banović, B.: Obezbeđenje dokaza u kriminalističkoj obradi krivičnih dela privrednog kriminaliteta", Viša škola unutrašnjih poslova, Beograd, 2002

[3] Brvar, B.: Pojavne oblike zlorabe računalnika", Revija za kriminalistiko in kriminologijo, 2/82

[4] Gačić, M.: „Kompjuterski kriminal, inostrana iskustva", „13. maj", br. 5, Zagreb, 1982

[5] Ignjatović, Đ.: „Pojmovno određenje kompjuterskog kriminaliteta", Anali Pravnog fakulteta, 1-3/91

[6] Parker, D.: „Computer Abuse", Springfield, 1973

[7] Parker, D.: "Fighting computer crime", New York, 1983

[8] Petrović, S.: „Kompjuterski kriminal", Bezbednost MUP RS, 1/94

[9] Council of Europe, Recommendation No. R (95) 13, http://www.justice.gov/criminal/cybercrime/crycoe.htm

[10] Encarta, World English Dictionary [North American Edition], 2001 Microsoft Corporation, http://encarta.msn.com/encnet/features/dictionary/DictionaryResults.aspx?lextype=3&search=computer%20crime

[11] Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, year 2000, Background paper for the workshop on crimes related to the computer network: Crime-fighting on the Net, http://www.un.org/events/10thcongress/2088h.htm

[12] http://ekonomist.co.yu/

[13] http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc

[14] http://megatrender.blog.rs/blog/megatrender/megatrender-19/2008/03/06/tipovi-cyber-kriminala

[15] http://www.apisgroup.org/sec.html/Knjige/UMOB/sec.html?id=29

[16] http://www.justice.gov/criminal/cybercrime/intl.html

[17] http://www.scribd.com/doc/20262442/Encyclopedia-of-Cyber-Crime