Vrste internet prevara - pojam, značaj i uticaj na ekonomske i moralne aspekte društvene zajednice

Jelena Matijašević, Žaklina Spalević
Pravni fakultet za privredu i pravosuđe
Univerzitet Privredna akademija, Novi Sad
Srbija
jelena@pravni-fakultet.info, zaklinaspalevic@ymail.com

Svetlana Ignjatijević
Fakultet za ekonomiju i inženjerski menadžment
Univerzitet Privredna akademija, Novi Sad
Srbija
ceca@fimek.edu.rs

Sadržaj— **Kompjuterska tehnologija se danas može zloupotrebljavati na raznovrsne načine. Jedan od oblika zloupotrebe informacione tehnologije jesu računarske prevare. Predstavljaju najrašireniji vid kompjuterskog kriminaliteta, a imaju pretežno imovinski karakter(pribavljanje protivpravne imovinske koristi). Specifična vrsta računarskih prevara jesu „Nigerijske prevare" - metoda vršenja krivičnog dela prevare uz pomoć računara. Najčešće počinje pismom ili elektronskom porukom koja je tako osmišljena da izgleda kao da je namerno poslata primaocu poruke. U pitanju su lažne poruke o dobicima na igrama na sreću, dobrotvornim prilozima, i dr. Pitanje zloupotreba informacionih tehnologija nije samo pravno pitanje. S obzirom da se radi o problemu koji uzrokuje ogromne finansijske gubitke, potrebno je obratiti pažnju i na ekonomske efekte na privredne tokove u svakoj državi pojedinačno.**

Ključne riječi- računarski kriminalitet; računarske prevare; Nigerijske prevare; pravni i ekonomski efekti prevara.

I. UVOD

Velike mogućnosti u svim sferama društvenog života, koje su razvojem informacionih tehnologija i Interneta stavljene pred čoveka, pored brojnih, njemu do tada nepoznatih prednosti, uslovile su i njegovu izloženost novim i vrlo ozbiljnim rizicima.

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. [1, str. 852]. Računari I računarske mreže se danas mogu zloupotrebljavati na raznovrsne načine korišćenjem Interneta.

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. [2]

Jedan od značajnijih oblika zloupotrebe Interneta kao globalne računarske mreže jesu računarske prevare, koje se poslednjih godina ekspanzivno šire i razvijaju u smeru sve većeg broja i kompleksnosti manifestacionih oblika. Specifična vrsta računarskih prevara su Nigerijske prevare koje su zbog obima svoje zastupljenosti uveliko poprimile planetarne razmere sa ozbiljnim reperkusijama na ekonomske efekte nacionalnih privrednih tokova velikog broja država.

II. O RAČUNARSKIM PREVARAMA – POJAM I PARALELA SA INTERNET PREVARAMA

Na samom početku, „potrebno je naglasiti da pored krivičnih dela koja su usmerena protiv bezbednosti računarske tehnologije i elemenata informacionog sistema, postoji veliki broj tradicionalnih krivičnih dela koja se uz pomoć korišćenja računara i računarskih komponenti vrše brže, lakše, učiniocima se teže ulazi u trag, a posledice su daleko ozbiljnije i veće". [3, str. 599]

Kompjuterske prevare su po svojoj prirodi najbliže privrednom kriminalitetu, a i u literaturi se, skoro bez izuzetka, ove pojave tretiraju kao pojavni oblik privrednog kriminaliteta. [4, str. 140]

Kompjuterske prevare predstavljaju najrašireniji vid kompjuterskog kriminaliteta, koji često prouzrokuje enormne štetne posledice. Kompjuterske prevare se vrše u nameri pribavljanja za sebe ili drugoga protivpravne imovinske koristi, s tim što se kod njih u zabludu ne dovodi ili održava neko lice, kao u slučaju običnih prevara, kod imovinskih krivičnih dela, već se ta zabluda odnosi na kompjuter u koji se unose netačni podaci, ili se propušta unošenje tačnih podataka, ili se na bilo koji drugi način računar koristi, za ostvarenje prevare u krivičnopravnom smislu. [5, str. 389] Najbrojnije su u oblasti finansijskog poslovanja, osiguranja, poreskih obaveza, socijalnog osiguranja, u vezi sa proglašavanjem stečaja, pranjem novca, itd.

Kompjuterska prevara definisana je 1989. godine u dokumentu Saveta Evrope kao unošenje, menjanje, brisanje ili potiskivanje podataka ili kompjuterskih programa, ili na drugi način uticanje na proces obrade podataka, koje prouzrokuje štetu drugom licu ili imovini, sa namerom pribavljanja protivpravne ekonomske koristi za sebe ili drugo lice. [6]

Kompjuterske prevare mogu da se vrše na veoma raznovrsne načine i kompjuterski delinkventi u tom pogledu pokazuju zaista veliku inventivnost, a kompjuter za varalice predstavlja neku vrstu lakog "zalogaja", poput ljudskog mozga lišenog moći razlikovanja imaginarnog od stvarnog, čime se ispoljava kao savršena žrtva. [7, str. 76-77] U inostranoj praksi, zabeleženi su slučajevi dugogodišnjeg uplaćivanja dečijeg dodatka osobama koje nemaju decu, novčanih doznaka

fiktivnim firmama koje su radi toga i osnovane i koje se posle toga odmah gase, uplata penzija i naknada za nesrećni slučaj zaposlenima i zdravim osobama. U bankama, karakterističan način izvršenja sastoji se u zaokruživanju suma na računima klijenata na cele brojeve, pa se tako ostvarena razlika elektronskim putem usmerava na sopstveni račun. Slične transakcije moguće su kada dolazi do promena kamatnih stopa u korist štediša, ili promene kurseva valuta, pa se ta činjenica ne evidentira na vreme, itd. Tako je jedan službenik štedionice u Hamburgu izdao naredbu računaru da, prilikom obračunavanja kamata, zaokružuje stotinke i desetine pfeninga i ostatke do zaokruženog broja, automatski prebacuje na njegov račun u istoj banci. Na taj način, za samo dve godine, ostvario je protivpravnu korist od oko 500.000 nemačkih maraka. [8, str. 589]

Kompjuterski prevaranti zloupotrebljavaju upravo one karakteristike cyber -prostora koje doprinose rastu elektronske trgovine: anonimnost, distanca između prodavca i kupca i trenutna priroda transakcija. Uz to, oni koriste prednost činjenice da prevara preko Interneta ne zahteva pristup do nekog sistema za isplatu, kao što to zahteva svaka druga vrsta prevare, i što je digitalno tržište još uvek nedovoljno uređeno i kao takvo konfuzno za potrošače, što za njih predstavlja skoro idealne uslove za prevaru. [9]

Težina kompjuterske prevare je utoliko veća što one daleko dopiru zbog veličine Interneta, zatim, prilično se teško otkrivaju i dokazuju, a zbog male upadljivosti, vrlo često se ova dela vrše veoma dugo i u kontinuitetu.

Prema istraživanjima Internet Crime Complaint Center (IC3), u Sjedinjenim Američkim državama, gubici izraženi u oblasti prevara u 2006. godini iznose 198 miliona dolara, u 2007. godini gubici dostižu cifru od 239 miliona, gde je kompjuter bio sredstvo ili objekt napada, dok je u 2008. godini gubitak u SAD povećan na 264 miliona dolara samo na prevarama. [10]

Veoma je bitno napraviti paralelu između pojmova računarska prevara i Internet prevara, odnosno uočiti određene argumente za distinkciju ova dva pojma.

Internet prevara se odnosi na bilo koju prevaru pri čijem izvršenju se lice koje u nameri pribavljanja protivpravne imovinske koristi za sebe i drugoga iskoristi jednu ili više komponenti Interneta, kao što su chat rooms (sobe za ćaskanje), veb stranice (Web sites), elektronska pošta (e-mail), da bi se stvorili uslovi za lažno prikazivanje ili prikrivanje činjenica kojim bi se neko lice dovelo u zabludu ili u njoj održavalo, da bi to lice učinilo nešto na štetu svoje ili tuđe imovine, tako što bi na primer sprovelo neku finansijsku transakciju ili prenelo neke podatke nekoj finansijskoj instituciji koja je meta napada. Internet prevarom se obmanjuje, pre svega, lice. Internet prevara nije uvek i obavezno računarska prevara, jer neke Internet prevare odgovaraju klasičnim prevaramа koje za sredstvo izvršenja imaju Internet bez nekog posebnog uticaja na elektronsku obradu podataka ili rad računara (obmanjuju se ljudi). Nasuprot ovome, računarskom prevarom se „obmanjuje“ računar i elektronska obrada navodi na pogrešan rezultat koji je usmeren na sticanje protivpravne imovinske koristi i to je differentia specifica ova dva pojma. [11, str. 749-750]

Specifična vrsta Internet prevara jeste i svojevrsna grupacija prevara pod nazivom „Nigerijske prevare“, koja se detaljno razmatra u sledećem odeljku rada.

III. NIGERIJSKE PREVARE

„Nigerijska prevara“ spada u grupu prevara pod nazivom Advance-fee fraud, koje podrazumevaju ulaganje određene svote novca u određeni „posao“, uz obećanje da će se kao benefit ostvariti znatno veća suma novca od uložene. Osim termina „Nigerijska prevara“ ili „Nigerijska šema“- Nigerian scam, u upotrebi su još neki termini, poput: „Nigerijsko pismo“ - Nigerian Letter, „Prevara 419“ ili „Šema 419“ - 419 fraud, „Nigerijska bankarska prevara“ - Nigerian bank scam, „Nigerijska ponuda novca“ - Nigerian money offer, itd. Ova vrsta prevare se pojavila ranih 80-ih godina, sa naglim ekonomskim razvojem Republike Nigerije, koji se zasnivao na upotrebi naftnih resursa. Nekoliko nezaposlenih studenata sa nigerijskog Univerziteta je 80-ih i 90-ih godina koristilo razne varijacije ovih prevara kako bi doveli u zabludu poslovne ljude sa Zapada koji su bili zainteresovani za određene poslove u naftnom sektoru Nigerije. Kasnije su se oblici ovih prevara proširili i po broju i u odnosu na populaciju koja je predstavljala metu ovakvim prevaramа. U prvim godinama XXI veka „Nigerijske prevare“ postale su veoma zastupljene u Africi, Aziji i Istočnoj Evropi, a u poslednje vreme i u Severnoj Americi, Zapadnoj Evropi (Velika Britanija) i Australiji. [12]

Naziv „Prevara 419“ potiče od člana broj 419 Nigerijskog krivičnog zakona (deo poglavlja 38 pod nazivom „Pribavljanje imovine pomoću prevarnih radnji: Prevara“, u kojem se definiše ovo krivično delo). Američko društvo za dijalektiku je utvrdilo da se izraz „Prevara 419“ koristi od 1992. godine. [12]

„Nigerijska prevara“ je metoda vršenja krivičnog dela prevare uz pomoć računara i najčešće počinje pismom ili elektronskom porukom koja je tako osmišljena da izgleda kao da je namerno poslata primaocu poruke. Radi se o prevaramа koje se vrše pomoću lažnih poruka o dobicima na igrama na sreću, lažnih poruka vezanih za dobrotvorne priloge, poruke u vezi sa „ljubavnim i poslovnim ponudama“, humanitarnim akcijama, nasleđa imovine preminulih osoba – najčešće daljih rođaka. Izvršenje „Nigerijske prevare“ uglavnom počinje ubeđivanjem „žrtve“ da učestvuju u podeli određenih novčanih fondova, i to ako unapred uplate određeni novčani iznos. Taj novčani iznos je u najvećem broju slučajeva neuporedivo manji od onog iznosa koji bi trebali da dobiju kao korist od nekog fonda, odnosno od pošiljaoca poruke. Elektronskom porukom (najčešće „spam“ porukom) od primaoca poruke se traži pomoć za transfer velikih novčanih iznosa, od par stotina hiljada do par desetina miliona dolara za koji će, nakon obavljenog transfera dobiti određeni procenat kao nadoknadu (procenat zarade koji se obećava kreće se i do 40% od sume novca koja je predmet posla. [13]

Elektronske poruke kao što su Spam-ovi sa ovakvom sadržinom , najčešće se šalju iz Internet kafea. U Nigeriji, u oblastima kao što su npr. Lagos ili Festak, postoje mnogi Internet kafei koji su otvoreni upravo u te svrhe, a radno vreme im je od 22,30 časova do 07,00 časova, radi izbegavanja kontrole od strane državnih službenika. [14, str. 149]

Ukoliko žrtva prevare odgovori na prvu poruku, ona se metodom socijalnog inženjeringa, odnosno, aktivnim manipulativnim delovanjem da žrtva otkrije poverljive informacije o sebi, navodi da pomisli da je njena pomoć neophodna da bi se određena radnja izvršila. Nakon što oštećeni uplati određeni novčani iznos prema instrukcijama izvršilaca krivičnih dela sledi odlaganje novčanih transakcija vezanih za isplatu obećane sume novca. Stalno se pojavljuju novi troškovi za oštećenog na ime realizacije posla i traže nova odlaganja, stalno se obećava „ekspresna“ isplata novca, uz ubeđivanje žrtve prevare da će joj se ulaganje u dogovoreni posao višestruko isplatiti. [14, str. 148]

Izvršioci koji vrše ove prevare često koriste lažne podatke i krađu identiteta, vrlo često pri predstavljanju koriste fotografije drugih lica koje su prikupili sa Interneta, kako bi se lažno predstavili oštećenima. Najveći broj izvršilaca ovih krivičnih dela pripada manjim organizovanim kriminalnim grupama, ali se ponekad dešava da funkcionišu i samostalno. Ukoliko izvršioci krivičnih dela nisu dobro organizovani, onda ne mogu da izvrše prevare većih razmera i oštete veće kompanije, ali su jako opasni za srednju klasu građana i mala preduzeća. U mnogim državama postoje i preduzeća koja uz novčanu nadoknadu obezbeđuju lažna dokumenta koja se koriste u ovim prevarama.

„Nigerijske prevare“ dostigle su svoj vrhunac u 2009. godini, kada su žrtve prevara izgubile više novca nego ikad pre. Ovi rezultati su zasnovani na analizama iz istraživanja holandske kompanije Ultrascan [15] (Ultrascan Advanced Global Investigations), koja se još od 1996. godine bavi praćenjem aktivnosti e-mail prevaranata. Rezultati pokazuju da je izgubljeno gotovo 50% više novca u 2009. godini, nego u 2008.

Ultrascan tvrdi da lica koja se bave ovakvim zloupotrebama šire svoja poslovanja na tržišta gde se Internet tek razvija, i gde ne postoji veoma malo ili skoro nikakvo znanje o ovakvim načinima prevare. Prema izveštaju ove kompanije, koja je analizirala 8.503 slučaja u preko 152 zemlje u toku 2009. godine, žrtve su izgubile 9,3 milijarde dolara, u odnosu na 6,3 milijarde dolara u 2008. godini. Iako je većina nigerijskih prevara još uvek organizovana od strane ljudi koji stvarno žive u Nigeriji, same prevare nisu uvek obavljene od strane osoba iz Nigerije. Prema Izveštaju Ultrascan-a, 51.761 prevara je počinjeno iz 69 drugih zemalja, dok je ostalih 250.000 prevara počinjeno iz Nigerije. Po zaključku Ultrascan-a, prevare su prilagođene mogućnostima i potrebama države u kojoj se izvode. Na primer, u Kini se obično koriste prevare sa lutrijom ili prevare „gotovina na dostavu“, dok u Indiji obično koriste prevare sa ponudama za brzo zaposlenje i prevare sa studentskim vizama. Sa više od 41 milijarde dolara izgubljenih do danas i stopom rasta od 5% godišnje, sasvim je jasno da ove vrste prevara postaju sve opasnije, a samim tim sve teže za otkrivanje i suzbijanje. Ultrascan je takođe upozorio da su njihove procene zasnovane samo na otkrivenim slučajevima, odnosno da su realne procene ekspanzivnog razvoja ove pojave daleko veće. [15, 16]

Na teritoriji Republike Srbije u toku 2008. i 2009. godine od strane oštećenih lica prijavljeno je devet krivičnih dela prevare sa elementima „Nigerijskih prevara“, protiv nepoznatih učinilaca. Ovim krivičnim delima oštećeni su državljani Republike Srbije i preduzeća sa naše teritorije, a ukupna imovinska šteta iznosila je preko 60.000 EUR-a. Oštećena lica su novac izvršiocima krivičnih dela slali preko servisa Western Union i MoneyGram. Prevare su uglavnom vršene pomoću Spam poruka uz korišćenje metode socijalnog inženjeringa, a komunikacija je, nakon odgovora od strane oštećenih na Spam poruku, uglavnom vršena preko besplatni naloga za elektronsku poštu koja je otvarana na internet servisima Yahoo, Hotmail i dr. Takođe su upotrebljavane i lažne internet adrese na kojima se se nalazile internet prezentacije postavljene od strane izvršilaca krivičnih dela sa namerom da obmanu oštećene. Upotrebljavana je i falsifikovana dokumentacija državnih organa i preduzeća Nigerije, Gane i drugih država sa teritorije Zapadne Afrike. [14, str. 152] U slučajevima „Nigerijskih prevara“ čije su žrtve državljani Republike Srbije radilo se o prevarama izvršenim na nekoliko načina, i to: slanjem obaveštenja o lažnim dobicima na lutriji pomoću kojih su žrtve prevara metodama socijalnog inženjeringa navođene da poveruju da su dobitnici nagrada, nakon čega su uplaćivali određene sume novca da bi im se omogućilo podizanje nagrade, kao i slanjem obaveštenja o nasledstvu pomoću kojih su žrtve prevara metodama socijalnog inženjeringa navođene da poveruju da su nasledile određenu količinu novca, nakon čega su uplaćivali određene sume novca da bi im se omogućila isplata nasleđenog novca. Krivična dela su inicirana sa područja Nigerije, Senegala i Benina, a međunarodna policijska saradnja sa navedenim državama do danas nije dovela do značajnijih rezultata. [14, str. 154]

IV. ZAKLJUČAK

Iako je danas nemoguć život i funkcionisanje društva u celini bez upotrebe računara i savremene informatičke tehnologije, sazrela je svest da se ova korisna i potrebna sredstva mogu koristiti za nedopuštene, protivpravne ciljeve, u prvom redu za pribavljanje protivpravne imovinske koristi za neko lice ili za nanošenje štete drugima.

Pored zaključka da je u nacionalnim zakonodavstvima nephodno u što kraćem roku usvojiti adekvatne materijalne i procesne zakone koji će inkorporisati mere usaglašene sa Konvencijom o visokotehnološkog kriminala, a u skladu sa mogućnostima na prostoru svake države pojedinačno, neophodno je istaći i činjenicu da je potreban i veći stepen pažnje naučne i stručne javnosti, makar u onom segmentu koji je potreban da se karakteristike zloupotreba informacionih tehnologija uvaže na adekvatan način.

Isto tako, pitanje zloupotreba informacionih tehnologija, naročito ukoliko su u pitanju pojavni oblici koji obuhvataju različite vrste prevarnih manipulacija elementima računarskih sistema, nije samo pravno pitanje. Naime, „sasvim je jasno da se određenoj pojavi društvo adekvatno može suprotstaviti ukoliko sagleda sve njene karakteristike i uđe u sve pore njenih specifičnosti“. [17] S obzirom da se radi o problemu koji uzrokuje ogromne finansijske gubitke velikog broja ne samo razvijenih zemalja, već i država koje prolaze kroz proces tranzicije, potrebno je obratiti pažnju na ekonomske efekte ovih pojava na privredne tokove u svakoj državi pojedinačno. „Mesto i uloga ICT sektora u ekonomskom razvoju države strateški je važno pitanje”. [18, str. 684]

LITERATURA

[1] J. Matijašević and S. Ignjatijević, "Kompjuterski kriminalitet u pravnoj teoriji, pojam karakteristike, posledice" – "Cybercrime in legal theory, the concept, characteristics, consequenses", Zbornik radova sa međunarodnog naučno-stručnog Simpozijuma INFOTEH®-JAHORINA 2010, održanog od 17.-19. marta 2010. godine, Vol. 9, Ref. E-VI-8, p. 852-856, Elektrotehnički fakultet, Istočno Sarajevo, 2010, ISBN-99938-624-2-8.

[2] J. Matijasevic and Z. Spalevic, „Comparative review of criminal legislations in the field of computer crime" – Nineteenth International Electrotechnical and Computer Science Conference – ERK 2010, Portoroz, Slovenia, 20th -22nd September, 2010, Proceedings, Sekc./Sect. CS.6 22.09.2010 ob/at 10:30 v/in A, Security, Communications; Section Index: CS Računalništvo in informatika.

[3] J. Matijašević and M. Petković, „Krivična dela protiv bezbednosti računarskih podataka – analiza pozitivnopravnih rešenja i značaj u kontekstu suzbijanja visokotehnološkog kriminala", Zbornik radova sa međunarodne naučno-stručne konferencije „Kriminalističko-forenzička istraživanja", održane od 14.-15. oktobra 2011. godine, Internacionalna asocijacija kriminalista - IAK, Banja Luka, str. 598-609,Vol. 4, Broj 1, ISBN 978-99955-691-1-2.

[4] B. Banović, „Obezbeđenje dokaza u kriminalističkoj obradi krivičnih dela privrednog kriminaliteta", Viša škola unutrašnjih poslova, Beograd - Zemun, 2002.

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

[6] Council of Europe, Recommendation No. R (89) 9 of the Committee of Ministers to member states on Computer-related crime, https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2 (pregledano: 8.1.2011.)

[7] J. C. Bellour , „Međunarodna prevara", Izbor br.1, Zagreb, 1981.

[8] H. Wolfgang, „Taglich 500 Milliarden USD – Transaktionen uber EDV", Kriminalistik, 12/1984.

[9] Kompjuterski kriminalitet, APIS Security Consulting; http://www.apisgroup.org/sec.html/Knjige/UMOB/sec.html?id=29 (pregledano: 5.9.2010.)

[10] The Latest Cybercrime Statistics On The Internet, Tech Watch, http://www.techwatch.co.uk/2008/04/04/the-latest-cybercrime-statistics/ (преузето: 12.2.2011.)

[11] M. Babović, „Hakerska subkultura i kompjuterski kriminal", Pravni život – časopis za pravnu teoriju i praksu, br. 9/2004, Godina LIII, Knjiga 485, 1-1356, Udruženje pravnika Srbije, Beograd.

[12] Advance-fee fraud, From Wikipedia, the free encyclopedia; http://en.wikipedia.org/wiki/Advance-fee_fraud (pregledano: 8.1.2011.)

[13] http://www.vesti-online.com/Vesti/Hronika/48828/MUP-Nigerijska-prevara-odnela-Srbima-stotine-hiljada-evra (pregledano: 8.1.2011.)

[14] V. Urošević, „Nigerijska prevara u Republici Srbiji", Bezbednost – časopis Ministarstva unutrašnjih poslova Republike Srbije, Br. 3/2009, Godina LI, Beograd.

[15] Ultrascan Advanced Global Investigations, http://www.ultrascan-agi.com/ (pregledano: 9.1.2011.)

[16] Nigerijska prevara odnela devet milijardi dolara u 2009. godini, http://onlinetrziste.com/2010/01/30/nigerijska-prevara-odnijela-9-milijardi-dolara-u-2009/ (pregledano: 8.1.2011.)

[17] J. Matijasevic and Z. Spalevic, „Specific characteristics of computer criminal offenses with regard to the law regulations", XLV International Scientific Conference on Information, Communication and Energy Systems and Technologies – ICEST 2010 CONFERENCE, 23.-26. June 2010., Faculty of Technical Sciences, University „St. Clement Ohridski", Bitola, Ohrid, Macedonia, 2010, Proceedings, (http://www.icestconf.org/index.php?option=com_content&view=frontpage&Itemid=98, Preuzeto: 5.2.2011.)

[18] S. Ignjatijević, J. Matijašević and M. Carić, „Uslovi poslovanja i poslovnog okruženja u Republici Srbiji sa akcentom na upotrebu informaciono-komunikacione tehnologije", Zbornik radova sa međunarodnog naučno-stručnog Simpozijuma INFOTEH®-JAHORINA 2011, održanog od 16.-18. marta 2011. godine, Vol. 10, Ref. E-IV-6, p. 681-684, Elektrotehnički fakultet, Istočno Sarajevo, 2011; str. 684; Zbornik radova dostupan na Internet sajtu: http://www.infoteh.rs.ba/zbornik/2011/radovi.html,(preuzeto:27.1.2012.)

ABSTRACT

Computer technology can be abused in various ways. One form of abuse of Information Technology are computer fraud. They represent the most common form of computer crime, and have mostly the property character (obtaining illegal material benefit). Specific types of computer fraud are "Nigerian scam" - the method of the criminal act which includes the computer abuse. It most often begins by letter or electronic message that is designed to look like it was intentionally sent to the recipient of the message. These are false messages about the gains in the games of chance, charitable contributions, and others. Misuse of information technologies is not just a legal question. Given that this is a problem that is causing huge financial losses, it is necessary to pay attention to the economic effects of the economic trends in each country individually.

TYPES OF INTERNET FRAUD - NIGERIAN SCAM, TERM, THE SIGNIFICANCE AND IMPACT OF THE ECONOMIC AND MORAL ASPECTS OF THE COMMUNITY

Jelena Matijašević, Žaklina Spalević, Svetlana Ignjatijević