Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-277-281

KORIŠĆENJE INTERNETA U VISOKOTEHNOLOŠKOM KRIMINALU

Nada Arežina, Vule Mizdraković, Goranka Knežević
Univerzitet Singidunum, Beograd

Abstract:
Poslovne organizacije se danas suočavaju sa povećanom opasnošću od visokotehnološkog ili cyber kriminala. Različita istraživanja na globalnom nivou, pokazuju porast ove vrste kriminalnih radnji koje su počinjene na računaru i mreži, s obzirom na to da se danas sve više ljudi i organizacija oslanja upravo na internet i informacione tehnologije. Kao novi podsistem ekonomskog kriminala, visokotehnološki kriminal predstavlja opasnu pretnju. Počinioci kriminalnih radnji mogu uz pomoć interneta, pored ostalih sredstava, na veoma brz i lak način, iz raznih delova sveta, naneti značajne štete, kako fizičkim, tako i pravnim licima. U ovom radu, pokušaćemo da pružimo više informacija u vezi implikacija koje pomenute aktivnosti mogu imati na poslovne organizacije.

Key words:
internet,
kriminalne radnje,
pravna lica.

UVOD

Sam razvoj internet tehnologija uticao je na unapređenje različitih oblasti, počevši od istraživanja u edukativne svrhe, administracije, poslovnih transakcija, industrijske proizvodnje, do globalnog prenosa informacija koji sa internetom postaje dostupan svima i omogućava bezbroj mogućnosti. U 2011. godini, najmanje 2,3 milijarde ljudi, tačnije više od jedne trećine ukupne svetske populacije, je imao pristup internetu. Preko 60 procenata svih korisnika interneta čini stanovništvo država u razvoju, gde 45 procenata svih korisnika interneta čini populacija mlađa od 25 godina. Procenjuje se da će, do 2020. godine, broj umreženih uređaja (internet aparata) nadmašiti broj ljudi, čak šest puta [1]. U svom nacrtu izveštaja, iz 2013. godine, kancelarija Ujedinjenih nacija za pitanja droge i kriminala (UNODC) navodi da će u budućnosti postati nezamislivo da bilo koja kriminalna radnja ne bude povezana sa internet konekcijom. Danas se ne može zamisliti poslovanje bez interneta, počevši od slanja elektronske pošte, traženja informacija preko internet pretraživača, posete web stranica privrednih društava raznovrsnih delatnosti, usluga koje nam pruža on-line trgovina itd. Ipak, iako pruža mnoge pogodnosti, internet se može koristiti u druge nezakonite svrhe od strane lica koja vrlo često koriste ovu mrežu kao sredstvo kako bi počinili prevare i na taj način stekli protivpravnu korist.

POJAM I KARAKTERISTIKE VISOKOTEHNOLOŠKOG KRIMINALA

U širem smislu, prevara može obuhvatiti bilo koju vrstu kriminalne radnje zarad sticanja koristi, koja upotrebljava obmanu kao osnovni čin izvršenja. Prevare se mogu definisati kao oblici svih ljudskih radnji, koje su zakonima određene kao krivična dela i koje u svom načinu izvođenja koriste obmanu kao sredstvo za pribavljanje protivpravne imovinske koristi [2]. Kriminalna radnja predstavlja opšti izraz i podrazumeva različite načine prevare koje ljudski um može osmisliti i kojima pojedini pribegavaju, kako bi kroz lažne tvrdnje ostvarili prednost nad drugima [3]. Stoga, pojedinim tehnikama visokotehnološkog ili *cyber* kriminala se takođe može vršiti protivpravno prisvajanje sredstava pravnog lica, ili se krađom podataka iz baze podataka sa istom namenom prikrivati identitet. Kancelarija Ujedinjenih nacija za pitanja droge i kriminala definiše visokotehnološki kriminal kao bilo koju kriminalnu radnju koja se vrši u elektronskom ambijentu. Visokotehnološki kriminal takođe može podrazumevati i kriminalnu radnju koja koristi infrastrukturu informacione tehnologije, sa ciljem nezakonitog pristupa, nezakonitog presretanja i ometanja podataka, sistemskih uticaja, zloupotrebe opreme, krivotvorenja ili krađe identiteta i elektronske prevare [2]. Symantec, kao jedna od najpoznatijih kompanija na svetu, koja pruža usluge zaštite računarskih sistema od virusnih i drugih napada, definiše visokotehnološki kriminal kao

bilo koju vrstu kriminalne radnje počinjene korišćenjem računara, mreže ili hardverskog uređaja.

U Krivičnom Zakoniku Republike Srbije, pod visokotehnološkim kriminalom podrazumeva se skup sledećih krivičnih dela: [4]

- Oštećenje računarskih podataka i programa
- Računarska sabotaža
- Pravljenje i unošenje računarskih virusa
- Računarska prevara
- Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka
- Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži i
- Neovlašćeno korišćenje računara ili računarske mreže.

Ovde spadaju još i dela protiv intelektualne svojine, imovine pravnog saobraćaja, prevare, zloupotreba platnih kartica na internetu, zloupotreba u oblasti elektronske trgovine i bankarstva, zloupotrebe dece u pornografske svrhe na internetu kao i govora mržnje na internetu kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju, računarske mreže i računarski podaci.

Prema podacima Ministarstva unutrašnjih poslova Republike Srbije (MUP) najčešći oblici izvršenja krivičnih dela na internetu su računarske prevare vezane za aukcijske internet sajtove (elektronske prodavnice), kompromitovanje i upotreba platnih kartica, "Nigerijske prevare" i DDoS napadi [4]. Radi boljeg razumevanja samih šema visokotehnološkog kriminala, pojedine ćemo detaljnije obrazložiti u nastavku rada.

METODE ČINJENJA KRIMNALNIH AKTIVNOSTI NA INTERNETU

Jedan od najrasprostranjenijih oblika krivičnih dela internet prevare jeste prevara poznata kao „Nigerijska prevara" ili „Prevara 419[1]". *Nigerijska prevara* predstavlja specifičan način izvršenja krivičnog dela koji je nastao zahvaljujući globalnoj ulozi interneta kao sredstva za komunikaciju, elektronskog poslovanja, kao i sve većoj upotrebi savremenih informacionih tehnologija od strane velikog broja krajnjih korisnika, širom sveta [5]. Radnja izvršenja „nigerijske prevare" počinje ubeđivanjem „žrtve" prevare da učestvuje u podeli određenih novčanih fondova, ako unapred uplati traženi novčani iznos koji je, u najvećem broju slučajeva, neuporedivo manji od onog iznosa koji bi trebalo da dobije kao korist od tog fonda [6]. Osoba koja se obraća žrtvi najčešće se predstavlja kao ministar, direktor banke, vlasnik korporacije, diplomata ili lekar, advokat, udovac/udovica ili čak bankarski predstavnik. Predlog saradnje obavezno sadrži opis neke neverovatne situacije, kao što je višak novčanih sredstava na nekom ugovoru, nasledstvo, zaplenjena sredstva strane vlade, uključujući plemenite metale i dijamante, gde je neophodno da se sredstva prebace na račun „žrtve" kako ista ne bi bila zauvek izgubljena. Dalje, potrebno je da osoba uplati neznatnu količiinu novca kako bi učestvovala u transakciji. U toku 2008. i 2009. godine na teritoriji Republike Srbije od strane oštećenih lica prijavljeno je devet krivičnih dela prevare sa elementima „nigerijskih prevara" protiv nepoznatih počinilaca. Ovim krivičnim delima oštećeni su državljani Republike Srbije i pravna lica sa naše teritorije, a ukupna imovinska šteta iznosila je preko 60.000 evra [5]. Prema istraživanju holandske agencije Ultrascan, koja se bavi istragama i analizom internet prevara, u svom izveštaju *419 Advance Fee Fraud Statistics 2009* u kom je analizirano 8.503 slučajeva u preko 152 zemalja u toku 2009. godine, žrtve su izgubile 9,3 milijardi dolara zahvaljujući ovoj prevari. Ultrascan, navodi da su njihove procene minimalne, jer ne postoji centraliziovano mesto za praćenje i izveštaj prevara 419, dok su stvarni brojevi daleko veći [7].

Krađa identiteta, jeste takođe čest oblik kriminalne aktivnosti i iako možda nose veći rizik za pojedinca, napadi na poslovne organizacije ovog tipa nisu izuzetak. Primer su pecaroške ili fišing *(engl. phishing)* elektronske poruke koje navodno potiču sa određenog sajta za kupovinu putem interneta, koje zahtevaju od klijenta da im se dostave određene ažurirane lične informacije, broj kreditnih kartica, lozinki itd. Prema Saši Živanoviću, načelniku Odeljenja za visokotehnološki kriminal MUP-a Republike Srbije, jedna od taktika koja se primenjuje jeste da klijent od svoje banke dobije mail o povećanju bezbednosti, gde se od njega traži da klikne na link i popuni podatke o svojoj kartici. Kada to učini, otvara se identična stranica na koju je klijent već ulazio i dobija se drugi mejl, gde je ispisano obaveštenje *"uneli ste podatke sa pogrešne kartice*, jer prestupnici pretpostavljaju da svaki građanin danas ima dve kartice. Podaci koje *"pecaroši"* tako prikupe se dalje koriste u kriminalne svrhe. Ovakav primer u Srbiji poznat je pod nazivom "Subotička prevara", u kojoj se osoba registrovala kao pravno lice samo da bi dobila POS terminal (engl. *Point of Sale*),[2] koji je isključivo služio za provlačenje lažnih kartica [8].

Još jedna alatka koju prestupnici mogu koristiti u svrhe tajnog prikupljanja podataka o korisniku jeste *Spyware*. Ovaj softver tajno prikupljanja podatake koristeći internet konekciju korisnika bez njegovog znanja, uglavnom u svhe reklamiranja, ali može se koristiti i u druge nezakonite svrhe. Spyware aplikacije su često spakovane u paketu kao skrivena komponenta besplatnih programa ili softverskog programa i mogu se takođe preuzeti sa interneta [3]. Naime, pomoću ovog softvera može se snimiti sve što se dešava na računaru i prebaciti na udaljeni sajt, te se mogu prikupiti lični podaci korisnika, brojevi kreditne kartice, e-mail adrese, lozinke itd. Na primer, u 2006. godini približno 79 procenata svih računara u organizacijama u SAD-u su bili inficirani nekim oblikom Spyware [9].

Ucena predstavlja oblast visokokriminalne aktivnosti, gde su često na meti poslovne organizacije koje imaju razvijenu internet prodaju. Odnosi se na pretnju ili napad na samu organizaciju uz zahtev za značajnu sumu novca kako bi napad bio sprečen ili zaustavljen. Jedan od najčešćih oblika jeste napad odbijanja usluge (engl. *Denial of Service-DoS*) koji je usmeren na obaranje i zastoj rada

1 Dobila je naziv po članu broj 419 Nigerijskog krivičnog zakona.

2 Terminal koji je opremljen softverom za procesiranje transakcija platnim karticama i koji omogućava plaćanje robe i usluga. Koristi se u uslužnim i trgovačkim radnjama.

računarskih sistema, a pogotovo web servera na mreži koji omogućavaju elektronsku trgovinu. Najjednostavniji DoS napad zapravo je pretrpavanje web servisa ili stranice sa izrazito velikim brojem posebno konstruisanih zahteva, sve dok se server ne zaguši ili uspori do te mere da posetioci više ne mogu da otvore tu web stranicu [3]. Sa druge strane, DDoS (engl. *Distributed Denial of Service*) napad se sprovodi korišćenjem više računara i služi se snagom višestrukih posrednih korisnika. Napadač obično koristi jednu izabranu mašinu kao glavnu i koordinira napadom preko drugih računara. Masovniji DDoS napadi počeli su 2000. godine kada su „oboreni" popularni sajtovi kao što su Amazon, CNN, eBay, Yahoo i drugi [10]. Prema istraživanju Ponemon Instituta, u izveštaju *2013 Cost of Cyber Crime Study,* navodi se da je američku kompaniju u proseku u 2013. godini koštalo oko 240 hiljada američkih dolara zbog napada DoS vrste koja se inače nalazi u vrhu liste najskupljih metoda napada [11].

Virusi predstavljaju jednu od najznačajnijih pretnji poslovnim organizacijama, u smislu izgubljenih resursa. Virusi mogu izbrisati ili onesposobiti sistemske podatke, operativni sistem ili aplikativni softver. Procenjuje se da virusi godišnje nanose štetu američkim kompanijama u iznosu od 55 milijardi dolara. Poznat je slučaj internet prestupnika koji je skoro uništio jednu organizaciju koja se bavila konsultantskim uslugama, tako što je uz pomoć virusa izbrisao sve značajne datoteke koje su čuvane na mreži. Ova konsultantska kuća nije u to vreme imala rezervnu kopiju što je zloupotrebljeno i na ovaj način izgubila je sve trenutne informacije o projektima, što je rezultiralo da je njeno poslovanje bilo na rubu kolapsa [3].

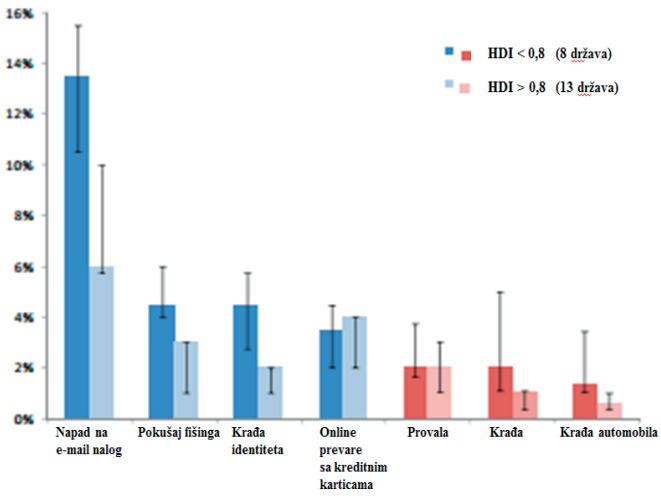
U 2013. godini poznat je slučaj *Gozi* virusa koji su kreirala tri osobe iz Evrope, kasnije optužene za kreiranje i distribuciju računarskog virusa koji je inficirao više od million računara širom sveta, omogućavajući im pristup ličnim podacima banaka i krađom najmanje 50 miliona dolara u periodu između 2005. i 2011. godine. Smatra se jednim od najdestruktivnijih finansijskih prevara ovog tipa do sada [1].

Internet aukcije predstavljaju proces kupovine i prodaje raznovrsnih sredstava na internetu, po metodi ko ponudi (izlicitira) više, u kome onaj ponuđač koji ponudi najviše cene pobeđuje i dobija. Sa više miliona transakcija koje se odvijaju svakodnevno na online aukcijiskim sajtovima, ovakav način kupovine i prodaje na internetu sve više postaje uobičajen način trgovine. Pogodnosti online trgovine navode se i u časopisu *Economist*, kroz obrazloženje da je internet uveo mogućnost nastanka internacionalnog bazara u kome nema definitivno određene cene, gde su sve informacije na raspolaganju i odmah dostupne, a gde kupci i prodavci kroz cenkanje pokušavaju da za sebe postignu najpovoljniju cenu [12]. Ipak, aukcijski sajtovi zbog svoje aktuelnosti i velikog broja korisnika pružaju mogućnost i za činjenje prevara. Neki od primera nezakonitih radnji mogu biti: lažno predstavljanje, neisporučivanja robe, isporučivanje robe koja ne odgovara kvalitetu, uključivanje naknadnih troškova dostave koji se dodaju tek nakon što je izvršena kupovina, veštačko naduvavanje cena određenog predmeta od strane lažnih ponuda korisnika lažne lične karte ili saučesnika, prodaje robe sa crnog tržišta itd.

UTICAJ INTERNETA NA RASPROSTRANJENOST VISOKOTEHNOLOŠKOG KRIMINALA

Kompanija Symantec, iznela je rezultate istraživanja visokotehnološkog kriminala u svom godišnjem izveštaju u kom ukazuje na konstantan rast pojave ove vrste kriminala u čitavom svetu. U izveštaju se navodi da na globalnom nivou visokotehnološki kriminal nanosi štete od 113 milijardi dolara godišnje, a da prosečan trošak po žrtvi visokotehnološkog kriminala iznosi 298 dolara i predstavlja porast od 50% u odnosu na 2012. godinu, pa su rezultati zabrinjavajući, s obzirom na aktuelnu svetsku ekonomsku krizu [13].

Ispitivanja pokazuju da je procenat pojedinačnog visokotehnološkog kriminala znatno viši nego kod klasičnih formi kriminala. Stope viktimizacije[3] se kreću između 1 i 17 procenata online populacije za online prevare vezane za kreditne kartice, krađu identiteta u smislu pokušaja fišinga, kao i neovlaščene upade na e-mail naloge. Za razliku od prethodno navedenih kriminalnih radnji, kod običnih provala, razbojništva i krađa automobila, stope su se kretale ispod 5 procenata za 21 državu koje su činile uzorak istraživanja [1]. Na slici 1, na horizontalnoj osi, prikazani su različiti oblici kiminalnih radnji, dok su na vertikalnoj osi prikazani procenti respondenata kao žrtvi navedenih kriminalnih radnji u 2012. i 2011. godini. Možemo uočiti da su stope napada na e-mail nalog, pokušaj fišinga kao i krađe identiteta znatno više kod država sa nižim stepenom razvoja, koje Ujedinjene nacije rangraju prema indeksu razvijenosti države (HDI-Human Development Index). Otuda više stope viktimizacije visokotehnološkog kriminala u državama sa nižim stepenom razvoja naglašavaju potrebu da se usmeri posebna pažnja u cilju jačanja prevencije od ove vrste kriminalnih aktivnosti u pomenutim državama.

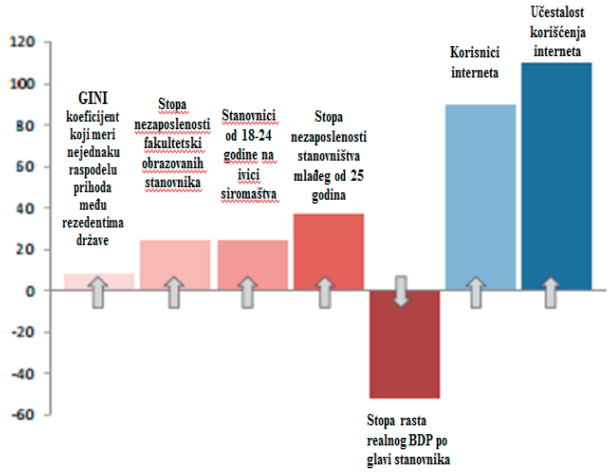


Sl. 1: Viktimizacija visokotehnološkog kriminala i klasičnih oblika kriminalnih radnji [1]

Još jedan faktor koji može da doprinese ekspanziji visokotehnološkog kriminala jeste potreba globalnog povezivanja u kontekstu svetske ekonomske i demografske transformacije. Od ukupno 15 ispitanih država, istraživanje

3 Viktimizacija je proces u kome pojedinac/poslovna organizacija postaje žrtva kriminalnih aktivnosti.

ukazuje na moguću povezanost između promena ekonomskih pokazatelja i tri klasične vrste kriminalnih radnji u 12 država [1]. Na slici 2 na horizontalnoj osi, prikazano je kretanje ekonomskih parametara sa jedne i korinsika interneta i učestalosti njegovog korišćenja sa druge strane, dok je na vertikalnoj osi izražen procenat promene u periodu od 2006. do 2011. godine. U pomenutom periodu možemo videti povećanje stope rasta nejednake raspodele prihoda među rezidentima države, stope siromašnog stanovništva, stope nezaposlenosti kako obrazovanih tako i stanovništva mlađeg od 25 godina, ali i pad stope realnog Bruto domaćeg proizvoda (BDP) po glavi stanovnika. Ipak, primetno je i da su prethodno pomenuti pokazatelji istovremeno praćeni značajnim rastom korisnika interneta kao i njegove učestalosti korišćenja. Prethodna istraživanja naglašavaju da socio-ekonomski faktori igraju važnu ulogu u razvoju trenda klasičnih kriminalnih aktivnosti, ali i visokotehnološkog kriminala.



Sl. 2: Socio-ekonomske promene i učestalost korišćenja interneta u zemljama Istočne Evrope u periodu od 2006.-2011. godine [1]

Dalje, uticaj ekonomske krize može doprineti da organizacije smanje svoju potrošnju kao i broj zaposlenih. Prethodno može da dovede, na primer, do smanjenja bezbednosti, dok se verovatnoća za iskorišćavanjem slabosti informacione tehnologije na ovaj način povećava. Ukoliko su zaposleni postali nezadovoljni nižim platama ili postoji strah od gubitka posla, rizik od kriminalnih radnji može porasti. Neke informatičke kompanije su izrazile zabrinutost da bivši zaposleni koji su proglašeni tehnološkim viškom, predstavljaju jednu od mogućih pretnji tokom perioda pada ekonomskih aktivnosti. Takođe, sve veći broj zaposlenih ili nezaposlenih osoba sa računarskim veštinama, naročito onih koji su fakultetski obrazovani, smatraju se potencijalom novih resursa za organizovani visokotehnološki kriminal [1].

ZAKLJUČNA RAZMATRANJA

U današnjim uslovima, poslovanje većine poslovnih organizacija u značajnoj meri zavisi od interneta, kao sredstva uz pomoć kog se obavljaju svakodnevne poslovne aktivnosti. Različiti sistemi, počevši od kontrole leta, elektronskog bankarskog poslovanja, finansijskog izveštavanja i izveštavanja o stečajnim postupcima, elektronske trgovine, u velikoj meri zavise od informacionih tehnologija. Na ovaj način poslovne organizacije postaju sve više ranjive na nove i sofisticirane metode visokotehnološkog kriminala. Kako visokotehnološki kriminal ima transnacionalni karakter, što omogućava uključenje više različitih država u proces njegovog izvršenja, ovo otežava mogućnost da kriminalna radnja bude otkrivena, kao i da prestupnik bude uhvaćen. Dalje, štete koje ovakve vrste kriminalnih radnji nanose organizacijama mogu usporiti funkcionisanje njihovog poslovanja, narušiti njihov ugled ili naneti značajnu ekonomsku štetu, koja može neretko rezultirati i prestankom poslovanja. Ipak, iako su različite države u svom krivičnom zakonodavstvu uvrstile različite tipove visokotehnološkog kriminala kao krivična dela, i dalje ovaj vid kriminalnih aktivnosti predstavlja veliku pretnju za poslovanje. Razlozi mogu biti različiti, od napredovanja i razvoja tehnologije, većeg broja korisnika interneta, integrisanja interneta u sve veći broj poslovnih aktivnosti, kao i novih metoda i šema kriminalnih radnji, koje otežavaju otkrivanje i iznošenje počinioca pred lice pravde. S obzirom na to da je uprava poslovnih organizacija odgovorna za uspostavljanje osnovnih ciljeva u vezi sa bezbednošću, ona mora identifikovati imovinu koju je potrebno zaštiti od rizika. Imajući u vidu da je internet kao komunikaciona mreža postao neizostavan element naših svakodnevnih aktivnosti, potrebno je što više edukovati stanovništvo i zaposlene o osnovnim metodama činjenja visokotehnološkog kriminala.

LITERATURA

[1] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime Draft-February 2013,* (pristup: 22.01.2014.), [dostupno na: http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf]

[2] Petković, A. *Forenzička revizija.* Proleter, Bečej, 2010.

Singleton, T., and Singleton, A., *Fraud auditing and forensic accounting,* New Jersey: John Wiley & Sons, 2010.

[3] MUP Republike Srbije, *Visokotehnološki kriminal- Šta je to?*, (pristup: 23.01.2014.), [dostupno na: http://www.mup.gov.rs/cms_lat/saveti.nsf/saveti-sajber-kriminal.h]

[4] Urošević, V., Nigerijska prevara u Republici Srbiji. *Bezbednost* , 2009, str. 1-12.

[5] Smith, R. G., Holmes, M. N., & Kaufmann, P. Nigerian Advance Fee Fraud. *Trends and Issues in in Crime and Criminal Justice*, (1999), str.1.

[6] Ultrascan Advanced Global Investigation, *419 Advance Fee Fraud Statistics 2009*. (pristup: 09.01.2014), [dostupno na: http://www.ultrascan-agi.com/public_html/html/pdf_files/419_Advance_Fee_Fraud_Statistics_2009.pdf]

[7] Vučetić, L. (2013). *SAJBER KRIMINAL: Kako srpska "internet policija" lovi pirate, prevarante i on-lajn pedofile!* (pristup: 20. 01. 2014.), [dostupno na: http://www.telegraf.rs/vesti/633771-sajber-kriminal-kako-srpska-internet-policija-lovi-pirate-prevarante-i-online-pedofile]

[8] Cistra Technologies Inc, *The Cost of Spyware to your Business,* (pristup: 29. 01. 2014.) [dostupno na:http://www.cistratech.com/whitepapers/costofspyware.pdf]

[9] Vuletić, D., Napadi na računarske sisteme. *Ministarstvo odbrane Republike Srbije Institut za strategijska istraživanja*, 2012., str. 235-249.

[10] Ponemon Institute, *2013 Cost of Cyber Crime Study:*. (pristup: 10.01.2014.) [dostupno na: http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf]

[11] The Economist, In The Great Web Bazaar. (pristup: 20.02.2014.) [dostupno na: http://www.economist.com/node/285614]

[12] Symantec, *2013 Norton Report*, (pristup 22. 01. 2014.), [dostupno na: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013]

INTERNET USE IN CYBER CRIME

Abstract:
Nowdays, business organizations are facing an increased risk of cyber crime. Different studies on the global level, show the growth of fraud committed by computer or internet, due to the fact that today more people and organizations rely on the internet and information technologies. As a new subsystem of economic crime, cyber crime represents a serious threat. The perpetrators of fraud, by using the internet, can very rapidly, from various parts of the world, cause significant damage to persons and legal entities as well. In this paper, we will attemp to provide more information regarding the implications that aforementioned activities may have on business organizations.

Key words:
internet,
fraud,
legal entities