ISSN 2334-718X
ISSN 2334-704X (Online)
DOI 10.12709/issn.2334-704X

46 69 6E 61
6E 63 65

42 75 73 69 6E
65 73 73

49 6E 66 6F 72
6D 61 74 69 6F
6E 20 26 20 49
6E 64 75 73 74
72 69 61 6C 20
74 65 63 68 6E
6F 6C 6F 67 69
65 73

4D 61 6E 61 67
65 6D 65 6E 74

FBIM Transactions

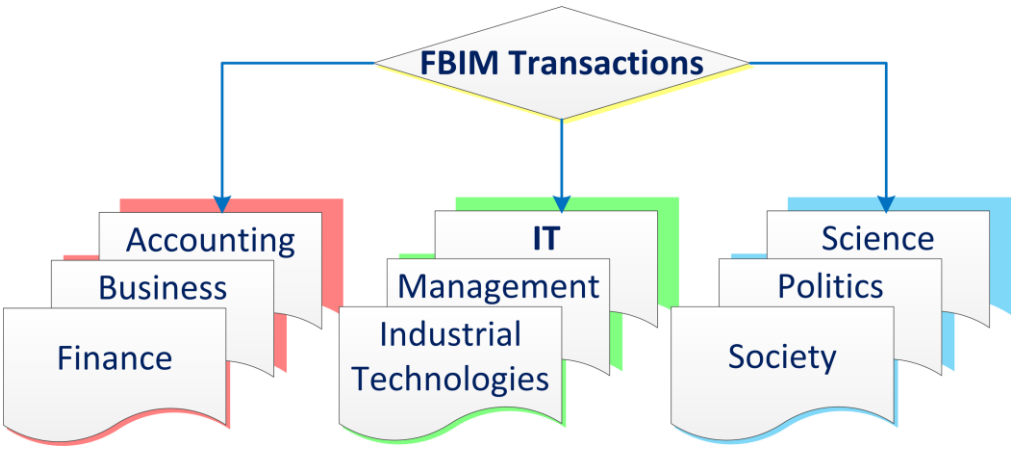
Edited by
Zoran Čekerevac

MESTE Year VII Vol. 7 No. 2 October 2019

ISSN 2334-718X
ISSN 2334-704X (Online)
DOI 10.12709/issn.2334-704X

This issue:
DOI: 10.12709/fbim.07.07.02.00

FBIM Transactions



Edited by
Zoran Čekerevac

MESTE Year VII Vol. 7 Issue 2 October 2019

CIP – Каталогизација у публикацији
Народна библиотека Србије, Београд

336+004+005

FBIM Transactions : Finance, Business, Information & Industrial technologies, Management / glavni i odgovorni urednik Zoran P. Čekerevac. – [Štampano izd.]. – Year 7, No. 2 (2019) - . – Beograd : MESTE NVO : Fakultet za poslovno industrijski menadžment ; Toronto : SZ & Associates, 2013- (Beograd : ICIM+). – 30 cm

Polugodišnje. – Tekst na srp. i engl. jeziku.
- Drugo izdanje na drugom medijumu: FBIM Transactions (Online) = ISSN 2334-704X
ISSN 2334-718X = FBIM Transactions (Štampano Izd.)
COBISS.SR- ID 196184844

Circulation: 100copies
Tiraž: 100 primeraka

FBIM Transactions

DOI 10.12709/issn.2334-704X
DOI of this issue: **10.12709/fbim.07.07.02.00**

FBIM Transactions is an international academic journal published online, as well as print (subscription), which publishes scientific and professional research articles and reviews in English and/or Serbian, or similar language. FBIM Transactions is published in Belgrade - Serbia and in Toronto - Canada. The focal point of the journal is at international level, with the view on matters from a global perspective, but, also, some papers concerning some local specific events could be published. The science and technological advancements and their socio-political impact that happens all over the world can find place in the FBIM Transactions. The journal is indexed by Index Copernicus in ICI Journals Master List ICV from 2016.

Publishers

- **MESTE NGO** – Belgrade
- **Faculty of Business and Law** of the "Union – Nikola Tesla" University in Belgrade, Belgrade, Serbia
- **SZ & Associates**, Toronto, Canada

Printed by: **ICIM+, Belgrade** Circulation: 100 copies
The journal was published online at URL: http://fbim.meste.org/FBIM_2_2019/K1.html

The FBIM Transactions is registered by ICI World of Journals, ICI Journals Master List, Crossref, doiSerbia of the National Library of Serbia, COBIB.SR, Matica Srpska Library, COBISS.SR and KoBSON EleCas database, Google Scholar, ResearchBib, Scilit, ROAD, ERIH PLUS...

All published papers have been double-blind peer reviewed.

Two issues of the journal are published annually: April 15th and October 15th.

ISSN 2334-704X (Online) and
ISSN 2334-718X

FBIM Transactions

DOI 10.12709/issn.2334-704X
DOI ovog izdanja: **10.12709/fbim.07.07.02.00**

FBIM Transactions je međunarodni akademski časopis koji se publikuje onlajn i u štampanoj verziji (za pretplatnike) i koji prihvata naučne i stručne, istraživačke i pregledne članke na engleskom i/ili srpskom jeziku (ili srodnim jezicima). FBIM Transactions se publikuje iz Beograda - Srbija i Toronta - Kanada. Časopis je fokusiran na međunarodni nivo, sa gledanjem na predmetnu materiju iz globalne perspektive, ali i neki od radova koji se odnose na lokalne, specifične, pojave, takođe, mogu biti publikovani. Naučna i tehnološka unapređenja i njihovi društveno-politički uticaji širom sveta mogu da nađu svoje mesto u FBIM Transactions. FBIM Transactions je indeksiran kod Index Copernicus-a u ICI Journals Master List od 2016. godine.

Izdavači

Izvršni izdavač
- **MESTE -** Beograd

Suizdavači
- **Poslovni i pravni fakultet –** "Union – Nikola Tesla" Univerziteta iz Beograda
- **SZ & Associates** – Toronto, Kanada

Uredništvo - Redakcija:

Izdavački savet - Naučni odbor:

Štampa: **ICIM+, Beograd** Tiraž: 100 primeraka
Žurnal je publikovan i onlajn na URL adresi: http://fbim.meste.org/FBIM_2_2019/K1.html

Žurnal FBIM Transactions je registrovan u ICI World of Journals, ICI Journals Master List, Crossref, doiSerbia of the National Library of Serbia, COBIB.SR, Matica Srpska Library, COBISS.SR and KoBSON EleCas database, Google Scholar, ResearchBib, Scilit, ROAD, ERIH PLUS...

Svi publikovani radovi su recenzirani od strane dva recenzenta.

Časopis se publikuje dva puta godišnje: 15. aprila i 15. oktobra.

ISSN 2334-704X (Online) i
ISSN 2334-718X

FBIM Transactions
Year VII, Vol. 7, Issue 2
DOI: 10.12709/fbim.07.07.02.00

Editorial on FBIM Transactions 2019-2

Prof. Dr. Dr. h. c. Zoran Čekerevac[1]
(1) Faculty of Business and Law, "Union - Nikola Tesla" University, Knez Mihailova 33, Belgrade, Serbia
Email: zoran@cekerevac.eu

Belgrade
October 15th, 2019

(Without Abstract)

Welcome to the October 2019 issue of the FBIM Transactions, an international peer-reviewed academic journal, the official journal of the non-profit organization MESTE, and the Faculty of Business and Law of the "Union – Nikola Tesla" University in Belgrade, and the SZ & Associates - Toronto. This issue is published online and in print.

The focal point of the journal remained at international level, with the view on matters from a global perspective. However, due to their importance, in this issue have been published some papers relating to some specific local events. Sixteen papers have been published in this issue. Most of the articles are multidisciplinary, but connected with use of Internet and IT.

All articles published in this issue, as well as in the previous issues of the FBIM Transactions journal have their own DOIs.

We keep the practice that articles, that have undergone peer review, and will be published in the next issues, we make available to readers in the form of preview - early reading.

We follow the mission and vision of the journal, and we help authors to publish their works and present their achievements in the most convenient way. It should be borne in mind that the editors do not censor the works that we publish. The published works can contain and/or proclaim views that could differ from the views of the editorial board. We check articles on plagiarism, but we are not able to guarantee the accuracy of the data published in scientific and professional works of our authors. We believe that our authors are honorable and publish only their original works with really achieved results. For the quality of the papers we publish, we thank the authors and reviewers who did their job well and conscientiously.

You can follow us on the Facebook:
https://www.facebook.com/www.meste.org?ref=profile
as well as on the Twitter:
https://twitter.com/MesteZc

We invite you to publish your works with our motto:
"If you wish to be quoted, people first have to hear for you".
We will help you!

Prof. Dr. Zoran Čekerevac
Editor-in-Chief

FBIM Transactions
Godina VII, Vol. 7, Broj 2
DOI: 10.12709/fbim.07.07.02.00

Reč urednika kao predgovor za FBIM Transactions 2019-2

Prof. dr Dr. h. c. Zoran Čekerevac[1]
(1) Poslovni i pravni fakultet „Union – Nikola Tesla" Univerziteta, Knez Mihailova 33, Beograd, Srbija
zoran@cekerevac.eu

Beograd
15.10.2019.

(Bez apstrakta)

Dobro došli u aprilski broj FBIM Transactions, međunarodnog dvostruko „peer review" recenziranog akademskog časopisa organizacije MESTE, Poslovnog i pravnog fakulteta Univerziteta „Union – Nikola Tesla" iz Beograda i SZ & Associates iz Toronta (Kanada). Ovaj broj je objavljen onlajn, kao i u štampanom obliku (za pretplatnike).

Žurnal je fokusiran na teme od internacionalnog značaja, sa pogledom na te teme iz globalne perspektive. Ipak, zbog svog značaja, i u ovom broju su publikovani i neki radovi koji se odnose na neke lokalne specifične događaje. U ovom broju je objavljeno šesnaest radova. Većina radova je multidisciplinarna, ali i povezana sa upotrebom Interneta i IT.

Svi radovi objavljeni u ovom broju časopisa kao i svi radovi objavljeni u prethodnim brojevima FBIM Transactions imaju svoje DOI brojeve.

Zadržali smo praksu da radove koji su pozitivno recenzirani i koji će biti objavljeni u narednim brojevima časopisa, učinimo dostupnim čitaocima u obliku ranog prikaza - prikaza pre zvaničnog publikovanja. Tako je i većina objavljenih radova bila dostupna javnosti i pre zvaničnog publikovanja.

Mi sledimo misiju i viziju časopisa da pomogne autorima da objave svoje radove i prezentuju svoja dostignuća na najadekvatniji način. Treba imati u vidu da uredništvo ne cenzuriše radove koje publikuje, kao i da u radovima objavljeni stavovi ne moraju da se poklapaju sa stavovima uredništva. Mi kontrolišemo radove na plagijarizam, ali nismo u mogućnosti da garantujemo za tačnost podataka i rezultata objavljenih u radovima naših autora. Mi verujemo da su naši autori časni ljudi i da publikuju svoje originalne radove. Za ostvareni kvalitet publikovanih radova posebno smo zahvalni autorima i recenzentima koji ovaj težak zadatak obavljaju kvalitetno i savesno.

Možete nas pratiti na Fejsbuku *(Facebook):*
https://www.facebook.com/www.meste.org?ref=profile
kao i na Tviteru *(Twitter):*
https://twitter.com/MesteZc

Želimo vam puno uspeha i pozivamo vas da publikujete svoje radove našom devizom:
„Ako želite da budete citirani, ljudi prvo treba da čuju za vas!"
Mi ćemo vam u tome pomoći!

Zoran Čekerevac
Urednik

Finance
- Banking
- Behavioral finance
- Business finance
- Corporate finance
- Finance theory
- Financial markets
- Financial strategies
- International finance
- Modeling in finance
- Public finance
- Taxation

Business
- Accounting and auditing
- Business communications
- Business economics
- Business information system
- Business taxation
- E-business
- Economics, including economic: policy,systems, and theory
- Education for business
- Enterpreneurship
- Inovation and technology
- International trade
- Life long learning
- Marketing

Information and industrial technologies
- Application of IT in management
- Application of IT in higher education
- Cloud computing
- Computers and new technologies
- Data protection
- Industrial research
- Information technology
- New services
- Information security
- Information system security

Management
- Politics and society
- Public management
- Public administration
- Legal Aspects of Management
- Management in agribusiness
- Management in crisis situations
- Management in ecology
- Management in economics
- Management in education
- Management in industry
- Management in Transport
- Technologies and quality tools in management

Finansije
- Bankarstvo
- Bihejvioralne finansije
- Poslovne finansije
- Korporativne finansije
- Finansijsku teoriju
- Finansijska tržišta
- Finansijske strategije
- Međunarodne finansije
- Modeliranje u finansijama
- Javne finansije
- Oporezivanje

Biznis
- Računovodstvo i revizija
- Poslovne komunikacije
- Poslovna ekonomija
- Poslovni informacioni sistemi
- Oporezivanje u poslovanju
- E-poslovanje
- Ekonomija, uključujući ekonomsku: politiku, sisteme, i teoriju
- Obrazovanje za potrebe poslovanja
- Preduzetništvo
- Inovacije i nove tehnologije
- Međunarodna trgovina
- Celoživotno učenje
- Marketing

Informacione i industrijske tehnologije
- Primena IT u menadžmentu
- Primena IT u visokom obrazovanju
- Računarstvo u oblaku - Cloud computing
- Računari i nove tehnologije
- Zaštita podataka
- Industrijska istraživanja
- Informacione tehnologije
- Nove usluge
- Zaštita informacija
- Zaštita informacionih sistema

Menadžment
- Politika i društvo
- Menadžment javne uprave
- Javna uprava
- Pravni aspekti menadžmenta
- Menadžment u poljoprivredi
- Menadžment u kriznim situacijama
- Menadžment u ekologiji
- Menadžment u ekonomiji
- Menadžment u obrazovanju
- Menadžment u industriji
- Menadžment u transportu
- Tehnologije i alati kvaliteta u menadžment

FBIM Transactions
DOI 10.12709/fbim.07.07.02.01

MJERE PREVENCIJE I SIGURNOSNE POLITIKE PROTIV CYBER TERORIZMA

PREVENTION MEASURES AND SECURITY POLICIES AGAINST CYBER TERRORISM

Vladica Babić
Visoka Škola Logos, Mostar, Bosna i Hercegovina

JEL kategorija rada: **L86**

Apstrakt

Cyber terorizam predstavlja možda i najveću prijetnju nacionalnoj i međunarodnoj sigurnosti država od vremena stvaranja oružja za masovno uništenje. Kako države i njihova privreda postaju sve umreženiji, uglavnom putem informacijskih mreža, te Interneta, i na međunarodnom financijskom sustavu globalne trgovine, učinci cyber terorističkih napada će imati sve veći utjecaj. Isto tako, važno je kako će cyber teroristi steći iskustvo u narušavanju nacionalne sigurnosti i otvorenosti informacijske infrastrukture, njihovi napadi će vjerojatno postati sve uspješniji. Iako su države, privatne industrije i međunarodne organizacije učinile značajne napore za povećanje međunarodne suradnje, još puno toga treba biti učinjeno. Pri tome moramo shvatiti da je, s obzirom na temeljne slabosti u strukturi Interneta, potrebno načiniti i dodatne napore kako bi u potpunosti spriječili cyber terorizam. U vezi s tim, a i u svrhu otkrivanja ovakve prijetnje na pravi način, neophodna je obavještajna i sigurnosna suradnja, kako bilateralno tako i multilateralno, uključujući i razmjenu iskustava i relevantnih informacija iz ovog područja.

Ključne riječi: *Terorizam, cyber kriminal, prevencija, sigurnosna politika.*

Abstract

Cyber terrorism is perhaps the biggest threat to the national and international security of states since the time of mass destruction. As the state and their business become more and more networked, mostly through information networks, the Internet, and the international financial system of global trade, the effects of cyber-terrorist attacks will have an increasing impact. Likewise, it is important that cyber terrorists gain experience in disrupting national security and openness of information infrastructure, and their attacks will probably become more successful. Although the state, private industry, and international organizations have made significant efforts to increase international co-operation, much more needs to be done. We must realize that, given the fundamental weaknesses in the structure of the Internet, further efforts are needed to fully prevent cyber terrorism. In this respect, and in order to detect this threat in the right way, intelligence and security cooperation, both bilaterally and multilaterally, including exchange of experience and relevant information in this area is necessary.

Keywords: *Terrorism, cybercrime, prevention, security policy.*

Adresa autora:
Vladica Babić
vladica.babic@net.hr

1 UVOD

Terorizam je jedan od najsloženijih, najizazovnijih i najopasnijih političko-sigurnosnih fenomena današnjice. Cyber terorizam, kao njegov poseban oblik zahtijeva specifičnu pozornost pri njegovom suzbijanju. Kao spoj politike i nasilja, kao uporaba terora (nasilja, zastrašivanja), i pri tome još uključenost u suvremene tehnologije, cyber terorizam je uvijek u cilju udara na državni, politički i društveni sustav, te građane jedne države. Stoga odgovor na cyber terorizam i sam terorizam zahtijeva ukupnost koordiniranog državnog i društvenog djelovanja. Da bismo se uspješno branili od cyber terorizma potrebne su mjere preventivnog djelovanja, mjere suzbijanja cyber terorizma, mjere zaštite od cyber terorizma, saniranje posljedica nastalih djelovanjem cyber terorizma, izgradnja pravnog sustava za borbu protiv cyber terorizma, zatim edukacija, osposobljavanje i trening za borbu protiv cyber terorizma, te provođenje koordinacije i međunarodne suradnje.

Donošenje ključnih dokumenata kao što su Strategija, Akcioni planovi, Konvencije, te drugi pravni akti po pitanju rada na prevenciji i suzbijanju cyber terorizma predstavljaju upravo takav pristup i okvir djelovanja svake države prema ovoj pojavi. Sustavni pristup u takvim dokumentima bi sigurno smanjio mogućnost pojave, djelovanja i u dobroj mjeri pomogao u suzbijanju cyber terorizma. Ove mjere predstavljaju detaljno razrađene postavke i aktivnosti koje bi svakako trebale biti provedene. Pri tome, pod pojmom cyber terorizam svrstavamo osmišljenu, sustavnu, namjernu uporabu nasilja, ili prijetnje nasiljem protiv ljudi i/ili materijalnih dobara, uključujući i informacijske mreže i sredstva, kao sredstvo za izazivanje straha ili usmjerenog protiv njega, a sve unutar neke etničke ili vjerske zajednice, javnosti, države ili cijele međunarodne zajednice, u cilju ostvarenja političkih, vjerskih, ideoloških ili društvenih ciljeva. Jedna od glavnih karakteristika cyber terorizma je da se za djelovanje koristi cyber prostor, da ga prakticiraju najčešće nedržavne organizacije ili grupe, koje mogu imati potporu izvana od strane neke države ili država, a često i od organizacije čija javno deklarirana namjera i ciljevi nemaju veze s terorizmom, ali svojim prikrivenim ciljevima i djelovanjem služe kao potpora terorističkom djelovanju. Cyber terorizam je određen namjerom izazivanja razornih političkih i psiholoških posljedica koje mogu značajno nadilaziti sam cilj nekog pojedinog terorističkog čina, te namjerama onih koji pribjegavaju stvaranju klime bezvlašća ili izazivanja represivnog i neselektivnog odgovora vlasti s ciljem njenog kompromitiranja u očima javnosti i opravdanja terorističkih sredstava i namjera.

2 STANJE U BOSNI I HERCEGOVINI

Bosna i Hercegovina je ratificirala Konvenciju o cyber kriminalu („Službeni glasnik BiH – Međunarodni ugovori“, br. 6/206) i Dodatni protokol Konvenciji o cyber kriminalu, a u svezi s kažnjavanjem djela rasističke i ksenofobske prirode počinjenih putem računalnih sustava („Službeni glasnik BiH – Međunarodni ugovori“, broj 6/206) 2006. godine. Kada je u pitanju implementacija Konvencije u kaznene zakone, posebna napomena je da se u Bosni i Hercegovini primjenjuju četiri kaznena zakona s obzirom na podijeljenu nadležnost u propisivanju kaznenih djela između države i entiteta. Kazneni zakon Bosne i Hercegovine („Službeni glasnik BiH“, br. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10, 47/14, 22/15, 40/15) sadrži kaznena djela kojima se štite vrijednosti čija zaštita je u isključivoj nadležnosti države, dok su u kaznenim zakonima entiteta i Brčko Distrikta propisana sva ostala kaznena djela uključujući i kaznena djela iz domena cyber kriminala. Zakoni o kaznenom postupku, kojih je u Bosni i Hercegovini četiri, su kao i kazneni zakoni donekle usklađeni sa kazneno procesnim odredbama iz Konvencije.

Na državnom nivou Bosne i Hercegovine ne postoji strategija ili akcioni plan za borbu protiv cyber kriminala, no u Strategiji za borbu protiv organizovanog kriminala u Bosni i Hercegovini (2017 – 2020) i Strategiji Bosne i Hercegovine za prevenciju i borbu protiv terorizma (2015 – 2020) utvrđene su mjere za borbu u oblasti računarskog kriminaliteta, a koje se ogledaju u:

I. donošenju strateških dokumenata u borbi protiv visokotehnološkog kriminala u Bosni i Hercegovini,
II. poboljšanju suradnje sa privatnim sektorom u borbi protiv računarskog

kriminala kroz razvijanje konkretnih sporazuma,

III. podizanju svijesti vezano za korištenje informacionih tehnologija,

IV. edukaciji policijskih službenika i tužitelja o savremenom visokotehnološkom kriminalu i njihovim trendovima i modusima, te pojavnim oblicima,

V. kontinuiranom unaprjeđenju tehnologija koje koriste agencije za provedbu zakona u Bosni i Hercegovini,

VI. opremanju i razvoju sigurnosti računarskih sistema u institucijama Bosne i Hercegovine,

VII. provedbi međunarodnih direktiva i najboljih praksi u ovoj oblasti,

VIII. jačanju suradnje sa nevladinim organizacijama u oblasti cyber sigurnosti i zaštite autorskih prava,

IX. potpunoj implementaciji međunarodnih standarda koji se odnose na uspostavljanje Tima za odgovor na računarske incidente (*Computer Emergency Response Team*, CERT) u Bosni i Hercegovini i mehanizama za praćenje i suzbijanje zloupotrebe Interneta u terorističke svrhe.

Sukladno sa prethodno navedenim stanjem, na 80. sjednici Vijeća ministara BiH, održanoj 10. 11.2016. godine, na prijedlog Ministarstva sigurnosti BiH (MSBiH), donijeta je odluka o uspostavi Interresorne radne grupe, koja će u ime Bosne i Hercegovine biti zadužena za provođenje projekta Vijeća Evrope i Evropske unije koji za cilj ima izgradnju kapaciteta zemalja Jugoistočne Evrope u borbi protiv cyber kriminala - iPROCEEDS. Evropska unija i Savjet Evrope su u januaru 2016. godine potpisali ugovor o regionalnom projektu koji će trajati 42 mjeseca. Članovi tima su predstavnici svih zainteresovanih strana u ovoj oblasti, tj. ministarstva pravde nadležnog za predmetnu kaznenu oblast, predstavnika tužilaštva, policije, financijsko obavještajnog odjeljenja i drugih. Također, na istoj sjednici je Vijeće ministara BiH dalo podršku Ministarstvu sigurnosti BiH i policijskim tijelima da se u okviru IPA 2017 državnog paketa zatraži pomoć Evropske unije u daljem razvoju i jačanju kapaciteta nadležnih tijela u Bosni i Hercegovini u oblasti borbe protiv cyber kriminala. Dodatno, MSBiH vrši koordinaciju i kontakt tačka je za: (I) implementaciju dodatnih mjera za izgradnju povjerenja u oblasti cyber sigurnosti (OSCE), (II) International Telecommunication Union (ITU) Global Cybersecurity Index (GCI), te (III) NATO Science for Peace and Security Programme – specijalizirani treninzi cyber sigurnosti za državne službenike Bosne i Hercegovine.

3 CYBER TERORIZAM U BOSNI I HERCEGOVINI I NJEN ZAKONDAVNI OKVIR

Cyber terorizam, odnosno *zlouporaba Interneta u terorističke svrhe* predstavlja jedan od najopasnijih uzroka narušavanja globalne sigurnosti. U svijetu Internet prostora aktivnosti terorističkih organizacija se svode na traženje talenata koji su već osposobljeni za djelovanje u cyber prostoru.

„*Cyber terorizam je svaki oblik terorističke aktivnosti u sprezi sa cyber tehnologijom.“* Prema autoru Babiću, Cyber terorizam se isto tako može definirati i kao „*klasična teroristička aktivnost uz uporabu kompjutora i kompjutorskih sustava*." (Babić, 2009, str. 58)

Preporuke međunarodne zajednice u borbi protiv terorizma, koje je Bosna i Hercegovina,, implemenatirala u svoj zakonodavni okvir na državnom nivou, odnose se na kaznena djela vezana za terorizam.[1]

Različitosti od drugih kaznenih zakona i specifičnosti propisanih kaznenih djela terorizma u Kaznenom zakonu Bosne i Hercegovine su navedena u glavi XVII, pod naslovom *Kaznena djela protiv čovječnosti i vrijednosti zaštićenih međunarodnim pravom*. Pored kaznenih djela koja su u oblasti ratnog zločina i humanitarnog prava, u toj glavi nalaze se i djela trgovine ljudima, djela koja se odnose na međunarodne službenike, piratstva i otmice, te kaznena djela terorističkih aktivnosti propisana za obavljanje sljedećih radnji:

- Terorizam (čl.201. KZ BiH),

[1] Kazneni zakon Bosne i Hercegovine (Sl. gl. BiH br. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10, 47/14)

- Financiranje terorističkih aktivnosti (čl.202. KZ BiH),
- Javno poticanje na terorističke aktivnosti (čl.202.a KZ BiH),
- Vrbovanje radi terorističkih aktivnosti (čl.202.b KZ BiH),
- Obuka za izvođenje terorističkih aktivnosti (čl.202.c KZ BiH),
- Organiziranje terorističke grupe (čl.202.d KZ BiH),
- Protuzakonito formiranje i pridruživanje stranim paravojnim ili parapolicijskim formacijama(čl.162.b KZ BiH),

Pojedinačna objašnjenja svakog od nabrojanih kaznenih djela su rečena i kroz temeljne odrednice članaka KZ BiH, na početku KZ BiH je i čl.1. čijim je st.21. propisano što to čini terorističku grupu prema KZ BiH. Tako tim stavkom se kaže da je: "*Teroristička grupa organizirana grupa koju čine najmanje tri osobe, koja je formirana i djeluje u određenom vremenskom periodu s ciljem izvršenja nekog od kaznenih djela terorizma.*" Također, istim člankom st.22. KZ BiH podrobnije se određuje što to čini osoba koje sudjeluje u aktivnostima terorističke grupe, te tako: „*Učestvovanje u aktivnostima terorističke grupe je pristupanje ili uključivanje u aktivnosti terorističke grupe ili pružanje informacija ili materijalnih resursa ili financiranje njenih aktivnosti na bilo koji način, sa znanjem da će takvo učešće doprinijeti kriminalnim aktivnostima terorističke grupe.*"

U zakonodavstvu Bosne i Hercegovine nema posebne odredbe vezane za kazneno djelo cyber terorizma, ali postoji mogućnost za sankcioniranje kroz kaznena djela čl.201.st.5.toč.d), gdje se: "*s ciljem ozbiljnog zastrašivanja stanovništva, ili prisiljavanja organa vlasti BiH ili vlade druge zemlje ili međunarodne zajednice da što izvrši ili ne izvrši, ili ozbiljne destabilizacije ili uništavanja temeljnih ustavnih, političkih, gospodarskih ili društvenih struktura BiH, druge zemlje ili međunarodne organizacije, počini jedno od sljedećih djela koje može ozbiljno naštetiti državi ili međunarodnoj organizaciji…uništenje državnih ili javnih…uključujući i informacijski sustav*" čime se uvodi teroristično djelovanje kroz informacijski sustav.

Također po pitanju zakona o kaznenom postupku može se reći da počinitelj kaznenog djela čl.162b. u st.3. stoji da "nabavlja ili osposobljava sredstva, uklanja prepreke, stvara plan ili se dogovara s drugima ili vrbuje drugoga ili poduzme bilo koju drugu radnju kojom se stvaraju uvjeti za direktno počinjenje ovog kaznenog djela," isto tako u st.4. istog članka onaj koji "javno, putem sredstava informiranja, distribuira ili na bilo koji drugi način uputi poruku javnosti, koja ima za cilj poticanje drugog na izvršenje ovog kaznenog djela," se može inkriminirati kao djelo cyber terorizma.

4 MJERE PREVENCIJE CYBER TERORIZMA

U tom kontekstu, mjere za borbu protiv cyber terorizma sastoje se od dva stuba kojima bi se taj problem znatno smanjio ili u dobroj mjeri suzbio. Kao prvi stup navodi se *Prevencija cyber terorizma* koja se odnosi na stvaranje takvih političkih, društvenih i ekonomskih okolnosti koje uklanjaju preduvjete nastanka i širenja cyber terorizma u svim segmentima njegove pojave. Ove mjere prevencije prvenstveno se odnose na:

- onemogućavanje promoviranja i pozivanja na terorizam putem informacijskih sustava;
- prepoznavanje i eliminacija pojava koje uvjetuju nastanak cyber terorizma na lokalnoj razini i međunarodnoj razini;
- onemogućavanje širenja ekstremističkih ideologija, te povećanje razumijevanja i tolerancije društva na nacionalnoj i međunarodnoj razini;
- koordinacija i suradnja svih državnih i međunarodnih institucija usmjerenih na eliminiranje sociooloških, političkih i ekonomskih izvora koji uvjetuju nastanak cyber terorizma.

Suzbijanje cyber terorizma podrazumijeva poduzimanje mjera i postupaka usmjerenih protiv stvaranja, širenja i djelovanja terorističkih mreža i organizacija u cyber prostoru, kao i blagovremeno otkrivanje planiranja, pripremanja, organiziranja i/ili provođenja aktivnosti s obilježjima cyber terorizma, te aktivnosti se ogledaju kroz:

- organizacijsko i logističko djelovanje,
- iskorištavanja teritorija BiH za uspostavljanje i rad cyber terorističkih grupa, njihovu obuku i educiranje,
- kontrola, nadzor i evidencija:
- prolaska i dolaska osoba sumnjive i potencijalne terorističke prošlosti,
- prijenosa i nabave oružja i opreme, te drugih materija namijenjenih potencijalnim cyber terorističkim aktivnostima,

- prikupljanja financijskih sredstava ili pomaganja na drugi način cyber terorističkih organizacija i pokreta,
- onemogućavanja vrbovanja i novačenja pojedinaca za cyber terorističke organizacije i pokrete,
- druge kriminalne aktivnosti u vezi sa cyber prostorom.

5 MJERE SIGURNOSNE POLITIKE PROTIV CYBER TERORIZMA

Osnovne mjere suzbijanja terorističkih aktivnosti koje se mogu dovesti u vezu sa fenomenom cyber terorizma su ostvarive kroz dosljednu primjenu nacionalnog zakonodavstva i propisanih kaznenih djela terorizma i njemu sličnih djela, kao i onim djelima za koja nisu propisane norme unutar državnog zakonodavstva, ali postoje međunarodne preporuke za njihovo donošenje, te ratifikaciju i usvajanje univerzalne nadležnosti za navedena djela. Unutar postojećeg zakonodavstva potrebno je uskladiti mjere koje se tiču:

- onemogućavanja organizacijskog i logističkog djelovanja terorističkih organizacija i pojedinaca u cyber prostoru;
- sprječavanja korištenja cyber prostora unutar teritorija države za organiziranje, uspostavljanje i djelovanje terorističkih grupa, njihovu obuku i uvježbavanje, te pojedinaca i subjekata koji se dovode u vezu s terorizmom, čije je djelovanje usmjereno protiv država i/ili međunarodnih organizacija;
- onemogućavanja svih oblika regrutiranja i mobilizacije terorističkih grupa putem cyber prostora;
- sprječavanja kriminalne aktivnosti koje mogu biti izravno i neizravno povezane s terorizmom prvenstveno zbog zlouporabe cyber prostora;
- onemogućavanja prijenosa i nabavke oružja, eksploziva, te tehničkih i drugih sredstava namijenjenih potencijalnim terorističkim aktivnostima;
- sprječavanja korištenja sredstava za masovno uništavanje, te roba vojne i druge namjene u terorističke svrhe;
- onemogućavanja financiranja, prikupljanja sredstava i pomaganja na bilo koji način terorističkim organizacijama ili pojedincima koji se dovode u vezu s terorizmom;
- zaštitite od terorističkih djelovanja svih materijalnih i nematerijalnih dobra države: građana, imovine, pravnih subjekata, državnih institucija, svojih i stranih diplomatskih predstavništava, prometne i informacijske komunikacije, te državne granice i pravnog poretka;
- definiranja i provođenja programa osposobljavanja, obuke i treninga stanovništva, zaposlenika državne uprave za protuterorističko djelovanje u području prevencije i pojedinih elemenata zaštite;
- definiranja i provođenja obrazovnih i studijskih programa na temu upravljanja krizama, profesionalnog usavršavanja, te stvaranja organizacijskih i funkcionalnih preduvjeta za znanstvena istraživanja, znanstveni i stručni rad u području cyber terorizma.

6 ZAKLJUČAK

Navedenim, generalno se može reći kako su kaznena djela terorizma u bosanskohercegovačkom zakonodavstvu detaljno propisana sukladno međunarodnim preporukama, te da se većinom inkriminacija grupiranih u vezi s terorizmom može izreći sankcija za djela počinjena kao djela cyber terorizma, iako za isto nema posebno propisane norme. Preporuka je uvođenje već do sad više puta navedene univerzalne nadležnosti za progon počinitelja djela cyber terorizma. Također dopunu KZ BiH bi trebalo opisati kroz odrednicu koja se veže za *javno mjesto*, što bi se odnosilo i na internet prostor i društvene mreže, jer bi se time u značajnoj mjeri omogućilo djelovanje u ranoj fazi pojave cyber terorizma čime bi se preventivno djelovalo na širenje ove pojave u BiH i svijetu.

CITIRANA DELA

Babić, V. (2009). *Kompjuterski kriminal*, Sarajevo, Rabic.

Babić, V. (2016). *Cyber terorizam - suvremena sigurnosna prijetnja.* Vitez.

Kazneni zakon Bosne i Hercegovine (Sl. gl. BiH br. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10, 47/14)

Datum prve prijave: 18.09.2019.
Datum prijema korigovanog članka: 07.10.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Babić, V. (2019, 10 15). Mjere prevencije i sigurnosne politike protiv cyber terorizma. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 1-6. doi:10.12709/fbim.07.07.02.01

*Style – **Chicago** Sixteenth Edition:*

Babić, Vladica. 2019. "Mjere prevencije i sigurnosne politike protiv cyber terorizma." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 1-6. doi:10.12709/fbim.07.07.02.01.

*Style – **GOST** Name Sort:*

Babić Vladica Mjere prevencije i sigurnosne politike protiv cyber terorizma [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 1-6.

*Style – **Harvard** Anglia:*

Babić, V., 2019. Mjere prevencije i sigurnosne politike protiv cyber terorizma. *FBIM Transactions,* 15 10, 7(2), pp. 1-6.

Style – **ISO 690** Numerical Reference:

Mjere prevencije i sigurnosne politike protiv cyber terorizma. **Babić, Vladica.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 1-6.

FBIM Transactions
DOI 10.12709/fbim.07.07.02.02

TERORISTIČKE ORANIZACIJE U SIRIJI

TERRORIST ORGANIZATIONS IN SYRIA

Boris Bursać
Gradska opština Čukarica, Beograd, Srbija

JEL Category: **Z12**

Apstrakt

Poslednjih sto godina Sirija je bila sinonim za turbulentna dešavanja, politička previranja ratove, tako da možemo reći da nije iznenađujući sled događaja koji je zadesio Siriju. Sukob koji je počeo u vidu demonstracija 2011. godine odnosno, u vidu svojevrsnog konflikta vlasti i opozicije prerastao je u oružani sukob sa više od 200.000 mrtvih i 10.000.000 raseljenih. Usled ovakvog haosa iz „pandorine kutije" izletele su islamističke terorističke organizacije iza kojih ostaju beda i siromaštvo, nezaposlenost, politički haos, destabilizacija, nasilje, masakri, borba bilo kad i svuda u svakom gradu, selu, zaseoku, dakle stanje opšteg rasula gde se konfliktima ne nazire kraj. Sve je počelo takozvanim „Arapskim prolećem" u Tunisu, da bi se kasnije proširilo na Egipat, Libiju, Bahrein, Siriju, Jemen, Alžir, ponovo Irak, Jordan, Maroko, Oman i još nekoliko država gde su sukobi bili manjeg intenziteta. Cilj ovog rada je ideja da se pruže potrebna znanja proistekla iz opsežne analize, pre svega ideoloških, politikoloških, sociološkog gledišta odnosno stanovišta terorističkih organizacija sa prostora Sirije i da se na najbolji način u pravom smislu omogući razumevanje njihovih delatnosti i njihovog velikog uticaja na razvoj terorizma u celini.

Ključne reči: *terorizam, Al Nusra, Al Šam, Liva al Tavhid, Liva al Hak, Sirijski islamski front*

Abstract

For the past hundred years, Syria has been a synonym for turbulent events, political turmoil, and wars, so we can say that the current situation that has hit Syria is not surprising. The conflict that began in the form of the demonstration in the 2011-th , or, in the form of a sort of conflict of power and opposition, grew into an armed conflict with more than 200,000 dead and 10,000,000 displaced persons. As a result of such a chaos from the "pandora's box" Islamist terrorist organizations have gone out, which lead to misery and poverty, unemployment, political chaos, destabilization, violence, massacres, fighting anytime and anyplace in every city, village, hamlet, therefore, the situation of a general chaos where end of conflicts is not yet seen. It all began with the so-called "Arab Spring" in Tunisia, to expand later to Egypt, Libya, Bahrain, Syria, Yemen, Algeria, Iraq, Jordan, Morocco, Oman and other countries where conflicts were of lesser intensity. The aim of this research is the idea to provide the necessary knowledge stemmed from an extensive analysis, primarily ideological, political, sociological point of view or the point of view of terrorist organizations on the territory of Syria and that the best way to enable

Adresa autora:
Boris Bursać
boris.bursac89@gmail.com

true sense of understanding of their business and their great influence on the development of terrorism in general.

Keywords: *Terrorism, Al Nusra, Ahrar al-Sham, Liwa al-Tawhid, Liwa al-Haqq, Syrian Islamic Front*

1 UVOD

Nakon povlačenja koalicionih snaga iz Iraka, i borbe Zapada za demokratizaciju sveta žarište daljih borbi prenosi se na sever Afrike i delom na Bliski Istok. Zašto su se sukobi baš ovde preneli? Ko stoji iza arapskog proleća? Ko su žrtve a ko agresori? Da li iza svega stoji samo prost kapital? Je li „crno zlato“ uzrok svemu? Jesmo li nepodobni ili neposlušni? Ko je sledeći? Samo su neka od pitanja na koje nemamo odgovor ili imamo al ne smemo da kažemo - sami zaključimo. Dakle ova gore napomenuta događanja samo su otvorile put širenju verskog ekstremizma i produbile sve opštu krizu u svetu. Sirija je sada „svetska pozornica“ a igrači u njoj su u suštini podeljeni u četri grupacije:

- Jedan deo okrenut je Asadu i njegovom režimu
- Drugi deo su opozicione snage na čelu sa Sirijskim nacionalnim većem
- Al kaida u Iraku kasnije poznatija kao Islamska država
- Sirijski Kurdistan

Sve ove snage da bi se održale tu gde jesu, imaju direktnu ili indirektnu podršku, vojnu ili političku nekih vanjskih sila, svaka ima svoje ideale, svaka svoje ciljeve i samo na taj način opstaju. Asadov režim ima podršku: Rusije, Irana i Hezbolaha (Schmidt, 2012), Sirijsko nacionalno veće se oslanja na: Tursku, Saudijsku Arabiju, Katar, SAD, Ujedinjeno Kraljevstvo. Sirijski Kurdistan sasvim logično ima podršku Iračkog Kurdistana, a Islamska država ima svoje sestre pridružnice, manje terorističke organizacije o kojima ću pisati u nastavku rada. Na osnovu svega napomenutog sa apsolutnim pravom možemo reći da trenutni sukob u Siriji nije ništa drugo do najveće ratno žarište u svetu. Rat je možda počeo sa namerom da se svrgne režim Bašara el Asada (Bashar Hafez al-Assad), koji istini za volju nije bio toliko diktatorski kako se predstavlja, čak šta više verovalo se da su Asad - otac i sin faktori stabilnosti u ovom regionu, jer se za njihovo vreme Sirija transformisala u jednu moćnu i razvijenu državu u ekonomskom, obrazovnom, i privrednom smislu, pre svega samostalnu suverenu državu. Gde Sirija ne duguje nijedan dinar, ni unutra ni van zemlje. Obrazovanje do fakulteta je besplatno. Zdravstvo je besplatno. Tako da se Sirija nametnula kao jedna centralna zemlja na Bliskom istoku koja je uvek morala da bude pitana, i to očigledno nije nekom odgovaralo te se krenulo u opštu ofanzivu protiv nje. Prema nekim podacima Asad se nametnuo kao meta teroristima iz prostog razloga što je pripadao Alavitima sekti sklonoj misticizmu koja pripada šiitskoj školi i koja čini 12% ukupnog stanovništva u Siriji dok sa druge strane imamo sunitsku većinu. U narednom delu istraživanja bavićemo se terorističim organizacijama koje su delovale ili još deluju na ovom prostoru ali su u senci najvećeg zlotvora današnjice poznatijeg kao Islamska država o kojem sam već pisao te ću se u nastavku rada fokusirati upravo na te terorističke organizacije.

2 AL NUSRA

Al Nusra front ili u originalu Džabat Al Nusra (Jabhat al-Nusra) osnovan je krajem 2011. godine i to od strane Al Kaide u Iraku koja se u tom trenutku nalazila pod vođstvom Abu Bakar al Bagdadija (Abu Bakr al-Baghdadi). Naime Al Bagdadi je poslao grupu operativaca na čelu sa Abu Muhamed al Džulanijem (Abu Muhammad al-Julani), da osnuje dobro organizovanu džihad ćeliju ali ovaj put na prostoru Sirije (Joscelyn, Al Qaeda in Iraq, Al Nusrah Front Emerge as Rebranded Single Entity, 2013). Vrlo brzo Al Nusra doživljava ekspanziju, iz razloga koje sam napomenuo – trenutne političke situacije u Siriji. Pobunjenicima, Al Nusra je bio izvor opstanka pre svega zbog dobro organizovanog dotoka oružja i boraca, naravno finansiranih od Al Kaide u Iraku. Svoj uspeh ova teroristička organizacija brzo je doživela zbog profesionalnih ratnika koji su svoju obuku prošli u Avganistanu i Iraku i time pridobila veliki broj pobunjeničkih grupa na novom, ratom zahvaćenom području.

Povučena iskustvom iz Iraka Al Kaida odnosno njena produžena ruka Al Nusra izbegavala je brutalna pogubljen i bombaške napade ali ne zadugo već u januaru 2012. godine preuzima

odgovornost za napad u Al Midanu distriktu Damaska. Ovim postupkom izgubila je deo podrške u narodu Sirije ali ne tako veliki kao što je bila situacija u Iraku, čak je pobunjenička vojska Sirije javno demonstrirala američkom proglašenju Al Nusre za terorističku organizaciju. (Gordon, Barnard, 2012). U međuvremenu je došlo do sukoba između Al Nusre i Al Kaide u Iraku zbog namere iračke Al Kaide da formira organizaciju koja će se nazivati Islamska država Iraka i Sirije i kojoj će Al Nusra biti potčinjena. Ne želivši tavu podelu autoriteta, Al Nusra polaže zakletvu Ajmanu al Zavahiriju (Ayman al-Zawahiri) inače novom vođi Al Kaide koji je na mesto glavno komandujućeg došao nakon ubistva Osame bin Ladena 2011. godine. Taj korak je produbio, već postojeću krizu u odnosima između Al Kaide u Iraku i Al Nusre što je kasnije dovelo do ukupno 3000 poginulih do jučerašnjih saboraca. Ne samo što je Al Kaida iz Iraka, u ovom periodu već Islamska država Iraka i Sirije ubila veliki broj Al Nusrinih boraca ili ih primorala na fuziju sa svojom organizacijom već je zauzela njihov centar Deir ez Zor - inače sirijski centar naftne industrije i samim tim sebi obezbedila stalni izvor prihoda. Gubeći ovaj centar Al Nusra je morala brže da se organizuje inače bi svi njeni borci polako prelazili u tabor Islamske države Iraka i Sirije. Kako bi to sprečila vraća se starom terorističkom izvoru prihoda - kidnapovanju. Neki od najpoznatijih kidnapovanja koje su objavili svetski mediji, a vezani su za Al Nusru svakako su: grupa grčkih pravoslavnih monahinja koje su puštene uz pomoć Katara i Libana, američki novinar Petar Teo Kurtis (Peter Theo Curtis), 45 fidžijskih pripadnika mirovnih snaga takođe su pušteni, već kasnije Al Nusra je pobila nekoliko taoca, a neki su još u procesu pregovora. Svi ovi događaji koje smo naveli doveli su do problema unutar organizacije i sumnji u samo rukovodstvo, koje je nakon toga okrenulo svoju politiku i delovanja prema Idlib provinciji u Siriji. U međuvremenu došlo je do preokreta odnosa između Al Nusre i pobunjenika koji su iz stanja prijateljstva prešli u stanje otvorenog sukoba, pre svega zbog saradnje pobunjenika i vlade SAD koja je Al Nusru proglasila za terorističku organizaciju. Tako da je sad Al Nusra pored napada na vlasti u Idlibu za neprijatelja imala i neke pobunjeničke grupacije. Ubrzo se na terenu pojavila i organizacija pod nazivom Ahrar al Šam (Ahrar al-Sham), koja će zajedno sa Al Nusrom delovati protiv zajedničkih neprijatelja. Prema poslednjim podacima Al Nusra je brojala oko 20.000 boraca i u januaru 2017. godine je sa nekoliko selafističkih odreda poput (FDD's Long War Journal, 2017):

- Ansar al-Din Front
- Liwa al-Haqq
- Jaysh al-Sunna

formirala organizaciju *Hay'at Tahrir al-Sham* (Organizacija za oslobođanje Levanta), koja se smatra jednom od najuticajnijih teorističkih organizacija na prostoru Sirije. Ova organizacija ostaje vodeća u Idlib provinciji i ima veliku podršku Al Kaide i prema nekim informacijama Katara. (Karouny, 2015). Novo formiranu organizaciju odnosno njen vojno-operativni deo i dalje vodi Abu Muhamed al Džulani (Abu Muhammad al-Julani), dok savet Šure (savetodavno veće) vodi Abu Džaber Šaik (Abu Jaber Shaykh) bivši general - komadant Ahrar al Šama.

3 AL ŠAM

Al Šam (Ahrar al Sham) ili kasnije Harakat Ahrar al-Sham al-Islamiyya, ili islamski pokret slobodnih ljudi Levanta, još je jedna sunitska teroristička organizacija koja deluje na prostoru Sirije i bori se protiv Asadovog režima. Cilj je dakle jasan rušenje autoritarnog i diktatorskog režima i uspostavljanje islamske vlade. Organizacija je osnovana od strane bivših političkih zatvorenika na čelu sa šeikom Hasan Abudom (Abu Abdullah al-Hamawi).

Zvanično, prema postojećim podacima organizacija je osnovana u 2011. godini, ali nije učestvovala u nekim ozbiljnijim sukobima sve do 2012. godine. (Abouzeid, 2012). Ova teroristička organizacija se veoma brzo širila da bi u roku od dve godine imala 83 borbene jedinice. Njihov brzi uspeh svakako je vezan za njihove finansijere koji imaju težnju da ujedine sve salafi islamiste pod jedan barjak.

Tu pre svega mislim na vođu salafi pokreta u Kuvajtu Hakima al Mutarija (Hakim al-Mutairi) inače osnivača Hezb al Uma (Hezb al-Umma) nepriznate političke partije Kuvajta. (Lund, 2013) Dok sa druge strane postoje tvrdnje da se Al Šam finansira još od nekih grupacija iz Katara i čak Muslimanskog bratstva. Sad se sigurno pitate

kakve veze imaju Muslimasko bratstvo i Al Šam. E pa svakako nemaju ideoliških veza jer kao što znamo Muslimansko bratstvo propagira jedan pramatičniji tip islamizma dok Al Šam predstavlja jedan radikalniji pravac. Ono što ih veže jeste namera da se Muslimansko bratstvo što pre vrati na sirijsku pozornicu iz koje su proterani, dal to bilo kroz oružane sukobe ili putem veza koje Muslimansko bratstvo ima u Idlib i Hama provincijama. Zaboravio sam napomenuti da i Al Šam kao i Al Nusra najviše deluje baš na prostorima Idlib i Hama provincija i da tu čine svojevrsnu vlast. Već od 2013. godine Al Šam širi svoja delovanja preko cele teritorije Sirije, najviše na severu zemlje. Protive se pro zapadnoj intervenciji ali ipak učestvuju u ratnim dejstvima na strani pobunjenika koji kao što znamo imaju direktnu podršku vlade SAD i NATO pakta. Dakle kroz donacije Kuvajta, Katara, Saudijske Arabije, Turske ali i grupacija unutar Muslimanskog bratsva sa jedne strane i kroz otimanja vojnih sredstava sirijske armije ova teroristička organizacija morala se nametnuti kao jedna od vodećih, možda ne baš na celoj sirijskoj teriroriji ali zasigurno na delu teritorije na kojem je delovala - dakle sever zemlje. Apsolutno je sarađivala sa Al Nusra frontom i u bliskim vezama je sa Islamskom državom. Smatra se izuzetno samostalnom organizacijom koja nema javno poznatih veza sa Al Kaidom, dakle ne smatra se još jednom produženom rukom te organizacije. Borci unutar organizacije su uglavnom članovi lokalnih brigada vernih Al Šamu a podržani su, koordinisani i kontrolisani od strane centrale organizacije sa sedištem u Idlibu. Napadaju u najvećoj meri vojne baze u cilju osvajanja naoružanja koje će kasnije upotrebiti za visoko organizovane akcije. Predstavlja se kao salafi organizacija koja teži uspostavljanju teokratske države na bazi šerijatskog prava. Prima strane borce ali ne u meri u kojoj to radi Al Nusra jer jednostavno Al Šam nije toliko agresivan i fokusiran je samo na dejstva u Siriji pa i nema konstantnu potrebu za borcima. Neke od najpoznatijih akcija ove organizacije su:

- Napad na Međunarodni centar za poljoprivredna istraživanja u suvim oblastima (ICARDA), uz pomoć Al Nusre, novembra 2012. godine
- Oslobađanje dopisnika NBC-a Ričarda Engela, decembra 2012. godine
- Upad u vazduhoplovnu bazu Taftanaz, 2012. godine
- Napad na Al Zaru 2016. godine

U januaru 2013. godine Al Šam najavljuje stvaranje nove organizacije pod nazivom Harakat Ahrar al-Sham al-Islamiyya, koja je sastavljena od islamskih grupacija koje su u tom trenutku delovale na teriroriji Sirije a to su (Lund, 2013):

- Harakat al-Fajr al-Islamiya iz Alepa
- Jamaat al-Taliaa al-Islamiya iz Idleba
- Kataeb al-Iman al-Muqatila iz Damaska

Ove gore navedene organizacije spojene su sa Al Šamom koji je u tom trenutku imao 83 grupacije odnosno brigade koje su delovale na prostoru Sirije a pod okriljem su Al Šama i formirale su organizaciju koja se zove Harakat Ahrar al-Sham al-Islamiyya koja svoje delovanje bazira na severo-zapadu Sirije. Ova grupacija dolazi često u sukobe sa Islamskom državom pogotovu posle kritike upućene direktno njoj od strane šeika Hasana Abuda. Naime šeik Hasan Abud javno je osudio Al Bagdadija i to u dve tačke (Joscelyn, 2014):

- Zbog odbijanja napora da se uspostavi bilo kakvo pomirenje ostalih milatntnih grupa sa Islamskom državom
- Zbog stava Al Bagadadija koji kaže da sve ostale grupe koje nisu pod komandom Islamske države u suštini su neverničke

Ovaj postupak šeika Hasana Abuda samo je produbio već postojeću krizu u odnosima ovih dveju organizacija a rezultiralo je ubistvom jednog člana Al Šama i kasnije sukobima u Raki gde je Al Šam imao pomoć više organizacija od kojih sam neke već pominjao a to su Al Nusra i Liva al Tavhid (Liwa al-Tawhid). Baza Al Šama je kasnije bombardovana, a u tom napadu je poginuo jedan od osnivača ove organizacije i Al Kaidin predstavnik za Siriju Abu Kalid al Suri (Abu Khalid al-Suri) (Joscelyn, 2014). Kasnije se ispostavilo da je Kalid al Suri poslat tu od strane samog vrha Al Kaide kako bi popravio izuzetno loše odnose i zaustavio sukobe između ovih militantnih organizacija. Naravno ovaj postupak je odmah naišao na osudu, a krivac se savim logično mada nije dokazano - nalazio u redovima Islamske države. U februaru 2018. godine Ahrar Al Šam i Pokret Nour al Din al Zenki (Nour al-Din al-Zenki Movement) formiraju Sirijski oslobodilački front

(Syrian Liberation Front) na čelo novonastale organizacije postavljen je Hasan Sufan (Hassan Soufan), inače vođa Ahrar Al Šama a za njegovog zamenika postavljen je šeik Tafik Sabahudin (Sheikh Tawfiq Shahabuddin) lider pokreta Nour al Din al Zenki. Procenjuje se da ova teroristička organizacija ima između 18.000 do 20.000 boraca, u otvorenom je sukobu sa sirijskom vojskom i Tahrir al Šamom i ima jaku podršku Turske (Zelin, 2017).

3 LIVA AL TAVHID

Liva al Tavhid (Liwa al-Tawhid) je teroristička organizacija odnosno brigada u početku, koju sam više puta pominjao i mislim da bih trebao nešto više napisati o njoj. Dakle ova grupa je osnovana od strane manjih opozicionih grupa na prostoru Alepa sa ciljem rušenja režima predsednika Bašara al Asada. Za samo mesec dana uspela je da se nametne kao prva opoziciona grupacija koja poseduje teritoriju. Kako je ova organizacija rasla tako počela da dobija sve više na značaju a njen lider Abdel Kader Saleh (Abdel Qader Saleh) inače jedan od dva osnivača, postaje izuzetno poznat u ovoj regiji. Na samom početku Al Tavhid je bio deo odnosno brigada Slobodne vojske Sirije (Free Syrian Army- FSA), jedna izuzetno autonomna grupacija koja nije primala naređenja od FSA već je delovala prema svojim nahođenjima.

Ova grupacija se na početku zalagala za jednu umereniju islamsku ideologiju baziranu na šerijatskom pravu gde će postojati slobodni izbori i zaštita manjina, ali je bila protiv pro - zapadnog intervencionizma što će je kasnije radikalizovati. Smatra se da je u je u jednom momentu u svojim jedinicama imala između 8.000 i 10.000 vojnika i da je finansirana od strane Katara (Sinjab, 2013). Za sedište organizacije po logici stvari nametnuo se Alep a postoje podaci da je ova brigada kontrolisala jedan važan deo granice sa Turskom i da je posedovala veliki medicinski i medijski centar gde je zapošljavala preko 1000 civila (Lund, 2014). Retko kada je ova organizacija napadala samostalno neku metu već je imala pomoć najčešće Al Nusre. Najpoznatiji napadi ove grupacije su (Roggio, 2014):

- Napad na Alep jula 2012. godine kada ova organizacija zauzima i stavlja pod svoju vlast 40 % grada Alepa
- Liva al Tavhid, Al Nusra, Brigada Nasera Salahudina, Dera al Asima, Liva al Habib al Mustafa aprila 2013. godine organizovali su niz napada na sirijsku vojsku u Damasku tom prilikom ubili su oko 150 vojnika i uništili su nekoliko tenkova sirijske vojske
- Liva al Tavhid, zajedno sa Al Nusrom i Al Šamom maja 2013. godine napada vojne logore sirijske vojske u Idlib provinciji

Al Tavhid organizacija doživljava jak udarac u 2013. godini kada Sirijsko vazduhoplovstvo bombarduje njihovu bazu u Alepu i ubija Al Abasa (Youssef al-Abbas) jednog od osnivača ove brigade odnosno organizacije, a samog Saleha ranjava i on umire nigde drugo do u Turskoj. Ovaj udarac je ozbiljno uzdrmao organizaciju, što je kasnije dovelo do raznih podela. Deo organizacije pomagao je FSA, deo Islamsku državu, deo je pritekao u pomoć Al Nusri. Takođe postoje podaci da su se delovi brigade priključili PPU (People's Protection Units) većinski kurdskoj jedinici, a preostala 4 bataljona Liva al Tavhida su zvanično ušla u sastav Nur Al Din Al Zenki pokreta (Zaman, 2014).

Dakle na osnovu toga možemo reći da se ova organizacija dezintegrisala ali su pojedine jedinice ili bataljoni ove organizacije i dalje aktivni unutar drugih grupacija.

4 LIVA AL HAK

Liva al Hak (Liwa al-Haqq) je još jedna opoziciona snaga koja se javlja na području Sirije. Zvanično je osnovana avgusta 2012. godine od raznih islamističkih grupacija koje su delovale na području Homsa inače veoma važnog industijskog centra Sirije. Homs takođe predstavlja izuzetno važan geostratečki položaj jer predstavlja prelaz između mediteranske obale i unutrašnjosti zemlje. Jedanaest grupacija ili brigada nazovimo ih kako hoćemo, čine Liva al Hak organizaciju a to su (Lund, 2014):

- Katibat al-Siddiq
- Katibat al-Furati
- Katibat al-Huda
- Katibat al-Naser li-Din Allah
- Katibat Sebaa al-Birr
- Katibat Shuhada Baba Amr
- Kataeb Atbaa al-Rasoul
- Katibat al-Ansar
- Kataeb al-Bara

- Katibat Seif Allah
- Katibat al-Bara bin Malek

Ono što je izuzetno bitno za ovu organizaciju, koja je aktivno delovala na sirijskom frontu svakako jeste to da nije označena kao teroristička organizacija već kao militantna i ideologija koju zastupa nije selafistička. Veruje se da je razlog ovakvom stavu informacija koja kaže da je ova organizacija osnovana uz pomoć jedne sekularne frakcije unutar Slobodne vojske Sirije – FSA i velikog broja studenata koji su učestvovali u protestima pred početak rata (Lund, 2013). Dakle iz ovoga samostalno možemo izvući cilj organizacije a to je svakako rušenje Asadovog režima i uspostavljanje nove islamske vlade. Takođe Liva al Hak ne nastupa sama već uz pomoć drugih organizacija pre svega Al Nusre, Al Šama , Al Tavhida. U novembru 2013. godine Liva Al Hak zajedno sa nekoliko teorističkih organizacija formira jednu od najvećih militantnih snaga na prostoru Sirije poznatiju kao Islamski front koju još čine (Lund, 2014):

- Ahrar Al Šam
- Ansar Al Šam
- Sukor Al Šam
- Liva Al Tavhid
- Džaiš al Islam
- Kurdski islamski front

Ova novoosnovana organizacija imala je za cilj smenu Asadovog režima, uspostavljenje nove islamske vlade i na vrhuncu svoje moći imala je između 40.000 i 70.000 boraca (Hassan, 2014). Komadant Liva Al Haka šeik Abu Rateb je bio generalni sekretar Islamskog fronta koji se zbog neslaganja Ahrar Al Šama i Džaiš al Islama raspustio 2014. godine. Nakon raspada Islamskog fronta deo Liva Al Haka je pristupio Ahrar Al Šamu a deo je delovao pod upravom organizacije poznatije pod imenom Džaiš Al Fatah.

5 SIRIJSKI ISLAMSKI FRONT

Kao što smo mogli zaključiti iz gore navedenog sadržaja, 2012. godina odnosno njena druga polovina je bila izuzetno turbulentna. Slobodna vojska Sirije – FSA počela je polako da se raspada u manje frakcije odnosno manje radiklane grupe koje samostalno deluju pre svega na severu i istoku zemlje. Većina tih organizacija obeležene su kao terorističke tako da pored režima predsednika Bašara el Asada sa kojim su u stalnom sukobu, kao neprijatelja imaju i izuzetno moćne države sveta. Tako da se nametnula jedna sasvim logična ideja koja podrazumeva osnivanje jedne krovne organizacije sa ciljem opstanka na sirijskom frontu i borbe protiv zajedničkih neprijatelja. To se i desilo već 21.12. 2012. godine, kada Al Šam javno obelodanjuje osnivanje organizacije pod nazivom “ Sirijski islamski front” koji u svom sastavu ima 11 moćnih grupacija (Lund, 2013):

- Kataeb Ahrar al-Sham - deluje na celoj teriroriji Sirije
- Liwa al-Haqq - deluje u Homsu
- Harakat al-Fajr al - Islamiya- deluje u Alepu i njegovoj okolini
- Jamaat al-Taliaa al-Islamiya - deluje u okolini Idliba
- Kataeb Ansar al-Sham - deluje u Latakiji i njenoj okolini
- Katibat Moussaab bin Omeir - deluje u okolini Alepa
- Jaish al-Tawhid - deluje u Deir al Zoru
- Kataeb Suqour al-Islam - deluje u Damasku
- Kataeb al-Iman al-Muqatila - deluje u Damasku i njegovoj okolini
- Saraya al-Mahamm al-Khass - deluje u Damasku i njegovoj okolini
- Katibat Hamza bin Abdelmuttaleb - deluje u Damasku i njegovoj okolini

Al Šam organizacija se nametnula kao liderska pre svega što najžešće propagira selafizam, fokusirana je na Siriju, najveći broj boraca u njenim redovima je iz Sirije (mada prima i strane borce), svi njeni lideri koji su poznati javosti su Sirijci a i delom zbog toga što je protivnik pro - zapadnog intervencionizma u sirijsku krizu. Dakle novoosnovana organizacija definiše se kao sunitska odnosno selafistička i teži uspostavljanju islamske države i širenju islamske kuture. Većina članova organizacije je takođe salafi opredeljenja unutar islama izuzev kao što smo već naveli Liva al Haka. Bilo da su radikalni islamisti ili ne, borci su regrutovani a prednost su imali ljudi iz Sirije jer jedan od ciljeva približavanje narodu odnosno ideja je da se sirijski narod poistoveti sa ovom grupacijom i eventualno je pomogne. Organizacija pored ovog (ne svojstvenog svim članicama) ima i jasno definisane ciljeve oko kojih su se složile sve članice a to je (Lund, 2013):

- Svrgavanje režima Bašara al Asada i širenje bezbednosti na celu teriroriju voljene Sirije
- Rad na verskoj konsolidaciji pojedinaca, grupe i same države
- Rad na očuvanju islamskog identiteta društva tako šo će se izgraditi kompletna islamska ličnost
- Izgradnja Sirije ali na temeljima pravde, nezavisnosti i solidarnosti uz korespodenciju sa islamskim principima
- Realno učešće u razvoju društva
- Priprema budućih lidera i naučnika u raznim sferama života koji će kasnije svoje znanje i veštine putem edukacije prenositi mlađim naraštajima

Dakle vidimo na osnovu ovih ciljeva da Islamski front teži osnivanju jedne teokratske države bazirane na šerijatskom pravu. Organizacija smatra da šerijatsko pravo treba imati primat iz prostog razloga što je jednostavno, efikasno i nepristrasno za primenu. A sama revolucija u Siriji je islamska revolucija jer u njenim sukobima najviše učestvuju muslimani tako da se šerijatsko pravo nameće samo kao jedinstveno rešenje i ovom idejom automatski se isključuje bilo kakav vid liberalne demokratije. Kada govorimo o taktici Sirijski islamski front jasno je stavio do znanja da pojedinci, grupe i plemena koje na bilo koji način podržavaju režim Bašara al Asad svakako mogu biti meta napada ovog fronta. Najčešće pribegavaju gerilskom načinu ratovanja, detoniranju bombi iz daleka, prepadima i zasedama. Borci su uglavnom Sirijci mada su neke članice pre osnivanja Sirijskog islamskog fronta primale i dobrovoljce iz drugih zemalja tu pre svega mislim na Al Šam, ali ne u nekom impozantnom broju jer većina dobrovoljaca koja nije iz Sirije popunjavala borbene redove Al Nusre. Sve formacije koje čine Sirijski islamski front imale su nameru da kroz formiranje ove krovne organizacije obezbede sebi podršku, odnosno da sarađuju i da pomažu jedni drugima uz obavezan stav da se zadrži njihov individualni organizacioni identitet. Nakon godinu dana broj članova ove organizacije sa početnih 11 sveo se na 6. Dakle ova ideja ipak nije uzela toliko maha koliko se smatralo da će uzeti.

Ipak, i posle ovih podela organizacija je ostala na impozantnom broju od 30.000 boraca što je može se reći jedna osrednja armija. Kad se sve ovo uzme u obzir Sirijski islamski front ne možemo stvarno zvati alijansom već svojevrsnom "aglomeracijom lokalnih jedinica". Jer svaka od ovih grupacija ukorenjena je u nekom selu, gradu, ili provinciji odnosno nekoj familiji ili klanu i kao takva ostaje lojalna samo svom komadantu. Možemo uzeti za primer prebacivanje boraca iz jednog područja u drugi - nikad se neće boriti istim žarom kao što bi se borili za svoju bazu odnosno svoju familiju, svoj klan. Ili pak možemo doći do situacije kad dve ili više frakcija zajedno zauzmu neki krucijalni resurs ili vojnu opremu - kako to podeliti. Sve su to razlozi koji su i doveli do slabljenja ove organizacije odnosno gubljenja podrške od strane njenih prvobitnih članica. Tako da kada uzmemo ovaj broj od 30.000 vojnika na prvi pogled deluje impozantno al kad malo bolje razmislite i shvatite da je ovaj broj raspršen po celoj sirijskoj teritoriji i da nikad ne nastupa u punom sastavu već u manjim odredima i nije toliko zastrašujuć. Često se postavljalo pitanje ko finansira ovaj projekat odnosno Sirijski islamski front i stvarala se bezpotrebna fama i misterija oko toga. Ako uzmemo na primer Al Šam jednu od najjačih i najmasovnijih organizacija unutar ovog fronta i javno se zna da Al Šam funkcioniše na osnovu finansijske pomoći koja stižu najviše iz Kuvajta i Katara da li treba dalje da analiziramo ili možemo izvesti logičan zaključak. Za razliku od drugih organizacija kad govorimo o vođenju same organizacije ova nema titulu "emira", već "savet lidera" sastavljen od predstavnika svih frakcija koje su članice Sirijskog islamskog fronta. Na čelu saveta je šef (al-qaid al-amm) koji je politička a ne religijska figura. Na ovoj funkciji je od samog osnivanja bio Abu Abdullahal-Hamawi poznatiji kao Hasan Abud o kojem sam već pisao dakle lider Al Šama. Iako je postojao veliki broj funkcija unutar organizacije najveći broj odnosno najvažnije funkcije su bile u rukama Al Šama. Tako na primer javnosti se uvek obraćao potparol organizacije Abu Abderahman al Suri (Abu Abderrahman al-Souri) čije je pravo ime Muhamed Talal Bazerbaši (Mohammed Talal Bazerbashi) takođe vodeći član Al Šam mreže (Lund, 2013). Jako bitnu stvar nisam pomenuo a to je da je pored svoje vojne podrške Sirijski islamski front pružao i humanitarnu pomoć Asadovim ne-istomišljenicima. Pored distribucije hrane, vode, šatora, ćebadi Sirijski islamski front je pružao i nastavnu, odnosno pomoć u vidu edukacije stanovništva u ratom razorenim područjima. Takođe uspostavljali su šerijatske

sudove tamo gde je došlo do totalnog kolapsa pravnog sistema usled ratnih dejstava. Dakle vidimo da je pored svoje vojne funkcije ova organizacija za razliku od drugih imala i svoju humanu stranu. Ipak to nije bilo dovoljno, dešavale su se razne podele unutar organizacije te je morala da se sprovede ozbiljna reorganizacija koja se desila novembra 2013. godine. Razlog je jasan od početnih 11 osnivača 6 je preostalo i one sada čine centralu Sirijskog islamskog fronta odnosno novonastale organizacije Islamskog fronta koji smo već pominjali. Takođe neke od ovih organizacija su u svoje redove akvizirali neke od grupacija, brigada i frakcija. Ključne grupacije koje su bile sastavni deo Islamskog fronta i koje su ga vodile su:

- Ahrar Al Šam – deluje na celoj teritoriji Sirije
- Ansar Al Šam – deluje u severnoj Latakiji
- Sukor Al Šam – deluje u Idlib provinciji
- Liva Al Tavhid – deluje u Alepu
- Džaiš al Islam – deluje u okolini Damaska
- Kurdski islamski front – deluje na granici sa Turskom

Rukovodstvo ove organizacije podeljeno je na sledeći način, na mesto lidera saveta-Šure postavljen je Ahmed abu Isa iz Sukor Al Šama, na mesto negovog zamenika postavljen je Abu Omar Hreitan iz Liva Al Tavhida, mesto generalnog sekretara pripao je Liva Al Haku i na tu poziciju postavljen je šeik Abu Rateb, ured za šerijat pripao je Al Šamu i na tu poziciju postavljen je Abul Abas Al Šami, politički sektor pripao je takođe Al Šamu i na tu poziciju postavljen je Hasan Abud dok je vojni sektor pripao Džaiš al Islamu i na tu poziciju je postavljen Zahran Alouš (Lund, 2013). Ovako organizovana grupacija koja je na vrhuncu moći imala između 40.000 i 70.000 boraca a uz to je bila potpomognuta od strane Saudijske Arabije, Turske i Katara, obećavala je mnogo ali je 2014 godina bila fatalna za ovu organizacije jer je većina njenih lidera ubijena uključujući i njenog političkog lidera Hasana Abuda. Do početka 2015. godine Islamski front se gotovo raspao gde Ahrar al Šam manje više apsorbuje preostale grupacije ili brigade Islamskog fronta.

6 ZAKLJUČAK

Na osnovu gore navedenog teksta, možemo zaključiti da su mnoge terorističke organizacije delovale ili još deluju na prostoru Sirije ali su zbog prevelikog fokusa na jednu od najpoznatijih terorističkih organizacija poznatiju kao Islamska država, totalno skrajnute. Zahvaljujući svojoj sposobnosti da se brzo prilagodi, terorizam samim tim i terorističke organizacije koje se ovde pominju, menjaju se po svojoj sadržini, tipovima, oblicima, načinima delovanja ali njihov cilj ostaje isti a to je izazivanje osećanja straha i borba svim raspoloživim sredstvima radi ostvarenja svojih ideoloških, verskih i političkih ideja. Svaki vid terorizma pa i ovaj koji je predstavljen u ovom radu oduzima ono za šta smo se vekovima borili i što nam je najdraže a to je sloboda, on predstavlja iskru straha i širi osećaj nepoverenja u društvu samim tim remeti njegovo normalno funkcionisanje. U ovom radu predstavljene su neke od najznačajnihijih terorističkih organizacija na teriroriji Sirije koje su doprinele razvoju terorizma na ovim prostorima i postavile temelje razvoja ekstremnih delovanja u ovom ratom zahvaćenom području. Neke od pomenutih terorističkih organizacija su nestale, neke su se pregrupisale a većina je apsorbovana od strane većih i bolje organizovanih grupacija. Zahvaljujući globalnim centrima moći odnosno njihovim političkim a pre svega ekonomskim ciljevima, otvara se prostor sa dalje funkcionisanje i širenje ovih radikalnih organizacija. Neprijatelj je sada spreman i na otvorenu borbu jer je zahvlajujući „petrodolaru“ i složenom finansijskom i fiskalnom mehanizmu opremio svoju vojsku od kalašnjikova do tenkova i uradio ono što nije niko u poslednjih sto godina, a to je brisanje kolonijalnih granica čime pojedine terorističke organizacije postaju značajan geopolitički faktor na Bliskom istoku i šire.

CITIRANI RADOVI

Abouzeid, R. (2012). *Meet the Islamist Militants Fighting Alongside Syria's Rebels.* New York: Time.

FDD's Long War Journal. (2017). *Al Qaeda and allies announce 'new entity' in Syria.* FDD's Long War Journal.

Gordon, Barnard. (2012). *U.S. Places Militant Syrian Rebel Group on List of Terrorist Organizations.* New York : New York Times.

Hassan, H. (2014). *Front to Back.* Washington, D.C: The FP Group.

Joscelyn, T. (2014). *Ahrar Al Sham Leader Criticizes Head of Islamic State of Iraq and the Sham.* Long War Journal, Foundation for the Defense of Democracy.

Joscelyn, T. (2013). *Al Qaeda in Iraq, Al Nusrah Front Emerge as Rebranded Single Entity.* Washington D.C.: Long War Journal, Foundation for Defense of Democracies.

Joscelyn, T. (2014). *Al Qaeda's Chief Representative in Syria Killed in Suicide Attack.* Long War Journal, Foundation for the Defense of Democracy,.

Karouny, M. (2015). *Insight - Syria's Nusra Front May Leave Qaeda to Form New Entity.* London: Reuters UK.

Lund, A. (2014). *Fighting in Aleppo, Resisting Geneva: An Interview With the Tawhid Brigade.* Washington, D.C: Carnegie Endowment for International Peace.

Lund, A. (2013). *Say Hello to the Islamic Front.* Stockholm: Swedish Institute of International Affairs.

Lund, A. (2013). *Syria's salafi insurgents: The rise of the Syrian Islamic Front.* Stockholm: Swedish Institute of International Affairs.

Lund, A. (2014). *The Politics of the Islamic Front, Part 1: Structure and Support.* Washington, D.C.: Carnegie Endowment for International Peace.

Roggio, B. (2014). *Al Nusrah Front Launches Joint Assaults with Numerous Syrian Rebel Groups.* Long War Journal. Foundation for the Defense of Democracies.

Schmidt, E. (2012). *C.I.A. Said to Aid in Steering Arms to Syrian Opposition.* New York: The New York Times.

Sinjab, L. (2013). *Guide to the Syrian Rebels.* London: BBC News.

Zaman, A. (2014). *Fight against IS helps PKK gain global legitimacy.* Babelmed.

Zelin, A. (2017). *How Al Qaeda survived drones, uprisings and the Islamic State.* Washington D.C.: Washington Institute for Near East Policy.

Datum prve prijave: 19.07. 2018.
Datum prijema korigovanog članka: 27.11.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Bursać, B. (2019, 10 15). Terorističke organizacije u Siriji. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 7-16. doi:10.12709/fbim.07.07.02.02

*Style – **Chicago** Sixteenth Edition:*

Bursać, Boris. 2019. "Terorističke organizacije u Siriji." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 7-16. doi:10.12709/fbim.07.07.02.02.

*Style – **GOST** Name Sort:*

Bursać Boris Terorističke organizacije u Siriji [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 7-16.

*Style – **Harvard** Anglia:*

Bursać, B., 2019. Terorističke organizacije u Siriji. *FBIM Transactions,* 15 10, 7(2), pp. 7-16.

Style – **ISO 690** Numerical Reference:

Terorističke organizacije u Siriji. **Bursać, Boris.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 7-16.

FBIM Transactions
DOI 10.12709/fbim.07.07.02.03

RAZVOJ TRŽIŠTA DIGITALNIH VALUTA

DIGITAL CURRENCY MARKET DEVELOPMENT

Tamara Cvetković
Poslovni i pravni fakultet, „Union – Nikola Tesla" Unuverzitet u Beogradu, Beograd, Srbija

JEL Kategorija rada: **D85**

Apstrakt

Nakon stabilnog rasta tokom poslednjih nekoliko godina, tržište kriptovaluta je od 2017. godine unaglom porastu.Kriptovalute, poput Bitcoina, sastoje se od mreže peer-to-peer čvorova koji zajedno održavaju zajedničku evidenciju istorijskih transakcija otpornih na neovlašćeni rad. Koristi tehnike šifriranja za kontrolu stvaranja novčanih jedinica i za verifikaciju prenosa sredstava. Kriptovaluta je koncept koji je alternativa fiat valuti koja se koristi u sadašnjem monetarnom sistemu. Preduzetnici, početna i velika, kao i mala i srednja preduzeća (MSP) interesuju se za kriptovalute i smatraju da je to revolucionarni koncept za vršenje transakcija.Tehnologija napreduje velikom brzinom, a uspeh date tehnologije gotovo isključivo diktira tržište na kome se želi poboljšati. Kriptovalute mogu revolucionirati tržišta digitalne trgovine stvarajući sistem slobodnog prometa bez naknade i ima veliku prednost u odnosu na tradicionalne valute s obzirom da poseduje veliku fleksibilnosti u pravljenju brzih peer-to-peer transakcija, naročito u međunarodnim scenarijima. Po svojoj prirodi, ona je u stanju da popuni nedostatke u trenutnim finansijskim tehnologijama i da pomogne u rešavanju tradicionalnih bankarskih problema tako što je sistem ravnopravnih kompanija.Bitcoin je krajem prošle godine bio valuta sa najviše vrednosti u celom svetu. Da je tržište kriptovaluta u ekspanzijipotvrđuju i primeri Južne Amerike, koja je imala ogroman porast transakcija s bitcoinima nakon 2014. godine kao i Argentine koja je središte za povećanu upotrebu kriptovalute.

Ključne reči:*kriptovalute, bitkoin, digitalne valute, digitalne transakcije, kriptografija*

Abstract

After steady growth over the last few years, the cryptocurrency market has been on the rise since 2017. Cryptocurrencies, like Bitcoin, consist of a network of peer-to-peer nodes that together maintain common record of historical transactions resistant to tampering. It uses encryption techniques to control the creation of monetary units and to verify the transfer of funds. Cryptocurrency is a concept that is an alternative to the fiat currency used in the current monetary system. Entrepreneurs, start-ups and large as well as small and medium-sized enterprises (SMEs) are interested in cryptocurrencies and consider it a revolutionary concept for counteraction to transactions. Technology is advancing at high speed, and the success of the technology is almost exclusively dictated by the market in

Adresa autora:
Tamara Cvetković
tamara.cvetkovic.office@gmail.com

which it wants to improve. Cryptocurrencies can revolutionize digital commerce markets by creating a royalty-free system of free circulation and has a great advantage over traditional value and since it presents great flexibility in making fast peer-to-peer transactions, especially in international scenarios.By its nature, it can fill gaps in current financial technologies and be able to help solve traditional banking problems by being a peer-to-peer system.Bitcoin was the highest value currency in the world at the end of last year. The cryptocurrency market is in expansion what is also confirmed by the examples of South America, which saw a huge increase in transactions with bitcoins after 2014, as well as Argentina, which is the hub for increased use of cryptocurrency.

Keywords:*cryptocurrencies, bitcoin, digital currencies, digital transactions, cryptography*

1 UVOD

Kriptovalute uključuju bilo koji digitalni objekat koji koristi kriptografiju. U novijoj literaturi identifikovane su tri potklase kriptovaluta: kriptovalute, kriptokomodnosti i kriptotokeni (Burniske & Tatar, 2017).

Blockchain kao ključna inovacija je novi mehanizam za snimanje transakcija isastavljen je od blokova - to jest, serija overenih transakcija - koje su vezane zajedno - to jest, logički su povezane ili povezane međusobno na takav način da je svaki pokušaj uređivanja ili oštećenja istorijskog zapisa preterano skup ili postaje odmah evidentan. Prema tome, DLT kao što je Bitcoin omogućava svojim učesnicima da zajedno naprave nepobitnu evidenciju transakcija (Gurguc & Knottenbelt, 2017, str. 7).

Kriptovalute (npr. Bitcoin, Litecoin, Monero) su digitalni novčići dizajnirani da izvrše tradicionalnu ulogu valuta u stvarnom svetu, ali u digitalnom prostoru, tj. da deluju kao globalni medij razmene. Kriptotokeni, poznati kao tokeni u sferi DLT, sadrže trgovačku imovinu ili mehanizme razmene vrednosti i/ili mehanizme za kreiranje robe ili usluga, često u kontekstu koji se odnosi na industriju ili domen. Kriptotoken uključuje tokeniziranu investicijsku imovinu, naime kripto vrednosne papire. Relativno noviji termin „kriptokonzumiran“ odnosi se na model tokena koji je konstruisan kao potrošna kriptovaluta, tako da mu se smanjuje vrednost tokom vremena upotrebom funkcije propadanja ili sagorevanja (Gurguc & Knottenbelt, 2017, str. 7).

Bitcoin koristi peer-to-peer tehnologiju da bi radio bez centralnog autoriteta ili banaka; mreža se bavi upravljanjem transakcijama i izdavanjem bitcoina. Bitcoin je otvorenog koda; njegov dizajn je javan, niko ne poseduje i ne kontroliše Bitcoin i svi mogu da učestvuju. Putem svojih jedinstvenih svojstava Bitcoin omogućava načine upotrebe koje nije mogao pokriti nijedan prethodni sistem plaćanja.

Lanac blokova je zajednička javna knjiga na koju se oslanja cela Bitcoin mreža. Sve potvrđene transakcije uključene su u blok lanaca. U slučaju Bitcoin-a, koristi se kriptografija, koja onemogućuje bilo kome da troši sredstva iz novčanika drugog korisnika i omogućava šifriranje novčanika, tako da se ne može koristiti bez lozinke. Kriptografija štiti informacije pretvaranjem u nečitljiv format koji može da dešifruje samo neko ko poseduje tajni ključ. Lanac blokova je javni zapis o Bitcoin transakcijama u hronološkom redosledu. Lanac blokova se deli između svih korisnika Bitcoina. Koristi se za proveru postojanosti Bitcoin transakcija i za sprečavanje dvostruke potrošnje (Nakamoto, 2016).

Većina kreatora politike kriptovalutama pristupa kao podskupu ili obliku virtualne ili digitalne valute. Kriptovaluta, kao digitalni prikaz vrednosti koja treba da predstavlja ravnopravnu („P2P“) alternativu i legalno sredstvo plaćanja koje izdaje država, koristi se kao sredstvo razmene opšte namene i osigurana je mehanizmom poznatim kao kriptografija (Houben & Snyers, 2018, str. 23).

2 EVOLUCIJA NOVCA I POJAVA KRIPTOVALUTA

Kroz istoriju se primećuje da su mnoge kulturne, političke i ekonomske stvarnosti uzrokovale promenu oblika novca. U 7. veku pre nove ere, Lidijsko carstvo, u sadašnjoj Turskoj, je prva civilizacija koja je koristila kovane srebrne ili zlatne kovanice. Međutim, od samog početka trgovinskih odnosa, pojedinci su koristili neku vrstu plaćanja prvo u obliku razmenjene robe, a na kraju i novca koji je držao više oblika, od

školjke i stoke, do kuglice od plemenitih metala, pa čak i soli. Prva valuta koju je država proglasila legalnom korištena je u Kini i datira još iz 1000. godine nove ere, ali je legalni novac postao prevladavajući tek nakon odvajanja američkog dolara od zlata 1971. godine, čime je efektivno okončan Bretton Woods sistem. Do tada, većina novca je bila konvertibilna u plemenite metale (što se u 20. veku zvalo zlatni standard). Prema sistemu Bretton Woodsa, valute zemalja članica držale su se režima fiksnog kursa, koji se održavao u razlici od jednog procenta, u odnosu na američke dolare, koji je zauzvrat bio konvertivan u zlato. Ovi monetarni sistemi podržani robom iz prošlosti mogu biti skupi i neefikasni; međutim, ponudili su stabilnost. Suprotno tome, postojeći nekonvertibilni sistemi nude slobodu vlada u oblikovanju monetarne politike, ali žrtvuju stabilnost cena i mogu rezultirati inflacijom (Gurguc & Knottenbelt, 2017, str. 11). Iako kriptovalute verovatno neće zameniti tradicionalnu fiat valutu, one bi mogle da promene način na koji globalno tržište povezano sa Internetom komunicira, uklanjajući prepreke oko normativnih nacionalnih valuta i deviznih kurseva (DeVries, 2016).

Bitcoin, najčešća i najpoznatija kriptovaluta u svetu, sve je više popularna. Njegova osnovna struktura je ostala ista kao 2008. godine, kada je i nastala, a promene na svetskom tržištu su dovele do mnogo većeg povećanja potražnje za kriptovalutama od očekivanja. Korištenjem kriptovalute korisnici mogu digitalno razmenjivati vrednost bez nadzora treće strane. Kriptovaluta radi na teoriji rešavanja algoritama za šifrovanje kako bi stvorio jedinstvene heševe koji su brojčano ograničeni. U kombinaciji sa mrežom računara koji potvrđuju transakcije korisnici mogu da razmenjuju heševe kao da razmenjuju fizičku valutu. Postoji ograničeni broj bitcoina koji će se ikada generisati, sprečavajući preveliku količinu i osiguravajući njegovu retkost. Voda je, uprkos svojim zahtevima kao životnim materijalom, opšte prihvaćena kao besplatna ili sa malo troškova, jer je obilna. Da je voda bila retka, bila bi vrednija od dijamanata. Vrednost bitcoina postoji zato što njegovi korisnici imaju poverenja da bi ga, ukoliko ga prihvate kao plaćanje, mogli koristiti negde drugde za kupovinu nečega što žele ili trebaju. Sve dok korisnici održavaju tu veru, vrednovani predmet može biti bilo šta. Bitcoin nema unutrašnju vrednost poput zlata po tome što se ne može koristiti za pravljenje fizičkih predmeta poput nakita koji imaju vrednost. Ipak, vrednost i dalje postoji zbog poverenja i prihvatanja (DeVries, 2016).

3 OBLICI KRIPTOVALUTA

Kriptovalute se odnose na široku lepezu tehnoloških dostignuća koja koriste tehniku poznatiju kao kriptografija. Jednostavno rečeno, kriptografija kao tehnika za zaštitu informacija pretvaranjem (tj. šifriranjem) u nečitljiv format koji može samo da dešifruje neko ko poseduje tajni ključ, osigurava kriptovalute kao što su Bitcoin koristeći genijalan sistem javnih i privatnih digitalnih ključeva (Houben & Snyers, 2018, str. 20).

Evropska centralna banka („ECB“) je kriptovalute klasifikovala kao podskup virtualnih valuta. U Izveštaju o šemi virtuelne valute iz 2012. Definisane su takve valute kao oblik neregulisanog digitalnog novca, koji obično izdaju i kontrolišu njegovi programeri, a koristi se i prihvata među članovima određene virtualne zajednice (ECB, 2012). Postoji nekoliko razloga zbog kojih virtualna zajednica izdaje svoju virtualnu valutu. Upotreba virtualnih valuta može pomoći motiviranju korisnika pojednostavljivanjem transakcija i sprečavanjem da se unesu u svoje lično plaćanje detalji svaki put kada žele izvršiti kupovinu. Takođe može pomoći zaključavanju korisnika. Moguće je zaraditi virtualni novac periodičnim pojavljivanjem. Korisnik može otkriti svoje sklonosti ukoliko popuni anketu ili da odgovore na druga pitanja kako bi zaradio dodatni virtualni novac, i tako odaje važne informacije za komercijalnu upotrebu. Virtualne valute se takođe mogu koristiti kao važan alat za programere aplikacija i oglašivače prilikom dizajniranja strategije za iskorištavanje prednosti tržišta virtualne robe (Houben & Snyers, 2018, str. 18). Korisnik kriptovalute je fizičko ili pravno lice koje pribavlja kovanice kako bi ih koristio za kupovinu stvarne ili virtuelne robe ili usluga (iz skupa određenih trgovaca), da izvrše uplate P2P, ili da ih drže u investicione svrhe (tj. na špekulativni način) (FATF, 2014).

Bitcoin (BTC) je konsenzusna mreža koja omogućava novi sistem plaćanja i potpuno

digitalnu valutu. Pojedinac ili grupa pojedinaca koji posluju pod pseudonimom „Satoshi Nakamoto“ objavili su Bitcoin Vhitepaper i opisali ga kao „čisto vertikalnu verziju elektronskog novca koja bi omogućila slanje plaćanja putem Interneta direktno od jedne do druge strane bez prolaska kroz finansijsku instituciju" (Coinmarketcap, 2019). Bitcoin (BTC) se obično opisuje kao virtualna, decentralizovana i (na prvi pogled) anonimna valuta koja nije podržana od vlade ili ne podržava nijedno drugo pravno lice i ne može se razmeniti u zlato ili bilo koju drugu robu (Grinberg, 2011). „Bitcoin“ je uspešno implementirao koncept p2p elektronskog novca. I profesionalci i šira javnost cenili su pogodan spoj javnih transakcija i dokaza o radu kao model poverenja. Danas baza korisnika elektronskog gotovine neprestano raste; kupce privlače niske naknade i pružena je anonimnost elektronskim novcem i trgovci vrednuju njegovu predviđenu i decentralizovanu emisiju. Bitcoin je efikasno dokazao da elektronski novac može biti jednostavan kao papirni novac i podjednako prikladan kao kreditne kartice (Saberhagen, 2013, str. 1). Altkoini su sve kovanice koje su alternativa Bitcoin-u (FATF, 2014). Ukratko, postoje dve vrste Altkoina: - Altkoini koji su napravljeni korišćenjem originalnog protokola otvorenog koda Bitcoin, sa brojnim izmenama njegove osnovne šifre, smišljajući novi novčić sa drugačijim setom karakteristika (ECB, 2012). Primer takvog Altcoina je Litecoin (Martidale, 2018)- Altkoini koji se ne baziraju na Bitcoin otvorenom izvornom protokolu, ali imaju svoj protokol. Dobro poznati primeri takvih Altcoina su Ethereum i Ripple (Zainuddin, 2017).

3.1 Razvoj ugovorne platforme

Etherum (ETH) je pametna ugovorna platforma koja omogućava programerima da izrade decentralizovane aplikacije. ETH je matična valuta za Ethereum platformu i takođe funkcioniše kao naknada za transakcije rudarima u Ethereum mreži. Ethereum je pionir za pametne ugovore zasnovane na blockchainu. Kada se izvodi na blockchainu, pametni ugovor postaje poput računarskog programa koji radi sam koji se automatski izvršava kada su ispunjeni određeni uslovi. Pametni ugovori na blockchainu omogućavaju da se kod izvodi tačno onako kako je programirano bez ikakvih prekida rada, cenzure, prevare ili smetnji trećih strana. To može olakšati razmenu novca, sadržaja, imovine, akcija ili bilo čega vrednog. Mreža Ethereum predstavila se 30. jula 2015. sa 72 miliona Ethereuma (Coinmarketcap, 2019). Ethereum (ETH), lansiran je kao decentralizovana platforma koja pokreće takozvane „pametne ugovore“. Pametni ugovori su „samoizvršavajući“ ugovori ili aplikacije koje rade tačno onako kako su programirani bez ikakve mogućnosti zastoja (tj. blockchain se nikad ne spušta, već se pokreće), cenzura, prevara ili uplitanja treće strane, predstavljaju temelj nove ere interneta, internet na kome su ugrađeni novac i plaćanja (Ethereum, 2019). Kao i drugi blokeri, Ethereum ima izvornu kriptovalutu koja se zove Ether (ETH). ETH je digitalni novac i ima mnogo funkcija poput Bitcoina. Snabdevanje ETH-om ne kontroliše nijedna vlada ili kompanija - decentralizovano je i malo je. Ljudi širom sveta koriste ETH za plaćanje, kao skladište vrednosti ili kao obezbeđenje. Veliki je značaj Ethereum-a, programeri mogu da ga koriste za pravljenje novih vrsta aplikacija: novčanice sa kriptovalutama koje omogućavaju jeftino, trenutno plaćanje ETH-om ili drugim sredstvima, finansijske aplikacije koje omogućuju pozajmljivanje ili ulaganje digitalnih sredstava, decentralizovana tržišta koja omogućavaju trgovinu digitalnom imovinom ili „predviđanjima“ o događajima u stvarnom svetu... Ove decentralizovane aplikacije (ili „dapps“) koje nijedan entitet ili osoba ne kontroliše dobijaju koristi od kriptovalutne i blockchain tehnologije. Oni mogu kontrolisati digitalna sredstva kako bi kreirali nove vrste finansijskih aplikacija. Ethereum zajednica je najveća i najaktivnija blockchain zajednica na svetu. Obuhvata programere osnovnih protokola, kriptoekonomske istraživače, rudarske organizacije, vlasnike ETH-a, programere aplikacija, obične korisnike, kompanije od 500 ljudi (Houben & Snyers, 2018, str. 33).

Ripple (XRP) je nezavisno digitalno sredstvo koje je izvorno iz knjige Ripple Consensus Ledger. Uz dokazano upravljanje i najbržu potvrdu transakcije takve vrste, KSRP se smatra najefikasnijom nagodbom za finansijske institucije i pružaoce likvidnosti koji traže globalni domet, pristupačnost i brzu konačnost poravnanja za međubankarske tokove

(Coinmarketcap, 2019). Ripple kao open-source, P2P platforma za digitalno plaćanje omogućava skoro trenutni transfer valute bez obzira na oblik (npr. američki dolar, jen, bitcoin,…) . Pokrenut je 2012.od strane privatne kompanije Ripple (Labs), Inc.162 Ripple (Labs), Inc., odgovorne za dalji razvoj protokola Ripple, prva je kompanija koja je dobila „BitLicense“ za slučaj institucionalne upotrebe digitalne imovine od Njujorškog Odeljenja za finansijske usluge. Takođe dobija podršku velikog broja velikih igrača u industriji finansijskih usluga, kao što su Merill Linch, Santander, Bank of America, Santander itd. (Houben & Snyers, 2018, str. 35).

Stellar, kreiran 2014. od strane jednog od osnivača kompanije Ripple sa ciljem povezivanja ljudi sa jeftinim finansijskim uslugama koji se bore protiv siromaštva, je dom kriptovalute Lumen (KSLM). Lumeni se koriste za plaćanje transakcija na Stellar mreži; doprinose sposobnosti kretanja novca po svetu i na brzo i sigurno vrše transakcije između različitih valuta (Houben & Snyers, 2018).

U osnovi, Stellar je sistem za praćenje vlasništva koji koristi računovodstvenu knjigu, podeljenu preko mreže nezavisnih računara, za smeštanje dve važne stvari za svakog vlasnika računa: šta on poseduje (stanja na njegovom računu) i šta želi da radi sa onim što poseduje. Stellar knjiga je robusnija od ostalih blockchaina. Bitcoin, na primer, čuva samo stanje. Dodavanje operacija u knjigu znači da kada se ponude korisnika preklapaju (recimo, kupovina i prodaja), trgovina se može izvršiti automatski. Računari koji pokreću Stellar i objavljuju knjigu nazivaju se čvorovi. Oni sistematski potvrđuju sadržaj knjige tako da je ona uvek dosledna širom mreže. Na primer, kada nekome pošaljete dolar na Stellar-ugrađenoj aplikaciji, čvorovi provere da li su ispravni bilansi zaduženi i kreditirani i svaki čvor osigurava da svaki drugi čvor vidi i pristaje na transakciju (Stellar, 2019).

Lumen, često skraćeno XLM, je znak protokola Stellar mreže. Sto milijardi lumena stvoreno je istog trenutka kada je Stellar počeo da radi uživo, kao deo dizajna protokola. Ovi tokeni igraju jedinstvenu ulogu u radu mreže.

Lumeni su dostupni na svakoj glavnoj berzi kriptovaluta. Svako ko želi zadržati ili premestiti novac na Stellar takođe mora držati lumene. Prema protokolu, svaki račun mora da izdvoji mali prirast lumena za svaku vrstu imovine koju poseduje. Slično tome, račun mora rezervisati lumene za svaku otvorenu ponudu u odnosu na svoju imovinu. Ukupno zadržavanje za tipični račun je malo - nekoliko XLM. Stellar takođe nameće veoma malu naknadu za svaku transakciju, a ta naknada može se platiti samo u lumenima (Stellar Lumens, 2019).

3.2 Prednosti, nedostaci i značaj kriptovaluta

Kriptovaluta je pomogla u prevazilaženju nekoliko ključnih izazova povezanih sa međubankarskim transakcijama i prekograničnim doznakama. Iako međubankarske transakcije često trebaju dane za odobrenje i poravnanje, transakcije s kriptovalutama mogu se obaviti u mnogo kraćem roku. Brže transakcije i nagodbe mogu pomoći potrošačima da lakše izvršavaju transakcije, a istovremeno uklanjaju potrebu za plaćanjem naknada posrednicima radi pojednostavljenja procesa. Ovo može pomoći bankama da uštede na napornim procedurama sa svojim klijentima i razmenama. Kada kupac izvrši kupovinu koristeći kriptovalutu kao plaćanje, transakcija često prolazi kroz vrata plaćanja po fiksnom tečaju i automatski se pretvara u tradicionalno priznatu fiat valutu kako bi trgovac mogao da izbegne volatilnost tržišta kriptovaluta. Plaćanje putem kriptovalute ima nekoliko prednosti kao što su poboljšana sigurnost transakcija, zaštita od prevare, decentralizovani sistem, niske naknade, zaštita od povrata potrošača i brzi međunarodni transferi (Cryptocurrency Market by Offering (Hardware: GPU, FPGA, ASIC, & Wallet, and Software), Process (Mining and Transaction), Type, Application (Trading, Remittance, Payment: Peer-to-Peer Payment, Ecommerce, and Retail), and Geography - Global Forecast to 2024, 2018). Kriptovaluta je na jedinstvenom položaju kao prethodnica u potencijalno transformativnoj tehnologiji dugogodišnjim finansijskim sistemima. Značajan deo stanovništva u zemljama u razvoju je nebankiran. U Latinskoj Americi 60% od 600 miliona stanovnika nema pristup bankovnim računima. Bitcoin tehnologija omogućava pojedincima da razmenjuju valutu bez potrebe da treća osoba sa poverenjem, poput banke, nadgleda transakciju. Sve što je potrebno za upotrebu Bitcoina je

mobilni telefon, kojem 70% Latinoamerikanaca ima pristup. Zbog mogućnosti ad hoc umrežavanja bitcoina, dva korisnika mogu međusobno trgovati bitcoinima skeniranjem KR kodova prikazanih na njihovim telefonima odštampanima u aplikaciji. Preduzeća počinju da vide vrednost upotrebe kriptovaluta za međunarodne transakcije, posebno kada transakcije moraju da se brzo dogode kao odgovor na hitne slučajeve. Kriptovalute su postavljene isključivo za rešavanje ovog problema zahvaljujući brzini i lakoći transakcija u sistemu peer-to-peer. Novac se može oživeti u inostranstvu, ali obično stiže danima nakon slanja. Transakcija se može pogoditi bilo kojim brojem neobjašnjivih naknada jer prelazi granice, što otežava slanje tačnog iznosa drugom preduzeću. Dobar primer hitnih potreba je internetska kompanija koja pati od napada uskraćivanja usluge i traži trenutnu zaštitu kompanije za zaštitu mreže. U ovom je scenariju brzina transakcije od suštinske važnosti jer svaki minut kada veb lokacija kompanije bude u padu, profit se gubi. Kriptovaluta ima veliku prednost u odnosu na tradicionalne valute zahvaljujući svojoj fleksibilnosti u pravljenju brzih transakcija (peer-to-peer) transakcija, posebno u međunarodnim scenarijima. Ebai.com već koristi sistem plaćanja koji je sličan Bitcoin-u koji se zove PayPal, i bio je vrlo uspešan u njegovom korišćenju kako bi olakšao sve kupovine na njegovoj veb lokaciji. Put svile bio je još jedan primer uspešnog internet tržišta, iako je to vrlo ilegalna priroda. Povezao je kupce i prodavce koji su uglavnom koristili bitcoin za dovršavanje transakcija. Ovo tržište pokazalo je kako digitalna valuta može povezati kupce i prodavce bez većeg uplitanja predsedavajućih vlada i još uvek uspeva. Internet kupovina uspeva, a bitcoin je spreman da proširuje svoj domet efikasnim i lakim plaćanjem i za prodavce i za kupce. Internet kupovina opšte namene za pojedince činila je gotovo 23 procenata transakcija koje je Bitpai obrađivao u drugom kvartalu 2015. Kriptovaluta ima prednost u odnosu na tradicionalne prodavače bazirane na karticama jer eliminiše te takse. Neke nacije poput Islanda čak su počele osnivati sopstvenekriptovalute. Moguće je da budućnost ima mesto za kriptovalute kao glavno valutno rešenje, a Bitcoin će biti od presudne važnosti u probijanju puta za razvoj ovih valuta. Tržišta Evrope i Latinske Amerike eksplodiraju transakcijama s Bitcoin-om (DeVries, 2016, str. 8).

Nažalost, Bitcoin pati od nekoliko nedostataka. Na primer, distribuirana priroda sistema je nefleksibilna, sprečavajući primenu novih funkcija dok skoro svi korisnici mreže ne ažuriraju svoje klijente. Neke kritične mane koje se ne mogu brzo otkloniti odvraćaju od širenja bitkoina. U tako nefleksibilnim modelima, efikasnije je izvesti novi projekat, a ne stalno popraviti originalni projekat (Saberhagen, 2013, str. 1). Virtuelne šeme ne predstavljaju rizik po stabilnost cena, pod uslovom da stvaranje novca i dalje ostane na niskom nivou nivo; imaju tendenciju da budu inherentno nestabilni, ali ne mogu ugroziti svoju finansijsku stabilnost. Trenutno nisu regulisane i ne nadgleda ih nijedan javni organ, iako učešće u ovim šemama izlaže korisnike kreditima, likvidnošću, operativnim i pravnim rizicima. Mogle bi predstavljati izazov za javne organe, imajući u vidu pravnu nesigurnost, jer ih mogu koristiti kriminalci, prevaranti da bi ih izvršili ilegalne aktivnosti (Houben & Snyers, 2018, str. 47).

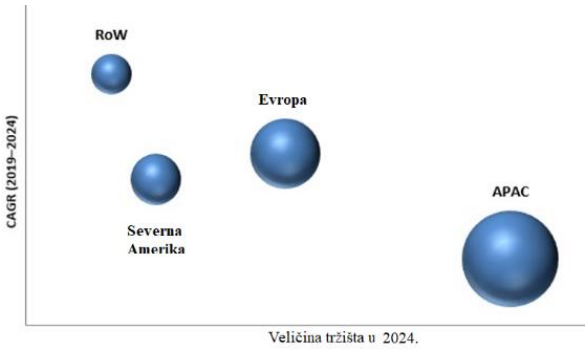
4 USPON TRŽIŠTA KRIPTOVALUTA

Nakon što je imalo stabilan rast tokom poslednjih nekoliko godina, tržište kriptovaluta je u 2017. godini naglo skočilo, povećavajući više od 1.200% (Bovairo, 2017). Trenutno je u opticaju nekoliko stotina kovanica (ukupna tržišna kapitalizacija od preko 300 milijardi evra) (Coinmarketcap, 2019). Predviđa se da će celokupno tržište kriptovaluta dostići 1,40 milijardi USD do 2024. godine, pri CAGR od 6,18% tokom predviđenog perioda.

Kriptovaluta je digitalna valuta koja se stvara i pohranjuje elektronski u blockchain. Zahvaljujući ovim faktorima, ekosistem je privukao široko finansiranje, saradnju i partnerstva među dobavljačima rešenja za kriptovalute radi pružanja krajnjih rešenja (Cryptocurrency Market by Offering (Hardware: GPU, FPGA, ASIC, & Wallet, and Software), Process (Mining and Transaction), Type, Application (Trading, Remittance, Payment: Peer-to-Peer Payment, Ecommerce, and Retail), and Geography - Global Forecast to 2024, 2018).

Bitcoin je krajem 2015. godine bio valuta sa najviše vrednosti u celom svetu ito nije mali

podvig u globalnoj ekonomiji (DeVries, 2016, str. 2).



Slika 1. Veličina tržišta kriptovaluta, po regionu, 2024 (USD milioni)

Izvor: (Cryptocurrency Market by Offering (Hardware: GPU, FPGA, ASIC, & Wallet, and Software), Process (Mining and Transaction), Type, Application (Trading, Remittance, Payment: Peer-to-Peer Payment, Ecommerce, and Retail), and Geography - Global Forecast to 2024, 2018).

Južna Amerika je imala ogroman porast transakcija s bitcoinima, povećavajući se za 510% od 2014. do 2015. godine. Argentina je središte za povećanu upotrebu kriptovalute zbog izuzetno visoke stope inflacije i velikog broja stanovništva nebankiranih građana. U prošlosti su Argentinci konvertovali svoju valutu u američke dolare kako bi sačuvali svoju vrednost. Međutim, Argentina je nedavno postavila ograničenja na to koliko američkih dolara mogu da pretvore njeni građani. Kao rezultat toga, nastalo je i crno tržište za kupovinu USD po višoj ceni i povećano usvajanje bitkoina (DeVries, 2016, str. 2).

Situacija Argentine nije izolovan slučaj. Iznova i iznova, investitori su videli pad globalnog tržišta (uglavnom iz političkih razloga), a kriptovalute povećavaju vrednost i upotrebu. Ujedinjeno Kraljevstvo je nedavno glasalo za izlazak iz Evropske Unije. Pre glasanja, cena bitcoina pala je gotovo 15%. Nakon što je Velika Britanija glasala za odlazak, cena je skočila sa 550 na 650 dolara dan kasnije (DeVries, 2016, str. 3).

Suprotno tome, na internacionalnim tržištima se primetio značajan pad vrednosti bitcoina, zbog pada poverenja investitora u to šta će glasanje za izlazak Velike Britanije iz Evropske Unije značiti u finansijskom smislu. Kriptovaluta je jaka u ovoj situaciji jer je jedina valuta koja se može brzo kupiti i prodati, a i dalje se koristi širom sveta. Druge valute mogu se razmenjivati, ali za tu aktivnost je potrebno lično razmeniti novac i taj novac ne može da se troši ukoliko se lokalno ne prihvati. Na primer, Amerikanac nije mogao brzo da razmeni USD za japanski jen, a zatim da tu valutu iskoristi za kupovinu. Morali bi da posete menjačnicu, što može zahtevati vožnju do najbližeg međunarodnog aerodroma. Drugo, kad dobiju valutu, ne bi imali načina da koriste jen, jer to nije lokalno priznata valuta. Ovakva situacija nije slučaj sa Bitcoin-om (ili bilo kojom drugom kripto-valutom). Da biste kupili bitcoin, potrebno je samo postaviti internetski račun sa mrežnom razmenom, uputiti svoj zahtev i transakcija se obično završava za nekoliko minuta. Jednom kada se bitcoin uđe u njihov digitalni novčanik, oni će moći da kupuju od hiljada dobavljača širom sveta. U ovom primeru, Bitcoin je održivije rešenje kao brzi ulazak i izlazak za valutu koja brzo može dobiti vrednost. Druge fijat valute mogu postati jače i poželjnije, ali ne mogu se takmičiti sa okretnošću kriptovaluta (DeVries, 2016, str. 3).

5 ZAKLJUČAK

Kriptovaluta se koristi za razne aplikacije, kao što su trgovanje, doznake i plaćanja. Ove aplikacije pokreću tržište kriptovaluta. Trgovanje kriptovalutama uključuje razmenu fiat valuta sa kriptovalutama, kao i kupovinu i prodaju kriptovaluta. Broj kriptovaluta se eksponencijalno povećao; trenutno je na raspolaganju više od 1.500 kriptovaluta. Nekoliko ovih kovanica može se nabaviti samo korišćenjem glavnih kriptovaluta kao što su Bitcoin ili Ethereum.

Bitcoin zajednica nastoji da se uvuče u glavni tok kroz inovacije i rešavanje starih problema. Ostali oblici kriptovalute već su se pojavili i stekli sopstvene sledove, a svaki se malo razlikuje od Bitcoina i, verovatno, validnih. Trebalo bi obaviti opsežne studije o ekonomskim efektima efekta Bitcoina na dugogodišnje performanse fiat valute i uporediti rezultate sa zemljama koje počinju da usvajaju kriptovalute koje sponzoriše država. Sposobnost kriptovalute da obavlja mikro transakcije može joj omogućiti da premosti ekonomski jaz koji tradicionalne valute

sponzorisane od strane države ne bi bile u stanju da reše, ali za to je potrebna mnogo dublja tržišna i ekonomska analiza. Takođe, tehnologija lančanog bloka koja deluje kao okosnica Bitcoina ima potencijalnu upotrebu na druge načine, poput pametnih ugovora. Ovi ugovori su programirana plaćanja koja nastaju kada se dogodi postavljeni uslov. Kriptovaluta je proizvod korišćenja kriptografije za stvaranje digitalnog svojstva. Granica digitalne svojine popularizovana je prelaskom muzičke industrije na infrastrukturu zasnovanu na oblaku. Ova granica je još uvek prilično nova i neistražena, uglavnom naseljena različitim vrstama medija. Drugi oblici digitalne svojine mogu postati toliko popularni koliko i muzika i kriptovaluta. Pre osam godina, digitalni novac je bio potpuno nečuven, a tvorac Bitcoin singla je to promenio. Kriptologija, osnovna nauka ispod bitcoina i svih kriptovaluta, može biti mehanizam koji stoji iza granice za nove i uzbudljive digitalne izume (DeVries, 2016, str. 8).

CITIRANA DELA

Bovairo, C. (2017, November). *Forbes.* Retrieved September 05, 2019, from https://www.forbes.com/sites/cbovaird/2017/11/17/why-the-crypto-market-has-appreciated-more-than-1200-this-yea

Burniske, C., & Tatar, J. T. (2017). *The Innovative Investor's Guide to Bitcoin and Beyond, Cryptoassets.* McGraw-Hill.

Coinmarketcap. (2019). Retrieved September 01, 2019, from https://coinmarketcap.com/coins/views/all/

(2018). *Cryptocurrency Market by Offering (Hardware: GPU, FPGA, ASIC, & Wallet, and Software), Process (Mining and Transaction), Type, Application (Trading, Remittance, Payment: Peer-to-Peer Payment, Ecommerce, and Retail), and Geography - Global Forecast to 2024.* https://www.marketsandmarkets.com/Market-Reports/cryptocurrency-market-158061641.html. Retrieved from Markets and markets: https://www.marketsandmarkets.com/Market-Reports/cryptocurrency-market-158061641.html

DeVries, P. D. (2016). An Analysis of Cryptocurrency, Bitcoin, and the Future. *International Journal of Business Management and Commerce*.

ECB. (2012, October). *Virtual Currency Schemes*. Retrieved from ECB Europa EU: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

Ethereum. (2019). Retrieved September 05, 2019, from https://www.ethereum.org

FATF. (2014, June). *Virtual Currencies – Key Definitions and Potential AML/CFT Risks*. Retrieved September 07, 2019, from http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Grinberg, R. (2011). "Bitcoin: An Innovative Alternative Digital Currency" . *Hastings Science & Technology Law Journal, 2011, Vol. 4*, 160.

Gurguc, Z., & Knottenbelt, W. (2017). *Cryptocurrencies: overcoming barriers to trust and adoption.* London: Etoro.

Houben, R., & Snyers, A. (2018). *Cryptocurrencies and blockchain-Legal context and implications for financial crime, money laundering and tax evasion.* European Union: Policy Department for Economic, Scientific and Quality of Life Policies. Retrieved from http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

Martidale, J. (2018, January). *Digitaltrends.* Retrieved September 04, 2019, from “What is Litecoin? Here’s everything you need to know: https://www.digitaltrends.com/computing/what-is-litecoin/.

Nakamoto, S. (2016). *Bitcoin*. Retrieved September 01, 2019, from https://bitcoin.org/bitcoin

Saberhagen, N. v. (2013). CryptoNote v 2.0. https://cryptonote.org/whitepaper.pdf.

Stellar. (2019, September 07). *Stellar*. Retrieved from https://www.stellar.org/overview

Stellar Lumens. (2019, September 02). Retrieved from https://www.stellar.org/lumens/.

Zainuddin, A. (2017). *masterthecrypto.* Retrieved September 04, 2019, from Coins, Tokens & Altcoins: What's the Difference?: https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/

Datum prve prijave: 09.09.2019.
Datum prijema korigovanog članka: 07.10.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Cvetković, T. (2019, 10 15). Razvoj tržišta digitalnih valuta. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 17-25. doi:10.12709/fbim.07.07.02.03

*Style – **Chicago** Sixteenth Edition:*

Cvetković, Tamara. 2019. "Razvoj tržišta digitalnih valuta." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 17-25. doi:10.12709/fbim.07.07.02.03.

*Style – **GOST** Name Sort:*

Cvetković Tamara Razvoj tržišta digitalnih valuta [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 17-25.

*Style – **Harvard** Anglia:*

Cvetković, T., 2019. Razvoj tržišta digitalnih valuta. *FBIM Transactions,* 15 10, 7(2), pp. 17-25.

Style – **ISO 690** Numerical Reference:

Razvoj tržišta digitalnih valuta. **Cvetković, Tamara.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 17-25.

FBIM Transactions
DOI 10.12709/fbim.07.07.02.04

PREDUSLOVI ZA USPEH PLATNOG SISTEMA BAZIRANOG NA DIGITALNOJ (KRIPTO)VALUTI

PREREQUISITES FOR A SUCESSFULL PAYMENT SYSTEM BASED ON DIGITAL (CRYPTO)CURRENCY

Dragan Ćosić
Poslovni i pravni fakultet, Univerzitet „Union – Nikola Tesla“ u Beogradu, Beograd, Srbija

Predrag Radovanović
Visoka poslovna škola strukovnih studija, Leskovac, Srbija

JEL kategorija rada: **E42, E49, L86**

Apstrakt

Prvi platni sistemi bazirani na elektronskom/digitalnom novcu pojavili su se početkom i sredinom devedesetih godina prošloga veka. U svom razvoju, elektronski/digitalni novac prošao je kroz nekoliko generacija. Mada prva generacija platnih sistema baziranih na digitalnom novcu nije doživela veći komercijalni uspeh, jedna forma digitalne valute tiho je evoluirala tokom vremena u ono što danas poznajemo kao kriptovalute. Kriptovalute su generalno bazirane na decentralizovanim, direktnim P2P plaćanjima. U radu će biti predstavljen nastanak, razvoj i izvesni tehnički aspekti kriptovaluta. Biće sumirani preduslovi koje su brojni analitičari isticali kao najbitnije koje jedan platni sistem baziran na digitalnoj (kripto)valuti mora da ispuni kako bi bio uspešan. Spisku preduslova biće dodati i oni kojima u teoriji i praksi digitalnih (kripto)valuta do sada nije posvećena dovoljna pažnja. Zaključujemo da je cilj uspešnog platnog sistema baziranog na digitalnoj (kripto)valuti da što vernije preslika karakteristike realnog novca, zbog čega je, međutim, nužno pratiti slične modalitete kreiranja, opticaja i valuacije.

Ključne reči: *elektronski novac, digitalni novac, platni sistem, kriptovaluta, blokčejn.*

Abstract

The first electronic/digital money-based payment systems emerged in the early and mid-1990s. In its development, electronic/digital money has passed through several generations. Although the first generation of digital money-based payment systems failed to achieve commercial success, one form of digital currency has quietly evolved over time into what we now know as cryptocurrencies. Cryptocurrencies are generally based on decentralized, direct P2P payments. The origin, development and certain technical aspects of cryptocurrency will be presented in the paper. The

Adresa autora zaduženog za korespodenciju:
Dragan Ćosić
cosicdr@gmail.com

paper will also summarize the prerequisites that many analysts have highlighted as the most important that a digital (crypto)currency-based payment system must meet in order to be successful. The list of prerequisites will be extended with those who have not received enough attention in the theory and practice of digital (crypto)currencies so far. We conclude that the goal of a successful digital (crypto)currency-based payment system is to accurately capture the characteristics of real money; therefore, it is necessary to follow similar modalities creation, circulation, and valuation.

Keywords: *electronic money, digital money, payment system, cryptocurrency, blockchain.*

1 UVOD

Postoje, načelno, dve osnovne metode plaćanja preko interneta: (1) plaćanja sa centralizovanim obračunom i (2) plaćanja digitalnim novcem. Plaćanja sa centralizovanim obračunom izvršavaju se preko tekućih računa u bankama, dok se kliring takvih plaćanja obavlja preko nekog klirinškog sistema. Primera radi, plaćanje kreditnim karticama preko interneta mogli bismo svrstati u prvu kategoriju: bez obzira na to što se plaćanje obavlja preko interneta, neophodan je kliring ovakvih transakcija preko klirinškog centra, pri čemu se vrši zaduženje računa kupca uz istovremeno odobrenje računu trgovca.

Plaćanja digitalnim novcem mogu, takođe, biti bazirana na centralizovanom obračunu. Vremenom su, međutim, razvijeni platni sistemi bazirani na digitalnom novcu koji su u praksi pokazali da mogu funkcionisati bez potrebe za centralizovanim obračunom. Jedan od najpoznatijih sistema ove vrste bio je *Mondex*[1], koji je omogućavao direktne transakcije sa jedne kartice na drugu ili tzv. *peer–to–peer* (P2P)[2] transakcije, bez posredovanja neke treće strane u transakciji (npr. banke).

Razlika između navedenih modela plaćanja je od suštinskog značaja za novu, digitalnu ekonomiju. Centralizovani obračun je mnogo skuplji i uzrokuje veće troškove po transakciji, zbog čega ovakav obračun nije pogodan za plaćanja male vrednosti (npr. plaćanja u rasponu od nekoliko dolara do nekoliko centi). Procenjeno je da transakcije sa centralizovanim obračunom koštaju, u proseku, od 30 centi do 1 dolara po transakciji (Shaw, 2001, str. 9). To znači da bi troškovi obrade jedne transakcije, u slučaju plaćanja male vrednosti, lako mogli premašiti iznos same transakcije. Sa druge strane, P2P transakcije digitalnim novcem bez centralizovanog obračuna koštaju, u proseku, od 1 do 5 centi po transakciji (Shaw, 2001, str. 9).

Decentraliziovana plaćanja digitalnim novcem neophodna su za podršku novog sistema za distribuciju nematerijalnih dobara u digitalnoj formi preko interneta, koji pojedini autori nazivaju „superdistribucijom“ [za više detalja vidi: (Mori & Kawahara, 1990)]. U realnom svetu, distribucija nematerijalnih dobara (npr. film, muzika, softver) vezana je za neki fizički medijum (CD, DVD i sl.). U digitalnom svetu nematerijalna dobra su oslobođenja fizičkog medijuma i mogu nesmetano da se razmenjuju u čisto digitalnoj formi. U elektronskoj trgovini preko interneta, nematerijalna dobra poprimaju oblik digitalnih tokova informacija koji se prenose računarskim mrežama, nesputani fizičkim nosiocem (Radovanović & Ćosić, Elektronsko poslovanje i elektronsko bankarstvo, 2010, str. 88) i razmenjuju se za digitalni novac koji je, takođe, potpuno dematerijalizovan i oslobođen tradicionalnog fizičkog medijuma (papir, metal).

S obzirom na to da je veoma teško utvrditi spremnost nekog klijenta da plati digitalni sadržaj preko interneta (npr. preuzimanje melodije ili pozadinske slike za mobilni telefon, čitanje e–magazina, preuzimanje elektronske knjige ili nekog njenog poglavlja, nadogradnja i ažuriranje softvera i sl.) osnovna ideja u vezi sa konceptom superdistribucije je da se klijentima naplaćuje digitalni tok podataka. Pošto taj tok podataka može biti vrlo mali (npr. čitanje članka u nekom magazinu koji sadrži samo običan tekst), novi platni sistemi trebalo bi da omoguće plaćanja u vrlo malim iznosima, koja nazivamo „mikroplaćanjima“. Prema tome, decentralizovana plaćanja digitalnim novcem trenutno predstavljaju jedini logični izbor za mikroplaćanja (Radovanović P. , 2009, str. 158).

[1] Za više detalja o sistemu digitalnog novca *Mondex* vidi: (Radovanović P. , 2009, str. 135-137).

[2] U nekim izvorima P2P transakcije se označavaju i kao C2C (client–to–client).

Mada centralizovana platna arhitektura još uvek opstaje u B2C segmentu platnog tržišta, najviše zahvaljujući platnim karticama, ona nije troškovno efikasna za mikroplaćnja. Decentralizovana plaćanja digitalnim novcem imaju potencijal da ukinu dominaciju centralizovane platne arhitekture u B2C segmentu platnog tržišta.

Tokom vremena razvijeno je više različitih platnih sistema baziranih na digitalnom novcu, ali nisu svi bili pogodni za mikroplaćanja. Neki od najzanimljivijih i najsofisticiranijih decentralizovanih platnih sistema u okviru prve generacije digitalnog novca bili su *eCash*[3] i *Mondex*. *Mondex* je originalno bio baziran na hardverskim uređajima, nalik karticama, koji su mogli da komuniciraju jedan sa drugim i da izvrše direkne transakcije „sa kartice na karticu“, bez potrebe za centralizovanim kliringom. Sa druge strane, *eCash* sistem bio je baziran na softverskim „digitalnim novčićima“, koji su mogli potpuno anonimno da se razmenjuju između učesnika u sistemu (tzv. „peer–to–peer“ ili P2P plaćanja). Oba pomenuta sistema bila su krajnje sofisticirana i bezbedna u poređenju sa konkurentskim sistemima, ali nijedan od njih nije zabeležio veći komercijalni uspeh (kasnije su ih preuzele druge kompanije) zbog toga što nijedan od njih nije imao podršku banaka. Kako bi zadržale svoj monopol u B2C segmentu platnog tržišta, banke su uglavnom podržavale digitalna plaćanja sa centralizovanim obračunom, koja se izvršavaju preko tekućih računa u bankama. Ovakvi sistemi, međutim, predstavljali su samo on–lajn ekstenziju tradicionalnih platnih instrumenata (npr. platnih kartica i čekova). Pošto su se i dalje oslanjali na centralizovanu platnu arhitekturu, oni nisu bili dovoljno efikasni za mikroplaćanja.

2 POJAM I NASTANAK KRIPTOVALUTA I BLOKČEJN TEHNOLOGIJE

Često se termin *elektronski novac* (e–money, e–cash, electronic money) poistovećuje sa terminom *digitalni novac* (digicash, digital cash, cyber cash) iako sve veći broj autora povlači granicu između ova dva termina. Veoma je teško, međutim, povući preciznu granicu između elektronskog i digitalnog novca zbog toga što je elektronski novac stvorio preduslove za nastanak digitalnog novca, a sada se sve više preobražava u njega. Uopšteno, elektronski novac je širi koncept koji, između ostalog, obuhvata i digitalni novac [za precizno razgraničenje i definisanje elektronskog i digitalnog novca vidi: (Radovanović & Ćosić, 2010, pp. 164-168)].

Jedno od najkonciznijih razgraničenja glasi: „Dok elektronski novac (e–money) predstavlja širi koncept koji se odnosi na sve mehanizme za transfer novca bazirane na računarima (npr. kreditne ili debitne kartice, automatske klirinške kuće), kao i na odgovarajuću opremu za pristup ovim sistemima (npr. automatski samouslužni šalteri, POS terminali), digitalni novac (digital cash, cybercash) predstavlja uži termin koji se odnosi na sisteme za transfer novca putem Interneta“ (Guttmann, 2003, str. 9).

Kriptovalute su podskup digitalnih valuta. „Kriptovaluta u svom najčistijem obliku je P2P verzija elektronskog novca. Ona omogućava da se on–lajn plaćanja vrše direktno, od jedne strane ka drugoj, bez posredovanja neke finansijske institucije“ (Nian & Chuen, 2015, str. 8).

Čaumov [4] *eCash* može se smatrati prvom komercijalno dostupnom formom kriptovalute. *DigiCash Inc*. osnovana je 1990. u Holandiji [za više detalja vidi: (Chaum, 1983); (Chaum, Fiat, & Naor, 1990)]. Platni sistem baziran na elektronskom novcu ove kompanije — *eCash* — koristio je kriptografske protokole za prevenciju

[3] Za više detalja o sisemu *eCash* vidi: (Radovanović & Ćosić, 2010, str. 178-181).

[4] Dejvid Čaum (*David Chaum*) je pronalazač čitavog niza kriptografskih protokola. Njegov rad pod naslovom *“Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”* (1981) postavio je temelj za istraživanja u oblasti anonimnih komunikacija. Bio je profesor na Univerzitetu u Njujorku i Univerzitetu u Kaliforniji. Osnivač je Međunarodnog udruženja za kriptološka istraživanja (International Association for Cryptologic Research – IACR) i grupe za istraživanja u oblasti kriptografije pri Nacionalnom istraživačkom institutu za matematiku i informatiku u Amsterdamu. Osnovao je kompaniju koja se bavila elektronskim novcem, *DigiCash,* 1990. godine.

dvostrukog trošenja, kao i tzv. „slepe potpise“[5] za zaštitu privatnosti svojih korisnika. Uprkos činjenici da je visoko sofisticirani *eCash* sistem kompanije *DigiCash* bio dostupan preko više različitih banaka kao pilot–projekat i da je demonstrirao vrlo visok nivo pouzdanosti i bezbednosti transakcija, nije uspeo da stekne značajniji udeo na tržištu, uglavnom zbog činjenice da je njegovo prihvatanje umnogome zavisilo od banaka. Kompaniju *DigiCash Inc.* i njen tehnološki know–how kasnije je preuzela firma *eCash Technologies* koja je, nešto kasnije, i sama bila preuzeta od kompanije *InfoSpace* 1999. godine [za više detalja vidi: (Radovanović & Ćosić, 2010, str. 206-207)]. Interesovanje za kriptovalute je polako počelo da bledi.

Bitkoin se prvi put pominje u radu koji je publikovao *Satoshi Nakamoto*[6] 2008. godine, kao *kriptovaluta* koja koristi softver otvorenog koda, koji se izvršava na decentralizovanoj peer–to–peer mreži (Nakamoto, 2008). Bitcoin se ne oslanja na neku treću stranu od poverenja (banke, asocijacije za platne kartice i sl.) koja bi obrađivala transakcije, već umesto toga koristi kriptografski dokaz. Sa pronalaskom bitkoina bilo je moguće izvršiti plaćanja preko interneta bez kontrole nekog centralnog autoriteta (i troškova koji nastaju s tim u vezi). Pre pronalaska bitkoina, sve transakcije koje su se izvršavale on–lajn uvek su zahtevale neku treću stranu kao posrednika od poverenja koji će verifikovati transakciju (Brito & Castillo, 2013).

Bitkoin je digitalna valuta koja se kreira i čuva u elektronskom obliku. Bitkoini se šalju i primaju uz pomoć aplikacije za mobilni telefon, softvera za računar, ili putem pružaoca usluge bitkoin novčanika (bitcoin wallet). Ovaj novčanik generiše adresu, nalik na broj računa u banci. Bitkoin adresa je jedinstveni alfanumerički niz karaktera uz pomoć koga korisnik može da počne da prima plaćanja. Obično se bitkoini mogu steći putem kupovine na bitkoin berzi ili na automatu za prodaju, ili putem uplate za prodatu robu/usluge. Međutim, bitkoin je revolucionaran zbog toga što problem dvostruke potrošnje rešava bez potrebe za nekom trećom stranom u transakciji [vidi: (Nian & Chuen, 2015, str. 17-19)].

Ono što bitkoin čini inovativnim jeste jedinstvena mreža kao platna platforma; niski troškovi plaćanja; i činjenica da su transakcioni troškovi praktično nepostojeći i da međunarodne transakcije mogu da se obave mnogo brže u odnosu na tradicionalnu rutu, koja ide preko banaka. Nedostaci bitkoina su stepen složenosti; oscilacije u vrednosti; nedostatak centralnog supervizora platne platforme i, zbog toga, nedostatak bezbednosti (Cruysheer, 2015, str. 525).

Jedan od najvećih izazova za anonimne sisteme digitalnog novca bio je tzv. problem „dvostruke potrošnje“, tj. prevencija mogućnosti da se jedan isti digitalni novac koristiti za dva ili više različitih plaćanja pre nego što se izvrši kliring transakcije. Bitkoin i druge kriptovalute, slično ranijim sličnim sistemima digitalnog novca, rešavaju problem dvostruke potrošnje vođenjem evidencije o transakcijama. Osnovna razlika je, međutim, u tome što se bitkoin ne oslanja na neku pojedinačnu treću stranu od poverenja koja bi vodila ovu evidenciju, već umesto toga decentralizuje ovu odgovornost na čitavu mrežu. Bitkoin mreža neprestano prati saldo bitkoina putem javne evidencije („glavne knjige“) koja se naziva blokčejn (blockchain). „Blokčejn je javno dostupna autoritativna evidencija svih transakcija koje su ikada obrađene, koja omogućava bilo kome ko koristi bitkoinov softver da proveri ispravnost transakcije. Transfer bitkoina, ili transakcije, objavljuju se čitavoj mreži i uključuju se u blokčejn nakon uspešne verifikacije, tako da bitkoini koji su jednom potrošeni ne mogu biti ponovo potrošeni. Nove transakcije proveravaju blokčejn kako bi se utvrdilo da bitkoini nisu već potrošeni, čime se rešava problem dvostruke potrošnje (Nian & Chuen, 2015, str. 16).

Maksimalan broj bitkoina koji se može proizvesti procesom „rudarenja“ ograničen je na 21 milion bitkoina, a očekuje se da će ovaj limit biti dostignut otprilike 2040. godine. Nakon što se ovaj limit dostigne, „rudari“ koji ustupaju svoju računarsku

[5] „Slepi potpis“ (blind signature) je vrsta digitalnog potpisa kod koga se sadržaj neke poruke maskira pre nego što se ona potpiše. Slepe potpise izumeo je Dejvid Čaum i obično se koriste u protokolima koji se tiču privatnosti.

[6] *Satoshi Nakamoto* je pseudonim koji je koristila nepoznata osoba (ili više njih), koja je dizajnirala *Bitcoin* i kreirala njegovu originalnu implementaciju.

snagu u svrhu verifikacije transakcija biće nagrađeni provizijama za obradu transakcija, umesto bitkoinima. To će osigurati da „rudari“ još uvek imaju motiv da održavaju mrežu i vrše obradu transakcija [vidi: (Nian & Chuen, 2015, str. 20)].

Za razliku od tradicionalnih trgovaca, postoji mnoštvo on–lajn trgovaca koji primaju bitkoin i druge kriptovalute. Njihove cene su obično bazirane na „deviznom kursu“ između kriptovalute i neke realne valute. Korisnik koji želi da potroši bitkoine nabavlja ih tako što zamenjuje realnu valutu za bitkoine, što se može postići kupovinom bitkoina na aparatima za prodaju, na nekoj berzi ili, jednostavno, od neke druge osobe. „Bitkoin aparati za prodaju, koji se često nazivaju ’bankomatima’, predstavljaju najpogodniji način za kupovinu bitkoina, zbog toga što se jednostavno ubaci gotovina u aparat kako bi se odmah kupili bitkoini (Ulm, 2014).

3 PREDUSLOVI ZA USPEH PLATNOG SISTEMA BAZIRANOG NA DIGITALNOM NOVCU (KRIPTOVALUTAMA)

Monetarni režim koji je trenutno najzastupljeniji u svetu baziran je na savremenom kreditnom novcu. Savremeni novac može se podeliti na „opipljivu“ valutu (gotovina) i apstraktnu valutu. Apstraktnu valutu čine depoziti po viđenju na tekućim računima, tj. sva sredstva koja se sa tekućeg računa mogu povući direktno, putem kreditnih kartica, čekova, mobilnog ili internet bankarstva. I gotov novac i depoziti po viđenju predstavljaju *zakonsko sredstvo plaćanja*, ponajviše zbog državnog i bankarskog monopola nad procesom kreiranja novca. „*Oni imaju tzv. fiducijarni karakter* (tj. zasnovani su na poverenju); *drugim rečima, reč je o novčanim simbolima* (novcu koji nema podlogu u plemenitim metalima ili drugim odgovarajućim rezervama) *čija je vrednost izvedena iz poverenja koje su u njega investirali njegovi korisnici — slično kao i kod bitkoina*“ (Cruysheer, 2015, str. 520-521).

Ako sledimo iskustvo ranijih sistema baziranih na digitalnom novcu, bilo koja kriptovaluta koja se nadmeće sa državno sponzorisanim novcem, koji je podržan od strane države i banaka, svakako će se suočiti sa jakim otporom banaka. Takva kriptovaluta trebalo bi da ima slične mogućnosti i karakteristike. Valuta koja se koristi u plaćanjima na bitkoin mreži nije novčani simbol, već digitalna valuta (s obzirom na to da postoji samo u digitalnom obliku) koja „ ... za većinu namera i svrha zadovoljava ekonomsku definiciju novca: ona je prometno sredstvo, merilo vrednosti i sredstvo za tezaurisanje ... “ (Chen, 2011); dakle obavlja neke od osnovnih funkcija novca.

Brojni autori koji su proučavali sisteme bazirane na digitalnom novcu ističu da postoji više preduslova koje jedan sistem baziran na digitalnom novcu (kriptovalutama) mora da ispuni kako bi pretendovao na to da bude uspešan:

- **Sigurnost.** Sigurnost je jedna od ključnih karakteristika za uspeh pojedine forme digitalnog novca (kriptovalute), pa se preporučuje održavanje visokog stepena sigurnosti putem sofisticiranih tehnika šifrovanja. U transakcijama digitalnim novcem (kriptovalutama) mora se obezbediti visok stepen bezbednosti, kako bi se izbeglo njihovo falsifikovanje ili drugi vid zloupotrebe. Nijedna strana u transakciji, niti bilo ko drugi, ne bi trebalo da budu u stanju da izmene ili reprodukuju elektronske simbole koji se prenose od kupca ka prodavcu [vidi: (Okamoto & Ohta, 1992)]. Arhitektura privatnosti može se unaprediti ugradnjom dokaza o identitetu sa enkripcijom, što bi pomoglo u borbi protiv pranja novca i ostalih kriminalnih aktivnosti (Nian & Chuen, 2015, str. 14-15);
- **Anonimnost.** Anonimnost obezbeđuje privatnost neke transakcije na više nivoa. S obzirom na tehnološku prirodu digitalnog novca (kriptovaluta), veoma je jednostavno voditi detaljnu evidenciju o svim izvršenim transakcijama i identitetu transaktora. Korisnici će, međutim, zarad očuvanja svoje privatnosti, verovatno zahtevati da se ne vodi nikakva evidencija o transakcijama. Državni organi će, na drugoj strani, zahtevati evidentiranje svih transakcija kako bi sprečili utaju poreza, pranje novca i sl. Sigurno je da će anonimnost digitalnog novca biti predmet žestokih polemika u budućnosti. Kompromisno rešenje bilo bi da se obezbedi delimična anonimnost, tj. da se potrošačima omogući da sami donesu odluku o tome da li žele da ostanu

anonimni u odnosu na neku platnu transakciju. Prilikom elektronskog plaćanja računa, na primer, u interesu je samog potrošača da se takva transakcija evidentira, zbog toga što se ovakva evidencija, u slučaju spora, može iskoristi kao dokaz o izvršenom plaćanju. Ipak, veća je verovatnoća da će potrošači koristiti digitalni novac (kriptovalute) ako su ubeđeni da je u pitanju forma novca koju je nemoguće pratiti [vidi: (Okamoto & Ohta, 1992)]. Ako se neko plaćanje vrši papirnim novcem, klijent može ostati anoniman, ali kod digitalnog novca to nije tako jednostavno. Bitkoin se nalazi negde između ova dva ekstrema (tzv. „pseudo-anonimnost"). Za bitkoin se može reći da je poput gotovine u smislu da neka osoba može dati bitkoine drugoj osobi — budući da ne postoji treća strana kao posrednik, niko ne zna njihov identitet. Ipak, transakcije su zabeležene u blokčejnu, tako da plaćanje nije potpuno anonimno (mada postoji način da se sakrije on–lajn identitet i IP adresa, ali za to većina prosečnih korisnika nije osposobljena). Sem tehničkih aspekata bitkoina i drugih kriptovaluta, treba imati u vidu pritiske sa kojima se suočavaju bitkoin posrednici od strane regulatora. „Regulacija bitkoina (i ostalih kriptovaluta) evoluira, pa ako posrednici u poslovanju kriptovalutama počnu da podležu regulaciji, očekuje se da anonimnost neće baš biti čvrsto garantovana" (Brito & Castillo, 2013);

- **Prevazilaženje problema negativne mrežne eksternalije**. Mnogi istraživači koji su se bavili izučavanjem morfologije mreža upoznati su sa fenomenom mrežne eksternalije. Ekonomides, između ostalih, tvrdi da je „ ... suštinski odnos između komponenti neke mreže njihova komplementarnost ..." i da se neki od fundamentalnih ekonomskih principa ne ispoljavaju na isti način unutar i izvan neke mreže (Economides, 1993). U početku se gotovo svi platni sistemi bazirani na digitalnom novcu (kriptovalutama) suočavaju sa negativnom mrežnom eksternalijom. Vrlo je teško privući kritičan broj korisnika. Trgovci nisu zainteresovani da učestvuju u nekom sistemu koji ima mali broj potencijalnih kupaca dok, sa druge strane, potrošači nisu zainteresovani za sisteme sa ograničenim brojem trgovaca. Jedan od prvih sistema koji je uspeo da prevaziđe negativnu mrežnu eksternaliju upotrebom inovativnih marketinških tehnika (tzv. „virusni" marketing) bio je *PayPal* [za više detalja vidi: (Radovanović & Ćosić, 2010, str. 185-189; 271-272)]. Mrežna eksternalija postoji kada je vrednost neke robe ili usluge pod uticajem broja njenih kupaca ili korisnika. I sam novac je vrsta mrežnog dobra: što je veća mreža onih koji koriste izvesnu formu novca, veći je i podsticaj ostalim korisnicima da se pridruže takvoj mreži. Prema tome, veća je tražnja i, shodno tome, vrednost tog konkretnog novca u poređenju sa ostalim formama novca [vidi: (Radovanović P. , 2004)]. Kriptovalute takođe pokazuju pozitivnu mrežnu eksternaliju, pa je proučavanje ekonomije mreža ključni faktor u razumevanju interakcija između različitih strana u mreži kriptovalute. „Jedan veliki i dobro povezani skup korisnika je od suštinskog značaja za opstanak bitkoina ili bilo koje druge peer–to–peer kriptovalute. Ove interakcije utiču na evoluciju mreže, motivisanje „rudara" i ponudu i tražnju za novcem (Teo, 2015, str. 191);
- **Softver otvorenog koda**. Sistem digitalnog novca/kriptovaluta mora da bude baziran na softveru otvorenog koda, što znači da programski kôd softvera mora biti javno dostupan kako bi nezavisni programeri i grupe koji se bave razvojem softvera, a u koje javnost ima poverenje, mogli da provere pouzdanost i bezbednost softvera i otkriju eventualne bezbednosne i druge nedostatke i propuste (Nian & Chuen, 2015, str. 12-13);
- **Decentralizacija**. Sistem digitalnog novca/kriptovaluta mora da bude što je moguće više decentralizovan. Od suštinskog je značaja da neka digitalna kriptovaluta nije pod kontrolom pojedinca, grupe ljudi ili nekog pojedinačnog entiteta (Nian & Chuen, 2015, str. 12-13);
- **Dvosmernost (direktne P2P transakcije)**. Dvosmernost se odnosi na mogućnost direktnog prenosa digitalnog novca (kriptovalute) između dveju osoba,

bez potrebe da bilo koja strana u transakciji ima status registrovanog trgovca. Primera radi, ako se nekoliko osoba dogovori da zajednički kupe rođendanski poklon, pri čemu jedna od njih plaća punu cenu, sistem digitalnog novca trebalo bi da omogući da svaka od preostalih osoba prenese odgovarajući iznos osobi koja je platila poklon (Okamoto & Ohta, 1992). Dakle, sistem digitalnog novca treba da podržava direktne peer–to–peer (P2P) transakcije bez ikakvih posrednika (Nian & Chuen, 2015, str. 12-13);

- **Prenosivost**. Prenosivost je karakteristika koja se odnosi na bezbednu upotrebu digitalnog novca (kriptovalute) nezavisno od fizičke lokacije. Digitalni novac (kriptovaluta) ne treba da bude omeđen privatnom računarskom mrežom, koja ograničava njegovu cirkulaciju. On, takođe, ne treba da bude zavisan od fizičke lokacije, što znači da je potrebno omogućiti njegov slobodan transfer putem javnih računarskih mreža i/ili putem nekog uređaja za uskladištenje. Pored toga, potrebno je omogućiti transfer digitalnog novca (kriptovalute) putem alternativnih sistema prenosa koji ne zavise od računara, npr. putem mobilnih telefona (Okamoto & Ohta, 1992);
- **Deljivost**. Deljivost podrazumeva da jedna „digitalna novčanica“, koja glasi na određeni iznos, treba da bude deljiva na manje „novčanice“, koje glase na manje iznose. Vlasnicima digitalnog novca (kriptovaluta) treba dati mogućnost raščlanjivanja tog novca na najmanje moguće jedinice. Mnogi dizajneri sistema digitalnog novca planirali su da omoguće jedinice digitalnog novca sa vrednošću od jednog centa, pa čak i manje, jer su bili svesni da bi ovakva karakteristika dala digitalnom novcu konkurentsku prednost nad kreditnim karticama koje, generalno, ne mogu efikasno da se koriste za vrlo sitna plaćanja. Veoma veliki broj svakodnevnih kupovina (dnevna štampa, karte u javnom saobraćaju, ulaznice za bioskop i sl.) mogao bi da se obavlja on–lajn kada bi digitalni novac (kriptovaluta) mogao da se koristi za ovakva mikroplaćanja (Okamoto & Ohta, 1992);
- **„Of–lajn“ režim.** „Of–lajn“ režim odnosi se na postojanje mogućnosti da se transakcija između dveju strana može izvršiti „of–lajn“, što znači da nijedna od dveju strana ne mora da bude priključena na mrežu. U ovom slučaju digitalni novac (kriptovaluta) bi se mogao trošiti bilo gde i bilo kad, bez potrebe da bilo koja strana u transakciji bude povezana na računar radi autentikacije i/ili obrade transakcije (Okamoto & Ohta, 1992);
- **Neograničeno trajanje.** Neograničeno trajanje znači da digitalni novac (kriptovaluta) ne bi trebalo da ima ograničeni „rok trajanja“. Izuzev u slučaju bankrotstva emitenta, ovakav novac trebalo bi da održava svoju vrednost tokom vremena, tako da može da se čuva („tezauriše“) na nekom bezbednom mestu za kasniju upotrebu (Matonis J. W., 1995, str. 1-4);
- **Opšta prihvaćenost.** Opšta prihvaćenost je bitna karakteristika novca. Novac funkcioniše kao takav samo ako je opšteprihvaćen. Na bazi ovakve društvene prihvatljivosti, novac se može preneti drugim licima koja unapred znaju da će biti u mogućnosti da ga i sami potroše u toj formi. Što je veća prihvaćenost novca od strane drugih, veća je njegova korisnost. Ova pretpostavka svakako važi i za digitalni novac (kriptovalute). U slučaju da postoji veći broj emitenata digitalnog novca, njihove varijante digitalnog novca trebalo bi da budu prihvaćene i izvan njihovih sistema (Matonis J. W., 1995, str. 1-4);
- **Jednostavnost upotrebe.** Jednostavnost upotrebe je jedna od ključnih karakteristika kojoj su nedovoljno pažnje posvetili tvorci brojnih neuspešnih sistema digitalnog novca. Digitalni novac mora da bude jednostavan za upotrebu, kako iz aspekta trošenja tako i iz aspekta prijema. Jednostavnost upotrebe je najznačajnija za šire prihvatanje i upotrebu digitalnog novca, pogotovo od strane novih korisnika savremenih informaciono–komunikacionih tehnologija, a masovna upotreba vodi ka njegovoj širokoj i, eventualno, opštoj prihvaćenosti. Funkcionisanje protokola treba da bude transparentno za korisnike, tako da oni ne moraju poznavati tehnike

kriptografije i sl. (Matonis J. W., 1995, str. 1-4);

- **Globalni domet.** Digitalni novac (kriptovaluta) je nesputan državnim granicama i po samoj svojoj prirodi je globalan. Zbog toga bi i svaki sistem baziran na digitalnom novcu trebalo da bude dizajniran tako da ima globalni domet (Nian & Chuen, 2015, str. 12-13);
- **Brzina.** U savremenom svetu, a pogotovo u on–lajn okruženju, veoma je važno da se transakcije odvijaju što je moguće brže, kao i da vreme potvrde transakcije bude što je moguće kraće (Nian & Chuen, 2015, str. 12-13);
- **Pouzdanost.** Sistem baziran na digitalnom novcu (kriptovalutama) mora biti pouzdan, što znači da transakcije digitalnim novcem (kriptovalutama) moraju biti neporecive, a obračun transakcija mora se vršiti u realnom vremenu, bez tzv. obračunskog rizika[7] (Nian & Chuen, 2015, str. 12-13);
- **Sofisticiranost i fleksibilnost.** Sistem baziran na digitalnom novcu (kriptovalutama) trebalo bi da bude dovoljno sofisticiran i fleksibilan da podrži sve vrste aktive, finansijskih instrumenata i finansijskih tržišta (Nian & Chuen, 2015, str. 12-13);
- **Automatizacija.** Sistem baziran na digitalnom novcu (kriptovalutama) mora da omogući da se plaćanja digitalnim novcem (kriptovalutama) automatizuju i jednostavno inkorporiraju u različite platforme (Nian & Chuen, 2015, str. 12-13);
- **Skalabilnost.** S obzirom na to da je digitalni novac (kriptovalutama) globalan po svojoj prirodi, sistem baziran na digitalnom novcu treba da bude dizajniran tako da omogući veliki broj korisnika i/ili da može po potrebi brzo i jednostavno da se nadogradi i proširi (Nian & Chuen, 2015, str. 12-13);
- **Platforma za integraciju**. Sistem baziran na digitalnom novcu (kriptovalutama) trebalo bi da pruži platformu koja će omogućiti integraciju digitalnih finansija i digitalnog prava kako bi se obezbedila podrška za tvz. „pametne“ ugovore, pri čemu bi se finansijske transakcije izvršavale na bazi ugovora, koji mogu brzo i jednostavno da se prilagode različitim ugovornim stranama (Nian & Chuen, 2015, str. 12-13).

Popisu preduslova koje jedan sistem digitalnog novca mora da ispuni kako bi pretendovao na to da bude uspešan dodaćemo još jedan preduslov koji je pomalo zanemaren u teoriji i praksi, a to je **održavanje dugoročno stabilne vrednosti digitalnog novca (kriptovalute)**. Ne postoji ništa poraznije po neki sistem digitalnog novca od situacije kada njegova valuta počne naglo da gubi svoju vrednost u odnosu na druge valute. Tada obično nastaje panika, jer vlasnici konkretne digitalne (kripto)valute nastoje da je se što pre otarase i da je konvertuju u neku drugu „čvršću“ valutu, čime se proces gubitka vrednosti samo dodatno ubrzava, što u krajnjoj liniji može da dovede i do bankrotstva emitenta.

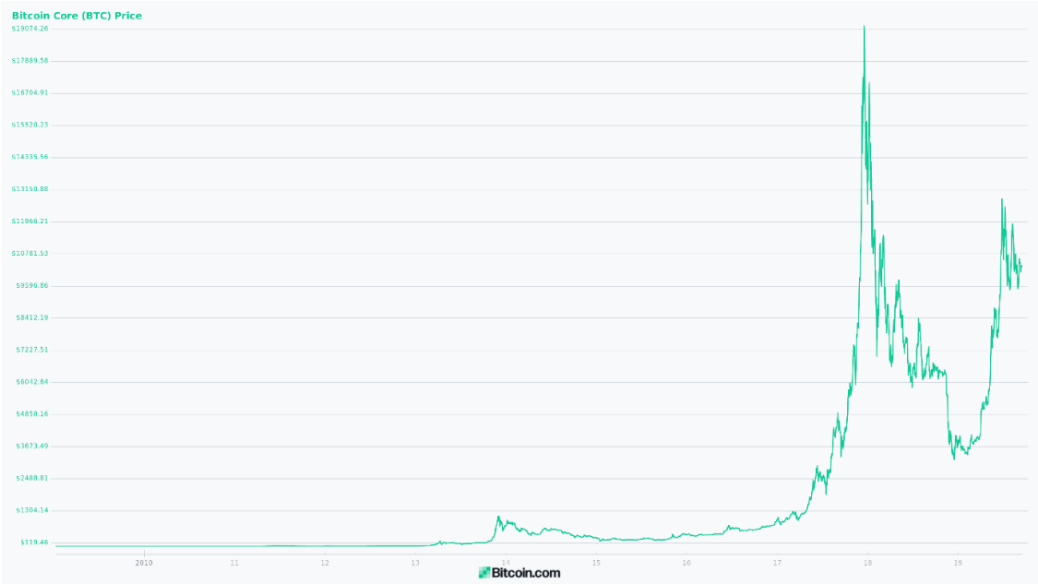
Sistem baziran na digitalnom novcu (kriptovalutama) trebalo bi da raspolaže mehanizmima za dugoročno održanje stabilne vrednosti. Na sličan način na koji centralna banka operacijama na otvorenom tržištu vrši dinamiziranje novčane mase, ili intervencijama na

[7] Jedan od potencijalno najvećih rizika u platnim i obračunskim sistemima je kreditni rizik. Kreditni rizik u platnim i obračunskim sistemima je rizik da suprotna strana u transakciji neće u potpunosti izmiriti svoju obavezu. Kreditni rizik u platnim sistemima može imati više oblika i izvora, a dva najznačajnija izvora kreditnog rizika u platnim i obračunskim sistemima na veliko su prekoračenja u koja klijenti sistema upadaju tokom dana i — *obračunski rizik*. U platnim sistemima na malo svaki instrument plaćanja ima specifičan proces obračuna, koji zavisi od entiteta koji učestvuju u obračunu (pored onoga ko inicira, i onoga ko prima plaćanje, u proces obrade i obračuna transakcija može biti uključen veći broj finansijskih institucija i spoljnih vršilaca usluga). I kod platnih sistema na malo jedan od osnovnih uzroka kreditnog rizika je obračunski rizik. Kod pojedinih instrumenata, na primer, obračun se ne vrši u realnom vremenu, zbog čega se učesnici izlažu kreditnom riziku. Postoji i mogućnost odbijanja pojedinih instrumenata (npr. vraćanje čekova zbog nedovoljnog pokrića, falsifikovanja i sl.), a vreme koje je potrebno za povraćaj, povećava izloženost kreditnom riziku. Vlasnici platnih kartica mogu osporiti platnu transakciju u slučaju da im nije isporučena roba/usluga odgovarajućeg kvaliteta, pri čemu će im biti izvršen povraćaj novca direktnim zaduživanjem računa odgovarajućeg trgovca. Finansijske institucije se obično oslanjaju na kreditnu sposobnost trgovaca, ali ako trgovac ne bude u mogućnosti da izvrši povraćaj novca, onda će njegova poslovna banka morati da izvrši povraćaj sredstava izdavaocu platne kartice.

deviznom tržištu drži devizni kurs u zacrtanim okvirima, i sistem baziran na digitalnom novcu trebalo bi da raspolaže adekvatnim mehanizmima koji su primereni zasebnoj monetarnoj sferi u kojoj on funkcioniše.

Ako je digitalna (kripto)valuta konvertibilna u neku drugu digitalnu (kripto)valutu, dolazi do preplitanja njihovih monetarnih sfera i svaka nestabilnost koja se pojavi u jednoj monetarnoj sferi može vrlo lako da se prenese na drugu monetarnu sferu. Konačno, ako je digitalna (kripto)valuta konvertibilna u zvaničnu državnu valutu, onda svaka nestabilnost u monetarnoj sferi digitalne (kripto)valute može da se prenese i na realnu monetarnu sferu.

Što su veće oscilacije u vrednosti neke digitalne (kripto)valute veći je i prostor za arbitražne poslove i berzanske špekulacije, koje mogu dodatno uzdrmati poverenje investitora i izazvati paniku. Od pojave kriptovaluta, njihova vrednost je prilično oscilirala, a delom se te oscilacije mogu pripisati i periodima panike, izazvane berzanskim špekulacijama. Na narednim slikama prikazano je kretanje vrednosti nekoliko najpoznatijih kriptovaluta u poslednjih 5–10 godina.



Slika 1. Kretanje cene Bitcoin-a od 2010. godine do danas
Izvor: (Bitcoin Core Charts, 2019)

Slika 2. Kretanje cene BitcoinCash-a od 2010. godine do danas
Izvor: (Bitcoin Core Charts, 2019)

Slika 3. Kretanje cene Ethereum-a od 2015. godine do danas
Izvor: (Coin Market Cap, 2019)

Kao što se može videti na prethodnim slikama, vrednost nekih od najznačajnijih kriptovaluta bila je veoma nestabilna u poslednjih nekoliko godina, naročito od 2017. godine kada je na berzama najpre dolazilo do strmoglavog rasta vrednosti, koji je potom praćen strmoglavim padom. Ako detaljnije proučimo grafikone većine najpoznatijih kriptovaluta videćemo da je u vreme kada je jednoj kriptovaluti vrednost strmoglavo padala, drugoj kriptovaluti vrednost strmoglavo rasla, što ukazuje na činjenicu da je delom za ovakve oscilacije vrednosti zaslužna panika među investitorima, koji su nastojali da se brzo otarase kriptovalute čija je vrednost naglo padala, kupujući kriptovalutu čija je vrednost rasla. Ovakve situacije se često dešavaju na berzama, kada gomila neiskusnih investitora po preporukama raznih „finansijskih savetnika“ i „analitičara“ kupuje berzansku robu kojoj se prognozira rast vrednosti (što se na kraju i dogodi), čime dolazi do kreiranja „balona“ od čijeg „pucanja“, na kraju, najveću korist izvuku oni koji su ga prvobitno i pokrenuli.

Da bi se izbegle ovakve situacije, novi sistemi bazirani na digitalnim (kripto)valutama trebalo bi (barem dok sistem ne uđe u fazu zrelosti a vrednost kriptovalute postane dugoročno stabilna) da preduzmu mere kojima će sprečiti nagle oscilacije vrednosti. Te mere mogu biti različite, npr. ukidanje ili ograničavanje konvertibilnosti u druge digitalne valute ili zvaničnu državnu valutu kako bi se sprečila interakcija sa drugim monetarnim sferama i prelivanje nestabilnosti; uzdržavanje od izlaska na berzu; ograničavanje trgovine na berzama i sl. Naravno, sve ove mere trebalo bi da budu privremenog karaktera i da se primenjuju dok se sistem ne stabilizuje i postane imun na uzroke nestabilnost. Kasnije je za dugoročno održavanje stabilne vrednosti potrebno pokrenuti mehanizme nalik onima koje koriste centralne banke u realnoj monetarnoj sferi.

4 ZAKLJUČAK

Nove tehnologije igraju sve značajniju ulogu u finansijama usled pojave platnih sistema baziranih na digitalnom novcu i kriptovalutama. Prednost kriptovaluta ogleda se u tome što su njihovi sistemi u mogućnosti da obrađuju transakcije preko distribuirane mreže, bez potrebe za klirinškom institucijom. Ovakva decentralizovana obrada transakcija daleko je jeftinija je od tradicionalnog centralizovanog obračuna na koji se oslanjaju banke, pa zbog toga postoji velika verovatnoća da će digitalne (kripto)valute biti široko prihvaćene u oblasti mikroplaćanja.

I sama blokčejn tehnologija nalazi nove primene. U NASDAQ–u su, recimo, nedavno objavili da će lansirati tehnologiju digitalne „glavne knjige“ nalik na blokčejn, koju će koristiti za upravljanje

akcijama na njihovoj *NASDAQ Private Market* platformi (Orcutt, 2015). Konsultantska kuća *Deloitte* osnovala je *Deloitte Cryptocurrency Community* da bi savetovala svoje klijente o koristima i mogućnostima primene blokčejn tehnologije (Rizzo, 2015). Čak i američki Sistem federalnih rezervi razmatra upotrebu blokčejn tehnologije („mehanizam za transfer digitalne vrednosti“) za obradu međubankarskih plaćanja (U.S. Federal Reserve System, 2015).

Kriptovalute će evoluirati tokom vremena, dok će njihov udeo u elektronskim transakcijama nastaviti da raste. Ako jedna kriptovaluta izgubi popularnost — iz bilo kog razloga — pojaviće se nova, koja će je zameniti i imati bolje karakteristike.

Kriptovalute će najverovatnije u početku funkcionisati u okviru pojedinih tržišnih niša. Vrlo je verovatno, takođe, da će se kriptovalute koje garantuju potpunu anonimnost koristiti i za nelegalne transakcije (Christin, 2012). Veću popularnost kriptovalute mogu steći u državama sa naročito slabim i nestabilnim valutama (Luther, 2016, str. 402).

Brojni analitičari isticali su preduslove koje jedan platni sistem baziran na digitalnom novcu (kriptovaluti) mora da ispuni kako bi bio uspešan (sigurnost, anonimnost, prevazilaženje negativne mrežne eksternalije, softver otvorenog koda, decentralizacija, dvosmernost tj. direktne P2P transakcije, prenosivost, deljivost, „of–lajn“ režim, neograničeno trajanje, opšta prihvaćenost, jednostavnost upotrebe, globalni domet, brzina, pouzdanost, sofisticiranost i fleksibilnost, automatizacija, skalabilnost, platforma za integraciju ...). Dobar deo pomenutih preduslova baziran je, zapravo, na karakteristikama realnog novca. Ovo zbog toga što najveći broj potencijalnih korisnika sistema baziranih na digitalnom novcu (kriptovalutama) ima višegodišnje iskustvo u upotrebi realnog novca, pa je veća šansa da će se opredeliti za onaj sistem digitalnog novca (kriptovaluta) koji najpribližnije oslikava osobine realnog novca i vrši osnovne funkcije novca. Ali, da bi bilo koji novac pravilno vršio svoje osnovne funkcije, svakako je vrlo bitno da je njegova vrednost dugoročno stabilna, zbog čega će i ovo, svakako, biti značajan preduslov za uspeh nekog sistema baziranog na digitalnom novcu. Konačno, ako je cilj da neki platni sistem baziran na digitalnom novcu što vernije oslika karakteristike realnog novca, on će morati da koristi i slične modalitete kreiranja (izdavanja), cirkulacije (opticaja) i valuacije (tj. održavanja dugoročno stabilne vrednosti).

CITIRANA DELA

Bitcoin Core Charts. (2019, 09 20). *Bitcoin Core Charts*. Retrieved from charts.bitcoin.com: https://charts.bitcoin.com/btc/press

Brito, J., & Castillo, A. (2013). *Bitcoin: A Primer for Policymakers.* Arlington: Mercatus Center, George Mason University.

Chaum, D. (1983). Blind signatures for untraceable payments. *Advances in Cryptology, Proceedings of Crypto, vol 82.* (pp. 199-203). Springer.

Chaum, D., Fiat, A., & Naor, M. (1990). Untraceable electronic cash. *Advances in Cryptology, Proceedings of Crypto 88* (pp. 319-327). Springer.

Chen, A. (2011, 01/ 06). *The underground website where you can buy any drug imaginable.* Retrieved 07/ 10, 2017, from Gawker.com: http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160

Christin, N. (2012). *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace.* Pittsburgh: CyLab Security and Privacy Institute, Carnegie Mellon University.

Coin Market Cap. (2019, 09 20). *Ethereum Charts*. Retrieved from coinmarketcap.com: https://coinmarketcap.com/currencies/ethereum/#charts

Cruysheer, A. (2015). Bitcoin: A Look at the Past and the Future. In D. Chuen, *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (pp. 519-526). London: Elsevier.

Economides, N. (1993). Network economics with application to finance. *Financial Markets, Institutions and Instruments 2(5)*, 89-97.

Guttmann, R. (2003). *Cybercash: The Coming Era of Electronic Money.* New York: Palgrave Macmillan.

Luther, W. (2016). Bitcoin and the Future of Digital Payments. *The Independent Review, Vol. 20, No. 3*, 397-404.

Matonis, J. (2013, 9/ 17). *Bitcoin gaining market-based legitimacy as XBT.* Retrieved 7/ 10, 2017, from CoinDesk.com: http://www.coindesk.com/bitcoin-gaining-market-based-legitimacy-xbt/

Matonis, J. W. (1995). Digital Cash and Monetary Freedom. *Proceedings of INET 95.* Hawaii: ISOC.

Mori, R., & Kawahara, M. (1990). Superdistribution: The Concept and the Architecture. *The Transactions of the IEICE, vol. E73, No. 7*.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved 6 /10, 2017, from Bitcoin.org: https://bitcoin.org/bitcoin.pdf

Nian, L. P., & Chuen, D. L. (2015). Introduction to Bitcoin. In D. Chuen, *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments and Big Data* (pp. 5-30). London: Elsevier Inc.

Okamoto, T., & Ohta, K. (1992). Universal Electronic Cash. In J. Feigenbaum, *Advances in Cryptology - Proceedings of 11th Annual International Cryptology Conferece on Advances in Cryptology - CRYPTO '91* (pp. 324-337). Berlin: Springer-Verlag.

Orcutt, M. (2015, 7/ 9). *Why NASDAQ is Betting on Bitcoin's Blockchain.* Retrieved 7/ 10, 2017, from MIT TechnologyReview.com: https://technologyreview.com/s/539171/why-nasdaq-is-betting-on-bitcoins-blockchain/

Radovanović, P. (2004). Perspektiva platnih sistema baziranih na digitalnom novcu. *Zbornik radova 4. međunarodnog simpozijuma o elektronskoj trgovini i elektronskom poslovanju "E-Trgovina 2004".* Palić: E-Trgovina.

Radovanović, P. (2009). Digital Economy, Digital Money and Digital Banking. *FACTA UNIVERSITATIS, Series: Economics and Organization, Vol. 6, No. 2*, 153-160.

Radovanović, P. (2009). *Elektronsko bankarstvo kao okosnica digitalne ekonomije.* Leskovac: Visoka poslovna škola.

Radovanović, P., & Ćosić, D. (2010). *Elektronsko poslovanje i elektronsko bankarstvo.* Beograd: Beogradska poslovna škola.

Rizzo, P. (2015, 07/ 14). *Deloitte Trials Blockchain Tech for Client Auditing.* Retrieved 7/ 10, 2017, from CoinDesk.com: http://www.coindesk.com/deloitte-blockchain-auditing-consulting/

Shaw, R. (2001). The Bank is Dead, Long Live the Bank. In E. Gardener, , & P. Versluijs, *Bank Strategies and Challenges in the New Europe* (pp. 1-18). New York: Palgrave.

Teo, E. G. (2015). Emergence, Growth, and Sustainability of Bitcoin: The Network Eco. In D. Chuen, *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (pp. 191-200). London: Elsevier.

U.S. Federal Reserve System. (2015). *Strategies for Improving the U.S. Payment System.* Washington, D.C.: U. S. Federal Reserve System.

Ulm, B. (2014). *Bitcoin ATMs boom: new locations.* Retrieved 6 8/10, 2017, from CoinTelegraph.com: http://cointelegraph.com/news/112163/bitcoin-atms-boom-new-locations

Datum prve prijave: 23.09.2019.
Datum prijema korigovanog članka: 07.10.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Ćosić, D., & Radovanović, P. (2019, 10 15). Preduslovi za uspeh platnog sistema baziranog na digitalnoj (kripto)valuti. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 26-38. doi:10.12709/fbim.07.07.02.04

*Style – **Chicago** Sixteenth Edition:*

Ćosić, Dragan, and Predrag Radovanović. 2019. "Preduslovi za uspeh platnog sistema baziranog na digitalnoj (kripto)valuti." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 26-38. doi:10.12709/fbim.07.07.02.04.

*Style – **GOST** Name Sort:*

Ćosić Dragan and Radovanović Predrag Preduslovi za uspeh platnog sistema baziranog na digitalnoj (kripto)valuti [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 26-38.

*Style – **Harvard** Anglia:*

Ćosić, D. & Radovanović, P., 2019. Preduslovi za uspeh platnog sistema baziranog na digitalnoj (kripto)valuti. *FBIM Transactions,* 15 10, 7(2), pp. 26-38.

Style – **ISO 690** Numerical Reference:

Preduslovi za uspeh platnog sistema baziranog na digitalnoj (kripto)valuti. **Ćosić, Dragan and Radovanović, Predrag.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 26-38.

FBIM Transactions
DOI 10.12709/fbim.07.07.02.05

PROCJENA UČINKA NA ZAŠTITU LIČNIH PODATAKA

PRIVACY IMPACT ASSESSMENT

Haris Hamidović
MKF/MKD EKI Sarajevo, Sarajevo, Bosna i Hercegovina

JEL Kategorija rada: **K22, M15**

Apstrakt

Integracija zahtjeva privatnosti u dizajn informacionog sistema nije jednostavan zadatak. Kao prvo, privatnost je sama po sebi složen, višestruk i kontekstualni pojam. Osim toga, pitanje privatnosti uglavnom nije primarni zahtjev sistema, a ponekad čak ovaj zahtjev može doći i u sukob s drugim (funkcionalnim ili nefunkcionalnim) zahtjevima sistema. Stoga je od najveće važnosti da se precizno definišu ciljevi privatnosti u procesu realizovanja privatnosti po dizajnu. Jedan od načina da se definišu ciljevi informacionog sistema u smislu zahtjeva privatnosti je provođenje procjene učinka na zaštitu podataka ili analize rizika privatnosti. Provođenje procjene učinka na zaštitu podataka u skladu je i sa načelima tehničke i integrisane zaštite podataka iz člana 25. Opšte uredbe o zaštiti podataka EU - GDPR. U skladu s načelima tehničke i integrisane zaštite podataka procjenu učinka na zaštitu podataka trebalo bi provesti prije same obrade, a s ciljem korištenja iste kao pomoćnog alata za donošenje odluka o obradi, a posebice izbora odgovarajućih mjera tehničke i integrisane zaštite. Iako Opšta uredba o zaštiti podataka ne propisuje niti jednu konkretnu metodologiju ili standard za izvođenje procjene učinka na privatnost u smjernicama Radne skupine za zaštitu podataka iz članka 29 EU navedene su preporuke za korištenje međunarodnih standarda. U radu je ukratko predstavljena metoda procjene učinka na zaštitu podataka temeljem preporuka francuske agencije za zaštitu privatnosti podataka i preporuka međunarodnih standarda ISO/IEC 29134 i ISO/IEC 27005.

Ključne reči: *privatnost, lični podaci, zaštita podataka, procjena učinka na privatnost, GDPR, PIA, ISO/IEC 29134*

Abstract

Integrating the privacy requirement in the information system design is not an easy task. First of all, privacy is a complex, multiple, and contextual concept in itself. In addition, the issue of privacy is not a primary requirement of the system, and sometimes even this requirement can come into conflict with other (functional or non-functional) requirements of the information system. Therefore, it is of utmost importance to precisely define the objectives of privacy in the process of realizing privacy by design. One way to define the objectives of the information system in terms of the privacy requirement is to conduct a privacy impact assessment or a privacy risk analysis. Conducting a privacy impact assessment is in line with the principles of technical and integrated

Adresa autora:
Haris Hamidović
haris.hamidovic@eki.ba

data protection under Article 25 of the General Data Protection Regulation – GDPR. In accordance with the principles of technical and integrated data protection, a privacy impact assessment should be carried out before the processing itself with the aim of using it as a tool for decision-making, in particular for the selection of appropriate technical protection measures. Although the General Data Protection Regulation does not prescribe any specific methodology or standard for privacy impact assessment in the guidelines of the Article 29 Working Group on Data Protection, there are recommendations for the use of international standards. This paper presents the method of privacy impact assessment based on the recommendations of the French Data Protection Agency and the recommendations of international standards ISO/IEC 29134 and ISO/IEC 27005.

Keywords: *privacy, personal data, data protection, privacy impact assessment, GDPR, PIA, ISO/IEC 29134*

1. UVOD

Opšta uredba o zaštiti podataka EU - Uredba, koja je na snazi od 25. maja 2018. uvodi koncept procjene učinka na zaštitu podataka. Procjena učinka na zaštitu podataka je postupak osmišljen za opisivanje obrade, procjenu njezine nužnosti i proporcionalnosti te pružanje pomoći u upravljanju rizicima za prava i slobode pojedinaca koji nastaju obradom ličnih podataka, njihovom procjenom i određivanjem mjera za njihovo uklanjanje. Provođenje procjene učinka na zaštitu podataka važno je za odgovornost, jer pomaže voditeljima obrade da se usklade sa zahtjevima Opšte uredbe o zaštiti podataka i da dokažu da su poduzete potrebne mjere za osiguravanje usklađenosti s Uredbom. Drugim riječima, procjena učinka na zaštitu podataka postupak je za uspostavu i dokazivanje usklađenosti, naglašava se iz Radne skupine za zaštitu podataka iz članka 29. (Smjernica, 2017) (Uredba, 2016)

U skladu s Opštom uredbom o zaštiti podataka neusklađenost sa zahtjevima procjene učinka na zaštitu podataka može rezultirati novčanim kaznama koje izriče nadležno nadzorno tijelo. Propust u provođenju procjene učinka na zaštitu podataka u slučaju da obrada podliježe njezinu provođenju, neispravno provođenje procjene učinka na zaštitu podataka, ili nesavjetovanje s nadležnim nadzornim tijelom kad je to potrebno može rezultirati upravnim novčanim kaznama do najviše 10 miliona EUR ili, u slučaju preduzeća, do 2% ukupnog godišnjeg prometa na svjetskom nivou za prethodnu finansijsku godinu, ovisno o tome koji je iznos viši. (Smjernica, 2017) (Uredba, 2016)

Opšta uredba o zaštiti podataka ne propisuje niti jednu konkretnu metodologiju ili standard za izvođenje procjene učinka na privatnost. Međutim, u smjernicama Radne skupine za zaštitu podataka iz člana 29 EU (eng. Article 29 Working Party - Art. 29 WP)) prezentirane su neke preporuke, kao što je ISO/IEC 29134, Informaciona tehnologija – Sigurnosne tehnike - Smjernice za procjenu utjecaja na privatnost. U nastavku rada predstavljemo osnovne smijernice za provođenje procjena učinka na zaštitu podataka temeljem dobrih praksi predstavljenih od strane francuske agencije za zaštitu privatnosti podataka (CNIL) i međunarodnih standarda.

2. OBAVEZA PROVOĐENJA PROCJENE UČINKA NA ZAŠTITU PODATAKA

U skladu s pristupom temeljenim na riziku, utvrđenim u Opšoj uredbi o zaštiti podataka, provođenje procjene učinka na zaštitu podataka nije obavezno za svaki postupak obrade. Procjena učinka na zaštitu podataka potrebna je ako će obrada vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca: „Ako je vjerojatno da će neka vrsta obrade, posebno putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade prije obrade provodi procjenu učinka predviđenih postupaka obrade na zaštitu ličnih podataka“. (član 35. stav 1. Uredbe)

Jedna procjena učinka na zaštitu podataka može se upotrijebiti za procjenu višestrukih postupaka obrade koji su slični s obzirom na prirodu, opseg, kontekst, svrhu i rizike. To može biti slučaj ako se koristi slična tehnologija za prikupljanje iste vrste podataka u iste svrhe. Art. 29 WP navodi kao primjer, skupinu opštinskih tijela, od kojih svako postavlja sličan sistem kamera televizije zatvorenog kruga (CCTV), gdje se može provesti jedna procjena učinka na zaštitu podataka koja obuhvaća postupke pojedinačnih voditelja obrade

ili primjer željezničkog prijevoznika (jedan voditelj obrade) gdje se mogu jednom procjenom učinka na zaštitu podataka obuhvatiti sve nadzorne kamere na svim željezničkim stanicama. To može biti primjenjivo i u sličnim postupcima obrade koje provode razni voditelji obrade podataka. U tim je slučajevima referentnu procjenu učinka na zaštitu podataka potrebno zajednički upotrebljavati ili učiniti javno dostupnom, moraju se provesti mjere opisane u procjeni učinka na zaštitu podataka, a provođenje jedne procjene učinka na zaštitu podataka potrebno je obrazložiti, navode iz Art. 29 WP. (Smjernica, 2017)

Procjena učinka na zaštitu podataka može biti korisna i u procjeni učinka nekog tehnološkog proizvoda na zaštitu podataka, na primjer neke opreme ili nekog računarskog programa, koje će različiti voditelji obrade podataka vjerojatno upotrebljavati za provođenje različitih postupaka obrade. Art. 29 WP naglašava da u ovom slučaju voditelj obrade podataka koji upotrebljava proizvod i dalje mora provesti vlastitu procjenu učinka na zaštitu podataka s obzirom na specifičnu provedbu, ali te se informacije mogu nalaziti i u procjeni učinka na zaštitu podataka koju prema potrebi priprema dobavljač proizvoda. (Smjernica, 2017)

U smjernicama Radne skupine za zaštitu podataka iz članka 29 se navodi i pojašnjava sljedećih devet kriterija koje je potrebno uzeti u obzir prilikom procjene da li namjerava obrada zahtijeva provođenje procjene učinka na zaštitu podataka. Predmetne kriterije detaljno navodimo u nastavku (Smjernica, 2017):

"1. Procjena ili bodovanje, uključujući izradu profila i predviđanje, posebno na temelju aspekata ispitanikovog učinka na poslu, ekonomskog stanja, zdravlja, ličnih preferencija ili interesa, pouzdanosti ili ponašanja, lokacije ili kretanja. Primjeri mogu obuhvaćati finansijsku instituciju koja provjerava svoje klijente u referentnoj bazi podataka o kreditnoj sposobnosti, u bazama podataka o suzbijanju pranja novca i financiranja terorizma ili u bazi podataka o prijevarama; biotehnološko preduzeće koje izravno svojim kupcima nudi genetska testiranja radi procjene i predviđanja bolesti/zdravstvenih rizika ili preduzeće koje izrađuje bihevioralne i marketinške profile utemeljene na upotrebi ili pregledavanju njihove internetske stranice.

2. Automatizirano donošenje odluka s pravnim ili sličnim znatnim učinkom. Obrada čiji je cilj donošenje odluka o ispitanicima proizvodeći pravne učinke koji se odnose na pojedinca ili na sličan način značajno utječu na pojedinca. Na primjer, obrada može rezultirati isključivanjem ili diskriminacijom pojedinaca. Obrada čiji je učinak na pojedince neznatan ili nikakav ne odgovara ovom specifičnom kriteriju.

3. Sistemsko praćenje. Obrada koja se koristi za posmatranje, praćenje ili kontrolu ispitanika, uključujući podatke prikupljene putem mreža ili „sistemskog praćenja javno dostupnog područja". Ova je vrsta praćenja jedan od kriterija jer se lični podaci mogu prikupljati u situacijama u kojima ispitanici nisu svjesni tko prikuplja njihove podatke i u koje će svrhe ti podaci biti upotrijebljeni. Usto, pojedinci možda neće moći izbjeći takvu obradu na javnim (ili javno dostupnim) mjestima.

4. Osjetljivi podaci ili podaci vrlo lične prirode. Ovo uključuje posebne kategorije ličnih podataka, kako je utvrđeno u članu 9. Uredbe (na primjer informacije o političkim mišljenjima pojedinaca), kao i lične podatke koji se odnose na krivične osude ili kažnjiva djela, kako je utvrđeno u članu 10 Uredbe. Primjer je opšta bolnica koja čuva medicinsku dokumentaciju pacijenata ili privatni istražitelj koji čuva pojedinosti o prijestupnicima. Osim onoga što je obuhvaćeno odredbama Opšte uredbe o zaštiti podataka, za neke se kategorije podataka može smatrati da povećavaju mogući rizik za prava i slobode pojedinaca. Ti lični podaci smatraju se osjetljivima (kako se uobičajeno i shvaća ovaj pojam) jer su povezani s kućanstvom i privatnim aktivnostima (poput elektronske komunikacije čija povjerljivost treba biti zaštićena) ili zato što utječu na ostvarivanje temeljnog prava (poput lokacijskih podataka čije prikupljanje dovodi u pitanje slobodu kretanja) ili zato što njihova povreda očito podrazumijeva ozbiljne učinke na svakodnevni život ispitanika (poput finansijskih podataka koji mogu biti upotrijebljeni za prijevaru u platnom prometu). U tom pogledu može biti važno je li te podatke

već javno objavio ispitanik ili treća strana. Činjenica da su lični podaci javno dostupni može se smatrati činjenicom u procjeni ako se očekivalo daljnje korištenje tim podacima u određene svrhe. Taj kriterij može obuhvaćati i podatke poput ličnih dokumenata, e-pošte, dnevnika, bilježaka s e-čitača na kojima se mogu praviti bilješke i vrlo ličnih informacija sadržanih u aplikacijama za bilježenje životnih događaja.

5. Opsežna obrada podataka. U Općoj uredbi o zaštiti podataka nije određeno što obuhvaća pojam „opsežno", ali se u uvodnoj izjavi 91. nalaze određene smjernice. U svakom slučaju, Radna skupina za zaštitu podataka iz članka 29. preporučuje da se, pri utvrđivanju je li obrada opsežna, posebno razmotre slijedeći elementi:
   a. broj uključenih ispitanika, bilo kao određeni broj ili udio relevantnog stanovništva;
   b. količina podataka i/ili niz različitih podataka koji se obrađuju;
   c. trajanje ili stalnost postupka obrade podataka;
   d. zemljopisni opseg aktivnosti obrade.
6. Podudarajući ili kombinirani skupovi podataka, na primjer oni koji potječu iz dva postupka obrade ili više njih, a koji su provedeni u različite svrhe i/ili koje su proveli različiti voditelji obrade podataka na način koji može premašiti razumna očekivanja ispitanika.
7. Podaci koji se odnose na osjetljive ispitanike (uvodna izjava 75.). brada ove vrste podataka jest kriterij zbog povećane neravnoteže moći između ispitanika i voditelja obrade podataka, što znači da pojedinci ne mogu jednostavno dati saglasnost ili se usprotiviti obradi svojih podataka ili ostvarivati svoja prava. Osjetljivi ispitanici mogu biti djeca (smatra se da ne mogu svjesno i promišljeno dati pristanak ili se usprotiviti obradi podataka), zaposlenici, osjetljivije skupine stanovništva koje trebaju posebnu zaštitu (osobe s duševnim smetnjama, tražitelji azila ili starije osobe, pacijenti itd.). Time su obuhvaćene i situacije u kojima se može utvrditi neravnoteža između položaja ispitanika i voditelja obrade.
8. Inovativna upotreba ili primjena novih tehnoloških ili organizacijskih rješenja, poput kombiniranja otisaka prstiju i prepoznavanja lica radi poboljšane kontrole fizičkog pristupa itd. Iz Opšte je uredbe o zaštiti podataka jasno (član 35. stav 1. i uvodne izjave 89. i 91.) da upotreba nove tehnologije, definisane u skladu s postignutim nivoom tehnološkog znanja (uvodna izjava 91.) može dovesti do potrebe za provođenjem procjene učinka na zaštitu podataka. To je zato što upotreba takve tehnologije može obuhvaćati inovativne oblike prikupljanja i upotrebe podataka s mogućim visokim rizikom za prava i slobode pojedinaca. Doista, lične i društvene posljedice implementacije nove tehnologije još nisu posve poznate. Procjena učinka na zaštitu podataka pomoći će voditelju obrade podataka u razumijevanju takvih rizika i postupanju s njima. Na primjer, određene aplikacije „internet stvari" mogu znatno utjecati na svakodnevni život i privatnost pojedinaca; stoga je potrebno provesti procjenu učinka na zaštitu podataka.
9. Situacija u kojoj sama obrada sprečava ispitanike u ostvarivanju prava ili upotrebi usluge i ugovora (član 22. i uvodna izjava 91.). To uključuje i postupke obrade kojima se ispitanicima dopušta, mijenja ili odbija pristup pojedinoj usluzi ili sklapanje ugovora. Primjer je banka koja provjerava klijente u referentnoj bazi podataka o kreditnoj sposobnosti pri odlučivanju o dodjeli kredita."

U većini slučajeva, voditelj obrade podataka može smatrati da obrada koja ispunjava bar dva od prethodno navedenih kriterija zahtijeva provođenje procjene učinka na zaštitu podataka. Općenito, Radna skupina za zaštitu podataka iz članka 29 smatra da što je više kriterija ispunjeno obradom, to je veća mogućnost da ona predstavlja visok rizik za prava i slobode ispitanika i stoga je nužno provođenje procjene učinka na zaštitu podataka, bez obzira na mjere koje voditelj obrade namjerava donijeti. (Smjernica, 2017)

Međutim, u određenim slučajevima voditelj obrade podataka može smatrati da je zbog obrade koja ispunjava samo jedan od tih kriterija nužno provesti procjenu učinka na zaštitu podataka. (Smjernica, 2017)

U slijedećim je primjerima prikazano na koji se način trebaju upotrijebiti kriteriji kako bi se procijenilo da li je za određeni postupak obrade nužno provesti procjenu učinka na zaštitu podataka. (Smjernica, 2017)

Primjer obrade 1

Bolnica koja obrađuje genetske i zdravstvene podatke svojih pacijenata (bolnički informacijski sistem).

Mogući relevantni kriteriji:
- Osjetljivi podaci ili podaci vrlo lične prirode.
- Podaci koji se odnose na osjetljive ispitanike.
- Opsežne obrade podataka

Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebni - DA

Primjer obrade 2

Upotreba sistema nadzornih kamera za praćenje ponašanja vozača na autocestama. Voditelj obrade namjerava upotrijebiti sistem pametne video analize za izdvajanje automobila i automatsko prepoznavanje registarskih tablica.

Mogući relevantni kriteriji:
- Sistemsko praćenje.
- Inovativna upotreba ili primjena tehnoloških ili organizacijskih rješenja.

Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebna - DA

Primjer obrade 3

Preduzeće sistemski prati aktivnosti svojih zaposlenika, uključujući praćenje radne stanice, aktivnost na internetu itd.

Mogući relevantni kriteriji:
- Sistemsko praćenje.
- Podaci koji se odnose na osjetljive ispitanike.

Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebna - DA

Primjer obrade 4

Prikupljanje podataka s javnih društvenih medija za izradu profila.

Mogući relevantni kriteriji:
- Procjena ili bodovanje.
- Automatizirano donošenje odluka s pravnim ili sličnim znatnim učinkom.
- Sprečava ispitanika u ostvarivanju prava, korištenju uslugom ili ugovorom.
- Osjetljivi podaci ili podaci vrlo lične prirode.

Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebna - DA

Primjer obrade 5

Internetski časopis čiji se urednici koriste popisom adresa za slanje generičkih dnevnih novosti svojim pretplatnicima.

Mogući relevantni kriteriji:
- Osjetljivi podaci.
- Podaci koji se odnose na osjetljive ispitanike.
- Sprečava ispitanike u ostvarivanju prava, korištenju uslugom ili ugovorom.

Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebna - DA

Primjer obrade 6

Pohrana u svrhu arhiviranja pseudonimiziranih ličnih osjetljivih podataka koji se odnose na osjetljive ispitanike u okviru istraživačkih projekata ili kliničkih ispitivanja.

Mogući relevantni kriterij:
- Opsežna obrada podataka.

Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebna - NIJE NUŽNO

Primjer obrade 7

Internetska stranica e-trgovine koja prikazuje reklame za dijelove oldtajmera, što obuhvaća i ograničenu izradu profila na temelju pregleda ili kupnji na vlastitoj internetskoj stranici.

Mogući relevantni kriterij:
- Procjena ili bodovanje.

Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebna - NIJE NUŽNO

Ako nije jasno je li procjena učinka na zaštitu podataka potrebna, Art. 29 WP preporučuje da se ona ipak provede jer voditeljima obrade olakšava usklađivanje sa zakonodavstvom o zaštiti podataka. (Smjernica, 2017)

3. OBAVEZA SAVJETOVANJA SA NADZORNIM TIJELOM

Procjenu učinka na zaštitu podataka potrebno je provesti prije obrade. To je u skladu s načelima tehničke i integrisane zaštite podataka: “Uzimajući u obzir najnovija dostignuća, trošak provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca koji proizlaze iz obrade podataka, voditelj obrade, i u vrijeme određivanja

sredstava obrade i u vrijeme same obrade, provodi odgovarajuće tehničke i organizacijske mjere …" (Uredba, 2016 – Član 25) (Hamidović, 2019)

Radna skupina za zaštitu podataka iz članka 29 navodi da bi procjenu učinka na zaštitu podataka trebalo posmatrati kao pomoćni alat za donošenje odluka o obradi, te preporučuje da bi s provođenjem procjene učinka na zaštitu podataka trebalo započeti što je prije moguće tijekom planiranja postupka obrade, čak i ako su neki postupci obrade još uvijek nepoznati. Ažuriranjem procjene učinka na zaštitu podataka tijekom trajanja projekta osigurat će se da se vodi računa o zaštiti podataka i privatnosti i potaknut će se iznalaženje rješenja kojima se potiče usklađenost. Pojedine će korake procjene možda biti potrebno ponoviti u tijeku postupka razvoja jer odabir određenih tehničkih ili organizacijskih mjera može utjecati na ozbiljnost i vjerojatnost rizika koje predstavlja obrada. (Smjernica, 2017)

Činjenica da će procjena učinka na zaštitu podataka možda trebati biti ažurirana nakon što obrada stvarno započne nije valjan razlog za odgodu ili neprovođenje procjene učinka na zaštitu podataka. Procjena učinka na zaštitu podataka kontinuiran je proces, posebno ako je postupak obrade dinamičan i podložan stalnim promjenama. Procjena učinka na zaštitu podataka provodi se kontinuirano, a ne jednom. (Smjernica, 2017)

U smjernicama Radne skupine za zaštitu podataka iz članka 29 se navodi kao primjer pohranjivanje ličnih podataka u prijenosni računar uz upotrebu prikladnih tehničkih i organizacijskih sigurnosnih mjera (učinkovito kriptanje cijelog diska, sigurno upravljanje ključem, prikladni nadzor pristupa, zaštićene sigurnosne kopije itd.) uz postojeće politike (obavijest, saglasnost, pravo pristupa, pravo na prigovor itd.). U navedenom primjeru prijenosnog računara, ukoliko voditelj obrade podataka smatra da je rizik dovoljno umanjen te u skladu s tekstom člana 36. stavka 1. i uvodnih izjava 84. i 94., obrada se može nastaviti bez savjetovanja s nadzornim tijelom. Samo u slučajevima u kojima utvrđene rizike voditelj obrade podataka ne može ukloniti na odgovarajući način, (tj. preostali rizici su i dalje visoki), voditelj obrade podataka mora potražiti savjet nadzornog tijela. (Smjernica, 2017)

U vezi sa prethodno navedenim primjerom Radna skupina za zaštitu podataka iz članka 29 napominje da pseudonimizacija i enkripcija osobnih podataka (kao i minimizacija podataka, mehanizmi nadzora itd.) nisu nužno odgovarajuće mjere. Riječ je samo o primjerima. Odgovarajuće mjere ovise o kontekstu i rizicima koji su specifični za postupke obrade.

Primjer neprihvatljivog visokog preostalog rizika uključuje slučajeve u kojima se ispitanici mogu suočiti sa znatnim ili čak nepopravljivim posljedicama, koje možda neće moći ukloniti (npr. neovlašteni pristup podacima kojim se može ugroziti život ispitanika, otpuštanje, financijski rizik) i/ili ako je očito da će doći do pojave rizika (npr. ako se ne može smanjiti broj osoba koje pristupaju podacima zbog razmjene podataka, njihove upotrebe ili načina distribucije ili ako dobro poznata slabost nije uklonjena). (Smjernica, 2017)

Ako voditelj obrade podataka ne može pronaći odgovarajuće mjere za smanjenje rizika na prihvatljiv nivo (tj. ako su preostali rizici i dalje visoki), mora se savjetovati s nadzornim tijelom, a temeljem zahtjeva iz Člana 35 Uredbe "Voditelj obrade savjetuje se s nadzornim tijelom prije obrade ako se procjenom učinka na zaštitu podataka iz članka 35. pokazalo da bi, u slučaju da voditelj obrade ne donese mjere za ublažavanje rizika, obrada dovela do visokog rizika." (Uredba, 2016)

Trebalo bi međutim istaknuti da, bez obzira na to je li savjetovanje s nadzornim tijelom potrebno s obzirom na nivo preostalog rizika, čuvanje zapisa o procjeni učinka na zaštitu podataka i pravodobno ažuriranje procjene učinka na zaštitu podataka i dalje su nužni. (Smjernica, 2017)

4. PRIMJER METODE PROCJENE RIZIKA

Francuska agencija za zaštitu privatnosti podataka (CNIL) navodi u svojim smjernicama da, što se tiče oblasti privatnosti, primarni rizici koje treba uzeti u obzir su oni koji predstavlja obrada ličnih podataka za privatnost. Ti rizici se sastoje od događaja kojih se plašimo (eng. feared event) (čega se plašimo?) i svih prijetnji koje ih mogu omogućiti (kako se to može dogoditi?) (CNIL, 2012)

Primjeri događaja od kojih strahujemo:

- Podaci o navikama zaposlenih nezakonito se prikupljaju i koriste od strane njihovih nadređenih za usmjeravanje istraživačkih dokaza s ciljem otpuštanja uposlenika.
- Koordinate se preuzimaju i koriste u komercijalne svrhe (spam, ciljano oglašavanje…).
- Identiteti su lažirani za vršenje nezakonitih aktivnosti u ime subjekata podataka, koji se suočavaju sa krivičnim gonjenjem.
- Nakon neželjene modifikacije zdravstvenih podataka, pacijenti su neadekvatno zbrinuti, pogoršava im se stanje što može da uzrokuje invalidnost ili smrt.
- Prijave za socijalnu pomoć nestaju, čime se korisnici lišavaju ovih pogodnosti i prisiljava ih se da ponove administrativne formalnosti.

Da bi se desio događaj od koga strahujemo, mora postojati jedan ili više izvora rizika koji ga uzrokuju, bilo slučajno ili namjerno. Izvori rizika mogu uključivati:

- Osobe koje pripadaju organizaciji - korisnik, kompjuterski stručnjak ...
- Osobe izvan organizacije - primalac, provajder, konkurent, ovlašteno treće lice, vladina organizacija …
- Ne-ljudski izvori - kompjuterski virus, prirodna katastrofa, zapaljivi materijali, epidemija, glodari…

Izvori rizika će djelovati, slučajno ili namjerno, na različite komponente informacionog sistema, na koje se oslanjaju primarna sredstva (procesi i podaci). Ova podržavajuća sredstva mogu uključivati:

- Hardver - računari, komunikacijski releji, USB uređaji, hard diskovi ...
- Softver - operativni sistemi, poruke, baze podataka, poslovne aplikacije…
- Mreže - kablovska, bežična, optička ...
- Ljudi - korisnici, administratori, top menadžment…
- Papirni mediji - štampanje, fotokopiranje ...
- Kanali prijenosa papira - pošta, radni procesi (eng. workflow) ...

Djelovanje izvora rizika na sredstva podrške može se dogoditi kroz različite prijetnje:

- Zloupotreba funkcija - pomoćna sredstva se preusmjeravaju iz svoga namjeravanog konteksta upotrebe bez promjene ili oštećenja istih;
- Špijunaža - prateća sredstva se posmatraju bez oštećenja istih;
- Prekoračene granice operacije - sredstva podrške su preopterećena, pretjerano eksploatisana ili korištena pod uslovima koji im ne dozvoljavaju da pravilno funkcionišu;
- Oštećenje - sredstva podrške su djelomično ili potpuno oštećena;
- Promjene - sredstva podrške se transformišu;
- Imovinski gubici - sredstva podrške su izgubljena, ukradena, prodata ili predata, tako da više nije moguće ostvarivati imovinska prava.

Primjeri prijetnji:

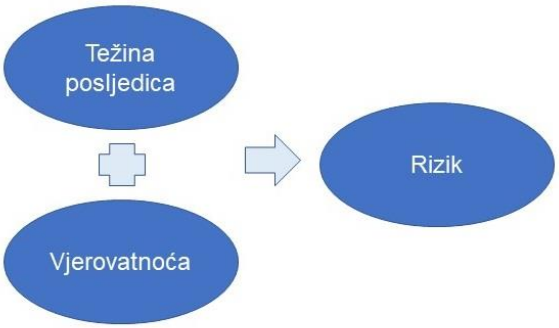
- Zlonamjerni napadač ubacuje neočekivane upite u formu na web lokaciji.
- Tržišni suparnik koji inkognito posjećuje preduzeće i pri tome ukrade prenosivi hard disk.
- Član osoblja greškom uklanja tabele iz baze podataka.
- Štete od vode uzrokuju uništavanje računarskih servera i telekomunikacijske opreme.

CNIL navodi da rizik predstavlja scenarij koji opisuje kako izvori rizika mogu iskoristiti ranjivosti podržavajućih sredstava što vodi do izazivanja incidenta na primarnoj imovini i uticaja na privatnost.

Nivo rizika se procjenjuje u smislu ozbiljnosti i vjerovatnoće.

Ozbiljnost u suštini zavisi od stepena identifikacije ličnih podataka i nivoa posljedica potencijalnih utjecaja.

Vjerovatnoća predstavlja izvedivost dešavanja rizika, i u suštini zavisi od stepena ranjivosti podržavajućih sredstava koji se suočavaju sa nivoom mogućnosti izvora rizika da ih iskoriste.



Slika 1. Određivanje nivoa rizika (CNIL, 2012)

Slika 2 predstavlja sintezu prethodno spomenutih pojmova.

CNIL navodi sljedeću skalu koja se može koristiti za procjenu ozbiljnosti neželjenih događaja (CNIL, 2018):

Slika 2. Komponente rizika (CNIL, 2012)

Tabela 1 Primjeri nivoa utjecaja na temelju vrste ličnih podatak

Vrsta ličnih podataka	Nivo utjecaja
Javno dostupni lični podaci (npr. telefonski direktorij, imenik ili selekcijske liste).	1
Lični podaci koji zahtijevaju opravdani interes za pristup (npr. ograničene javne datoteke ili članovi distribucijskog popisa).	2
Lični podaci čija neovlaštena objava može utjecati na reputaciju nosioca podataka (npr. podaci o prihodima, socijalne naknade, porez na imovinu ili kazne).	3
Lični podaci čija neovlaštena objava, izmjena, gubitak ili uništenje može utjecati na postojanje ili zdravlje, slobodu i život nosioca podataka (npr. informacije o pripadnosti stranci, lične sklonosti, podaci o zdravlju, nepodmireni dugovi, ili ako je pak nositelj podataka pod rizikom da postane žrtva u krivičnom predmetu).	4

1. *Zanemarivo* - Subjekti podataka neće biti pogođeni ili će možda naići na nekoliko neugodnosti koje će moći prevazići bez ikakvih problema, kao na primjer u slučaju gubitaka vremena u ponavljanju već obavljenih formalnosti ili prijema neželjene pošte.
2. *Ograničeno* - Subjekti podataka mogu naići na značajne neugodnosti, koje će moći prevazići uprkos nekoliko poteškoća, kao na primjer u slučaju propuštenih prilika za udobnost (otkazivanje odmora, kupovine, ukidanje online računa), propuštenih prilika za napredovanja u karijeri, prijema neželjenih ciljanih poruka koje bi mogle da oštete reputaciju subjekata podataka.
3. *Značajano* - Subjekti podataka mogu naići na značajne posljedice, koje bi trebali biti u stanju prevazići iako sa stvarnim i ozbiljnim poteškoćama, kao na primjer u slučaju zloupotrebe novca subjekta podataka koji nije nadoknađen, gubitka zaposlenja ili razvoda.
4. *Maksimalno* - Subjekti podataka mogu osjetiti značajne, ili čak i nepovratne, posljedice koje oni ne mogu prevazići, kao na primjer u slučaju oboljevanja od dugotrajnih ili trajnih fizičkih bolesti (zbog zanemarivanja kontraindikacija), oboljevanja od dugotrajne ili trajne psihološke bolesti ili u slučaju krivične odgovornosti subjekta podataka.

U međunarodnom standardu ISO/IEC 29134 se navodi primjer nivoa utjecaja na temelju vrste ličnih podataka (Tabela 1).

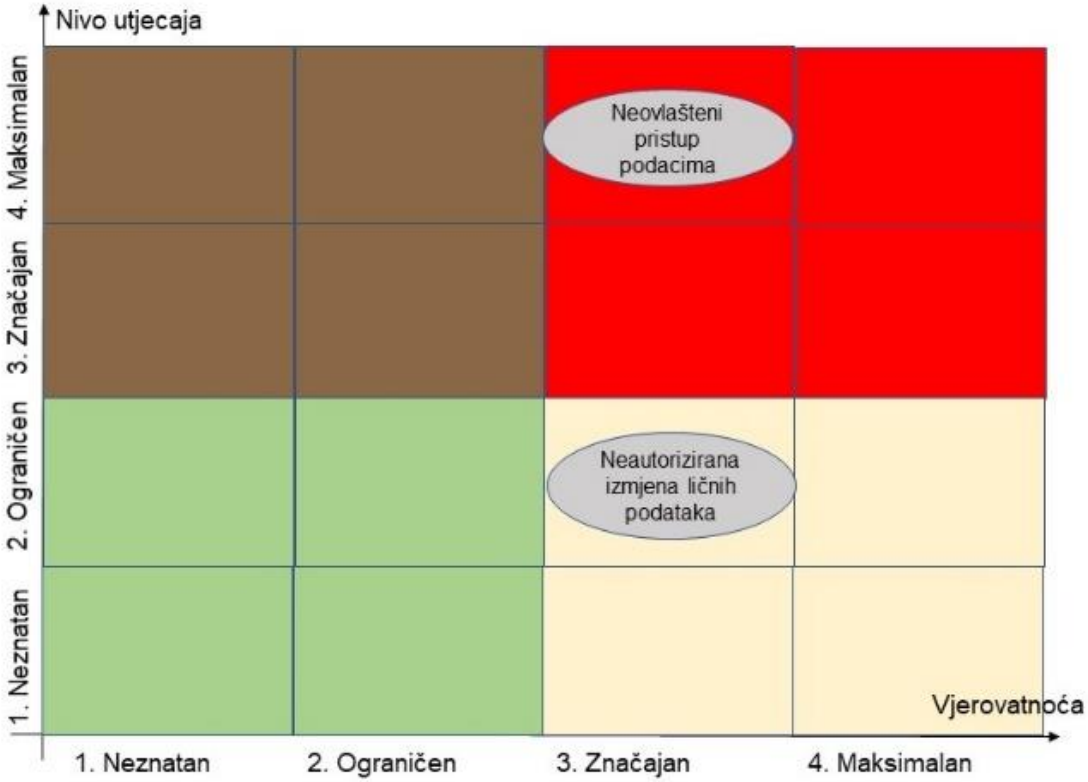
Što se tiče prijetnji, njihova vjerovatnoća se izračunava iz ranjivosti podržavajuće imovine (u

kojoj mjeri se karakteristike podržavajuće imovine mogu iskoristiti da bi se izvršila prijetnja) i sposobnosti izvora rizika (napadači) da iskoriste ove ranjivosti (vještine, raspoloživo vrijeme, financijski resursi, bliskost sa sistemom, motivacija, itd.).

ISO/IEC 29134 navodi sljedeću skalu koja se može koristiti za izražavanje stupanj do kojeg prijetnja može iskoristiti ranjivosti podržavajuće imovine:

1. *Neznatan stupanj*. Izvršavanje prijetnje ne čini se moguće za odabrane izvore rizika (npr. krađa dokumenata pohranjenih u sobi koja je zaštićena čitačem i pristupnim kodom).
2. *Ograničen stupanj.* Izvršavanje prijetnje čini se teško moguće za odabrane izvore rizika (npr. krađa dokumenata pohranjenih u sobi koja je zaštićena čitačem – badge reader).
3. *Značajan stupanj*. Izvršavanje prijetnje čini se moguće za odabrane izvore rizika (npr. krađa dokumenata pohranjenih u uredu kojem se ne može pristupiti prije prethodne prijave na recepciji)
4. *Maksimalni stupanj*. Izvršavanje prijetnje čini se ekstremno lagano za odabrane izvore rizika (npr. krađa dokumenata pohranjenih u predvorju

Svaki rizik privatnosti koji se sastoji od neželjenih događaja i povezanih prijetnji može biti iscrtan u dvodimenzionalnom (vjerovatnoća i ozbiljnost) prostoru, kao na primjeru sa slike 3.



Slika 3. Primjer mape rizika

U zavisnosti od pozicije u ovom prostoru, rizik se može klasificirati kao „potrebno je u potpunosti ga izbjeći", „potrebno je da se ublaži" (kako bi se umanjila vjerovatnoća i/ili utjecaj), ili „prihvatljiv“ (vrlo vjerovatno i sa manjim uticajem).

Nakon procjene rizika, analitičar rizika privatnosti može odrediti kako reagirati. Vrsta odgovora mora uzeti u obzir ograničenja resursa u stvarnom svijetu, kao što su vrijeme, novac i ljudi, kao i sami rizici. Analitičar ima četiri izbora kada odgovara na rizik (Breaux, 2015):

- Prihvatite rizik. Ako je rizik nizak, onda može biti razumno i potrebno prihvatiti rizik.
- Prenesite rizik. Ako postoje drugi subjekti koji mogu bolje upravljati rizikom, transfer rizika može biti najbolja opcija. Na primjer, korišćenje usluga trećih strana koje mogu da upravljaju platnim spiskovima, plaćanjem i drugim finansijskim uslugama koristeći visoke

standarde privatnosti i bezbjednosti može biti poželjnije od internog razvoja ekvivalentnog sistema od temelja.
- Ublažiti rizik. Ublažavanje je najbolja opcija kada razvojni inženjer može implementirati kontrole privatnosti koje smanjuju rizik. To može na primjer biti kroz softversku komponentu ili kroz promjenu poslovnih procesa.
- Izbjegavajte rizik. Izbjegavanje nastaje kada se može izbjeći nepovoljan događaj promjenom dizajna sistema ili poslovnog procesa.

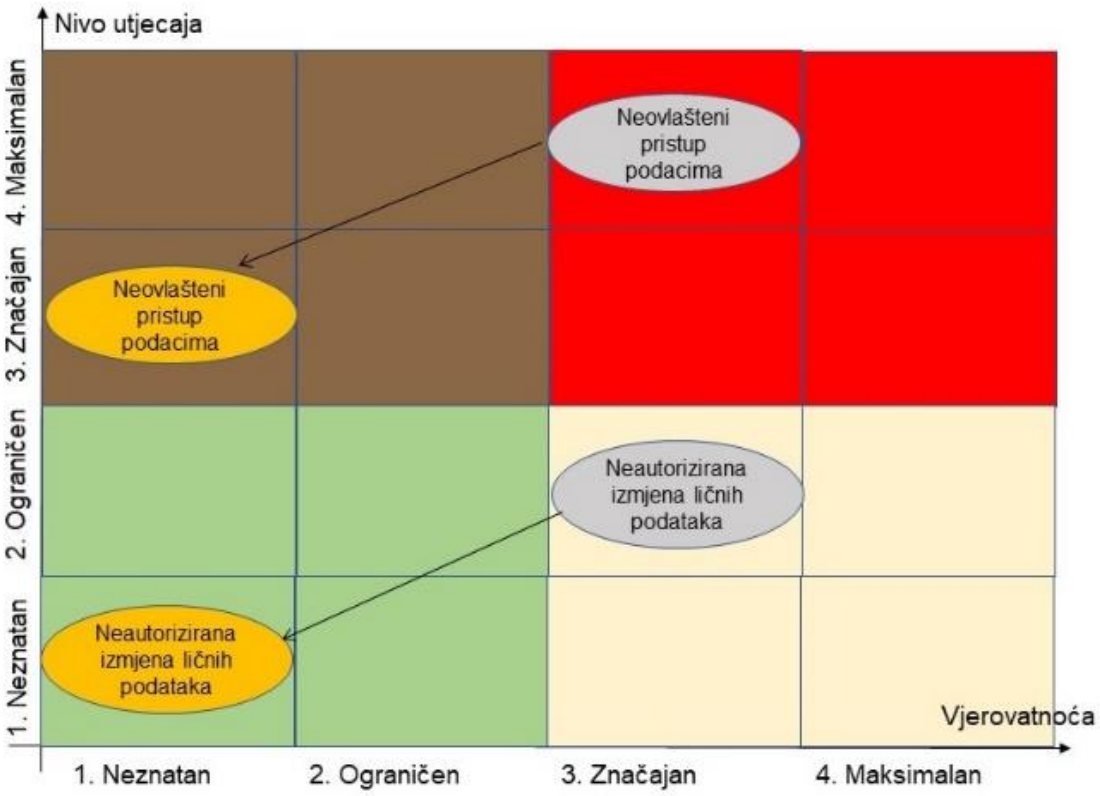
Kontrole rizika spadaju u tri kategorije (Breaux, 2015):
- administrativne kontrole, koje upravljaju poslovnom praksom organizacije;
- tehničke kontrole koje upravljaju softverskim procesima i podacima; i
- fizičke kontrole, koje npr. regulišu fizički pristup štampanim kopijama podataka i sistemima koji obrađuju i čuvaju elektronske kopije.

U oblasti zaštite privatnosti, primjer administrativnih kontrola uključuju:
- Imenovanje službenika za privatnost koji je odgovoran za koordiniranje dobrih praksi zaštite privatnosti na nivou cijele organizacije;
- Razvoj i dokumentiranje procedura privatnosti i sigurnosti;
- Obuka osoblja u oblasti zaštite privatnosti;
- Kreiranje inventara ličnih informacija radi praćenja praksi zaštite podataka…

Tehničke kontrole ciljaju informacione sisteme i treba da budu u fokusu softver inženjera prilikom dizajniranja sistema za očuvanje privatnosti. One uključuju:
- Implementacija mehanizama kontrole pristupa;
- Audit pristupa informacijama;
- Kriptanje osjetljivih podataka;
- Upravljanje individualnim pristankom;
- Objavljivanje obaveštenja o privatnosti…

Navedene mjere moraju se formalno odrediti, provesti, redovno pregledati i stalno poboljšavati.

Nakon implementiranja mjera za kontrolu rizika potrebno je procijeniti ozbiljnost i vjerovatnoću preostalih rizika (tj. rizika koji ostaju nakon provedbe odabranih mjera). Rizici se zatim mogu repozicionirati na mapi rizika, kao na Slici 4.



Slika 4. Mapa rizika nakon implementiranja mjera za kontrolu rizika

Za obavljanje procjene učinka na privatnost može se koristiti i matrica za određivanje rizika predstavljena međunarodnim standardom ISO/IEC 27005.

Kvalitativnom metodom odabire se jedna od pet opisnih nivoa vjerojatnosti, odnosno mogućnosti pojave rizika (ZIH, 2019):

1 - *vrlo niska* (nije vjerojatno da bi se razmatrani rizik mogao dogoditi, odnosno vjerojatnost njegove pojave je otprilike jednom u pet godina, ne postoje slučajevi, statistike ili motivi koji bi naznačili njegovo ostvarivanje, povezane ranjivosti procesa ili tehnologije se teško mogu iskoristiti, postojeće kontrole koje mogu spriječiti takav događaj su vrlo učinkovite),
2 - *niska* (malo vjerojatno da bi se razmatrani rizik mogao dogoditi, odnosno vjerojatnost njegove pojave je otprilike jednom u dvije godine, ali postoje slučajevi, statistike ili motivi koji bi naznačili njegovo ostvarivanje, povezane ranjivosti procesa, postojeće kontrole koje mogu spriječiti takav događaj su učinkovite),
3 - *srednja* (vjerojatnost pojave razmatranog rizika je jednom u godini, postoje slučajevi, statistike ili druge informacije koje ukazuju na to da se ovaj ili sličan događaj dogodio, ili postoji naznaka da bi mogli postojati neki razlozi za realizaciju scenarija; povezane ranjivosti bi se mogle iskoristiti; postojeće kontrole su uglavnom učinkovite),
4 - *visoka* (vjerojatnost pojave razmatranog rizika je jednom do dva puta u godini, postoje slučajevi, statistike ili druge informacije koje ukazuju na to da se ovaj ili sličan događaj nedavno dogodio (unutar godine dana), povezane ranjivosti bi se mogle lako iskoristiti; postojeće kontrole nisu dovoljno učinkovite),
5 - *vrlo visoka* (vjerojatnost pojave razmatranog rizika je više puta u godini, očekuje se pojava, odnosno postoje slučajevi, statistike ili druge informacije koje ukazuju na to da će se razmatrani scenarij vjerojatno pojaviti ili postoje jaki razlozi ili motivi za realizaciju scenarija; povezane ranjivosti se mogu vrlo lako iskoristiti; nisu implementirane kontrole, vjerojatnost pojave događaja je više puta u godini).

Treba odabrati jedan od pet nivoa utjecaja na ostvarenje ciljeva, koja najbolje opisuje kako će ostvareni rizik djelovati na organizaciju:

1 – *vrlo nizak*. Nema utjecaja na privatnost pojedinaca
2 – *nizak*. Zanemariv utjecaj na privatnost pojedinaca
3 – *srednji*. Manji utjecaj na privatnost – pojedinačni slučajevi ugrožavanja osobnih podataka
4 – *visok*. Značajniji utjecaj na privatnost – veći broj slučajeva ugrožavanja ličnih podataka
5 – *vrlo visok*. Vrlo veliki utjecaj na privatnost – vrlo veliki broj slučajeva ugrožavanja ličnih podataka.

Nivo rizika se izračunava po formuli:

*Nivo rizika = Vjerojatnost ostvarenja rizika * Utjecaj na ostvarenje ciljeva*

Nakon izračuna vrijednosti rizika isti se unosi u matricu procjene rizika sa slike 5.

	Vjerojatnost incident scenarija	Vrlo niska	Niska	Srednja	Visoka	Vrlo visoka
	Vrlo niska	0	1	2	3	4
	Niska	1	2	3	4	5
	Srednja	2	3	4	5	6
	Visoka	3	4	5	6	7
Utjecaj	Vrlo visoka	4	5	6	7	8

Slika 5. Matrica procjene rizika (Hamidović, 2010) (ISO/IEC, 2018)

Pri tom je skala ukupne ocjene rizika izražena kao:

- *Nizak rizik*: 0-2
- *Srednje rizičan*: 3-5
- *Visok rizik*: 6-8

5. ZAKLJUČCI

U skladu s pristupom temeljenim na riziku, utvrđenim u Opšoj uredbi o zaštiti podataka, provođenje procjene učinka na zaštitu podataka nije obavezno za svaki postupak obrade, već samo ukoliko će obrada vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca. No,

ukoliko nije jasno je li procjena učinka na zaštitu podataka potrebna, Radna skupina za zaštitu podataka iz članka 29 preporučuje da se ona ipak provede, jer voditeljima obrade olakšava usklađivanje sa zakonodavstvom o zaštiti podataka.

U skladu s načelima tehničke i integrisane zaštite podataka procjenu učinka na zaštitu podataka trebalo bi provesti prije same obrade, a s ciljem korištenja iste kao pomoćnog alata za donošenje odluka o obradi, a posebice izbora odgovarajućih mjera tehničke i integrisane zaštite.

Opšta uredba o zaštiti podataka ne propisuje niti jednu konkretnu metodologiju ili standard za izvođenje procjene učinka na privatnost, no u smjernicama Radne skupine za zaštitu podataka iz članka 29 navedene su preporuke za korištenje međunarodnih standarda kao što je ISO/IEC 29134. U radu je predstavljena i CNIL metoda za procjenu učinka na privatnost, a koja je u velikoj mjeri usklađena sa preporukama ISO/IEC 29134. Iako je sama CNIL metoda prilično opšta i na visokom nivou, ista je dopunjena katalogom dobrih praksi koje mogu pomoći voditeljima obrade podataka u njihovom zadatku (za procjenu uticaja neželjenih događaja, na identifikaciju izvora rizika, odabir mjera proporcionalno rizicima, itd.).

CITIRANA DJELA

Breaux T. (2015). Introduction to IT Privacy: A Handbook for Technologists, International Association of Privacy Professionals (IAPP)

CNIL. (2018). Privacy Impact Assessment (PIA) 3 : knowledge bases. Commission Nationale de l'Informatique et des Libertés

CNIL. (2012). Methodology for Privacy Risk Management. Commission Nationale de l'Informatique et des Libertés

Hamidovic, H. (2010). An Introduction to the Privacy Impact Assessment Based on ISO 22307. ISACA Journal. Volume 4, 2010, The Information Systems Audit and Control Association

Hamidović, H. (2010). Priručnik za izradu i reviziju plana sigurnosti osobnih podataka u automatskoj obradi, Info Press, Zagreb,

Hamidović, H. (2019). Obaveza poduzimanja tehničkih mjera zaštite podataka temeljem EU uredbe o zaštiti podataka. FBIM Transactions, 15 04, 7(1), pp. 67-73

Smjernica. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, Article 29 Working Party

Standard. (2017). ISO/IEC 29134:2017 Information technology -- Security techniques -- Guidelines for privacy impact assessment. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

Standard. (2018). ISO/IEC 27005:2018 Information technology -- Security techniques -- Information security risk management. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

Uredba. (2016, maj 4). Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. aprila 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka). Službeni list Europske unije, L 119/1

ZIH. (2019). Seminar - Primjena Uredbe o zaštiti osobnih podataka – Radni materijali, Zavod za informatičku djelatnost Hrvatske, Zagreb

Datum prve prijave: 20.07.2019.
Datum prijema korigovanog članka: 08.09.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Hamidović, H. (2019, 10 15). Procjena učinka na zaštitu ličnih podataka. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 39-51. doi:10.12709/fbim.07.07.02.05

*Style – **Chicago** Sixteenth Edition:*

Hamidović, Haris. 2019. "Procjena učinka na zaštitu ličnih podataka." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 39-51. doi:10.12709/fbim.07.07.02.05.

*Style – **GOST** Name Sort:*

Hamidović Haris Procjena učinka na zaštitu ličnih podataka [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 39-51.

*Style – **Harvard** Anglia:*

Hamidović, H., 2019. Procjena učinka na zaštitu ličnih podataka. *FBIM Transactions,* 15 10, 7(2), pp. 39-51.

Style – **ISO 690** Numerical Reference:

Procjena učinka na zaštitu ličnih podataka. **Hamidović, Haris.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 39-51.

FBIM Transactions
DOI 10.12709/fbim.07.07.02.06

MODEL UPRAVLJANJA BEZBEDNOSNIM RIZIKOM

SECURITY RISK MANAGEMENT MODEL

Nemanja Jovanov
Poslovni i pravni fakultet, Univerzitet „Union – Nikola Tesla”, Beograd, Srbija

Nikola Glođović
Kriminalističko policijska akademija-Beograd, Beograd, Srbija

Goran Jovanov
Kriminalističko policijska akademija-Beograd, Beograd, Srbija

JEL Kategorija rada: **D81, G32**

Apstrakt

Danas u svetu ima više razvijenih modela za upravljanje bezbednosnim rizikom, a u ovom radu će biti predstavljen model sa osam faza. Faza „Identifikacija poslovnog sistema treba da identifikuje sve objekte poslovnog sistema, aktivnosti koje se u njemu realizuju i zaposlene radnike, jer oni potencijalno mogu biti ugroženi nekom opasnošću. Znači, neophodno je izvršiti procenu zašto i kako bi potencijalni nepredviđeni događaj uticao na poslovni sistem i sve njegove resurse, a takođe treba da se utvrdi da li potencijalni nepredviđeni događaj koji bi mogao prouzrokovati određenu opasnost predstavlja događaj koji bi ostvario štetu koju poslovni sistem ne sme sebi da dozvoli, ili je za njega konkretni potencijalni događaj zanemarljiv. U fazi „Procena opasnosti“ vrši se predviđanje potencijalnih specifičnih opasnosti i situacija u kojima bi one mogle da se dese. U ovoj fazi se znači ne realizuje procena bezbednosnog rizika, ali se dolazi do potrebnih informacija i smernica koje će se koristiti za procenu. „Procena ranjivosti“ je faza modela upravljanja bezbednosnim rizikom u kojoj se trebaju prepoznati snaga i slabosti poslovnog sistema po pitanju bezbednosnih mera koje štite isti od uticaja iz okruženja. U narednoj fazi se realizuje procena bezbednosnog rizika. Vrši se kombinovanje svih raspoloživih relevantnih (direktnih i indirektnih) informacija po pitanju bezbednosti, kako bi se uspeo identifikovati potencijalni uticaj i verovatnoća pojave potencijalne opasnosti po poslovni sistem, tj. dobili trenutni nivo bezbednosnog rizika. U fazi „Bezbednosne mere i strategije“ realizuje se razvoj i stvaranje istih, kako bi se njihovom primenom ostvarilo smanjenje verovatnoće pojave bezbednosnog rizika i njegovog štetnog (opasnog) uticaja. U fazi „Donošenje odluke“ neophodno je da se donesu odluke po pitanju prioriteta, logističke podrške, vremenskih rokova, finansija, itd. Ova faza se realizuje u tri koraka, i to: (1) procedure za

Adresa autora:
Nemanja Jovanov
nemanjjajovanov@gmail.com

smanjenje bezbednosnog rizika na prihvatljiv nivo, (2) utvrđivanje prioriteta, i (3) odobravanje finansija i potrebnih resursa. Posle ove faze realizuje se po ovom modelu priprema i implementacija razvijenih bezbednosnih mera. Na kraju se vrši ocena svega što je urađeno, realizuju se potencijalno potrebne korekcije i vrše se pripreme za buduću modernizaciju bezbednosnih mera i strategija.

***Ključne reči**: Identifikacija, bezbednosni rizik,bezbednosne mere, strategija*

Abstract

Worldwide there are many developed models for managing security risks. Within this thesis, the developed model with eight phases will be represented. The phase "Business System Identification" should identify all objects of a business system, the activities realized within it, and employees, because these potentially can be jeopardized by some threat. Therefore, it is necessary to make an estimation why and how a potential unpredictable event could influence a business system and all of its resources, as well as it should be determined whether potential unpredictable event, which could cause certain threat, represents the event which would cause damage which business system must not allow, or a specific potential event is irrelevant for it. In the phase "Threat Estimation" potential specific threats and situations in which these may occur are predicted. In this phase, the security risk estimation is not made, but the necessary information and instructions that will be used for the estimate are gathered. "Vulnerability Estimation" is the phase of a security risk management model in which the strength and weakness of a business system should be recognized, related to security measures which protect the system from the surrounding influences. In the next phase, the security risk estimate is realized. All available, relevant (direct and indirect) security-related information are combined, in order to identify potential influence and the probability of the occurrence of a potential threat on the business system, i.e. to get the current level of security risk. In the phase "Security Measures and Strategies" their development and creation are realized, in order to accomplish the reduction of probable occurrence of security risk and its harmful (dangerous) influence by their application. In the phase „Decision Making" it is necessary to bring the decisions related to priorities, logistics support, timelines, financials, etc. This phase is realized in three steps, as follows: (1) Procedures for reducing the security risk to an acceptable level, (2) Priorities setting, and (3) Approving of financials and necessary resources. After this phase, the preparation and implementation of developed security measures are realized by this model. In the end, the evaluation of everything done is made, potentially, necessary corrections are realized, as well as the preparation for future modernization of security measures and strategies is made.

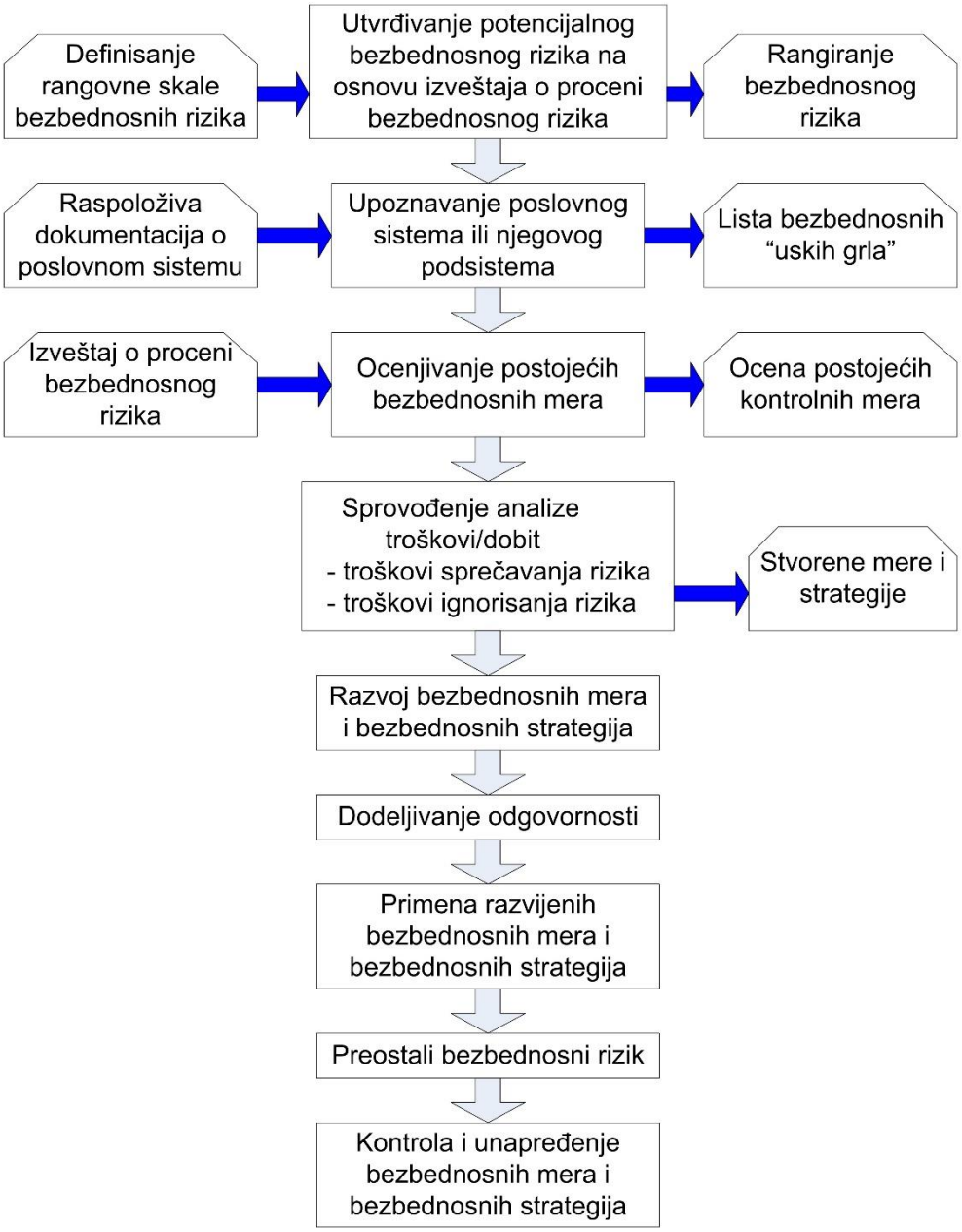
***Keywords:** identification, security risk, security measures, strategy*

1. UVOD

Vrlo je teško obezbediti apsolutnu sigurnost. Ako poslovni sistem nije fizički bezbedan, ništa što je u vezi sa istim ne može se smatrati bezbednim, uključujući zaposlene, tehničke sisteme, procese, dokumentaciju, finansijska sredstva poslovnog sistema, itd. Neki sigurnosni sistemi zahtevaju da pojedini tehnički sistemi (serveri, komunikacioni linkovi, itd.) u poslovnom sistemu budu naročito fizički obezbeđeni.

Standardi bezbednosnih rizika danas zahtevaju da poslovni sistemi obezbede kvalitetne i u skladu sa zakonom bezbednosne politike i procedure za otkrivanje i sprečavanje bezbednosnih rizika. Ukoliko se činjenicama argumentuje da bezbednosna politika poslovnog sistema nije primerena i/ili u skladu sa zakonom, poslovni sistem mora da na relevantan zahtev usvoji nove mere bezbednosne politike, koje će biti prihvaćene kao zadovoljavajuće.

Neki od bezbednosnih rizika su neznatni, a samim tim i zanemarljivi, dok drugi mogu imati štetne posledice koje su nedopustive za poslovni sistem. Procena bezbednosnih rizika pomaže u razvoju strategije bezbednosti i pruža osnovu za uspostavljanje isplativog bezbednosnog programa koji će minimizirati verovatnoću pojave bezbednosnog rizika, odnosno minimizirati efekte bezbednosnog rizika.



Slika.1. Metodologija za umanjenje bezbednosnog rizika

2. PROCENA BEZBEDNOSNOG RIZIKA

Za procenu bezbednosnog rizika možemo reći da je sastavni deo procesa upravljanja bezbednosnim rizicima i da ona predstavlja proces identifikacije opasnosti (koje bi mogle da utiču na zaposlene, procese u poslovnom sistemu ili materijalna sredstva poslovnog sistema), procene bezbednosnih rizika (po pitanju verovatnoće njihovog potencijalnog nastanka i uticaja), kao i utvrđivanje prioriteta tih bezbednosnih rizika i identifikovanje mera i strategija za njihovo sprečavanje, tj. umanjenje. U početnoj fazi procene bezbednosnog rizika, analitičari su nekada primorani da izvrše procenu bezbednosnog rizika (u nekim situacijama čak i da predlože bezbednosne mere i strategije za rešenje konkretnog bezbednosnog rizika) u odsustvu brojnih neophodnih parametara, što je nedopustivo. Metodologija za umanjenje rizika prikazana je šematski na slici 1 (Adamović, Jovanov, Radojević, & Meza, 2008, str. 128). Kako bi se identifikovao kritičan bezbednosni rizik koji zahteva kvalitetno bezbednosno rešenje najčešće se vrši rangiranje.

Rangiranje bezbednosnih rizika se vrši na osnovu relevantnih kriterijuma za poslovni sistem po pitanju mogućnosti poslovnog sistema da preuzme rizik. Kada se identifikuju i analiziraju ponuđena rešenja bezbednosnih rizika, vrši se njihovo ocenjivanje po pitanju efekata verovatnoće pojave i potencijalnih neželjenih događaja po poslovni sistem. Naravno, potencijalni neželjeni događaj nije jedini faktor koji utiče na odluku odabira rešenja između ponuđenih alternativa, jer različita rešenja mogu imati različite prateće posledice na poslovni sistem (npr. cenu proizvoda, nivo zarada zaposlenih, troškove zaštite životne sredine, itd.).

Izveštaj o proceni bezbednosnog rizika treba da kreira operativni menadžment jednog poslovnog sistema za potrebe višeg menadžmenta poslovnog sistema i vlasnika. Na osnovu dobijenog izveštaja, višem menadžmentu je u velikoj meri obezbeđen materijal koji mu je neophodan za donošenje ispravne i kvalitetne odluke o bezbednosnoj politici poslovnog sistema, bezbednosnim procedurama, budžetu za potrebe bezbednosti, sistemu upravljanja bezbednošću i određenim potencijalnim promenama u menadžmentu. Izveštaj o proceni bezbednosnog rizika treba da sadrži sledeće elemente: opšti pregled poslovnog sistema, tehničke sisteme poslovnog sistema, računarski hardver, softver, komunikacione linkove, analizu topologije računarske mreže, kritična mesta poslovnog sistema, metode sakupljanja podataka, analizu podataka, preporuke sigurnosnih mera, preporuke za strategije rešenja analiziranog bezbednosnog rizika, itd. (Vujović, 2003, str. 187).

3. MODEL UPRAVLJANJA BEZBEDNOSNIM RIZIKOM

Danas u svetu postoji više modela razvijenih za upravljanje bezbednosnim rizikom, a u ovom radu će se prikazati razvijeni model sa osam faza (slika 2).

Faza „Identifikacija poslovnog sistema“ treba da identifikuje sve objekte poslovnog sistema, aktivnosti koje se u njemu realizuju i zaposlene radnike, jer oni potencijalno mogu biti ugroženi nekom opasnošću. Znači, neophodno je izvršiti procenu zašto i kako bi potencijalni nepredviđeni događaj uticao na poslovni sistem i sve njegove resurse, a takođe treba da se utvrdi da li potencijalni nepredviđeni događaj, koji bi mogao prouzrokovati određenu opasnost, predstavlja događaj koji bi ostvario štetu koju poslovni sistem ne sme sebi da dozvoli, ili je konkretni potencijalni događaj zanemarljiv za sistem.

U fazi „Procena opasnosti“ vrši se predviđanje potencijalnih specifičnih opasnosti i situacija u kojima bi one mogle da se dese. U ovoj fazi se ne realizuje procena bezbednosnog rizika, ali se dolazi do potrebnih informacija i smernica koje će se koristiti za procenu.

„Procena ranjivosti“ je faza modela upravljanja bezbednosnim rizikom u kojoj treba prepoznati snagu i slabosti poslovnog sistema u pogledu bezbednosnih mera koje štite isti od uticaja iz okruženja (Starčević, Ilić, & Paunović-Pfaf, 2010, str.78).

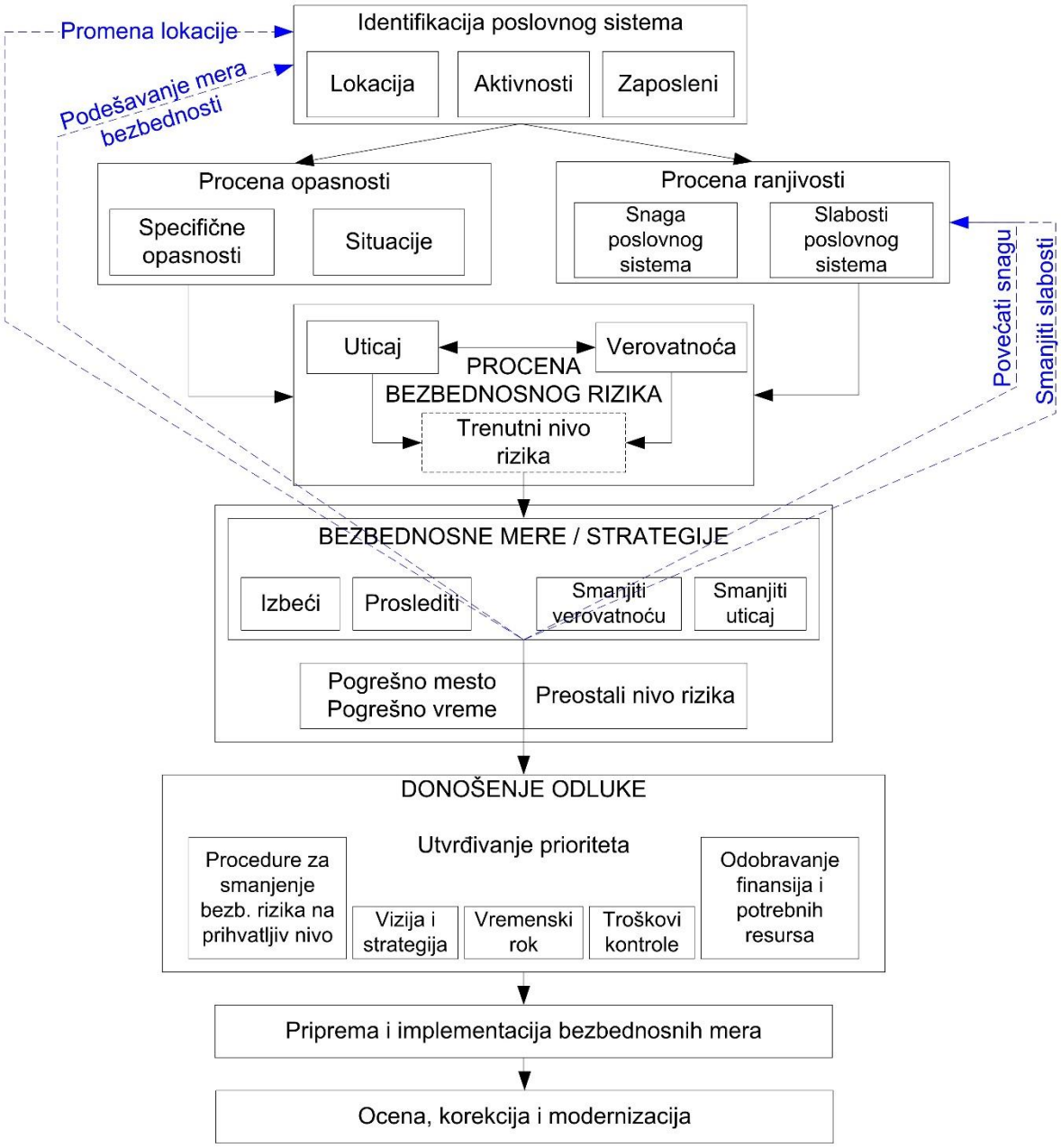
U narednoj fazi se realizuje procena bezbednosnog rizika. Vrši se kombinovanje svih raspoloživih relevantnih (direktnih i indirektnih) informacija po pitanju bezbednosti, kako bi se identifikovali potencijalni uticaj i verovatnoća pojave potencijalne opasnosti po poslovni sistem, tj. dobili trenutni nivo bezbednosnog rizika.

U fazi „Bezbednosne mere i strategije“ realizuje se razvoj i stvaranje istih, kako bi se njihovom primenom ostvarilo smanjenje verovatnoće pojave bezbednosnog rizika i njegovog štetnog (opasnog) uticaja.

U fazi „Donošenje odluke“ neophodno je da se donesu odluke po pitanju prioriteta, logističke podrške, vremenskih rokova, finansija, itd. Ova faza se realizuje u tri koraka, i to:

1. procedure za smanjenje bezbednosnog rizika na prihvatljiv nivo,
2. utvrđivanje prioriteta, i
3. odobravanje finansija i potrebnih resursa.

Posle ove faze realizuju se po ovom modelu priprema i implementacija razvijenih bezbednosnih mera (Adamović, Voskresenski, & Tul, 2007, str. 48).



Slika 2. Model upravljanja bezbednosnim rizikom

Na kraju se vrši ocena svega što je urađeno, realizuju se potencijalno potrebne korekcije i vrše se pripreme za buduću modernizaciju bezbednosnih mera i strategija.

Uzroci nastanka štetnog događaja su slučajni tako da su i štetni događaji slučajne pojave koje možemo modelirati i definisati zakonima verovatnoće.

Mogućnost da se šteta dogodi može se predstaviti na dva načina. Objektivan način je razlomak u kome je brojilac predstavljen brojem jedinica koje su pretrpele, ili za koje se očekuje da će pretrpeti štetu, a imenilac je predstavljen ukupnim brojem jedinica izloženih mogućem dejstvu štetnog događaja.

Objektivna ocena mogućnosti, zasnovana na verovatnoći, odnosi se na dugoročnu relativnu učestalost događaja prema pretpostavkama beskonačnog broja posmatranja i na nepostojanju izmene u datim uslovima.

U poslovnim industrijskim sistemima štetni događaj može biti u oblasti procesa rada

(oslobađanje štetnih materija kao što su to razne hemikalije ili radioaktivnost, prašina, dim, velika buka i vibracije, oslobađanje mikroorganizama, oslobađanje raznih alergenata, emitovanje štetnog nivoa energije iz industrijskih objekata ili opreme u čovekovu okolinu, itd.) Ovo se obično dešava u obliku eksplozije, požara, prosipanja, iscurivanja ili otpada. Ovakvi štetni događaji mogu nastati kao posledica faktora koji su unutrašnji u nekom industrijskom sistemu (tj. ljudski faktor), ili kao posledica spoljašnjih faktora (ekstremni događaji u prirodi). Oslobađanja mogu da budu iznenadna i intenzivna kao što je to eksplozija, ili postepena i opsežna kao što je to ispuštanje materijala u stratosferu koje uništavaju ozonski omotač, ili pak dugotrajno oticanje toksičnih materija koji nisu uništeni ili odloženi na odgovarajući način (na primer, oticanje otpadnih voda iz deponija u unutrašnjost zemlje pri čemu dolazi do zagađivanja podzemnih voda).

Pored štetnih događaja koji se mogu javiti u oblasti procesa rada jednog poslovnog sistema, imamo i štetne događaje koji se mogu dogoditi i kao posledica psihičkih i psihofizičkih napora (npr. stres na radnom mestu, monotonija radnih aktivnosti, psihička naprezanja usled velikog stepena odgovornosti, dugotrajno stajanje, dugotrajno sedenje dugotrajno klečanje, ručno guranje, nošenja ili vučenje velikog tereta, itd.), kao posledica loše organizacije rada (npr. neadekvatna organizacija rada zaposlenih u smenama, učestali rad u noćnoj smeni, čest prekovremeni rad, itd.), kao posledica rada u atmosferi sa visokim ili niskim pritiskom, kao posledica rada u blizini vode ili ispod površine vode, itd. (George, 2005, str.145).

Uzroci nastanka štetnog događaja su slučajni tako da su i štetni događaji slučajne pojave koje možemo modelirati i definisati zakonima verovatnoće. Uzroke štetnih događaja možemo grupisati u dve grupe a to su:

1. potencijalno predvidivi (koji se nalaze u propustima praktične primene, zakonima i tehničkim standardima, propisanim merama preventivne zaštite i sl.), i
2. potencijalno nepredvidivi (pojavne oblike nije moguće predvideti u realnom vremenu).

Pošto su svi faktori koji izazivaju štetni događaj, najčešće slučajnog karaktera, to je i štetni događaj u osnovi slučajna kategorija koja se pokorava zakonima verovatnoće. Drugim rečima, štetni događaji su neminovni i ne mogu se nikada potpuno sprečiti, ali verovatnoća njihovog nastanka može biti manja ili veća. Otuda i veoma dobar stav da su svi štetni događaji normalni, što znači da je mogućnost pojave štetnih događaja ugrađena u samu strukturu složenih sistema, te da se štetni događaji ne mogu potpuno sprečiti boljim konstrukcijama, kvalitetnijim informacijama ili pametnijim, odnosno boljim rukovodiocima, projektantima, inženjerima, radnicima.

Da bi se sagledao uticaj štetnih događaja na privredu neke zemlje potrebno je navesti da samo u štetnim događajima koji su posledica požara naša zemlja nepovratno gubi oko 2% bruto materijalnog proizvoda. Ostali štetni događaji samo povećavaju ovaj, nažalost poražavajući rezultat. Vrste i pojavni oblici štetnih događaja su brojni, raznorodni i često međusobno uzročno-posledični.

4. ZAKLJUČCI

Poslovanje savremenih proizvodno poslovnih sistema se odvija, u složenim, neizvesnim i dinamičnim uslovima koji zahtevaju stalne inovacije i promene. Uvođenje inovacija kroz inovativnost, inventivnost i kreativnost zaposlenih može znatno uticati na oblast menadžmenta rizicima u proizvodno poslovnim sistemima, što svakako zahteva novo znanje i veštine kod zaposlenih.

Posebnu pažnju treba posvetiti onim situacijama i scenarijima događaja u privrednim sistemima, a naročito u njihovim proizvodnim pogonima, koji kao posledicu mogu imati povrede na radu radnika, invalidnost, a u nekim slučajevima i katastrofalnu posledicu po zaposlenog, tj. smrt. Ove neželjene situacije, odnosno vanredne i akcidentne situacije mogu ostaviti štetne posledice kako po zaposlene radnike, privredni sistem, tako i po njegovo okruženje (lokalno, a u nekim slučajevima i daleko šire).

U svakom slučaju, prosečan broj povreda na radu u odeljenju održavanja je procentualno veći nego u proizvodnom delu, jer je broj radnika u odeljenju održavanja daleko manji. I zbog same prirode posla, radnici funkcije održavanja su izloženiji akcidentnim situacijama. Opravdano je tvrditi da

je rad na održavanju tehničkih sistema mnogo opasniji nego rad u proizvodnom sektoru.

Evidentna je korelacija između stepena tehnološke razvijenosti i broja akcidenata. Što je viši stepen tehnološkog razvoja, to je veći procentualni udeo aktivnosti održavanja, tj. veći je i broj akcidentnih situacija koje se javljaju tokom sprovođenja ovih aktivnosti.

Proizvodni pogoni sa aktivnostima održavanja baziranim na kriterijumu rizika imaće manju frekventnost akcidentnih situacija, a samim tim i manji broj izgubljenih radnih dana zbog povreda radnika na radu

REFERENCE

Adamović, Ž., Jovanov, G., Radojević, M., & Meza, S. (2008). *Upravljanje rizikom.* Univerzitet u Novom Sadu. Tehnički fakultet „Mihajlo Pupin“, Zrenjanin.

Adamović, Ž., Milošević, Ž., Popović, L., & Adamović, M. (2008). *Modeli održavanja na bazi rizika*. Društvo za energetsku efikasnost Bosne i Hercegovine, Banja Luka.

Adamović, Ž., Voskresenski, V., & Tul, R., (2007). *Održavanje na bazi rizika*. TEHDIS, Beograd

George, E. Rejda. (2005). *Principles of Risk Management and Insurance*. Ninth Edition, Addisom Wesley, Boston.

Starčević, J., Ilić, M., & Paunović-Pfaf, J. (2010) *Priručnik za procenu rizika*, Globe Design, Beograd.

Vujović, R., Jovanović, S., & Todorović, J. (2003). Unapređenje metoda upravljanja rizikom u industrijskim postrojenjima, *Tokovi osiguranja*, (1-2).

Datum prve prijave: 10.09.2018.
Datum prijema korigovanog članka: 11.07.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Jovanov, N., Glođović, N., & Jovanov, G. (2019, 10 15). Model upravljanja bezbednosnim rizikom. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 52-58. doi:10.12709/fbim.07.07.02.06

*Style – **Chicago** Sixteenth Edition:*

Jovanov, Nemanja, Nikola Glođović, and Goran Jovanov. 2019. "Model upravljanja bezbednosnim rizikom." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 52-58. doi:10.12709/fbim.07.07.02.06.

*Style – **GOST** Name Sort:*

Jovanov Nemanja, Glođović Nikola and Jovanov Goran Model upravljanja bezbednosnim rizikom [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 52-58.

*Style – **Harvard** Anglia:*

Jovanov, N., Glođović, N. & Jovanov, G., 2019. Model upravljanja bezbednosnim rizikom. *FBIM Transactions,* 15 10, 7(2), pp. 52-58.

Style – **ISO 690** Numerical Reference:

Model upravljanja bezbednosnim rizikom. **Jovanov, Nemanja, Glođović, Nikola and Jovanov, Goran.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 52-58.

FBIM Transactions
DOI 10.12709/fbim.07.07.02.07

DIGITALIZACIJA U RUSKOJ EKONOMIJI: PREDNOSTI I PRETNJE

DIGITALIZATION IN THE RUSSIAN ECONOMY: ADVANTAGES AND THREATS

Sergej Kirsanov
Ruski državni univerzitet za humanističke nauke (RGGU), Moskva, Rusija

Evgenij Safonov
Ruski državni univerzitet za humanističke nauke (RGGU), Moskva, Rusija

Galina Palamarenko
Ruski državni univerzitet za humanističke nauke (RGGU), Moskva, Rusija

JEL kategorija: **E22, E23, E24, F21, F41, L86**

Apstrakt

Značaj digitalne transformacije kako u poslovanju tako i u čitavim sektorima ekonomije budi sve veće interesovanje za izazove i pretnje, rizike i koristi koji mogu nastati u digitalnoj ekonomiji. U narednim godinama, sva područja vladine aktivnosti i tržišta će se preorijentisati u skladu sa zahtevima novih digitalnih ekonomskih modela. Nemoguće je zaustaviti tranziciju velikih razmera na „digital", jer je korisna za potrošača, korisna za poslovanje, a značajna za vlasti. Vrednost digitalnih rešenja raste, a cena njihovog dobijanja opada. Digitalizacija počinje da prevazilazi promene same tehnologije - postaje makroekonomski i politički faktor. U članku se govori o trenutnom stanju digitalne ekonomije Rusije, o programima finansiranja digitalizacije ekonomije. Rejting zemlje se analizira u skladu sa u međunarodnoj zajednici usvojenim indeksima, koji mere koliko dobro ruska ekonomija koristi digitalne tehnologije za povećanje konkurentnosti i blagostanja. Istovremeno, indeksima se i procenjujue faktori koji utiču na razvoj digitalne ekonomije. Značajno zaostajanje u razvoju digitalne ekonomije Rusije od svetskih lidera objašnjava se nedostatkom regulatornog okvira za digitalizaciju i nedovoljno povoljnim okruženjem za poslovanje i inovacijama i, kao rezultat toga, niskim nivoom primene digitalnih tehnologija u biznisu i vladinim strukturama.

***Ključne reči**: digitalna ekonomija, digitalizacija, digitalne tehnologije, međunarodni indeksi*

Abstract

The urgency of digital transformation, both in business and in entire sectors of the economy, is creating a growing interest in the challenges and threats, risks and benefits that are possible within the digital economy. In the coming years, all areas of state activity, and markets will be refocused in

Adresa autora zaduženog za korespodenciju:
Sergej Kirsanov
ksaimr@mail.ru

accordance with the requirements of new digital economic models. The large-scale transition to the "digital" cannot be stopped because it is valuable for the consumer, profitable for business, and significant for the government. The value of digital solutions is growing and the price of obtaining them is declining. Digitalization is beginning to go far beyond changes in technology itself - it is becoming a macroeconomic and political factor. The article examines the current state of Russia's digital economy and the financing of the program of digitization of the economy. The country's rating is analyzed in accordance with the indices adopted in the international community, which measure how well the Russian economy uses digital technologies to improve competitiveness and well-being, as well as estimate factors influencing the development of the digital economy. The significant lag in the development of Russia's digital economy from world leaders is due to gaps in the regulatory framework for digitalization and a poorly maintained environment for doing business and innovation and, as a result, low levels of digital applications.

Keywords: digital economy, digitalization, digital technologies, international indices

1 KONCEPT DIGITALNE EKONOMIJE

Postoje mnoge definicije digitalne ekonomije koje naglašavaju upotrebu inovativnih digitalnih informacionih i komunikacionih tehnologija; o korišćenju Interneta, mobilnih i senzorskih mreža; o korišćenju savremenih elektronskih komunikacionih kanala, metoda računovodstva i skladištenja informacija; o kreiranju novih poslovnih modela, itd.

Analiza najvažnijih definicija omogućava nam da damo sledeću definiciju. Digitalna ekonomija je sistem društveno-ekonomskih odnosa:

- usmeren na poboljšanje efikasnosti i konkurentnosti privrede;
- izražavanje savremene paradigme ubrzanog ekonomskog razvoja, u kojoj povećavanje konkurentnosti i efikasnosti postaje vitalna potreba;
- koji karakteriše moderne faze evolucijskog razvoja društveno-ekonomskog i proizvodnog modela društva;
- koji pokriva sferu javnog života, proizvodnje, poslovanja, nauke, menadžmenta, domaćinstava i pojedinaca;
- koji odražavaju specifičnosti nove tehnološke generacije,
- sa ciljem stvaranja profita za stvaranje novih industrija, modela upravljanja, novih tržišta i novih potrošača;
- zasnovana na digitalnoj transformaciji i drugima. (Khalin & Chernova, 2018)

U programu razvoja digitalne ekonomije u Rusiji do 2035. godine data je definicija digitalne ekonomije u obliku „ukupnost odnosa koji se razvijaju korišćenjem elektronskih tehnologija, elektronske infrastrukture i usluga, tehnologija za analizu velikih količina podataka i predviđanja radi optimizacije proizvodnje, distribucije, razmene, potrošnje i povećanja nivoa društveno-ekonomskog razvoja država.“ (Pravitel'stvo RF, 2017)

Da bi merila razvoj digitalne ekonomije zemlje, Organizacija za ekonomsku saradnju i razvoj (OECD) razvila je sistem pokazatelja koji karakterišu sledeće oblasti:

- razvoj visokotehnološkog sektora ekonomije, njegovo učešće u proizvodnji proizvoda i usluga;
- ulaganja u istraživanje, razvoj softvera, troškove obrazovanja i dodatnog usavršavanja;
- razvoj i proizvodnja informacione i komunikacione opreme;
- otvaranje novih radnih mesta u nauci i visokim tehnologijama;
- pokazatelji saradnje korporacija, preduzetničkih firmi, univerziteta i istraživačkih organizacija;
- međunarodni tokovi znanja, međunarodna saradnja u oblasti nauke i inovacija; mobilnost naučnika, inženjera, studenata;
- Internet dinamika; udeo visokotehnoloških proizvoda u međunarodnoj trgovini. (Pan'shin, 2016, str. 17)

Razvoj digitalne ekonomije u Rusiji počeo je u decembru 2016. Godine. Dekretom predsednika Ruske Federacije od 9. maja 2017. godine usvojena je „Strategija razvoja informacionog društva u Ruskoj Federaciji za 2017-2030“. Glavni cilj oblasti regulatornog uređenja je formiranje novog regulatornog okruženja koje pruža povoljan pravni režim za nastanak i razvoj savremenih

tehnologija, kao i za sprovođenje ekonomskih aktivnosti vezanih za njihovu upotrebu u digitalnoj ekonomiji. Sve ovo zahteva ne samo promene u određenim regulatornim zakonskim aktima, već, pre svega, izmene i dopune osnovnih zakona o industriji – Građanskog kodeksa, Kodeks rada Ruske Federacije, itd.

Glavne sveobuhvatne digitalne tehnologije za koje je potreban novi regulatorni pravni okvir su kao takve nedavno nastale pojave ekonomskog života kao što su veliki podaci; neurotehnologije i veštačka inteligencija; distribuirani sistemi registra - blockchain; kvantne tehnologije; nove proizvodne tehnologije; industrijski internet stvari; komponente robotike i senzora; bežična tehnologija; tehnologije virtualne i proširene stvarnosti.

Stvaranje informacione infrastrukture jedan je od osnovnih pravaca u razvoju digitalne ekonomije. Glavni ciljevi u vezi sa informacionom infrastrukturom su:

- razvoj komunikacionih mreža koje zadovoljavaju potrebe privrede za prikupljanjem i prenosom podataka od države, privrede i građana, uzimajući u obzir tehničke potrebe digitalnih tehnologija;
- razvoj sistema ruskih centara za obradu podataka, koji osigurava pružanje pristupačnih, stabilnih, sigurnih i isplativih usluga skladištenja i obrade podataka državi, privredi i građanima, uključujući mogućnost izvoza usluga skladištenja i obrade podataka;
- uvođenje platformi za digitalne podatke kako bi se zadovoljile potrebe vlade, preduzeća i građana;
- stvaranje efikasnog sistema za prikupljanje, obradu, skladištenje i pružanje potrošačima prostornih podataka koji zadovoljavaju potrebe države, privrede i građana u relevantnim i pouzdanim informacijama o prostornim objektima – geografski informacioni sistem (GIS).

Pored toga, potrebno je formirati integrisani sistem mera za osiguranje bezbednosti informacione infrastrukture, uključujući njen integritet, dostupnost i održiv rad, koristeći domaće informacione tehnologije i domaće proizvode. (Prezident RF, 2016)

2 POZITIVNE POSLEDICE I IZAZOVI ZA RAZVOJ DIGITALNE EKONOMIJE RUSIJE

Na nivou društva, to uključuje:

- pojave ekonomskog i socijalnog uticaja digitalnih tehnologija na poslovanje i društvo;
- poboljšanje kvaliteta života poboljšanjem zadovoljenja specifičnih potreba ljudi;
- povećanje produktivnosti socijalnog rada;
- pojava novih poslovnih modela i novih oblika poslovanja koji mogu povećati konkurentnost aktivnosti;
- povećanje transparentnosti ekonomskog poslovanja i obezbeđivanje mogućnosti njihovog praćenja;
- obezbeđivanje dostupnosti i promocije robe i usluga itd.

Na nivou kompanije, prednosti digitalizacije mogu se videti u:

- isključenju posrednika: digitalizacija omogućava proizvođačima da na svojim veb lokacijama organizuju prodaju robe ili usluga koje proizvode i dođu do potencijalnih kupaca;
- optimizaciji troškova koja omogućava smanjenje troškova pronalaženja informacija i transakcione troškove; smanjenje troškova za promociju robe i usluga;
- ubrzanju svih poslovnih procesa;
- smanjenju vremena za razvoj proizvoda i usluga i njihovo stavljanje na tržište;
- poboljšanju kvaliteta proizvoda i usluga;
- kreiranju novih proizvoda i usluga.

Tehnološke prednosti digitalizacije uključuju:

- deljenje informacija i nepostojanje konkurencije u upotrebi znanja i informacija;
- nagomilavanje velikih količina podataka, sprovođenje njihove automatske obrade i analize;
- sinhronizacija protoka informacija, mogućnost praćenja velikog broja lanaca između dobavljača i potrošača;
- prelazak na stvaranje novih inovativnih proizvoda;
- prelazak sa papirnih dokumenata na elektronske (bolovanja, radne knjižice itd.). (Khalin & Chernova, 2018)

Za rusku ekonomiju trend digitalizacije povezan je sa ozbiljnim izazovima, jer formiranje digitalne

ekonomije za Rusiju postaje pitanje njene nacionalne sigurnosti i konkurentnosti na svetskom tržištu, kao i pitanje nivoa i kvaliteta života stanovništva zemlje.

Zaostajanje Rusije u tempu digitalizacije u odnosu na druge zemlje može dovesti do promene njene uloge u globalnoj ekonomiji, može ostati uskraćena za perspektivu inovativnog razvoja, što bi moglo da ozbiljno smanji konkurentnost ruske ekonomije na svetskom tržištu.

Među pretnjama od digitalizacije, program „Digitalna ekonomija Ruske Federacije“ identifikuje sledeće probleme (Pravitel'stvo RF, 2017):

- obezbeđivanje ljudskih prava u digitalnom svetu,
- čuvanje digitalnih podataka korisnika,
- obezbeđivanje poverenja građana u digitalno okruženje,
- porast mogućnosti spoljnih informaciono-tehničkih uticaja na informacionu infrastrukturu,
- porast računarskog kriminala,
- zaostajanje za vodećim zemljama u razvoju konkurentskih informacionih tehnologija,
- zavisnost društveno-ekonomskog razvoja od izvoznih politika stranih zemalja,
- neefikasnost naučnog istraživanja,
- nedovoljno osoblje u oblasti informacione sigurnosti.

Važan problem je akutni nedostatak kvalifikovanog osoblja u IKT sektoru. Visoko obrazovanje treba da pruži mladima znanje, kompetencije i veštine koje su tražene u kontekstu digitalizacije ne samo u privredi, već i u društvu u celini. Prema SAP-u i VCIOM-u, na univerzitetima godišnje diplomira 25.000 IT stručnjaka, ali je velika većina poslodavaca u industriji nezadovoljna njihovim niskim nivoom obuke i površnim znanjima. Po trenutnim stopama, godišnji priliv novog osoblja u industriju do 2020. godine iznosiće ne više od 140 000 stručnjaka, umesto potrebnih 700 000. Samo 24% mladih specijalista govori engleski jezik neophodan za rad u globalnoj IT industriji. Istovremeno, samo 9% mladih IT profesionalaca mlađih od 30 godina ne može naći zaposlenje.

Kada se govori o broju IT stručnjaka, može se reći da postoji prognoza kompanije Evans Data, čije podatke prenosi ministarstvo bez reference na izvor. U dokumentu, na primer, stoji da će broj programera u Sjedinjenim Državama do 2018. godine biti oko 4,5 miliona, u Indiji - više od 5 miliona, u Kini - oko 2 miliona. Podaci za Rusiju nisu dati namerno ili zbog zaboravnosti zvaničnika. Ipak, prema proračunima Evans-ovih IT stručnjaka u Rusiji bi u 2018. godini trebalo da bude oko 1,3 miliona. (Goncharova, 2014)

Mogući negativni efekti digitalizacije na rusku ekonomiju uključuju:

- smanjenje ukupnog broja radnih mesta širom zemlje; prelazak na nove trendove u ekonomskom razvoju uvek je praćen padom broja zaposlenih;
- pojava beskrupuloznih korisnika novih usluga čije je pojavljivanje (misli se na usluge) prouzrokovano digitalizacijom;
- digitalna prevara;
- piratstvo i distribucija zlonamernih sadržaja, pomoću kojih (misli se na sadržaje), prema Verianu, se podrazumeva sve što se može digitalizovati. (Varian, 2005)

3 PROCENA DIGITALIZACIJE RUSIJE

Stepen uticaja digitalizacije na ekonomski i društveni život određuje mesto svake zemlje u svetskoj zajednici. Nekoliko pokazatelja se koristi za procenu stepena digitalizacije neke zemlje.

Pokazatelji koji indirektno mere digitalizaciju kao trend uključuju, na primer, Indeks mrežne spremnosti (NRI - Networked Readiness Index) i Globalni indeks inovacija (GII - Global innovation index). NRI - sveobuhvatni indikator razvijen je još 2001. godine, a karakteriše nivo razvoja informacionih i komunikacionih tehnologija (IKT) u različitim zemljama sveta. Za indirektnu procenu trenda digitalizacije koristi se zato što IKT igraju vodeću ulogu u poboljšanju efikasnosti ekonomije i poboljšanju kvaliteta života.

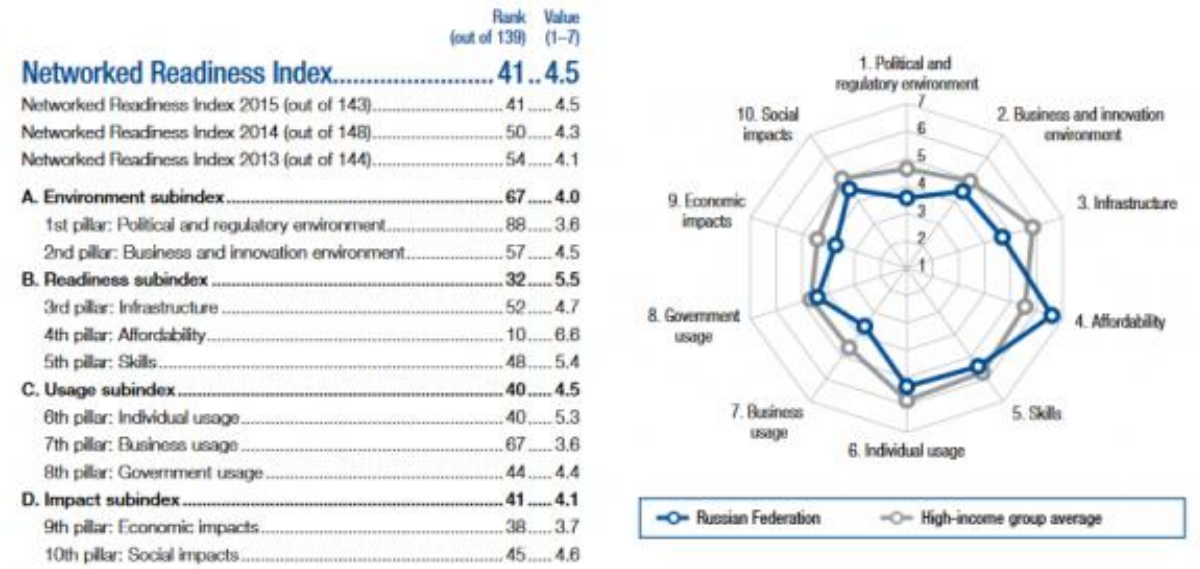
Godišnji rezultati proračuna ovog indeksa predstavljeni su Svetskom ekonomskom forumu u okviru izveštaja „Izveštaj o globalnoj informacionoj tehnologiji“ (The Global Information Technology Report) (World Economic Forum, 2015).

NRI indeks meri nivo razvoja IKT u određenoj zemlji prema 53 parametra, podeljena u 3 grupe: dostupnost uslova za razvoj IKT; spremnost

građana, preduzeća i vlade da koriste IKT; nivo upotrebe IKT-a u društvu, komercijalnom i javnom sektoru. (Khalin & Chernova, 2018)

U skladu sa vrednošću NRI indeksa za 2016. godinu sa velikim zaostatkom iza prvih deset zemalja (Singapur, Finska, Švedska, Norveška, Holandija, SAD, Švajcarska, Velika Britanija, Luksemburg i Japan), Rusija je zauzela 41. mesto na rang listi od 139 zemalja. (Kostyleva, 2016)

Ovaj izveštaj Svetskog ekonomskog foruma primećuje da je ruski napredak u oceni spremnosti mreža ograničen zbog slabog i pogoršanog pravnog okvira (pokazatelj „Političko okruženje i regulacija“, 88. mesto). Ruska pozicija je slaba u pokazateljima kao što su „Efikasnost zakonodavnih tela“ (81 mesto), „Pravosudni sistem“ (81 mesto), „Zaštita intelektualne svojine“ (123 mesto), itd. Rusija je pronašla dobre pozicije u oblastima kao što su „Pristupačnost“ i „Veštine“.



Slika 1. Indeks dostupnosti mreže, Rusija, 2016. (Kostilleva, 2016)

Rusija je generalno dobila 4,5 poena u rangu. Za poređenje, lideri - Singapur, Finska ostvarili su po 6 bodova.

Tabela 1. Deset najboljih lidera rangiranja (Kostilleva, 2016)

Rang	Ekonomija	Vrednost
1	Singapur	6,0
2	Finska	6,0
3	Švedska	5,8
4	Norveška	5,8
5	SAD	5,8
6	Holandija	5,8
7	Švajcarska	5,8
8	Velika Britanija	5,7
9	Luksemburg	5,7
10	Japan	5,6

Drugi indikator korišćen za procenu digitalizacije, Globalni indeks inovacija (GII), karakteriše potencijal inovativne aktivnosti i njen rezultat, služi kao glavna smernica kompanijama i donosiocima odluka da dobiju predstavu o inovativnim procesima koji se dešavaju u svetu. Političari, poslovni lideri i druge zainteresovane strane koriste GII da bi kontinuirano merili napredak. Od 2016. Globalni indeks inovacija izračunava se kao prosek dva podindeksa. *Podindeks Troškovi inovacija* omogućava nam da procenimo elemente nacionalne ekonomije u kojoj se odvijaju inovacijski procesi. Podeljen je u pet glavnih grupa:

1. institucije;
2. ljudski kapital i istraživanje;
3. infrastruktura;
4. nivo razvoja tržišta i
5. nivo razvoja poslovanja.

Podindeks Rezultati inovacija odražava stvarne rezultate takvih napora, podeljenih u dve glavne grupe (PR/2016/793, 2016):

- rezultati znanja i
- tehnologije i kreativni rezultati.

Rusija je zauzela 45. mesto od 127 država po inovativnom razvoju prema Svetskoj organizaciji

za intelektualno vlasništvo (WIPO) i većem broju istraživačkih partnerskih centara. Prva tri mesta u globalnom rangu za 2017. godinu dodeljena su Švajcarskoj, Švedskoj i Holandiji (Rusija je na 45. mestu između Grčke i Čilea). (TASS, 2017)

Navedeni zahtevi digitalizacije kao globalnog trenda u razvoju ekonomije i društva, koji obezbeđuju povećanje njihove efikasnosti i kvaliteta, moraju se uzeti u obzir prilikom procene stepena pokrivenosti digitalizacijom u različitim zemljama. Takav pokazatelj procene stepena pokrivenosti digitalizacijom kao trenda u globalnom razvoju ekonomije i društva predložen je DESI indeksom digitalne ekonomije i društva (Indeks digitalne ekonomije i društva). (EC, 2018)

Indeks digitalizacije ekonomije i društva DESI je agregatni indeks i izračunava se po metodologiji Evropske unije na osnovu vrednosti 5 dimenzija, sastavljenih od poddimenzija koje su definisane 31-nim indikatorom. Vrednosti parametara pokazuju stepen do kojeg država EU ispunjava neki od zahteva trenda digitalizacije, što omogućava da se indeks DESI smatra direktnim pokazateljem uticaja trenda digitalizacije na nacionalnu ekonomiju i društvo određene zemlje.

Ukupna vrednost DESI indeksa, izračunata za određenu zemlju Evropske unije, određuje mesto zemlje i njen rejting u digitalizaciji, a srednja vrednost ovog indeksa za sve zemlje EU daje nivo pokrivenosti digitalizacijom kao globalnim trendom poboljšanja efikasnosti ekonomije i kvaliteta života, svih zemalja EU u celini.

Prema proračunima DESI indeksa za sve zemlje EU, u 2017. Godini, njegova vrednost je porasla za 3% u odnosu na 2016. godinu, međutim, jaz između lidera i zemalja koje zaostaju u digitalizaciji u Evropskoj uniji sada je 37% (36% u 2014.) Ukupnu sliku digitalizacije zemalja cele Evropske unije za 2017. karakterišu sledeći podaci (EC, Digital Economy and Society Index (DESI) 2017, 2017):

- 76% evropskih domaćinstava ima širokopojasni pristup internetu (najmanje 30 Mbps);
- pretplata na mobilni internet u 2017. godini u odnosu na 2013. godinu porasla je sa 58 osoba na 100 ljudi na 84;
- 4 G mobilna usluga pokriva 84% stanovništva Evropske unije;
- broj IKT stručnjaka je 3,5% od ukupnog broja zaposlenih u Evropskoj uniji;
- skoro polovina Evropljana (44%) još uvek nema osnovne digitalne veštine, poput upotrebe poštanskog sandučeta, alata za uređivanje teksta ili instaliranja novih uređaja;
- 79% Evropljana koristi Internet najmanje jednom nedeljno - što je povećanje za 3% u odnosu na 2016. godinu;
- 78% korisnika interneta sluša (preuzima) muziku, gleda filmove, igra se;
- 70% evropskih korisnika Interneta čitalo je vesti na mreži, a u 2013. samo 64%;
- 63% koristi društvene mreže (57% u 2013.);
- 66% koristi Internet na mreži (61% u 2013.);
- 59% koristi online bankarstvo (56% u 2013.);
- 39% koristi Internet za pozive (33% u 2013.);
- 18% evropskih preduzeća šalje elektronske fakture (samo 10% u 2013.);
- 34% korisnika interneta ispunilo je obrasce putem interneta bez izrade papirnih kopija (27% u 2013.).

4 TRENUTNO STANJE DIGITALIZACIJE RUSKE EKONOMIJE

Trenutno stanje digitalizacije ruske ekonomije je sledeće:

- uprkos postojećim teškoćama ruske ekonomije, još uvek postoje perspektive u oblasti digitalizacije ruske ekonomije (softverski proizvodi za kiber-bezbednost, robotika, penetracija interneta u domaćinstva, itd.);
- sve industrije imaju mogućnost digitalne transformacije;
- digitalizacija je lakša za IKT sektore i industrije. Trenutno su najnaprednije u oblasti digitalnih tehnologija usluge, komunikacije, razvoj softvera, telekomunikacije, trgovina, finansijski sektor ekonomije - bankarski i osiguravajući segmenti, medijski biznis, saobraćaj, e-trgovina, automobilska industrija, energetika, e-vlada, stanovanje, građevinarstvo, medicina;
- najniži nivo digitalizacije je u proizvodnom sektoru koji karakteriše velika inertnost proizvodnih preduzeća. (BIT, 2019)

Razvojem digitalne ekonomije Rusija nije uključena u grupu lidera iz više razloga: nivo

digitalizacije, prosečno kašnjenje u savladavanju tehnologija koje se koriste u vodećim zemljama, udeo digitalne ekonomije u bruto domaćem proizvodu (BDP) zemlje. U 2017. godini konsultantska kompanija McKinsei objavila je studiju o ulozi digitalne tehnologije u ruskoj ekonomiji. Izveštaj predstavlja analizu trenutnog stanja razvoja digitalne ekonomije, uključujući industriju, njene perspektive, kao i prognozu uticaja koji će digitalizacija imati na glavna područja života stanovništva i poslovanja. (Aptekman, i drugi, 2017)

Prema procenama kompanija, potencijalni ekonomski efekat digitalizacije ruske ekonomije će povećati BDP zemlje za 4,1-8,9 biliona rubalja do 2025, što će predstavljati 19 do 34 odsto od ukupnog očekivanog rasta BDP. Prema Rosstat-u, u 2016. ukupan BDP u Rusiji je iznosio je oko 86 biliona Rubalja.

Takva smela ekonomska predviđanja povezana su ne samo sa efektom automatizacije postojećih procesa, već i uvođenjem fundamentalno novih, naprednih poslovnih modela i tehnologija. Ovo uključuje digitalne platforme, digitalne ekosisteme, detaljnu analitiku velikih skupova podataka, tehnologije „Industrija 4.0“, kao što su 3D štampanje, robotika, Internet stvari.

Vidljivi su i pozitivni trendovi. Poslednjih godina naglo raste jedan od najvažnijih pokazatelja - obim digitalne ekonomije. Na primer, BDP Rusije je od 2011. do 2015. godine povećan za 7%, a digitalna ekonomija je u istom periodu porasla za 59% - za 1,2 biliona rubalja. To je 8,5 puta brže od rasta ostalih sektora ruske ekonomije.

Težak, ali ostvariv cilj je utrostručivanje digitalne ekonomije sa 3,2 biliona rubalja u 2015. na 9,6 biliona rubalja 2025. godine, što će zahtevati održavanje prosečne godišnje stope rasta digitalne ekonomije na 12%, koja je primećena u periodu 2010-2015. Ovi rezultati biće ekvivalentni povećanju udela digitalne ekonomije sa sadašnjih 3,9% na 8-10% BDP-a (u zavisnosti od cena nafte i drugih makroekonomskih parametara), što u proseku odgovara trenutnom nivou zemalja vodećih u digitalnoj ekonomiji: SAD, Kina i zapadna Evropa.

U ukupnom obimu, najveći udeo digitalne ekonomije zauzima elektronska trgovina koja je u poslednjih nekoliko godina porasla za 35-40%. Najrasprostranjenije su kategorije kućnih aparata i elektronike, nameštaj i pokućstvo, i odeća i obuća. Oni zajedno čine 80% tržišta e-trgovine. Ljudske resurse Runeta čini 2,5 miliona zaposlenih; infrastruktura i softver procenjuju se na 2 biliona rubalja; digitalni sadržaji - 63 milijarde rubalja; marketing i oglašavanje - 171 milijardi rubalja, e-trgovina - 1,2 biliona rubalja.

Rusija već živi u digitalnoj eri: po broju korisnika Interneta ona je na prvom mestu u Evropi i na šestom mestu u svetu. U protekle tri godine imala je dvostruko više pametnih telefona - sada ih ima 60% populacije. To je više nego u Brazilu, Indiji i istočnoj Evropi. A broj korisnika portala državnih i opštinskih usluga udvostručio se za samo godinu 2016. i dostigao 40 miliona ljudi.

U izveštaju Više ekonomske škole „Digitalna ekonomija: globalni trendovi i praksa ruskog poslovanja“ naučnici su sproveli istraživanje među predstavnicima privrednih društava i stručnjacima iz industrije i izmerili dubinu prodora digitalnih tehnologija (KT) u ruski biznis. (Oganesyan, i drugi, 2017) Zaostatak Rusije od vodećih zemalja u oblasti digitalnih tehnologija otkriven je u sledećem:

- *Rasprostranjenost širokopojasnog interneta*. Ruski nivo je 15-20% niži nego u zemljama sa razvijenom IKT infrastrukturom. U većini zemalja EU udeo korisnika širokopojasne mreže prešao je 95%. Izvan Evrope vodeći su Koreja (99%) i Novi Zeland (96%).
- *Prisustvo kompanija na Internetu*. U odnosu na procenat kompanija koje imaju veb stranicu, Rusija je 1,8 puta iza EU (41% u Ruskoj Federaciji i 75% u EU), a po dostupnosti internet kataloga/cenovnika - 2,6 puta (21% i 54%, respektivno).
- Korišćenje e-trgovine od strane kompanija. Nivo u Rusiji je 5–7% niži od proseka u Evropi (24% organizacija kupuje na mreži, a 17% prodaje).
- Onlajn kupovine stanovništva. Zaostajanje za prosečnim evropskim nivoom gotovo je dvostruko: 23% i 55%. Niže stope su samo u Bugarskoj (17%) i Rumuniji (11%).
- Korišćenja ERP sistema (informacioni sistemi za upravljanje resursima preduzeća). Rusija je uporediva sa Mađarskom, Letonijom (16%) i Velikom Britanijom (17%), ali više od tri puta zaostaje za liderima EU - Nemačkom (56%), Belgijom (50%), Danskom (47%).

- Usluge oblaka. Ruski nivo je približno jednak proseku u EU - 21%, sa zaostajanjem za vodećim zemljama - Finskom (57%), Švedskom (48%) i Danskom (42%). Rusija je ispred Francuske i Austrije (po 17%), Nemačke (16%).

Glavne prepreke za implementaciju KT povezane su sa nedostatkom budžeta i visokim troškovima projekata.

Državni program "Digitalna ekonomija", čija je vrednost procenjena na 570 milijardi rubalja (oko 10 milijardi USD) 2024, može se dopuniti novim pravcima. Ruska vlada je napravila predloge za razvoj digitalne medicine i pametnih gradova, uključujući stvaranje mreže centara za telemedicinu i uvođenje bespilotnog javnog prevoza. Samo sredstva za Smart gradove procenjuju se na oko 100 milijardi rubalja. (Novyy, 2018)

5 ZAKLJUČAK

Analiza digitalne transformacije ruske ekonomije i društva potvrdila je da je, u cilju dobijanja dinamičnih rezultata digitalizacije u Rusiji, neophodno:

- takvo upravljanje svim aspektima ekonomskog i društvenog života koje bi osiguralo ispunjavanje uslova digitalizacije kao globalnog trenda efikasnog razvoja ekonomije i društva
- fokusiranje na tehnička rešenja koja će obezbediti potrebnu brzinu inovacija;
- ne samo da ulaže resurse i napor, već i da ih usmerava na prave oblasti razvoja;
- implementacija programa upravljanja digitalizacijom na svim nivoima ekonomskog i društvenog života, čime će se nacionalna ekonomija dovesti na efikasan nivo.

Uz to, uspeh u digitalnoj transformaciji zavisi od izvodljivosti, intenziteta i koherencije javne politike u ovoj oblasti. Za razvoj digitalne ekonomije u Rusiji, čini se relevantnim sledeće:

- otvorenost i dostupnost Interneta stanovništvu zemlje,
- stvaranje institucija koje će pomoći u izgradnji poverenja u digitalne tehnologije;
- aktivno korišćenje novih tehnologija u privredi, u proizvodnji (industrijski roboti, 3-D štampači, blokčejn, Internet tehnologije, itd.);
- stručno osposobljavanje kadrova i podučavanje studenata veštinama i razmišljanju digitalnog sveta;
- poboljšanje pristupa digitalnoj infrastrukturi i smanjivanje nejednakosti;
- razvoj javno-privatne saradnje u oblasti digitalnih inovacija.

Trenutni zadatak vlasti je da harmonizuje i efikasnije modernizuje zakonske propise kako bi se obezbedila konkurencija učesnika na tržištu. Za uspešnu primenu digitalnih tehnologija važna je spremnost investitora da ulažu u dugoročni digitalni razvoj.

Digitalizacija ekonomije ne može se odvojiti od procesa ekonomske globalizacije, jer nijedna država ne može da prosperira u izolaciji. Uobičajeni problemi za mnoge zemlje su otvorenost podataka, uvođenje jednoobraznih standarda, bezbednost mreže, zaštita ličnih informacija, itd. Za rešavanje ovih problema neophodni su saradnja i interakcija svih zemalja sveta. Samo na taj način moguće je stvoriti povoljne uslove za dinamičku digitalnu transformaciju. Potrošači i biznisi, država i društvo očekuju grandiozne rezultate od digitalizacije ekonomije.

CITIRANA DELA

Aptekman, A., Kalabin, V., Klintsov, V., Kuznetsova, Y., Kulagin, V., & Yasenovets, I. (2017, 07). *Tsifrovaya Rossiya: novaya real'nost' .* Preuzeto sa mckinsey: https://www.mckinsey.com/ru/~/media/McKinsey/Locations/Europe%20and%20Middle%20East/Russia/Our%20Insights/Digital%20Russia/Digital-Russia-report.ashx

BIT. (2019, 08 15). *Tsifrovizatsiya ekonomiki.* Preuzeto sa BIT: http://bit.samag.ru/uart/more/67

EC. (2017, 03 05). *Digital Economy and Society Index (DESI) 2017.* Preuzeto sa Information Policy Biz: http://www.infopolicy.biz/?p=9322

EC. (2018). *Digital Economy and Society Index.* Получено из EC Digital Single Market: https://digital-agenda-data.eu/datasets/desi/indicators

Goncharova, O. (2014, 11 24). *Gosudarstvo, planiruya uvelichit' chislo IT-spetsialistov, osoznanno zakryvayet glaza na ikh professionalizm.* Preuzeto sa Vedomosti: https://www.vedomosti.ru/management/articles/2014/11/24/professionaly-idut-lesom

Khalin, V. G., & Chernova, G. V. (2018). *Tsifrovizatsiya i yeye vliyaniye na rossiyskuyu ekonomiku i obshchestvo: preimushchestva, vyzovy, ugrozy i riski/*. Preuzeto sa CyberLeninka: https://cyberleninka.ru/article/n/tsifrovizatsiya-i-ee-vliyanie-na-rossiyskuyu-ekonomiku-i-obschestvo-preimuschestva-vyzovy-ugrozy-i-riski

Kostyleva, T. (07 07 2016 г.). *Rossiya ostalas' na 41 meste v reytinge setevoy gotovnosti Vsemirnogo ekonomicheskogo foruma 2016.* Получено из D-Russia.ru: http://d-russia.ru/rossiya-ostalas-na-41-meste-v-rejtinge-setevoj-gotovnosti-vsemirnogo-ekonomicheskogo-foruma-2016.html

Novyy, V. (2018, 03 07). Ekonomiku dopolnyat novymi tsiframi. *Gazeta "Kommersant"*(40), str. 6. Preuzeto sa https://www.kommersant.ru/doc/3568386

Oganesyan, T., Styrin, Y., Abdrakhmanova, G., Rozmirovich, S., Merkulova, D., & Bikbulatova, Y. (2017). *Tsifrovaya ekonomika: GTsifrovaya ekonomika: global'nyye trendy i praktika rossiyskogo biznesalobal'nyye trendy i praktika rossiyskogo biznesa.* Moskva, RU: Institut menedzhmenta innovatsiy. Preuzeto sa Institut menedzhmenta innovatsiy: https://imi.hse.ru/data/2017/10/06/1159517769/!Цифровая%20экономика%20-%20глобальные%20тренды%20и%20практика%20российского%20бизнеса.pdf

Pan'shin, B. (2016). Tsifrovaya ekonomika: osobennosti i tendentsii razvitiya. *Nauka i innovatsii*(157), 71.

PR/2016/793. (2016, 08 15). *Global Innovation Index 2016: Switzerland, Sweden, UK, U.S., Finland, Singapore Lead; China Joins Top 25.* Preuzeto sa WIPO: https://www.wipo.int/pressroom/en/articles/2016/article_0008.html

Pravitel'stvo RF. (2017). *"Programma" Tsifrovaya ekonomika Rossiyskoy Federatsii" utverzhdena Rasporyazheniyem Pravitel'stva RF ot 28.07.2017 № 1632-r.* Moskva.

Prezident RF. (2016). *Ukaz Prezidenta RF ot 5 dekabrya 2016 g. № 646 "Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii".* Moskva.

TASS. (2017, 06 15). *Rossiya zanyala 45-ye mesto v reytinge samykh innovatsionnykh stran.* Preuzeto sa TASS: http://tass.ru/ekonomika/4337930

Varian, H. R. (2005). Copying and Copyright. *Journal of Economic Perspectives, 19*(2), 121–138. Preuzeto sa https://www.amherst.edu/system/files/media/0657/VarianCopy.pdf

World Economic Forum. (01 04 2015 г.). *The Global Information Technology Report 2015.* Получено из global EDGE: http://www3.weforum.org/docs/WEF_GITR2015.pdf

Datum prve prijave: 22.08.2019.
Datum prijema korigovanog članka: 28.08.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Kirsanov, S., Safonov, E., & Palamarenko, G. (2019, 10 15). Digitalizacija u ruskoj ekonomiji: Prednosti i pretnje. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 59-68. doi:10.12709/fbim.07.07.02.07

*Style – **Chicago** Sixteenth Edition:*

Kirsanov, Sergej, Evgenij Safonov, and Galina Palamarenko. 2019. "Digitalizacija u ruskoj ekonomiji: Prednosti i pretnje." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 59-68. doi:10.12709/fbim.07.07.02.07.

*Style – **GOST** Name Sort:*

Kirsanov Sergej, Safonov Evgenij and Palamarenko Galina Digitalizacija u ruskoj ekonomiji: Prednosti i pretnje [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 59-68.

*Style – **Harvard** Anglia:*

Kirsanov, S., Safonov, E. & Palamarenko, G., 2019. Digitalizacija u ruskoj ekonomiji: Prednosti i pretnje. *FBIM Transactions,* 15 10, 7(2), pp. 59-68.

Style – **ISO 690** Numerical Reference:

Digitalizacija u ruskoj ekonomiji: Prednosti i pretnje. **Kirsanov, Sergej, Safonov, Evgenij and Palamarenko, Galina.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 59-68.

FBIM Transactions
DOI 10.12709/fbim.07.07.02.08

UPRAVLJANJE RIZIKOM – CYBER SIGURNOST

RISK MANAGEMENT - CYBER SECURITY

Branka Mijić
Fakultet za kriminologiju i sigurnosne studije, Sarajevo, Bosna i Hercegovina

JEL kategorija rada: **G32**

Apstrakt

Svjedoci smo velikog utjecaja interneta i informacijske tehnologije na ljudski život . U današnjem vremenu, za koje možemo sa sigurnošću reći da je postalo ovisno o informatičkoj tehnologiji i elektroničkim komunikacijama, poslovni subjekti i fizičke osobe sve više postaju izloženi raznim oblicima cyber napada i kriminala. Informacijsko - tehnološko doba sa sobom nosi određene izazove i rizike. Cyber napadi mogu imati razorne posljedice i velik utjecaj na državne, poslovne subjekte, njihove djelatnike, kupce ali i treće osobe. Takvi napadi i prijetnje danas su među najvećim rizicima s kojima se suočava korporativni sektor u svijetu i stalno se iznalaze neki novi modusi sigurnosti istih kako bi tržištu ponudila modernije i sofisticiranije proizvode koji sadrže pokrića za takve rizike. Upravljanje rizicima je moralna i zakonska obveza svake organizacije i društva. Upravljanje rizicima omogućuje organizaciji jasan pogled na rizike i mogućnost proaktivnog djelovanja u svrhu zaštite resursa i poslovanja organizacije. Cyber sigurnost je u posljednjih nekoliko godina nešto o čemu se napokon počelo više pričati i obraćati veća pozornost, a svjedoci smo sve brojnijih hakerskih napada kao jednog od najvećih izazova sa kojim se suočava menadžment najznačajnijih svjetskih kompanija.

Ključne riječi: *Cyber- sigurnost, cyber-kriminal, cyber-rizik, upravljanje rizikom.*

Abstract

We are witnessing the great impact of the Internet and information technology on human life. Today, we can say with certainty that business entities and individuals are becoming more and more exposed to various forms of cyber-attacks and crime. The information and technology carry certain challenges and risks. Cyber-attacks can have devastating consequences and huge impact on government, businesses subjects, their employees, customers, but also third parties. Such attacks and threats are among the biggest risks facing the corporate sector in the world today, and different modes of Internet and information technology security are used to cover risks. Risk management is a moral and legal obligation of every organization and society. Risk management gives the organization a clear view of the risks and the ability to act proactively to protect the resources and operations of the organization. Cyber security has been something

Adresa autora:
Branka Mijić
brankica_mijic@net.hr

that has finally started to be talked about and paid more attention in recent years, as we are witnessing an increasing number of hacking attacks, which represent one of the biggest challenges for managements of most prominent global companies.

***Keywords**: Cyber security; cybercrime; cyber risk; risk management;*

1 UVOD

Svjedoci smo da se modernizacijom i informatizacijom poslovanja sigurnosni rizik povećava, a kada informacije nisu adekvatno zaštićene postoji mogućnost da to ugrozi ne samo poslovne organizacije nego i cijelo društvo. Bez obzira kakva bila informacija ona je uvijek izložena različitim rizicima iz različitih izvora. Sa stalnim povećanjem korištenja novih tehnologija za pohranu, prijenos i pristup informacijama, informacije su postale mnogo ranjivije na povećan broj i vrstu prijetnji. Bez obzira koju formu ima ili na koji način je pohranjena ili na koji način se dijeli, informacija uvijek treba da bude zaštićena na odgovarajući način.

Prema riječima Roberta S. Mullera, direktora FBI-a koji navodi: „Postoje samo dvije vrste tvrtki: one koje su hakirane i one koje će biti hakirane. Pa čak i one konvergiraju u jednu kategoriju: tvrtke koje su hakirane i one koje će opet biti hakirane“ (Mueller, 2012).

Upravljanje rizicima je moralna i zakonska obveza svake organizacije i društva. Upravljanje rizicima omogućuje organizaciji jasan pogled na rizike i mogućnost pro aktivnog djelovanja u svrhu zaštite resursa i poslovanja organizacije.

Srž programa upravljanja rizikom predstavlja stalni ili tekući proces procjene rizika. Ovo uključuje razumijevanje tolerancije rizika, znanje o vjerojatnim rizicima i prijetnjama, izmjerene procjene uspostavljenih kontrola, i izvršnih planova da bi se adresirale identificirane ranjivosti. Strategija upravljanja rizikom informacija je usmjerena na čuvanje povjerljivosti, održavanje cjelovitosti podataka i osiguranje dostupnosti informacija za korisnike koji imaju odobrenje njihove upotrebe. Efektivan program upravljanja rizikom informacija može biti jedino osiguran kroz marljivost i predanost svake osobe koja ima pristup povjerljivim informacijama. Zajedno sa osobnim integritetom, predanost je jedna od ključnih pretpostavki koja se tiče svake odgovorne osobe unutar organizacije. Pojam osobne odgovornosti je model koji se ima pratiti ukoliko se ima zaista zaštiti informacija. Ključ za pro aktivnu zaštitu je prepoznavanje stvarne dinamike prijetnje. Ona se stalno mijenja i prilagođava naporima da se sačuvaju vitalne informacije (Courtney, Haynes, Paradice, 2005).;

2 SIGURNOSNI RIZIK INFORMACIJA I UPRAVLJANJE RIZIKOM

Prijetnje u oblasti informacijske sigurnosti potječu iz raznih izvora, te se manifestiraju takvim aktivnostima koje su usmjerene na pojedince, poslovne subjekte, nacionalne infrastrukture i vlade. Njihovo djelovanja nosi značajan rizik po opću sigurnost, nacionalnu sigurnost i stabilnost međusobno umrežene međunarodne zajednice (UN General Assembly, 2010).

Ključni rezultati sedmog Allianzovog barometra rizika kojeg svake godine objavljuje u izvješću za 2018. Godinu, a temelji se na uvidu rekordnih 1.911 stručnjaka za rizike iz 80 zemalja. A to je da zastoji u poslovanju i cyber incidenti ostaju na prvom mjestu kao i lani, cyber incidenti su ove godine skočili s trećeg na drugo mjesto i ciljaju na temelje povezanih ekonomija radi čega mogu ugroziti najveće prijetnje globalnog poslovnog rizika, zaključeno je u istraživanju Allianzova barometra rizika 2018. (Allianz Global Corporate & Specialty (AGCS), 2018). Također, procjenjuje se da prosječan trošak ispada digitalnog oblaka koji traje više od 12 sati za tvrtke u financijskom, zdravstvenom i maloprodajnom sektoru može ukupno iznositi 850 milijuna USD u Sjevernoj Americi i 700 milijuna USD u Europi.

Kako bi se smanjili cyber rizici definirani su četiri temeljne aktivnosti (CROForum, 2014):

1. **Priprema** Potrebno je razumjeti svoju kritičnu imovinu; razvijati sposobnosti za rješavanje različitih razina rizika; utvrditi sklonost riziku i upravljanje rizicima ugraditi u cijelu organizaciju.
2. **Zaštita** Osigurati dobro utemeljenu i ponovljivu *cyber*-pripravnost; poduzeti ocjenjivanje prijetnji i kontrola: osigurati odgovarajućom pozornošću provjeru procesa za treće osobe; omogućiti i osnažiti

upravljanje incidentima i sposobnost odgovora; razvijati i provoditi plan odgovora na incident, kontinuirano se obrazovati i usavršavati.

3. **Detekcija** Razviti otkrivanje i kontinuirano praćenje sposobnosti za rješavanje nepravilnosti i prijetnji prema imovini tvrtke.
4. **Poboljšanje** Izgraditi sveobuhvatnu bazu podataka sigurnosnih incidenata koji podržavaju kontinuirano učenje i omogućiti oporavak od incidenta u najkraćemu roku.

3 IZLOŽENOST CYBER RIZIKU

Cyber rizici su još u 2014.godini ušli među deset (10) najvećih globalnih poslovnih rizika. Svjetska ekonomija zbog cyber kriminala i raznih napada godišnje gubi cca 445 milijardi $.

Gubitci koji proizlaze iz cyber napada, nenamjernih ili namjernih IT propusta mogu se kategorizirati u 11 grupa što je prikazano u tablici 1.

Tablica 1. Kategorije gubitaka koji proizlaze iz cyber-napada i nenamjernih IT propusta. (Mersc, 2015).

	KATEGORIJA GUBITKA	OPIS
1.	Krađa intelektualnoga vlasništva	Gubitak vrijednosti imovine intelektualnoga vlasništva, izraženo u smislu gubitka prihoda kao rezultat smanjenoga udjela na tržištu.
2.	Prekid poslovanja	Izgubljena dobit ili drugi troškovi nastali zbog nedostupnosti IT sustava ili podataka kao posljedica *cyber*-napada ili ostalih zlonamjernih IT propusta.
3.	Gubitak podataka i aplikacija	Trošak rekonstrukcije podataka ili softvera koji je izbrisan ili korumpiran.
4.	*Cyber*-iznuda	Trošak stručnjaka za rukovanje incidentom *cyber*-iznude, u kombinaciji s iznosom plaćanja otkupnine.
5.	*Cyber*-kriminal/*cyber*-prijevara	Izravni financijski gubitak koji je pretrpjela organizacija, a koji proizlazi iz korištenja računala za počinjenje prijevare ili krađe novca, vrijednosnih papira ili druge imovine.
6.	Događaj povrede privatnosti	Trošak istraživanja i odgovora na događaj povrede privatnosti, uključujući i IT forenziku i obavještavanje zahvaćenih nositelja podataka. Odgovornosti potraživanja trećih strana koje proizlaze iz istoga incidenta. Kazne od regulatora i udruga.
7.	Mrežne pogreške	Obveze trećih strana koje proizlaze iz nekih sigurnosnih događaja koji se javljaju u organizaciji IT mreže ili prolaze kroz nju da bi napali treću osobu.
8.	Utjecaj na reputaciju	Gubitci prihoda koji proizlaze iz povećanja odljeva kupaca ili smanjenja volumena transakcija, koji se mogu izravno pripisati objavi događaja povrede sigurnosti.
9.	Fizičko oštećenje imovine	Gubitak prve strane zbog uništenja fizičke imovine koji proizlazi iz *cyber*-napada.
10.	Smrt i tjelesna oštećenja	Odgovornost trećih osoba za smrt i tjelesne ozljede proizašle iz *cyber*-napada.
11.	Istraživanje incidenta i troškovi odgovora	Izravni troškovi nastali istraživanjem i zatvaranjem incidenta i smanjivanje gubitaka nakon incidenta. Odnosi se na sve ostale kategorije/događaje.

Povećanje međusobne povezanosti, globalizacija i komercijalizacija cyber-kriminala dovode do veće učestalosti i ozbiljnosti cyber-incidenata, uključujući povrede podataka. Privatnost i zaštita podataka jedan je od ključnih cyber-rizika (European Cybercrime Centre - Europol., 2014).

Prekid poslovanja, krađe intelektualnoga vlasništva i cyber-iznude, bilo za financijsku, bilo za nefinancijsku dobit, povećavaju potencijalni rizik. Troškovi prekida poslovanja mogu biti jednaki ili čak premašiti izravne gubitke od povrede podataka. Utjecaj prekida poslovanja pokrenut tehničkim kvarom često je podcijenjen u odnosu na cyber-napad (Allianz, 2015).

Važno je napomenuti kako velike kompanije i državne tvrtke nisu jedine ranjive na razorne cyber-napade. Podatak je taj koji čini posao atraktivnim, a ne veličina — pogotovo ako je riječ o zanimljivim podatcima, kao što su kontakt-informacije o kupcima, podatci o kreditnim karticama, zdravstveni podatci ili vrijedno intelektualno vlasništvo (Armerding, 2015).

Manje su tvrtke atraktivne jer nemaju iste resurse kao velika poduzeća, stoga imaju tendenciju ka slabijoj strategiji cyber-sigurnosti. Zbog niskih troškova prodaje više posluju online[1] i putem različitih cloud-usluga[2]. Te se tvrtke koriste slabijom sigurnosnom zaštitom i slabijom tehnologijom enkriptiranja, tako da su izloženije riziku.

Danas, kako su rizici i prijetnje postali mnogo sofisticiraniji, javljaju se i dva dodatna temeljna zadatka (Yildirim, 2017):

- definirati ekosistem organizacije,
- predstaviti i uvesti obuku sigurnosne svjesnosti za zaposlenike

Upravljanje rizikom informacijskog sustava neizostavni je dio gotovo svakog okvira upravljanja informacijskom sigurnošću i zaštite osobnih podataka. Kao temelj za donošenje odluka, procjena rizika, a i cijeli proces upravljanja rizikom igra važnu ulogu u postupku implementacije sustava upravljanja informacijskom sigurnošću. Na temelju procjene rizika odabiru se financijski i poslovno opravdane sigurnosne kontrole koje će sigurnosni rizik umanjiti na prihvatljivu razinu.

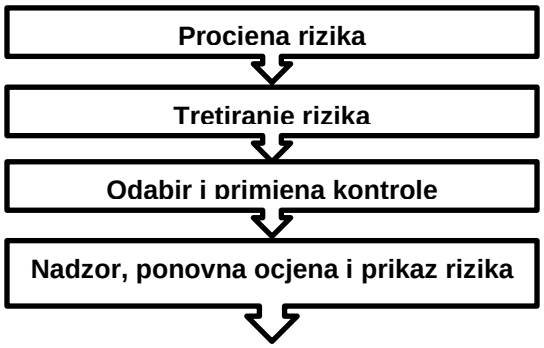
Učinkovito upravljanje rizicima započinje identificiranjem neposrednih rizika za poslovanje te educiranjem odbora i voditelja o tome što ti rizici predstavljaju i čime mogu rezultirati. Svi su odgovorni učinkovito upravljati rizicima. Neovlašteni pristup podacima može uzrokovati ogromnu financijsku štetu i dovesti do narušavanja ugleda. Upravljanje rizicima treba biti dio sveobuhvatnog programa procjene postupaka za upravljanje rizicima, primjene principa za upravljanje rizicima te, u konačnici, osvještavanja zaposlenika u vezi toga kako uočavanje rizika nije neuspjeh, već potvrda dogovorenih postupaka.

Slika 1. Komponente upravljanja rizikom

Izvor (Yildirim, 2017)

Upravljanje rizikom je ključ upravljanja organizacijom i ključ zaštite njenih informacionih kapaciteta. Ukoliko organizacija nije svjesna rizika sa kojima se susreće ona neće biti u stanju primijeniti odgovarajuću efektivnu zaštitu. Proces identifikacija rizika možemo prikazati kako slijedi na slici 2.

Uopćeno, opširna procjena rizika informacione sigurnosti je neophodna da bi se uspostavilo razumijevanje faktora rizika koji štete organizaciji. Dalje, takva procjena mora biti urađena sa uvažavanjem politika zasnovanih na riziku i standardima odsustva upotrebljive statistike o incidentima. Usvajanje procesa rigoroznog pristupa svim rizičnim poveznicama vezanim uz prijetnje informacionoj sigurnosti je ključno u razvoju koherentne strategije sigurnosnog upravljanja rizikom informacija (Young, 2010).



Slika 2. Proces upravljanja rizikom
Izvor: (Humphreys, 2008)

[1] Onlajn-poslovanje - obavljanje poslovnih procesa na internetu. http://searchcio.techtarget.com/definition/e-business,

[2]Cloud-opći termin koji se upotrebljava za pružanje iznajmljenih usluga putem interneta. http://searchcloudcomputing.techtarget.com/definition/cloud-computing

Svi sudionici u procesu, bilo organizacije ili individualne osobe, trebaju provoditi periodične procjene rizika kojima se identificiraju prijetnje i ranjivosti. Procjene rizika trebaju biti dovoljno široko usmjerene kako bi obuhvatile ključne unutarnje i vanjske faktore, kao što su tehnologije, fizički i ljudski faktori, politike i treća strana pružanja usluga. Procjene rizika trebaju omogućiti određivanje prihvatljive razine rizika, te pomoći u odabiru odgovarajućih kontrola za upravljanje rizikom od potencijalne štete informacijskim sistemima i mrežama u svjetlu prirode i važnosti informacija koje trebaju biti zaštićene.

KLJUČNI PRINCIPI UPRAVLJANJA RIZIKOM	PRIMIJENJENI NA KIBER CYBER RIZIK
1. Fokus na ono što je najvažnije Mora se poklapati sa vašom jedinstvenom kulturom posla i rizika	**Poznajete svoje kritične informacione kapacitete.** Identifikacija kritičnih poslovnih kapaciteta najranjivijih na cyber napade
2. Mjerenje i izvještavanje Uključuje kvalitativne obračune i kvantitativna mjerenja	**Učinite cyber napade opipljivijim.** Jasno definirati cyber rizik i osnovne matrice
3. Opširnost u suštini. Treba pokriti sve vrste rizika, trenutne i one koje očekujemo	**Uskladiti sa postojećim okvirima rizika.** Financijskim, operativnim, regulatornim, okvirom potražnje, reputacionim, itd.
4. Raspoređivanje apetita za rizik Raspoređivanje apetita na poslovne jedinice i vrste rizika.	**Učinite cyber rizike relevantnim u skladu s poslom.** Povezati rizike organizacionih nivoa sa individualnim poslovnim jedinicama i njihovim informacionim kapacitetima
5.Integracija sa poslovnim planiranjem Regulacije sve više traže dokaze	**Ugraditi rizične želje u investicione odluke.** Prioritizirati investicije gdje je kritično, ojačati poslove da se informiraju lokalne odluke.

Slika 3. Principi upravljanja rizikom
Izvor: (Carol, Siegel, Serritella, Serritella, 2002)

4 STANDARDI INFORMACIONE SIGURNOSTI (ISO 27001)

Standard ISO 27001 primorava organizacije da pripreme upravljanje rizikom i planove procesuiranja rizika, dužnosti i odgovornosti, planove poslovnog kontinuiteta, upravljačke proceduru u slučaju hitnog stanja i da vode zabilješke o njima. Organizacija, odnosno poduzeće moraju objaviti politike informacione sigurnosti i navesti njihov personal na zaključke o informacionoj sigurnosti i prijetnjama toj sigurnosti. Kao stalan proces, rukovodstvo informacione sigurnosti u organizaciji pokriva odabrane ciljeve kontrole i njihovu procjenu. Prikladnost kontrole njenom cilju i njena učinkovitost se neprestano nadziru i ovo može biti ostvareno jedino aktivnom podrškom rukovodstva i učešćem personala (Vural, Sagıroglu, 2008).

Informacioni sigurnosni standardi moraju biti primijenjeni u svim organizacijama radi upravljanja rizikom na svim nivoima. Ukoliko je upravljanje rizikom dobro rukovođeno, informaciona sigurnost će biti efektivnija. Svi nivoi unutar organizacije trebaju biti uređeni kako slijedi (Saint-Germain, 2005):

- Na organizacionom nivou, određuje odgovornosti i garantirane koristi od primjene poduzetničke/organizacijske informacione sigurnosti na svakom nivou.
- Na pravnom nivou, pokazuje vlastima da je poduzeće ili organizacija prihvatila sva važeća pravila i regulative i da ispunjava sve standarde i principe.
- Na poduzetničkom nivou, upućuje poduzetništvo na informacione sisteme, na njihove slabosti i kako će biti zaštićeni, pa se na taj način osigurava siguran pristup za informacioni sistem poduzetnika

- Na komercijalnom nivou, poslovni partneri, dioničari i kupci podižu stepen svog povjerenja prema poduzetniku; zahvaljujući važnosti koju je poduzetnik dao zaštiti informacija postiže se bolja pozicija na tržištu i povećava se konkurentnost.
- Na financijskom nivou, kao posljedica identificiranja sigurnosnih propusta (rupa) i poduzimanje mjera za njihovo saniranje, troškovi će se smanjiti.
- Na zaposleničkom nivou, povećava se znanje zaposlenika u sigurnosnim subjektima i njihove lične odgovornosti unutar organizacije i doprinosi tome da svaki zaposlenik bude svjesna jedinka.

5 DISKUSIJA

Sve organizacije ili institucije su izložene riziku, i najveći broj njih ima neku vrstu upravljanja rizikom. Ipak, ukoliko nastojimo točno razumjeti vrste i prirodu rizika, te ukoliko hoćemo da ih uredimo na sistematičan i efektivan način, trebamo dobro definiran proces za upravljanje rizikom. Nadalje, trebamo da razumijemo osnovne principe i okvire vezane uz proces upravljanja rizikom (Refsdal, Solhaug, Stølen, 2015).

Obzirom da možemo pretpostaviti da organizacije ne mogu prevenirati sve incidente, tradicionalna disciplina sigurnosti, izdvojena iz opširnijeg pristupa baziranom na riziku, nije dovoljna da se zaštiti od prijetnji. Unapređujući informaciono upravljanje rizikom ne znači uvijek trošenje više novca, te podjednako tome ne znači ni samo kupovinu posjednih tehnologija i alata upravljanja rizikom. Da bi bio efektivan, program upravljanja rizikom zahtijeva efektivno menadžersko znanje i sposobnosti, prosudbe i donošenje odluka što sve zajedno predstavlja pokretače uspješne dinamike sistema upravljanja rizikom. Sistemski faktori kao što je procijenjeni rizik od strane menadžmenta, željeni nivoi investicije upravljanja rizikom, kapaciteti detekcije rizika i povjerenje personala su u dinamičnoj interakciji i mogu stvoriti povratne sprege koje ili ojačavaju kapacitete smanjenja rizika ili proizvode i izlažu organizaciju unutrašnjim prijetnjama. Smanjenje takve ranjivosti na napade od unutrašnjih prijetnji uključuje unapređenje prikupljanje informacija o riziku, upravljanje takvim informacijama i ciljanu obuku personala u prosudbama i donošenju odluka (Martinez-Moyano, 2006). Uopćeno, opširna procjena informacionog sigurnosnog rizika je neophodna da bi se uspostavilo razumijevanje faktora rizika koji štete organizaciji. Dalje, takva procjena mora biti urađena u odnosu na standarde i politike koje su donesene po osnovu procijenjenih rizika uz odsustvo iskoristivih statistika o incidentima. Usvajajući proces rigoroznog pristupa rizik povezan sa sigurnosnom prijetnjom informacijama je ključan da bi se razvila konherentna strategija upravljanja rizikom kod sigurnosti informacija (Young, 2014). Efektivan proces unapređuje organizacijske sposobnosti u odnosu na suradnju sa vanjskim partnerima. Informaciona sigurnost osiguravajućih kompanija je, npr., je značajno i naglo porasla i postala sofisticiranija obzirom na njihove zahtijeva u kojima osiguravajuće kompanije, da bi bile profitabilne, zahtijevaju od svojih klijenata koji su pravna lica da im dostave svoje programe menadžmenta upravljanja rizikom. Osiguravatelji tako kreiraju izuzetke za pokriće na rizična ponašanja. Dodatno, rad za treće osobe kao pružač usluga, ili čak dolazak u priliku da se postane stalni suradnik, i sl. postaje mnogo lakše ukoliko se posjeduje utemeljen proces cyber sigurnosti. Praktično, danas svaki sporazum koji rezultira dobrom poslovnom transakcijom ima bitne zahtjeve vezane za predstavljanje i aktivnost informacione sigurnosti. Ovo pitanje se često previđa od strane kompanije sve dok dogovor ne postane konačan i kada jedna strana u svojoj predanosti poslu ne shvati da je druga strana zanemarila cyber sigurnost i da ih tim izlaže velikom riziku. Ovakav ishod je velika tragedija u vremenu kada je većina strategija start up kompanija vezana za ovo pitanje da ih kupe velike kompanije (Miller, 2011). Studija EY Globalne informacione sigurnosti iz 2015. godine, koja je ujedno jedna od najpriznatijih studija na godišnjem nivou unutar globalne informaciono-sigurnosne arene, istraživala je kreiranje povjerenja u svijetu digitalne sigurnosti, te ujedno i najvažnija pitanje cyber sigurnosti s kojima se susreću poslovi današnjice (Ernst, Young, 2015). Kao rezultat, ona pomaže kupcima da se fokusiraju na rizike koji identificiraju prednosti i manjkavosti njihovog informacionog sistema upravljanja rizikom i da daju analizu glede ovog pitanja. Jedno pitanje postavljeno u istraživanju kako bi se naglasila efektivnost informacione sigurnosti je bilo sljedeće: „Koju bi od pobrojanih

područja iz informacione sigurnosti definirali kao „važnu, srednje važnu ili nisku“ za vašu organizaciju, a u narednih 12 mjeseci? Rezultati su pokazali da su unutrašnji rizici i prijetnje odnijeli polovinu odgovora „srednje važno“ (Ernst, Young, 2015). Prema Deloitte (2014) „istraživanje informacione sigurnosti“ u Centralnoj Aziji ima tendenciju povećanja nivoa razumijevanja informacionih sigurnosnih programa i rukovodne strukture u organizaciji. Njihovo istraživanje se fokusiralo na informacione sigurnosne rizike u oko stotinu kompanija kroz online anketni upitnik. Rezultati su pokazali da su IT sektori kompanija svjesni sigurnosnih rizika vezanih uz informacije, dok je svijest poslovnog rukovodstva i krajnjih korisnika na niskom nivou, odnosno nedovoljna (Yildirim, 2016). Također, istraživanje je pokazalo da je svjesnost rizika na cyber prijetnje od strane IT odjela najviše proizvod javno dostupnih informacija. Pored toga, generalni je zaključak da se mnoge organizacije još uvijek muče da dostignu strateški nivo informacione sigurnosti. Ljudski faktor ostaje najslabija karika u cyber sigurnosti. Mnoge organizacije su nevoljne da iz vanjskih izvora potraže pomoć u aktivnostima zaštite informacija (Yildirim, 2017).

6 ZAKLJUČAK

Ovim radom se željelo prikazati osnove za uspostavu i zaštitu informacijskog sustava. Činjenica je da uvijek postoji mogućnost za opasnosti sustava pogotovo u suvremenom poslovanju pa stoga organizacije moraju biti toga svjesne i spremne na reakciju protiv mogućih prijetnji. Svjedoci smo da modernizacijom i informatizacijom poslovanja sigurnosni rizik se povećava, a kada informacije nisu adekvatno zaštićene postoji mogućnost da to ugrozi ne samo poslovne organizacije nego i cijelo društvo.

Zanemarimo li sustav informacijske sigurnosti, u smislu ne kontroliranja problema sigurnosti, vrlo lako možemo postati žrtvom napada. Sigurnosti sustava bi trebali pristupiti periodičnom kontroliranju, tražiti načine kako sustav učiniti još sigurnijim, otpornijim te implementirati dodatne sigurnosne kontrole koje savjetuju stručnjaci za informacijsku sigurnost. Nadalje, smo pokušali prikazati potencijalne gubitke koji proizlaze iz cyber napada. Poanta je da poslovne aktivnosti moraju biti zaštićene sa efektivnim sistemom upravljanja rizikom i da se ovaj sistem mora primjenjivati u ozbiljnom poslovanju, a prema standardu ISO 27001, a što je najvažnije da mora sve mora biti pokriveno zakonskim propisima.

Bitno je da se unutar poslovanja primjene ISMS standardi, da budu objašnjeni svim strankama u poslovanju, te da se uposle stručnjaci iz polja sigurnosti u aktivnosti poduzeća ili organizacije. Neophodnost upravljanja rizikom u cyber sigurnosti se odnosi i na obuku korisnika, tehničkog personala i menadžera ili uopćavanja savjetodavnih servisa. Nakon što su ISMS aplikacije primijenjene uspješno od strane poduzetnika, važno je da poduzetnici imaju međunarodno priznat certifikat za upravljanje informacionom sigurnošću (Yildirim, 2016). Aplikacijska sigurnost je proces koji se obavlja kako bi se primijenile odgovarajuće kontrole i mjerenja na organizacijske aplikacije, a s ciljem upravljanja rizikom njihovog korištenja. Kontrole i mjerenja mogu se primijeniti na samu aplikaciju (njene procese, komponente, softver i rezultate), na njene podatke (konfiguracijske podatke, korisničke podatke, organizacijske podatke), te na sve tehnologije, procese i aktere uključene u životni ciklus aplikacije.

Da bi omogućio visok nivo cyber sigurnosti u poduzeću, vrlo je važno razumijevanje i primjena standarda informacione sigurnosti kao i poznavanje trenutnih prijetnji. Pokazalo se, da bi se omogućio visok nivo cyber sigurnosti, da je neophodan pristup u trokutu tehnologija-čovjek-edukacija i da se on uvijek mora prvi razmatrati. Neophodno je za poduzetnike da se primjeni upravljanje rizikom u cyber sigurnosti u svrhu minimiziranja nivoa rizika i povećanja sigurnosti, te omogućavanja poslovnog kontinuiteta.

CITIRANA DELA

Allianz Global Corporate &Security (2015). *A Guide to Cyber Risk, Managing the Impact of Increasing Interconnectivity*, Editor: Greg Dobie (greg.dobie@allianz.com). https://www.agcs.allianz.com/news-and-insights/reports/a-guide-to-cyber-risk.html

Armerding, T. (2015). *Why criminals pick on small business*. http://www.csoonline.com/article/2866911/cyber-attacks-espionage/ why-criminals-pick-on-small-business.html

Carol A. Siegel, T. R., Serritella, S., Serritella, P. (2002). *Information Security Management Practices, Cyber-Risk Management:Technical and Insurance Controls for Enterprise-Level Security*, EBSCO,

Courtney, J. F., Haynes, J.D. , Paradice, B. D. (2005). Inquiring Organizations: Moving from Knowledge Management to Wisdom. England: Idea Group Inc (IGI),

CROForum (2014). „Cyber Resilience-The cyber risk challenge and the role of insurance", KPMG Advisory N.V. http://www.munichre.com/site/corporate/get/ ocuments_E-558890045/ mr/assetpool. shared/Documents/0_Corporate%20Website/1_The%20Group/Emerging-Risks/CRO-Forum-cyber -risk-paper -2014-12.pdf

Deloitte. (2016). Information Security Survey Report 2014,

Ernst & Young. EY's Global İnformation security Survey Report 2015: Creating trust in the digital world. (2016) http://www.ey.com/Publication/vwLUAssets/ey-globalinformation-security-survey-2015/$FILE/ey-globalinformation-security-survey-2015.pdf

European Cybercrime Centre (EC3) - Europol (2014). „The Internet Organised Crime Threat Assesment (iOCTA) ". file:///Users/Air/ Downloads/europol_iocta_web.pdf

Humphreys, E. (2008). Information Security Technical Report, Elsevier, "Information Security Management Standards: Compliance, Governance and Risk Management",

Martinez-Moyano, I. J. (2006). *Modeling the Emergence of Insider Threat*

Vulnerabilities. Proceedings of the 2006 Winter Simulation Conference,

Miller, K. L. (2016). *About "Reasonable Cybersecurity: A Proactive and Adaptive Approach*. The Florida Bar Journal/September/October, vol. 90,

Mueller, R., S.(2012). FBI Director speech on RSA Cyber Security Conference, San Fracisko, CA. http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

Refsdal, A., Solhaug, B., Stølen, K. (2015). *Cyber-Risk Management*. SpringerBriefs in Computer Science,

Saint-Germain, R. (2005). *Information Security Management Best Practice Based on ISO/IEC 17799*.The Information Management Journal, vol. 39,

Sutton, D. (2010). *Information Risk Management a Practitioner's Guide*. Bcs the Chartered Institute for IT,

UN General Assembly. (2010). *A/65/201 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*.

Vural, Y., Sagıroglu, S. (2008). *A Review on Enterprise Information Security and Standarts*. J. Fac. Eng. Arch., Gazi Univ., Vol. 23,

Yildirim, E. Y. (2016). *Advances in Human Factors in Cybersecurity*. The Importance of Information Security Awareness for the Success of Business Enterprises, vol.501, Springer, USA,

Yildirim, E. Y. (2017). *The importance of risk management in information security.* International Journal of Advances in Electronics and Computer Science, Vol. 4, Issue 1,

Yildirim, E. Y. Akalp, G,. Aytac, S., Bayram, N. (2011). *Factors Influencing Information Security Management in Small and Medium-sized Enterprises:A Case Study from Turkey*. International Journal of Information Management, Elsevier,

Young, C. (2010). *Metrics and Methods for Security Risk Management*. Boston, Yngres,

Young, C. (2014). *The science and technology of counterterrorism; measuring physical and electronic security risk*.

Datum prve prijave: 16.08.2019.
Datum prijema korigovanog članka: 02.09.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

Style – APA Sixth Edition:

Mijić, B. (2019, 10 15). Upravljanje rizikom – Cyber sigurnost. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 69-77. doi:10.12709/fbim.07.07.02.08

Style – Chicago Sixteenth Edition:

Mijić, Branka. 2019. "Upravljanje rizikom – Cyber sigurnost." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 69-77. doi:10.12709/fbim.07.07.02.08.

Style – GOST Name Sort:

Mijić Branka Upravljanje rizikom – Cyber sigurnost [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 69-77.

Style – Harvard Anglia:

Mijić, B., 2019. Upravljanje rizikom – Cyber sigurnost. *FBIM Transactions,* 15 10, 7(2), pp. 69-77.

Style – ISO 690 Numerical Reference:

Upravljanje rizikom – Cyber sigurnost. **Mijić, Branka**. [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 69-77.

FBIM Transactions
DOI 10.12709/fbim.07.07.02.09

RAČUNARSKA SABOTAŽA

COMPUTER SABOTAGE

Živanka Miladinović Bogavac
Poslovni i pravni fakultet, Univerzitet „Union - Nikola Tesla“, Beograd, Srbija

JEL kategorija rada: **D82, G32, L86**

Apstrakt

Sve je veća zainteresovanost pravnika vezano za kompjuterski kriminal, takozvani sajber kriminal. Pošto se on sve više razvija sa razvojem inovativnosti u oblasti informacionih tehnologija, neophodne su zakonodavne mere koje će ovu vrstu kriminala regulisati i sankcionisati. Kao učestalo krivično delo, danas se pojavljuje računarska sabotaža, koja je inkriminisana krivičnim zakonodavstvom Republike Srbije. Pošto je ona Krivičnim zakonikom veoma uopšteno određena, neophodno je odrediti sam pojam računarske sabotaže, kao i njene vrste, odnosno neophodno je predstaviti neke od mnogobrojnih mogućnosti za izvršenje ovog krivičnog dela. Međunarodnopravna regulativa je od velikog značaja zbog toga što se radi o krivičnom delu gde učinioci mogu biti iz različitih zemalja i tako udruženo delovati. Međunarodna Konvencija o visokotehnološkom kriminalu je definisala pojmove koji su od značaja za određivanje pojma računarske sabotaže. Svakako, računarska sabotaža i ostala krivična dela sajber kriminala se međusobno prožimaju, te je potrebno dovesti ih u vezu, uporediti sličnosti i razlike i analizirati u kom odnosu stoje. Od naročitog značaja je razgraničiti računarsku sabotažu i sajber terorizam koji predstavlja jednu od većih opasnosti u svetu računara, računarskih mreža, interneta i društvenih mreža. S obzirom na to da je danas nemoguće funkcionisati ni za pojedinca ni za državu bez upotrebe računara i savremenih tehnologija, važna je činjenica da je sve razvijenija svest o opasnosti istih, te je stoga neophodno da države preduzmu značajne korake ka regulisanju računarske sabotaže i ostalih opasnih radnji koje se vrše putem računarske tehnologije.

Ključne reči: *računarska sabotaža, visokotehnološki kriminal, zloupotreba računara, zaštita računara, zaštita u računarskim mrežama*

Abstract

There is a growing interest among lawyers in computer crime, otherwise known as cyber-crime. Since it is increasingly developing together with the development of innovations in the field of information technologies, legislative measures are necessary to regulate and sanction this type of crime. Nowadays, computer sabotage appears as a frequent criminal offense, which is incriminated by the Criminal Legislation of the Republic of Serbia. Since it is very generally defined by the Criminal Code, it is necessary to determine the very notion of computer sabotage as well as its types, i.e. it is necessary to present some of the many possibilities for the execution of this crime. International legal

Adresa autora
Živanka Miladinović Bogavac
zivankamiladinovic@gmail.com

regulation is of great importance because the criminal offense in question is the one where the perpetrators may be from different countries and thus work together. The International Convention on Cyber Crime defined terms that are important for determining the concept of computer sabotage. Certainly, computer sabotage and other criminal acts of cybercrime are mutually intertwined, and it is necessary to connect them, compare the similarities and differences and analyze in what relation they stand to each other. It is of particular importance to distinguish computer sabotage from cyber terrorism, which is one of the biggest dangers in the world of computers, computer networks, the internet, and social networks. Given that nowadays it is impossible for an individual or a country to function without the use of computers and modern technologies, it is important that the awareness about the danger of those above-mentioned spreads, and it is, therefore, necessary that countries take significant steps towards regulating computer sabotage and other dangerous activities that are carried out through computer technology.

Keywords: *computer sabotage, cyber crime, computer misuse, computer protection, computer network defense*

1 POJAM I TEORIJSKO ODREĐENJE RAČUNARSKE SABOTAŽE

Kako bi odredili pojam i teorijsko određenje računarske sabotaže, prvo treba da je kategorizujemo pod koju vrstu kriminaliteta ona potpada. Radi se, dakle, o kompjuterskom kriminalitetu, odnosno kako je pravilnije reći u našem jeziku, o računarskom kriminalitetu. Krivična dela u okviru ove vrste su takozvana kompjuterska krivična dela, tj. dela koja su usmerena protiv bezbednosti podataka u savremenim informatičkim sistemima. Pod kompjuterskim kriminalom obično se podrazumeva kriminalitet koji angažuje kompjuter kao sredstvoili kao cilj izvršenja krivičnih dela. (Lilić & Prlja, 2008, str. 85)

U literaturi je prisutno mišljenje da kriminal u vezi s kompjuterima nije samo još jedan oblik običnog kriminala, već je to opšti vid svih oblika kriminala. U krajnjoj liniji ovaj oblik će postati dominantna varijanta, tako da će kako nenasilni, tako i nasilni kriminal biti vezan za kompjutere. Iz tih razloga, ubuduće neće biti korisno razdvajati nekompjuterski od kompjuterskog kriminala“. (Parker, 1981, str. 10)

Ukoliko u obzir uzmemo podelu kompjuterskog kriminala prema načinu izvršenja na kopjuterski kriminal izvršen putem socijalnog inžinjeringa, malicioznim programima ili kombinovanom metodom, možemo zaključiti da računarska sabotaža podpada pod 2 i 3 vrstu kompjuterskog kriminala. (Miladinović Bogavac, Models of commiting cyber criminal offences, 2018)

Računarska sabotaža kao jedno od kompjuterskih krivičnih dela, već iz naziva upućuje šta ona predstavlja u kriminalnom svetu. Reč „sabotaža“ znači namerno, ilegalno izvedeno kvarenje ili uništavanje dobara radi nanošenja štete i izazivanja haosa. (Jezikoslovac, 2018) Reč vodi poreklo iz francuskog jezika –,,*sabotage*”,što u bukvalnom smislu znači „pravljenje drvenih cipela“ (Vokabular, 2006), aludirajućina to da su u revolucionarnoj Skupštini zastupnici sabotirali govore lupajući cipelama. (Jezikoslovac, 2018)

Na osnovu člana 299 Krivičnog zakonika Republike Srbije (2014, str. član 299), možemo zaključiti da je računarska sabotaža u našem pravu određena kao unošenje, uništenje, brisanje, izmena, oštećenje, prikrivanje ili na drugi način činjenje neupotrebljivim računarskog podatka ili programa ili uništenje ili oštećenje računara ili drugog uređaja za elektronsku obradu i prenos podataka sa namerom da se onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte.

Kada dovedemo u vezu zakonski opis ovog krivičnog dela i etimologiju reči „sabotaža“, dolazimo do zaključka da računarska sabotaža znači upravo namerno ilegalno kvarenje ili uništavanje računara ili onoga što je u vezi sa tim (računarski podatak, program i drugi uređaj za elektronsku obradu i prenos podataka), radi nanošenja neke štete zakonom navedenim subjektima.

Kao primer ovog krivičnog dela možemo uzeti slučaj iz 2007. godine kada je radnik na svemirskom programu američke svemirske

agencije NASA namerno oštetio računar koji je trebalo da bude isporučen na međunarodnu svemirsku stanicu šatlom Endevor, tako što je presekao žice unutar kompjutera koji je trebalo da bude dostavljen. (Gerstenmajer, 2007)

Za krivično delo računarske sabotaže značajan je subjektivni element postojanja namere da se onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za subjekte navedene u zakonskom opisu krivičnog dela. Dakle, delo se može učiniti samo uz postojanje direktnog umišljaja, s obzirom na postojanje namere. Delo je dovršeno preduzimanjem radnje izvršenja, a objekt radnje su računarski podatak ili program.

U zakonskom tekstu mogu se uočiti dva oblika izvršenja ovog krivičnog dela:

1. unošenje, uništenje, brisanje, izmena, oštećenje, prikrivanje ili na drugi način činjenje neupotrebljivim računarskog podatka ili programa.
2. uništenje ili oštećenje računara ili drugog uređaja za elektronsku obradu i prenos podataka.

Prvi oblik ovog krivičnog dela je usmeren na računarski podatak ili program.

Prema Zakonu o izmenama i dopunama Krivičnog zakonika, 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 program obavlja svoju funkciju. Krivični zakonik definiše šta je to računarski program. Njime se smatra uređeni skup naredbi koje služe za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara. Kod prvog oblika krivičnog dela računarske sabotaže radnja izvršenja je postavljena alternativno. Ona može da se sastoji u uništenju, brisanju, izmeni, oštećenju ili prikrivanju računarskog podatka ili programa. (Zakon o izmenama i dopunama Krivičnog zakonika, 2009)

Drugi oblik računarske sabotaže kao objekat ima računar ili drugi uređaj za elektronsku obradu i prenos podataka.

Radnja izvršenja kod drugog oblika je takođe postavljena alternativno i može se sastojati u uništenju ili oštećenju računara ili drugog uređaja za elektronsku obradu i prenos podataka sa namerom da se onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove preduzeća ili druge subjekte.Pod uništenjem računara ili drugog uređaja za elektronsku obradu i prenos podataka treba razumeti potpuno menjanje njihovih svojstava u negativnom smislu, tako da oni faktički više i ne postoje, a pod oštećenjem takvo menjanje njihovih svojstava u negativnom smislu koje umanjuje mogućnosti njihove dalje upotrebe u svrhu kojoj su namenjeni. (Stojanović & Perić, 2009, str. 253-254)

Drugi oblik dela je dovršen takođe preduzimanjem radnje izvršenja, uz postojanje navedene namere koja u ovom slučaju i ne mora biti realizovana. S obzirom na nameru, delo se može izvršiti samo sa direktnim umišljajem. Objekt radnje predstavljaju računar ili drugi računarski uređaj za elektronsku obradu podataka. Prema Zakonu o izmenama i dopunama Krivičnog zakonika, računar je svaki elektronski uređaj koji na osnovu programa automatski obrađuje i razmenjuje podatke. (2009, str. član 25)

Kao sredstvo izvršenja dela računarske sabotaže se koriste štetni softveri ”malware“ koji se mogu klasifikovati na:

- viruse
- tzv. „trojanski konj”
- crve
- bombe i dropere
- veb – preotimanje
- steganografiju. (Vestbi, 2004, str. 46-47)

Zlonamerni programi se mogu klasifikovati i po kriterijumu samostalnosti tj. potrebe za programom u kom će maliciozan program biti sakriven na:

1. one kojima je neophodan nosilac, tj. program u koji će biti sakriveni (trojanski konj, virusi); i
2. samostalne, kojima nije neophodan nosilac, koji nezavisno deluju (crvi) (Miladinović Bogavac, 2017)

2 PRAVNA REGULATIVA RAČUNARSKE SABOTAŽE

Pravnu regulativu visokotehnološkog kriminaliteta, i u tom smislu i računarske sabotaže možemo gledati kroz međunarodnopravne propise i kroz propise domaćeg zakonodavstva. Treba imati na

umu da je domaće zakonodavstvo usklađeno uvek sa međunarodim načelima, jer ratifikacijom međunarodnih konvencija, Republika Srbija se obavezuje da određene oblike, u ovom slučaju pojavne oblike visokotehnološkog kriminaliteta, inkriminiše u svom pozitivnom zakonodavstvu.

23. novembra 2001. godine Savet Evrope je doneo Konvenciju o visokotehnološkom kriminalu (takozvana Konvencija o sajber kriminalitetu) u Budimpešti u originalu na engleskom i francuskom jeziku. Ubrzo, naša zemlja je posebnim zakonom potvrdila ovu Konvenciju. U preambuli Konvencije (Skupština Srbije, 2009) se ukazuje na neophodnost međunarodne saradnje u ovoj oblasti krivičnog prava „s obzirom na duboke promene koje je donela digitalizacija, konvergencija i stalna globalizacija računarskih mreža“. Takođe, ističe se da su zemlje potpisnice zabrinute zbog rizika da se računarske mreže i elektronske informacije mogu koristiti i za izvršenje krivičnih dela i da dokazi koji se odnose na takva dela mogu biti sačuvani i preneseni preko tih mreža.

Ovom konvencijom su definisani pojmovi poput računarskog sistema, računarskog podatka, davaoca usluge, podatka o saobraćaju.

Drugi deo Konvencije koji se odnosi na procesne odredbe sadrži odeljak 2 (Skupština Srbije, 2009, str. član 16, stavovi 1-2) koji je posvećen isključivo hitnoj zaštiti sačuvanih računarskih podataka, koja nalazi primenu i u slučajevima računarske sabotaže. Svaka strana ugovornica treba da usvoji zakonodavne i druge mere, neophodne da bi svoje nadležne organe ovlastila da mogu da narede ili na sličan način postignu hitnu zaštitu određenih računarskih podataka, uključujući tu i podatke o saobraćaju koji su sačuvani preko računarskog sistema, a posebno u slučaju kada ima osnova da se veruje da su podaci naročio podložni gubitku ili izmeni. Nalaže se strani ugovornici da usvoji zakonodavne i druge mere neophodne da se to lice obaveže da štiti i sačuva celovitost tih računarskih podataka za neophodan vremenski period, a najviše do 90 dana, kako bi se nadležnim organima omogućilo da zahtevaju njihovo razotkrivanje .

Računarska sabotaža, samim tim što se vrši preko računara, korišćenjem interneta ili na neki drugi način, ima elemente međunrodnog krivičnog dela, jer učinilac ili grupa učinilaca mogu imati boravište ili prebivalište u različitim državama, pri čemu s obzirom na nadležnosti svake države, može biti komplikovano doći do potencijalnih izvršilaca krivičnog dela. Zato je međunarodna saradnja od velikog značaja kod ovog dela, pa i kod ostalih sajber krivičnih dela. Konvencijom se predviđa da strane ugovornice međusobno sarađuju u najširem mogućem obimu, kroz primenu odgovarajućih međunarodnih instrumenata o međunarodnoj saradnji u krivičnim stvarima, dogovora usaglašenih na osnovu jednoobraznih ili recipročnih propisa, u svrhu istraga ili postupaka koji se odnose na krivična dela u vezi sa računarskim sistemima i podacima ili u svrhu prikupljanja dokaza u elektronskom obliku o krivičnom delu. (Skupština Srbije, 2009, str. član 23)

Računarska sabotaža je u srpskom zakonodavstvu inkriminisana u Krivičnom zakoniku RS, kao krivično delo protiv bezbednosti računarskih podataka i to u članu 299.Kako zaključujuStojanović-Perić, ovim krivičnim delom se pruža zaštita elektronskim sistemima i mrežama za elektronsku obradu i prenos podataka koji imaju poseban društveni značaj. (Stojanović & Perić, 2009, str. 253) Taj društveni značaj je upravo ono što se može postaviti kao specifičnost ovog dela u odnosu na druga kompjuterska krivična dela. Računarska sabotaža se vrši u cilju da se onemogući ili znatnoomete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte.

Predviđena sankcija za ovo krivično delo je kazna zatvora od šest meseci do pet godina.

Zakonodavac je odredio osnovni oblik ovog krivičnog dela, izostavljajući njegove privilegujuće ili kvalifikovane oblike.

3 ODNOS RAČUNARSKE SABOTAŽE I DRUGIH KRIVIČNIH DELA SAJBER KRIMINALA

Zajedničko za sva krivična dela sajber kriminala je to što se računar koristi kao sredstvo izvršenja krivičnog dela. Samo vršenje krivičnih dela podrazumeva upotrebu kompjutera, odnosno kompjuterskog sistema u smislu sredstva ili cilja izvršenja krivičnog dela. (Stojanović & Perić, 2009, str. 248)

Grupni zaštitni objekt ovih krivičnih dela je bezbednost računarskih podataka i računarskih mreža. Iako naš Krivični zakonik propisuje samo nekoliko krivičnih dela ove kategorije, krivičnopravna zaštita računarskih podataka i računarskih mreža je sveobuhvatnija, jer se postiže primenom inkriminacija drugih krivičnih dela koja su po pretežnijem grupnom zaštitnom objektu svrstana u druge glave (protiv imovine, protiv sloboda i prava građana, protiv industrijske svojine, protiv privrede...). (Stojanović & Perić, 2009, str. 248)

Zajednička posledica krivičnih dela sajber kriminala bi bila pričinjavanje materijalne štete po neko pravno ili fizičko lice. Za kvalifikovane oblike je karakteristično da kvalifikatornu okolnost predstavlja uvek prouzrokovanje štete preko određenog novčanog iznosa ili nastupanje štetnih posledica.

Kao oblik krivice je uvek predviđen umišljaj, s obzirom na postojanje namere kao subjektivnog obeležja. Za ova krivična dela je naročito interesantno da zakonodavac propisuje da izvršilac može biti svako lice, te se radi odelicta communia.

Član 298. Krivičnog zakonika Republike Srbije, propisuje krivično delo oštećenje računarskih podataka i programa. S obzirom na uporednu analizu računarske sabotaže i oštećenja računarskih podataka i programa, oba dela imaju zajedničke karakteristike koje se ogledaju u načinu izvršenja, a to je brisanj e, izmena, oštećenje, prikrivanje ili na drugi način činjenje neupotrebljivim računarskog podatka ili programa.

Radnja izvršenja kod ovih krivičnih dela je ista, razlike možemo primetiti u odnosu na svojstvo izvršioca, objekat krivičnog dela i zaprećenoj kazni.

U slučaju krivičnog dela oštećenje računarskih podataka i programa radi se o „neovlašćenom“ (bez odgovarajuće dozvole) preduzimanju navedenih radnji, te potencijalni izvršilac je ograničen na lica koja imaju neko ovlašćenje, dok kod računarske sabotaže to nije slučaj. U slučaju računarske sabotaže zahteva se postojanje određene namere koja je usmerena prema državnim organima, javnoj službi, ustanovi, preduzeću ili drugom subjektu, dakle onimsubjektimakoji imaju poseban društveni značaj. Radnja izvršenja krivičnog dela računarske sabotaže se preduzima sa namerom da se onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja zadržavne organe, javnu službu, ustanove, preduzeća ili drugog subjekta.Kod oštećenja računarskog podataka i programa ova specifična namera ne postoji.Kvalifikovani oblicidela podrazumevaju da je nastupila šteta koja prelazi određeni iznos, dok kod računarske sabotaže nije određen iznos prouzrokovane štete, jer je kod nje u prvom planu postojanje namere. Sankcija predviđena za krivično delo oštećenja računarskih podataka i programa je za osnovni oblik novčana kazna ili kazna zatvora do jedne godine. U slučaju težih oblika oštećenja računarskih podataka i programa, ako je prouzrokovana šteta u iznosu koji prelazi četristopedeset hiljada dinara, učinilac će se kazniti zatvorom od tri meseca do tri godine. U najtežem slučaju ovog krivičnog dela tj. ako je prouzrokovana šteta u iznosu koja prelazi milion i petsto hiljada dinara, učinilac će se kazniti zatvorom od tri meseca do pet godina. Za krivično delo računarska sabotaža zakonodavac je predvideo kaznu zatvora od šest meseci do pet godina. (Skupština Srbije, Krivični zakonik RS, 2014, str. član 298)

Pravljenje i unošenje računarskih virusa , krivično delo predviđeno članom 300 Krivičnog zakonika Republike Srbije (2014), se sastoji u pravljenju računarskog virusa u nameri njegovog unošenja u tuđ računar ili računarsku mrežu. Radnja izvršenja podrazumeva primenu određenih tehnoloških postupaka kojima se računarski virus stvara. (Stojanović & Perić, 2009, str. 254) Upoređujući ovo delo sa računarskom sabotažom, površnom analizom mogli bismo reći da bi ovo delo moglo da se podvede pod računarsku sabotažu, samim tim što smo govorili o vidovima računarske sabotaže gde su kompjuterski virusi sredstvo da se sabotaža izvrši, dakle da se onemogući ili znatno omete postupak elektronske obrade i prenosa podataka. No, element namere koja je upravljena protiv društveno značajnih subjekata je ono što odvaja računarsku sabotažu kao zasebno krivično delo, kao i to da je delo iz člana 300. Krivičnog zakonika dovršeno samim pravljenjem računarskog virusa. Izvršilac može biti bilo koje lice, ali se ona svode na lica koja raspolažu stručnim znanjem za pravljenje računarskih virusa, tzv.virus makers.

Računarska prevara je posebno krivično delo u članu 301 Krivičnog zakonika Republike Srbije, koje ima osnovni, dva teža oblika (s obzirom na kvalifikatornu okolnost da je delom pribavljena imovinska korist preko određenih iznosa) i lakši oblik. Osnovni oblik se sastoji u unošenju netačnog podatka, propuštanja unošenja tačnog podatka ili na drugi način prikrivanje ili lažno prikazivanje podatka i time uticanje na rezultat elektronske obrade i prenosa podataka u nameri da sebi ili drugom bude pribavljena protivpravna imovinska korist i time drugome prouzrokuje imovinska šteta. (Krivični zakonik RS, član 301) U odnosu na delo računarske sabotaže, osnovna razlika je u samoj nameri, kao i u prethodnom slučaju. U slučaju prevare, namera se sastoji u pribavljanju protivpravne imovinske koristi, dok je kod sabotaže ta namera usmerena na to dase onemogući ili znatno omete postupak elektronske obrade i prenosa podataka.

Krivična dela - neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (Krivični zakonik RS, član 302) i sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (Krivični zakonik RS, član 303) takođe nemaju element namere karakterističan za sabotažu. Ipak sredstvo izvršenja je isto (računar) kao i objekt radnje (računarski podatak i javna računarska mreža).

Krivično zakonodavstvo Republike Srbije predviđa još dva krivična dela protiv bezbednosti računarskih podataka – neovlašćeno korišćenje računara ili računarske mreže i pribavljanje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka. (Krivični zakonik RS, član 304) U prvom slučaju namera je pribavljanje protivpravne imovinske koristi, što opet nije u skladu sa namerom kao kod krivičnog dela računarske sabotaže. U drugom slučaju radi se o radnji saučesništva, koja je inkriminisana kao zasebno krivično delo, te ovo delo može prethoditi izvršenju krivičnog dela računarske sabotaže.

Analizirajući odnos računarske sabotaže sa ostalim krivičnim delima sajber kriminala, ne možemo se ne osvrnuti na sajber terorizam. Sajber napadi predstavljaju novu pretnju za države i njihovu bezbednost. Terorističke organizacije manipulišući društvenim mrežama,koriste društvene mreže poput Twitter-a, Facebook-a, YouTube-a i drugih, i internet komunikaciju kao efikasno sredstvo za distribuciju svoje propagande, ideologije i slanje političkih poruka. Tri su bitna indikatora za kvalifikaciju sajberterorizma (Jonev, 2016, str. 208):

1. aktivnost mora imati političku, ideološku, religioznu, sociološku pozadinu;
2. sredstvo putem kojih se napad izvršava je kompjuter i računarske mreže;
3. napad mora imati posledicu – kao indikatori to mogu biti uništavanje informacionih sistema, fizičko uništenje objekata, ugrožavanje života civila (povreda, smrt). (Jonev, 2016, str. 210-211)

Dakle, biće krivičnog dela računarske sabotaže, ima zajedničku 2. i 3. Karakteristiku sa sajber terorizmom. Sredstvo izvršenja je isto, a to je računar, dok posledica nije ista u potpunosti. Sajber terorizam može imati za posledicu i ugrožavanje života civila, što ga kvalifikuje znatno težim krivičnim delom, a posebno kad na to dodamo i političku pozadinu koja kod računarske sabotaže ne postoji.

4 ZAKLJUČAK

S obzirom da je svakodnevni život vezan za računare, da se sprovodi digitalizacija u svim društvenim oblastima i društvenim institucijama, neophodno je zaštititi sistem od sajber kriminala i računarskih sabotaža koje su neizbežne, jer su računari dostupni svima, te i onima koji žele da ih koriste kao sredstvo izvršenja krivičnog dela. Računarska sabotaža je sve češća, jer se učinioci teško otkrivaju, a poznavaocima informacionih tehnologija koji se odluče za kriminal, s obzirom na njihova stručna znanja u ovoj oblasti, nije preveliki problem da se u tako nešto upuste samim tim što su svesni da za njihovo otkrivanje takođe treba posedovati visoke kvalifikacije. Međutim, s obzirom na to da je mnogo veći broj izvršenja ovog krivičnog dela kao i posledica koje su njime prouzrokovane, u odnosu na broj kompetentnih stručnjaka u ovoj oblasti kriminologije, svakako treba raditi na edukaciji onih koji se bave sajber kriminalom. Razvoj digitalne forenzike je od naročitog značaja, jer ona predstavlja noviji način u istrazi krivičnog dela. U smislu pravne regulative, Republika Srbija je dosta napredovala inkriminišući određen broj krivičnih dela protiv bezbednosti računarskih podataka. Možemo

primetiti da kao i u svim oblicima kriminaliteta, značajna je prevencija, a nakon toga kaznena politika. Možemo smatrati da kaznena politika naše zemlje polako dostiže nivo kaznenih politika ostalih evropskih zemalja. Takođe, Zakonom o potvrđivanju Konvencije o visokotehnološkom kriminalu, zagarantovana je međunarodna saradnja strana ugovornica koja je neophodna kada se radi o računarskoj sabotaži. Akcenat treba staviti na prevenciju koja bi trebalo da se razvija u smeru izrađivanja i ugrađivanja u računarske softvere programa (najčešće bi to bili antivirus programi) koji neće dozvoliti da do sabotaže uopšte dođe. Što su značajniji podaci koji se čuvaju u bazi informacionog sistema, to bi softverska zaštita od računarske sabotaže trebalo da bude veća. Zakon u oblasti prevencije treba da obezbedi, tj. propiše precizno u kojim slučajevima se daje sudska dozvola za presretanje i otkrivanje sadržaja kompjuterskih komunikacija i podataka. Ovakve odredbe bi mogle da budu suprotstavljene pravu na privatnost, te zbog toga treba istaći da bi one morale biti izuzetno precizne i formulisane tako da ne postoje pravne praznine koje bi onemogućile otkrivanje izvršilaca krivičnog dela računarske sabotaže.

CITIRANA DELA

Gerstenmajer. (2007, 07 28). Sabotaža u NASA. *Danas*. Preuzeto sa https://www.danas.rs/zivot/sabotaza-u-nasa/

Jezikoslovac. (2018, 08 07). ***sabotaža***. Preuzeto sa Jezikoslovac: https://jezikoslovac.com/word/0zep

Jonev, K. (2016). Sajber terorizam i upotreba sajber prostora u terorističke svrhe. *Bezbednost*(2).

Lilić, S., & Prlja, D. (2008). *Pravna informatika veština – Internet za pravnike.* Beograd: Dosije.

Miladinović Bogavac, Ž. (2017). Pojam, vrste i načini delovanja malicioznih programa kojima se sprovode internet prevare. *Časopis za istraživanje medija i društva Medijski dijalozi, X*(29), 239.

Miladinović Bogavac, Ž. (2018). Models of commiting cyber criminal offences. *Međunarodna naučna konferencija ,,PRAVO 2018" Zbornik radova, Poslovni i pravni fakultet Univerzitet Union Nikola Tesla* (str. 122-129). Beograd: ICIM Izdavački centar za industrijski menadžment.

Parker, D. (1981). *Fighting Computer Crime.* New York: Charles Scribner & Sons.

Skupština Srbije. (2009). Zakon o izmenama i dopunama Krivičnog zakonika. *Sl. glasnik RS", br. 72/2009*.

Skupština Srbije. (2009). Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu. *Sl. glasnik RS – Međunarodni ugovori", br. 19/2009*.

Skupština Srbije. (2014). Krivični zakonik RS. *Sl. glasnik, br. 108/2014*.

Stojanović, Z., & Perić, O. (2009). *Krivično pravo – posebni deo.* Beograd.

Vestbi, D. (Ur.). (2004). *Međunarodni vodič za borbu protiv kompjuterskog kriminala.* Beograd: Američka advokatska komora.

Vokabular. (2006). *Sabotaža*. Preuzeto sa Vokabular: https://vokabular.org/?search=sabota%C5%BEa&lang=sr-lat

Datum prve prijave: 02.09.2018.
Datum prijema korigovanog članka: 05.08.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

Style – APA Sixth Edition:

Miladinović Bogavac, Ž. (2019, 10 15). Računarska sabotaža. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 78-85. doi:10.12709/fbim.07.07.02.09

Style – Chicago Sixteenth Edition:

Miladinović Bogavac, Živanka. 2019. "Računarska sabotaža." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 78-85. doi:10.12709/fbim.07.07.02.09.

Style – GOST Name Sort:

Miladinović Bogavac Živanka Računarska sabotaža [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 78-85.

Style – Harvard Anglia:

Miladinović Bogavac, Ž., 2019. Računarska sabotaža. *FBIM Transactions,* 15 10, 7(2), pp. 78-85.

Style – ISO 690 Numerical Reference:

Računarska sabotaža. **Miladinović Bogavac, Živanka.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 78-85.

FBIM Transactions
DOI 10.12709/fbim.07.07.02.10

ZLOUPOTREBA NOVIH TEHNOLOGIJA I DIGITALNO NASILJE

NEW TECHNOLOGY ABUSE AND DIGITAL VIOLENCE

Zoran Milanović
Kriminalističko-policijski Univerzitet, Beograd, Srbija

JEL Kategorija rada: **L86**

Apstrakt

Super brzi razvoj novih tehnologija doneo je i njihovu nezakonitu primenu u tom obimu da ni napredni korisnici, ni bezbednosni stručnjaci nisu svesni brzine nastajanja digitalnih rizika, niti rešenja za svakodnevne digitalne probleme. Dobra poslovna i korisnička praksa ukazuje da korisnici digitalnih uređaja treba da budu naoružani aktuelnim činjenicama neophodnim za sopstvenu zaštitu, zaštitu svojih porodica, svojih kompanija i svojih zajednica, kako bi se odbranili od novonastalih digitalnih pretnji i rizika. Primarni cilj rada je da se kroz citiranje velikog broja elektronskih naslova, koji opisuju katastrofalne pojave u digitalnom svetu, podigne svest običnih korisnika i promeni njihova percepcija i ponašanje pri korišćenju digitalnih uređaja, jer jedino se praktičnim znanjem može boriti protiv zloupotrebe novih tehnologija i narastajućeg digitalnog nasilja.

Ključne reči: *informaciona bezbednost, zloupotreba novih tehnologija, digitalno nasilje.*

Abstract

The rapid development of new technologies has also led to their unlawful application to the extent that neither advanced users nor security professionals are aware of the rate of formation of digital risks, nor of solutions to everyday digital problems. Good business and customer practice indicate that digital device users should be armed with current facts necessary for their own protection, the protection of their families, their companies and their communities, to defend themselves against emerging digital threats and risks. The primary aim of the paper is to raise the awareness of ordinary users, change their perceptions and behavior when using digital devices by citing a large number of electronic titles describing catastrophic phenomena in the digital world, as only practical knowledge can combat the misuse of new technologies and the growing digital violence.

Keywords: *information security, new technology abuse, digital violence.*

Adresa autora:
Zoran Milanović
zoran.milanovic@kpu.edu.rs

1 UVOD

Kičmu civilizacije poverili smo mašinama i Internetu. Digitalne tehnologije, iako predstavljaju nasušnu potrebu savremenog društva, oduvek su

bile mač sa dve oštrice. Njihovom primenom pružaju nam se mnoge pogodnosti kojima puno dobijamo u svakodnevnom radu i životu, ali i isto toliko gubimo. Naš sveukupni digitalni svet: biznis, zabava, autorsko delo ili neka draga uspomena, mogu biti izgubljeni sa samo nekoliko klikova miša ili hardversko-softverskom greškom. Još mnogo gore od toga, na Internetu nisu ugroženi samo naši lični i poslovni digitalni sistemi i podaci, tu se direktno napadaju i vitalni sistemi civilizacije koji se oslanjaju na nove tehnologije i kojima se upravlja i kontroliše: elektro-energetski, gasovodni i vodni sistemi, avio saobraćaj, policijske, vatrogasne i medicinske službe, vojska, obrazovanje, finansije…

Ne treba da nas brinu samo kriminalci i odmetnički režimi koji za cilj imaju ugrožavanje i zloupotrebu novih tehnologija, već nas često, neverovatno ranjive ostavljaju i velike IT kompanije, proizvođači hardvera, softvera, pružaoci raznih servisa i usluga, kao i organizacije na koje se oslanjamo da nas štite i savetuju, a u stvari i one kontrolišu kod koji upravlja našim životima.

Zato, „što više priključujemo naše uređaje i živote u globalnu informacionu mrežu – bilo preko mobilnih telefona, društvenih mreža, liftova ili autonomnih vozila – to ranjiviji postajemo pred onima koji znaju kako funkcionišu osnove tehnologije i kako se mogu upotrebiti u njihovu korist, a na štetu običnih ljudi. Jednostavno rečeno, kad je sve povezano, svi su ranjivi. Tehnologija koju rutinski unosimo u svoj život sa malo ili nimalo promišljanja ili ispitivanja može sasvim lako da nam se vrati kao bumerang.”(Gudmen, 2017, str. 11)

Korisnici treba da budu svesni, svuda i u svakom trenutku, koje digitalne uređaje (računar, telefon...) nabavljaju i od koga, sa kakvim softverom i podrškom, gde i kako ih povezuju na mrežu, kao i kako ih koriste, a posebno da znaju, da sve što rade na njima, negde se beleži i pre ili kasnije, bez obzira da li postoji veza sa Internetom, biće javno dostupno i nekim drugim osobama ili organizacijama. Takođe, korisnici treba da znaju da skoro da ne postoji nijedan uređaj, nijedno softversko rešenje koje nema neki bezbednosni propust u sistemu, bez obzira da li je svesno napravljen od proizvođača, npr. upis u Firmware (Wodinsky, 2018) ili izvornog programera odn. hakera, npr. Backdoor – otvaranje zadnjih vrata radi ilegalnog pristupa (Stone, 2019), ili problemi i propusti koji nisu ni utvrđeni tokom testiranja proizvoda, npr. greške koje se koriste za Zero-Day – napad nultog dana (Schwartz, 2019).

Na sve navedeno, svakodnevno nas upozoravaju digitalni novinski naslovi, koji iznose puno crne statistike u brojkama (raznim valutama i procentima), puno rezultata stručnih istraživanja i primera iz prakse, koji posebno apostrofiraju digitalno nasilje, najčešće nad decom i mladima.

2 DIGITALNO NASILJE NAD DECOM I MLADIMA

Nedostatak bezbednosne kulture najviše pogađa decu i mlade i to kako zbog njihovog posebnog mesta u sistemu zaštite, tako i zbog njihove naivnosti. Prema Mišelu Sen Lou (2015), direktoru UNICEF-a u Srbiji, „sve više dece koristi digitalne alatke za učenje, društveno angažovanje i druženje. Međutim, putem njih se izlažu i novim rizicima – nasilju, neprikladnom sadržaju, nepoznatim ljudima“.

Naime, mladi imaju probleme koje ne mogu uvek da prepoznaju i objasne, susreću se sa različitim pojavama i pretnjama bez prethodne psihološke zaštite. Probleme uglavnom ne mogu sami da reše i/ili ne znaju kome da se obrate za pomoć.

Opasnosti i pretnje kojima je mlađa populacija korisnika Interneta svakodnevno izložena su brojne i raznovrsne, a posebno sa ekspanzivnim razvojem društvenih mreža i onlajn igrica. One danas predstavljaju sadržaje koji su popularni i kao takvi veoma uticajni na mlađu populaciju korisnika Interneta.

Mladi su najugroženija ciljna grupa većine pojavnih oblika zloupotrebe, a posebno nastajanju, razvoju i širenju dečije pornografije, pedofilije, onlajn igricama, kockanju i klađenju.

Mladi širom sveta, svakodnevno provode sate i sate igrajući onlajn multiplejer video igre. Pozitivna strana onlajn igranja je zabava, sklapanje prijateljstva i razmena iskustva sa ljudima iz raznih delova sveta, otkrivanje novih interesovanja, osećaj pripadnosti društvu i sl. No, postoji i negativna strana korišćenja onlajn gejmerskih servisa koja se ogleda u postojanju brojnih opasnosti koje mogu izuzetno loše uticati

na gejmere (e-igrače). Naime, istraživanje organizacije za ljudska prava Anti-Defamation League (ADL), pokazalo je da se radi o zlostavljanju koje je u onlajn multiplejer igrama doživelo čak 74% osoba koje su učestvovale u ovom istraživanju (Castello, 2019), od čega je 65% njih bilo "ozbiljno zlostavljano" što uključuje i pretnje fizičkim nasiljem i praćenjem. Kao razloge zlostavljanja više od 50% ispitanika navelo je zlostavljanje zasnovano na rasi, etničkoj pripadnosti, religiji i seksualnoj orijentaciji. Skoro 30% tvrdi da su bili doksovani (doxxed – objavljena adresa i broj telefona) u onlajn igri, a skoro četvrtina ispitanika kaže da je bila izložena ideologiji superiornosti bele rase. Takođe, primećeno je da neki gejmeri u toku igranja šire „ekstremističke ideologije“. (Rock, 2019)

Iako rezultati ADL istraživanja nisu definitivni (ispitano oko 1.000 ljudi) gejming zajednica je svesna da onlajn igranje može dovesti do nezdravog ponašanja (Fisher, 2019b). Tako je 24-godišnjak David Katz, posle izgubljenog turnira (ili diskvalifikacije) uzeo pištolj, ubio dvoje ljudi i više njih ranio, a potom i izvršio samoubistvo. Zatim, ubistvo oko 30 ljudi u dve masovne pucnjave u SAD, predsednik Donald Tramp (Donald Trump) je za te tragične događaje, između ostalog, okrivio “stravične i grozne video igre”, što nije prvi put da je uspostavio ovu vezu, niti je jedini koji je to učinio. (Landsverk, 2019)

Još jedan od roditeljskih problema, nakon “Plavog kita” koji se dovodi u vezu sa samoubistvom 130-toro dece u Rusiji (Adejn, 2019), stigao je novi izazov na sajtu YouTube Kids koji tera decu da izvrše samoubistvo. (Dough, 2019)

Takođe, prema studiji sprovedenoj u SAD, a nakon što je prikazivana Netfliks-ova serija "13 razloga zašto", od aprila 2017. godine broj samoubistava među decom od 10 do 17 godina je porastao za jednu trećinu. (Carey, 2019)

Što se tiče crne strane onlajn gejminga, primećeno je, takođe, npr. u igrici Super Mario Odyssey da se preko veoma specifičnih kanala u igru, kroz portrete i specijalne balone, ubacuju slike eksplicitnog pornografskog sadržaja. Kako je u pitanju onlajn deo igre, odnosno novi mod Luigi’s Balloon World, ovo su u svakom trenutku mogla da vide i brojna deca koja igraju Super Mario Odyssey, bez znanja njihovih roditelja, koji očekuju da im deca igraju igru prigodnu njihovom uzrastu. (Keach, 2018)

U najnovijem saslušanju koje je sprovela britanska vlada, otkriveno je da je jedan dečak u igri Runescape putem mikrotransakcija, naneo ogromne finansijske poteškoće svojim roditeljima, potrošivši neverovatnih 62.000 dolara. (Thubron, 2019)

Deca ne samo što su žrtve, mogu biti i napadači. Tako mališani od samo 10 godina pokreću velike kiber napade (DDoS – uskraćivanje usluga), putem besplatnih alata sa Interneta, kako bi dobili ili ostvarili prednost nad protivnicima u onlajn igricama (Fortnite), dok je jedan tinejdžer od 14 godina izveo skoro 500 kiber napada, za samo mesec dana, sa istim ciljem kao i njegov prethodnik. (Stevens, 2019) Deca, iako žive sa roditeljima, nisu svesna da vrše krivično delo, a takođe ni njihovi roditelji. Ovde se posebno upozoravaju roditelji da obrate pažnju na mrežne aktivnosti svoje dece, jer posledice su katastrofalne.

Posebno mesto u ovoj problematici zauzimaju kockanje i klađenje u onlajn varijantama, izuzetno atraktivno za decu i mlade osobe. Prema istraživanju iz 2013. godine, novosadskog centra "Život nije igra" problem patološkog kockanja javlja se već u osnovnoj školi, a ovaj porok sve više uzima maha. Od 790 ispitanika, uzrasta od 11 do 20 godina, skoro polovina igra igre na sreću. Od ukupnog broja ispitanika 48 se patološki kocka, a 20 odsto problematično. Zabrinjava podatak da najmlađi ispitanik koji se patološki kocka ima samo 12 godina (igra sa tatom rulet, a počeo je sa aparatima kad je imao manje od 10 godina uz brata ili tatu). (Život nije igra, 2013)

Komisija za praćenje i nadziranje kockanja u Velikoj Britaniji u svom izveštaju navodi da oko 25.000 dece uzrasta od 11 do 16 godina, pripada kategoriji problematičnih kockara, a mnogi uče da se klade putem računarskih igara tzv. E-sportova (igrice kao što su Counter-Strike, Dota2, Call Of Duty, Overwatch and League of Legends) i društvenih medija. Njih 70% je prve reklame za kockanje i klađenje videlo na društvenim mrežama, 66% na drugim web sajtovima, dok njih oko 10 % prate kompanije za kockanje i klađenje na društvenim mrežama. (Gambling, 2017)

Neočekivano, ispostavilo se da deci i mladima najčešće povrede privatnosti i psiho-fizičko ugrožavanje prete u najbližem okruženju – porodici i vaspitno obrazovnim ustanovama, a najčešće zbog objava na društvenim mrežama. Neodgovorni i nesmotreni roditelji prave probleme deci, kada objavljuju slike na Internetu bez njihovog odobrenja (Lyons, 2019). Oni treba da budu svesni i da čuvaju i zaštite prava deteta, a ne da ugrožavaju njihovu privatnost i da javno dele identitet deteta bez njihovog pristanka. (Hart, 2019) Tako je jedna 18-godišnjakinja iz Južne Australije tužila roditelje zbog objavljivanja njenih fotografija iz detinjstva na Facebooku. (Huggler, 2016)

Koliko je to učestala pojava ili uticaj sve popularnijih društvenih mreža, ukazuje i podatak da roditelji deteta od pet godina u proseku objave 1500 slika o njemu ili njoj na Facebook-u, Tvitter-u, Instagram-u i slično. (Mangan, 2016)

Ono što je posebno alarmantno u Srbiji, svaka treća mlada osoba trpi digitalno nasilje. (PC Press, 2019)

Rešenje i prevenciju za iznete probleme treba tražiti u edukaciji i upozorenju na nivou roditelja koji igraju možda najvažniju ulogu u prevenciji i rešavanju ovog problema. Adekvatna bezbednosna kultura svih korisnika, a naročito mladih, imperativ je savremenog društva.

Decu i mlade treba podsticati da postanu aktivniji, sa većim opsegom znanja, razumevanja i mogućnosti da se suoče sa problemima, kao i da neguju ona ponašanja koja će značajno podići nivo njihove bezbednosne kulture (Ejdus i dr. 2009). Da bi se ovaj cilj postigao neophodno je da informaciono-bezbednosna kultura postane sastavni deo planova i programa svih nivoa obrazovanja i vaspitanja. Prihvatanjem osnovnih načela informaciono-bezbednosne kulture stvorio bi se preduslov za uspostavljanje bezbednog ambijenta u kome bi mladi neometano mogli da koriste sve prednosti i blagodeti informacionih tehnologija i tako ostvare svoja prava na kvalitetno obrazovanje, informisanje i lični razvoj.

3 DRUŠTVENE MREŽE – SERVIS ZA USPEH ILI PROPAST SAVREMENOG DRUŠTVA

Društvene mreže su novi kreatori javnih dosijea, koji prikupljaju sve što je neko podelio, svesno ili ne, sortiraju i skladište, a onda to prodaju oglašivačima, vladama i trećim licima.

Rezultati istraživanja firme Security Baron su, blago rečeno, zastrašujući. Oni ukazuju koliko i kojih podataka velike IT kompanije (Facebook, Google, Microsoft, Amazon, Apple i Twitter) prikupljaju o svojim korisnicima i koliko mnogo zarađuju prodajući te informacije. Sprovedeno istraživanje se odnosi na pregled zvaničnih politika privatnosti navedenih kompanija i tabelarno prikazivanje vrste podataka koje svaka od njih prikuplja o svojim korisnicima. (Turner, 2019) Inače o kolikom bogatstvu se radi najbolje govore podaci dati u Forbsovoj listi za 2019. godinu, gde se među prvih 10, nalaze 4 vlasnika gore navedenih kompanija: 1. Džef Bezos, Amazon, USD 131 milijarda; 2. Bil Gejts, Microsoft, USD 96,5 milijardi; 8. Mark Zuckerberg, Facebook, USD 62.3 milijarde i 10. Leri Pejdž, Google, USD 54 milijardi. (Kroll & Dolan, 2019a)

Iz prethodnih brojki može se zaključiti da naizgled besplatne usluge koje nam nude velike tehnološke kompanije, to zapravo i nisu. Prodaja naših podataka, koje smo im, doduše, sami poklonili, učinila ih je, ne samo najbogatijim, već i najmoćnijim kompanijama na svetu.

Ljudi koji upotrebljavaju društvene mreže treba da budu svesni, da oni nisu korisnici tih servisa već njihov proizvod, koji se prodaje onima koji ponude najvišu cenu. Društvene mreže nisu napravljene da bi ih korisnici upotrebljavali za svoje potrebe, već su osmišljene sa konkretnom namerom da obmanu, zavedu i prevare korisnike, kako bi otkrili što veću količinu podataka o sebi i svom životu. Primeri i brojke o zloupotrebi društvenih mreža i narušavanje privatnosti korisnika gore sve.

- Od nastanka prvih društvenih mreža pa do danas one su prikupljale podatke bez našeg saznanja. Kada je to postalo očigledno, izbijanjem afere o Facebooku i Cambridge Analytice, koji su neovlašćeno prikupljali podatke od oko 87 miliona korisnika bez njihovog pristanka i koristili ih za ciljane oglase i političke kampanje, prešlo se na sledeći nivo tj. korisnicima se plaća za potpuni pristup njihovoj privatnosti.
- Facebook plaća 20 dolara, a Google 25 dolara, tinejdžerima (od 13 godina) da

instaliraju VPN na telefonima, kako bi ih špijunirali (Tech Crunch, 2019b). Facebook interesuje kako mladi koriste telefon i koji sadržaj pregledaju na vebu, a imali su i pristup privatnim porukama, mejlovima itd. Sve to interesuje i Google i mnogo više, kako se koriste njihovi proizvodi, ne samo na pametnim telefonima, već i na ličnim računarima, televiziji, pa čak i pristup ruterima za snimanje šta rade onlajn. Google, takođe interesuje i kako se koriste aplikacije konkurentskih kompanija poput Facebook-a i WhatsApp-a itd.

- Profit Facebook-a raste uprkos skandalima o narušavanju privatnosti, njihova čista dobit dosegla u četvrtom tromesečju 6,88 milijardi dolara, što je 62 odsto više nego godinu dana ranije (Carrie Wong, 2019b). Tako Facebook skandali nisu promenili ni navike korisnika, niti su uticali na promene u podešavanju privatnosti (Lee T., 2018).
- Činjenica da Facebook ugrožava privatnost korisnika više ne predstavlja iznenađenje, njihovo poslednje priznanje odnosi se na snimanje i prisluškivanje glasovnih poruka korisnika u Messenger-u (Hern, 2019).
- Facebook prati i prikuplja podatke korisnika i nakon što deaktiviraju svoje profile i to putem Facebook dugmeta za deljenje sadržaja, koje se nalazi na 275 miliona web stranica, a radi prikupljanja informacija za koje su sadržaje korisnici zainteresovani. Prikupljanje podataka se obalja i kod korisnika koji nisu imali nalog na toj društvenoj mreži, a posetili su stranicu na kojoj se nalazi njihov f-znak (Ng, 2019).
- Studija sa Stanforda i Univerziteta New York otkriva da su korisnici koji su deaktivirali svoj Facebook nalog mnogo srećniji, ali manje informisani (CORDIS, 2019).
- Veliki broj internih dokumenata ukazuje da Facebook-ova surova mašinerija ima informaciju da maloletnici roditeljima troše novac s kartica, ali ipak ništa ne preduzima (Lee D., 2019). A i što bi reagovali, kada je profit iznad svega.
- Bezbednosni stručnjaci su otkrili i osudili, a Facebook priznao da je učitao kontakte 1,5 miliona mejl adresa bez prethodnog znanja i odobrenja korisnika. Facebook je klasičnom fišing prevarom naterao nove korisnike, navodno kako bi potvrdili identitet i uvezli svoje kontakte da se prijave putem e-mail adrese i šifre. Na osnovu ta dva podatka Facebook je “slučajno“ skinuo sve kontakte sa dobijenih e-mail adresa (Porter, 2019c).
- Na Internetu je pronađena Facebook-ova nezaštićena baza podataka koja sadrži više od 419 miliona telefonskih brojeva (Carrie Wong, 2019b), a bezbednosni stručnjak Frank Abagnale tvrdi da bi u 98 odsto slučajeva, datum i mesto rođenja bili dovoljni da hakeri nekome ukradu identitet. Njegova preporuka je da korisnici društvenih mreža, prvenstveno korisnici Facebooka, sklone ove osetljive podatke sa svog profila. (Abagnale, 2019)
- YouTube je kažnjen sa 170 miliona dolara zbog narušavanja privatnosti dece. Oni su nezakonito prikupljali lične podatke dece, bez odobrenja njihovih roditelja (Bartz, 2019). Google je platio i 50 miliona eura francuskoj zbog nepoštovanja GDPR-a (Porter, 2019a), a Facebook kažnjen sa 5 milijardi dolara zbog pronevere privatnosti svojih korisnika (Kelly, 2019). Naravno, ove kazne ih nisu promenile, nastavili su po starom, sa minimalnim kozmetičkim promenama, jer upitanju su velike zarade, a navedeni izuzetno mali troškovi.

U prilog svemu navedenom govori i preporuka bezbednosnog uzbunjivača i stručnjaka Edvarda Snoudena (Edward Snowden) da treba da budemo svesni svaki put kada nešto poželimo da ostavimo ili preuzmemo sa Interneta: „Sve što sada radimo ostaje zapisano zauvek. Ne zato što mi to želimo da zapamtimo, već zato što nam više nije dozvoljeno da zaboravimo" (Sputnik International, 2019). On takođe kaže, „samo zamislite da otvorite računar i pronađete dokument koji niste napisali, a u kojem su svi vaši podaci o životu uredno sačuvani. Vaša matura, vaša fotografija na stadionu, slika sa zabave pre 10 godina u opijenom stanju, detalj poljupca koji ste dali ženi najboljeg prijatelja za koga ste se oboje zakleli da nikada nikome nećete reći. Zatim, lista svih porno snimaka koje ste ikada gledali, mapiranje svakog glupog i seksističkog komentara koji ste ikada napisali ili napravili. Goli

selfiji, fotografije snimljene na rođendanu vaše majke, video snimak u muzeju Louvr, itd. Pa, ovaj dokument postoji, ili bolje rečeno, mogao bi postojati, i nije distopijska fantazija.“ (La Repubblica, 2019)

Koliko istine ima u preporuci Snoudena, pokazuje i primer kako se štite oni koji najviše prikupljaju naše podatke. Tako, vlasnik Facebook-a na svom MacBook Pro ima traku zalepljenu preko web kamere, a da nije jedini, društvo mu pravi i direktor FBI Džejms Komi. S druge strane da i oni nisi svemogući i nedodirljivi i da u digitalnom svetu nema povlašćenih korisnika i apsolutno zaštićenih sistema, podataka, informacija i znanja, potvrđuju naredni primeri.

- Izvršnom direktoru Tvitera Jack Dorsey hakeri su preuzeli nalog i na njemu objavljuju uvredljive i rasističke poruke (Conger, 2019).
- Hakovan mobilni telefon najbogatijeg čoveka na svetu, Džefa Bezosa (Jeff Bezos), šefa kompanije Amazon (Badshah, 2019).
- Bivšem predsedniku SAD, Baraku Obami (Barack Obama, 2014.), ukradena novčana sredstva sa bankovnog računa i blokirana platna kartica (BBC, 2014a).

4 VISOKOTEHNOLOŠKE PRETNJE I HARDVERSKO-SOFTVERSKI BEZBEDNOSNI PROPUSTI

Osnovni razlog zbog koga je teško reagovati i boriti se protiv visokotehnoloških pretnji je postojanje nepoznatih hardversko-softverskih ranjivosti, koje se koriste za tzv. „napad nultog dana”. Velike IT kompanije ulažu mnogo novca kako bi motivisale istraživače da otkrivaju propuste i greške u sistemu, ali ne da bi obični korisnici bili bezbedniji, već da bi zaštitili svoj biznis.

Ono što je posebno važno, problemi sa kojima se susreće informaciona bezbednost daleko je složenija od tehničkih rešenja ili proizvoda. Shodno ovoj konstataciji je i izjava stručnjaka za bezbednost Šnejera (Bruce Schneier) „Ako mislite da tehnologijom možete rešiti vaš bezbednosni problem onda vi ne razumete ni problem ni tehnologiju“ (Schneier, 2015). Sledeći primeri ukazuju da problemi i propusti evidentno postoje.

- Napadi na operativni sistem Microsoft Windows su svakodnevni i učestali. Novo-stari trojanac (iz 2014. godine) RAT (remote access trojan) ugrožava sve verzije i sve uređaje sa ovim operativnim sistemom. Zlonamerni korisnici sa minimalnim tehničkim znanjima mogu da steknu potpunu kontrolu nad Windows uređajima. Svemogući maliciozni program može sa određene udaljenosti da isključi i ponovno pokrene pogođeni Windows uređaj, da pretražuje i pregleda fajlove, pristupi Task Manager-u, Registry Editor-u, i čak preuzme kontrolu nad mišom. Napadač može da otvara web stranice i isključi svetlo koje signalizira da je uključena web kamera, i tako neopaženo snima žrtvu po svojoj volji. Tu je i mogućnost prikupljanja lozinki i akreditiva za prijavljivanje pomoću keylogger-a, i na kraju zaključavanje pogođenog uređaja putem ransomeware. (Winder, 2019b)
- Stručnjaci za informacionu bezbednost iz kompanije Avast objavili su rezultate istraživanja na više od 160 miliona računara iz celog sveta, koja ukazuju da 55% korisnika na svojim ličnim računarima koristi zastareli softver, odnosno programe koji nisu nadograđeni na poslednju verziju, a koja uključuje i bezbednosnu nadogradnju. Tako jedan od 6 korisnika Microsoft Windowsa 7 i jedan od 10 korisnika aktualnog operativnog sistema Windows 10 ne koristi posljednju verziju, što hakerima potencijalno omogućava iskorišćavanje potencijalnih bezbednosnih propusta. (Palmer, 2019)
- Istraživači iz Google-a su otkrili više malicioznih sajtova, koji nakon posete omogućavaju hakerima da pristupe iPhone-u upotrebljavajući set do sada neotkrivenih ranjivosti u iOS-u, verzije od 10 do 12 (Whittaker, 2019). Sa druge strane, za najnoviji Apple operativni sistem iOS 13, bezbednosni stručnjaci i Američko ministarstvo odbrane (DoD) preporučuju da se nikako ne izvrši ažuriranje, jer je puno grešaka i kritičnih ranjivosti (Kelly, 2019).
- Velike probleme širom sveta izaziva specijalna vrsta zlonamernog softvera tzv.

Ransomware, koji uz pomoć enkripcije, ograničava pristup računarskim sistemima i sačuvanim fajlovima, a najčešće od žrtava traži otkup u bitkoinima. Ransomware je paralisao gradske službe u dva grada na Floridi (Ross & Leonard, 2019) koji su platili 1,1 milion dolara za otkup., kao i da je od 2013. godine najmanje 170 državnih i lokalnih samouprava u SAD priznalo da su imali iste probleme. Ransomware napad ostavio je skoro 12 sati bez struje najveći južnoafrički grad i finansijski centar, Johanezburg (Tech Radar, 2019). Takođe, ransomware napad odložio je početak školske godine. (Georg, 2019)

- Bezbednosni Istraživači su otkrili u Google Play prodavnici na desetine lažnih aplikacija za lepotu koje nemaju sopstvenu funkcionalnost, ali reprodukuju reklame na uređajima korisnika, kradu fotografije korisnika aplikacija i preusmeravaju korisnike na zlonamerne veb sajtove koji traže lične podatke (Teiss, 2019a). Takođe tu je pronađeno 15 aplikacija za GPS navigaciju, koje je preuzelo 50 miliona Android korisnika koji su sadržavali adver (softver za oglašavanje). (Teiss, 2019b)
- Više od 500 miliona Android korisnika instaliralo aplikacije sa opasnim malverom (Doffman, 2019).
- Preko 40 sertifikovanih drajvera omogućava instalaciju backdoor-a na Windows računarima (Khandelwal, 2019a).
- Chrome-ove ekstenzije i aplikacije, čak u 85% nemaju pravila o poštovanju privatnosti (Fisher, 2019a).
- Firefox ranjivost koja se eksploatiše čak 17 godina, omogućava krađu lokalnih fajlova i podataka sa računara (Dimitrova, 2019), a WinRAR program koji se često koristi na računarima, za arhiviranje fajlova, je dobio zakrpu za 19 godina star bezbednosni propust (Porter, 2019b).
- U PHP-u (Hypertext preprocessor) najpopularnijem programskom jeziku, koji se koristi u preko 78% servera na Internetu, pronađeni su mnogi nedostaci u izvršenju koda. Ova ranjivost može da omogući daljinski pristup napadačima i da kompromituje ciljani server (Wei, 2019b).
- Naizgled besplatno rešenje za gledanje prenosa sportskih događaja (fudbalske utakmice), uživo putem stream-a, može biti najopasnije i najskuplje, jer na takvim sajtovima postoje brojne skrivene opasnosti, virusi i maliciozni programi koji mogu preuzeti kontrolu nad računarom, ukrasti podatke i naneti veliku štetu (Cuthbertson, 2019).
- Nebezbedni uređaji, IoT (Internet stvari) i drugi digitalni sistemi koji se ne ažuriraju (što zbog proizvođača odn. njihovih korisnika), a povezani su sa Internetom, godinama pomažu različitim vrstama kiber kriminalaca. Najnoviji primer je Smominru, koji predstavlja zloglasni botnet, korišćen za DDoS napade, spam kampanje i ekstra profitabilno rudarenje kriptovaluta. Ovaj računarski virus se toliko brzo širi da mesečno zarazi preko 90.000 računara širom sveta (Khandelwal, 2019e).
- Milijardu mobilnih telefona rizično, zbog novootkrivenog propusta na SIM karticama, gde napadač slanjem SMS poruke može da izvrši ciljani nadzor korisnika (Chaparadza, 2019).
- Pronađeno 125 novih ranjivosti odn. nedostataka na ruterima i uređajima za bežično umrežavanje (ISBuzz News, 2019).
- Višestruke bezbednosne ranjivosti na WiFi ruterima D-Linka i Comba iz kojih cure šifre korisnika u otvorenom tekstu (Khandelwal, 2019b).
- Prevara koju je Google priznao, je da je njihov gadget Nest Secure imao ugrađen mikrofon, a da su “zaboravili” da napomene kupcima za taj dodatak (Bastone, 2019).
- Nedostaci u preko 600.000 nezaštićenih GPS pratilaca, otkrivaju podatke o lokaciji dece, starijih korisnika i kućnih ljubimaca, koji nose te uređaje sa sobom (AVAST, 2019), a aplikacije za fitnes otkrivaju informacije o vojnim bazama (Khandelwal, 2018). Ruska vojska je zabranila korišćenje mobilnih telefona zbog straha od špijunaže i društvenih medija (BBC, 2019b), a na drugoj strani, FBI, CIA i NSA preporučuju da se ne koriste Kineski telefoni marke Huawei (Vincent, 2018b) iz istih razloga.
- Hakeri ukrali lične podatke više od 70% punoletnih građana Bugarske (Wei, 2019).

- Petorica mladih srpskih hakera tvrde da poseduju JMBG gotovo svih građana Srbije (Blic, 2014).

Ipak, i pored svih navedenih primera zloupotrebe novih tehnologija i digitalnog nasilja, primat drži „digitalno crno tržište" na kome se mogu naručiti ubistva (TVC, 2019), trgovati ljudima, prodavati oružje i psihoaktivne supstance, gde cveta pedofilija i pornografija, odn. svo zlo savremenog društva. Nadu da nije baš sve tako crno daje primer uhapšene i privedene pravdi, svetske kriminalne grupe, koja je vodila onlajn prodaju "Wall Street Market" na crnom tržištu. Oni su prodavali sve što je zabranjeno od trgovine ljudima, preko narkotika i hakerskih alata do ilegalnih usluga i ukradenih finansijskih podataka. (New York Post, 2019)

5 INFORMACIONO-NEBEZBEDNA KULTURA KORISNIKA

Bez obzira na sve veći porast bezbednosnih incidenata korisnici ne žele da odustanu od svojih loših navika "zabava po svaku cenu", bahato ponašanje i ugrožavanje sebe, svoje porodice i okruženja, razmišljaju kratkoročno i neodgovorno, ne žele da se upoznaju sa problemima koje donose nove tehnologije. Moćne digitalne uređaje koriste kao pisaće mašine, e-mail kao papirnu poštu, onlajn igrice i društvene mreže, kao druženje na "poljančetu" sa prijateljima, a glavna bezbednosna mera zaštite im je "ma neće to mene, ništa ja ne krijem, nemam šta da štitim, ni da izgubim itd.", a sledeći primeri iz prakse ih demantuju:

- U Srbiji preko 50% kompjuterski nepismenih, izjavila Tatjana Matić, Državni sekretar u Ministarstvu trgovine, turizma i telekomunikacija (Ostojić, 2018b).
- 97% korisnika ne može da identifikuje fišing napade u svom e-mail-u, pokazuje istraživanje bezbednosnih stručnjaka iz kompanije Intel (Paganini, 2015).
- Uprkos rekordnom broju infekcija, korisnici još uvek ne znaju šta je ransomware (Informacija, 2016).
- Antivirusni softver nije svemoguć. Većina korisnika slepo veruje u antivirusni softver bez obzira na to da li je ažuriran ili ne, mada sledeće činjenice potvrđuju nešto sasvim drugo: antivirusni i drugi bezbednosni softveri nas štite samo od do sada poznatih malicioznih kodova (virusa), za novo kreirane zlonamerne kodove su beskorisni, i drugo, poverenje u antivirusne kompanije je narušeno njihovom čestom hakerskom kompromitacijom. Poslednji primer su tri glavne američke bezbednosne kompanije (McAfee, Symantec & Trend Micro) koje su bile ugrožene od elitnih ruskih hakera i čiji se izvorni kod (osnovni antivirusni kod, softver za web zaštitu, model veštačke inteligencije, razvojna dokumentacija kompanije) prodaje na crnom tržištu. (Mathews, 2019; CBR, 2019, Wagenseil, 2019).

6 ZAKLJUČAK

Iznete brojke govore sve. Korisnici novih tehnologija, zbog njih, gube živote, ugrožavaju zdravlje, uništavaju ugled, trpe nasilje, ostaju bez posla i finansija.

Nove tehnologije postale su „Ahilova peta" savremenog informacionog društva, posebno ako se zna da je kiber kriminal produkt i rezultat ljudske aktivnosti. Zasigurno, korisnici su najslabija karika i u situacijama kada je sistem besprekorno implementiran, a jedini pravi uzrok problema leži u njihovom neznanju ili nameri.

Posebnu pažnju treba skrenuti roditeljima da je njihova dobra namera ili povod da podele sa svojim prijateljima neke podatke, fotografije, video i sl. o svojoj deci, često nesmotrena i da lako mogu dovesti svoju decu čak i u životnu opasnost.

Roditelji, takođe, treba da budu svesni da su svojim ponašanjem očigledni primer deci, pa ako oni imaju nalog na društvenim mrežama, igraju onlajn igrice, kockaju se i klade, vrlo je verovatno da će to i njihova deca raditi.

Autor, prevashodno, rešenje vidi u podizanje svesti korisnika novih tehnologija kroz upoznavanje sa velikim brojem bezbednosnih primera iz prakse.

Svest o informacionoj bezbednosti je isto toliko važna, kao i bilo koja bezbednosna tehnika ili procedura koja može biti zloupotrebljena, pogrešno interpretirana ili je krajnji korisnici ne koriste, tako da se gubi njena prava korisnost.

CITIRANA DELA

Abagnale, F. (2019). *Never do these 2 things because 'that's 98% of me stealing your identity'.* https://finance.yahoo.com/news/frank-abagnale-it-only-takes-2-pieces-of-information-to-steal-98-of-your-identity-142210933.html?guccounter=1

Adejn, E. (2019). *Plavi kit: Šta je istina o onlajn „samoubilačkom izazovu“*. https://www.bbc.com/serbian/lat/svet-47672762

Associated Press. (2019). *Germany arrests 3 in the 'Wall Street Market' darknet probe.* https://nypost.com/2019/05/03/germany-arrests-3-in-wall-street-market-darknet-probe/

AVAST. (2019). *Avast Discovers Security Flaws in Widespread GPS Trackers Exposing Locations of Over Half a Million Children and Elderly* https://press.avast.com/avast-discovers-security-flaws-in-widespread-gps-trackers-exposing-locations-of-over-half-a-million-children-and-elderly

Badshah, N. (2019). *Saudis hacked Amazon chief Jeff Bezos's phone, says company's security adviser*. https://www.theguardian.com/technology/2019/mar/31/saudis-hacked-amazons-jeff-bezos-phone-claims-security-chief-jamal-khashoggi-mohammed-bin-salman

Bartz, D. (2019). Google's YouTube to pay $170 million penalty for collecting data on kids https://www.reuters.com/article/us-google-ftc/googles-youtube-to-pay-170-million-penalty-for-collecting-data-on-kids-idUSKCN1VP1RR

Bastone, N. (2019). *Google says the built-in microphone it never told Nest users about was 'never supposed to be a secret'.* https://www.businessinsider.com/nest-microphone-was-never-supposed-to-be-a-secret-2019-2

BBC. (2014.a). *Barack Obama's credit card 'declined'.* http://www.bbc.com/news/world-us-canada-29664831

BBC. (2019.b). *Russia bans smartphones for soldiers over social media fears.* https://www.bbc.com/news/world-europe-47302938

Blic. (2014). *DRŽIMO SRBIJU U ŠACI Hakeri tvrde da su ukrali JMBG "gotovo svih građana"* https://www.blic.rs/vesti/drustvo/drzimo-srbiju-u-saci-hakeri-tvrde-da-su-ukrali-jmbg-gotovo-svih-gradana/j59315x

Carey, B. (2019). *In Month After '13 Reasons Why' Debut on Netflix, Study Finds Teen Suicide Grew.* https://www.nytimes.com/2019/04/29/health/13-reasons-why-teen-suicide.html

Carrie Wong, J. (2019, 01 30). *Facebook posts record profit despite year of scandal.* https://www.theguardian.com/technology/2019/jan/30/facebook-fourth-quarter-profits-revenues-earnings

Carrie Wong, J. (2019b, 09 05). *Facebook confirms 419m phone numbers exposed in latest privacy lapse*. https://www.theguardian.com/technology/2019/sep/04/facebook-users-phone-numbers-privacy-lapse

Castello, J. (2019). *New study finds that 74% have been harassed in online multiplayer games*. https://www.rockpapershotgun.com/2019/07/27/new-study-finds-that-74-have-been-harassed-in-online-multiplayer-games/

CBR. (2019). *Trend Micro Admits it Was Hacked, Symantec Denies Claims of "Fxmsp" Breach.* https://www.cbronline.com/news/trend-micro-symantec-fxmsp

Chaparadza, A. (2019, 09 13). *New SIM Card Flaw Lets Hackers Hijack Any Phone Just By Sending SMS, 1 Billion Phones At Risk.* https://www.techzim.co.zw/2019/09/new-sim-card-flaw-lets-hackers-hijack-any-phone-just-by-sending-sms-1-billion-phones-at-risk/

Conger, K. (2019). *Twitter C.E.O. Jack Dorsey's Account Hacked.* https://www.nytimes.com/2019/08/30/technology/jack-dorsey-twitter-account-hacked.html?smid=tw-nytimes&smtyp=cur

Constine, J. (2019, 07 25). *Facebook pays teens to install VPN that spies on them.* https://www.techradar.com/news/johannesburg-ransomware-attack-leaves-city-without-power?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19

CORDIS. (2019). *Study finds users who leave Facebook are happier, but less informed.* https://phys.org/news/2019-02-users-facebook-happier.html

Cuthbertson, A. (2019). *Football live stream: Free Premier League links spreading online could 'wreak havoc'* https://www.independent.co.uk/sport/football/premier-league-live-stream-free-watch-reddit-football-fixtures-a9050316.html

Dimitrova, E. (2019). *17-Year Old Bug in Firefox Allows Local Files Theft Attacks.* https://sensorstechforum.com/17-year-old-bug-firefox-local-files-theft/

Doffman, Z. (2019). *New Android Warning: 500 Million Users Have Installed Apps Hiding Devious Malware—Uninstall Now.* https://www.forbes.com/sites/zakdoffman/2019/09/20/new-android-warning-500m-users-have-installed-apps-hiding-nasty-malwareuninstall-now/?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19#70c4e6c212be

Dough, C. (2019). A mom found videos on YouTube Kids that gave children instructions for suicide https://edition.cnn.com/2019/02/25/tech/youtube-suicide-videos-trnd/index.html

Ejdus, F., Unijat, J., Milošević M. (2009). Istraživanje i podizanje nivoa bezbednosne kulture mladih, http://www.bezbednost.org/Svi-projekti/700/Istrazivanje-i-podizanje-nivoa-bezbednosne.shtml#sthash.IRucHXPn.dpuf

Fisher, C. (2019a). 85 percent of Chrome apps and extensions lack a privacy policy. https://www.engadget.com/2019/02/22/chrome-app-extension-security-flaws/?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19

Fisher, C. (2019b). *Two-thirds of online gamers in the US experience 'severe' harassment.* https://www.engadget.com/2019/07/25/adl-harassment-online-gaming-survey/?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19

Gambling. (2017). Young people and gambling 2017. http://live-gamblecom.cloud.contensis.com/PDF/survey-data/Young-People-and-Gambling-2017-Report.pdf

Georg, M. (2019). *NY School Delays Start of Year After Ransomware Attack*. https://www.nbcnewyork.com/news/local/NY-School-Delays-Start-of-Year-After-Ransomware-Attack-559322971.html

Gudmen, M. (2017). *Zločini budućnosti*. Laguna, Beograd

Hart, B. (2019). Consider this before you share your kids' photos on social media without their consent. https://www.abc.net.au/life/sharing-photos-of-your-children-on-social-media-without-consent/10798576

Hern, A. (2019, 08 13). *Facebook admits contractors listened to users' recordings without their knowledge.* https://www.theguardian.com/technology/2019/aug/13/facebook-messenger-user-recordings-contractors-listening

Huggler, J. (2016, 09 14). *Austrian teenager sues parents for 'violating privacy' with childhood Facebook pictures.* https://www.telegraph.co.uk/news/2016/09/14/austrian-teenager-sues-parents-for-violating-privacy-with-childh/

Informacija, 26.5.2016., Uprkos rekordnom broju infekcija, korisnici još uvek ne znaju šta je ransomware. https://www.informacija.rs/Vesti/Uprkos-rekordnom-broju-infekcija-korisnici-jos-uvek-ne-znaju-sta-je-ransomware.html

ISBuzz News. (2019). *125 New Flaws Found In Routers And NAS Devices From Popular Brands.* https://www.informationsecuritybuzz.com/expert-comments/125-new-flaws-found-in-routers-and-nas-devices-from-popular-brands/

Keach, S. (2018). *Super Mario Odyssey porn warning as hackers add smutty pics into Nintendo Switch game.* https://www.thesun.co.uk/tech/6616353/super-mario-odyssey-porn-nintendo-switch-hacker-pictures/

Kelly, G. (2019). Apple iOS 13 Is Full Of Bugs, Reports Warn. https://www.forbes.com/sites/gordonkelly/2019/09/19/apple-ios13-upgrade-problems-iphone-11-pro-max-xs-max-xr-update/#6a23afa322bc

Kelly, M. (2019). *FTC hits Facebook with $5 billion fine and new privacy checks.* https://www.theverge.com/2019/7/24/20707013/ftc-facebook-settlement-data-cambridge-analytica-penalty-privacy-punishment-5-billion

Khandelwal, S. (2018, 01 29). *Heat Map Released by Fitness Tracker Reveals Location of Secret Military Bases.* https://thehackernews.com/2018/01/strava-heatmap-location-tracking.html

Khandelwal, S. (2019a). *Over 40 Drivers Could Let Hackers Install Persistent Backdoor On Windows PCs*. https://thehackernews.com/2019/08/windows-driver-vulnerability.html

Khandelwal, S. (2019b). *Some D-Link and Comba WiFi Routers Leak Their Passwords in Plaintext.* https://thehackernews.com/2019/09/router-password-hacking.html

Khandelwal, S. (2019c). *Smominru Botnet Indiscriminately Hacked Over 90,000 Computers Just Last Month.* https://thehackernews.com/2019/09/smominru-botnet.html

Kroll, L., & Dolan, A. (2019). *BillionaireS*. https://www.forbes.com/billionaires/#73e2013b251c

Landsverk, G. (2019). *Trump says 'gruesome and grisly video games' are to blame for mass violence, but the reality is more complicated.* https://www.insider.com/do-video-games-cause-mass-violence-not-according-to-research-2019-8

Lee, D. (2019). https://www.bbc.com/news/technology-46998055

Lee, T. (2018). *Despite Privacy Uproar, Facebook Users Aren't Changing Their Privacy Settings.* https://www.ubergizmo.com/2018/04/facebook-users-not-changing-privacy-settings/

Leković, J. (2013). *Život nije igra.* http://zivotnijeigra.com/zivotnijeigra/wp-content/uploads/2013/01/REZULTATI-ZA-KONFERENCIJU-NOVINARI-2.pdf

Lo, S., M. (2015). *Prvo razmisli – borba protiv digitalnog nasilja.* http://www.mpn.gov.rs/prvo-razmisli-borba-protiv-digital/

Lyons, K. (2019, 03 29). *Apple Martin tells off mother Gwyneth Paltrow for sharing photo without consent.* https://www.theguardian.com/film/2019/mar/29/apple-martin-tells-mother-gwyneth-paltrow-off-for-sharing-photo-without-consent

Mangan, L. (2016, 09 17). *I don't put pictures of my children on Facebook - and you shouldn't either.* https://www.telegraph.co.uk/family/parenting/i-dont-put-pictures-of-my-children-on-facebook---and-you-shouldn/

Mathews, L. (2019). *Elite Russian Hackers Claim To Have Breached Three Major U.S. Antivirus Makers.* https://www.forbes.com/sites/leemathews/2019/05/09/russian-hackers-breach-antivirus-makers/#7550a2c11db2

Ng, A. (2019). Facebook still tracks you after you deactivate account. https://www.cnet.com/news/facebook-is-still-tracking-you-after-you-deactivate-your-account/?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19

Ostojić, T. (2018). *U Srbiji preko 50% kompjuterski nepismenih.* https://pcpress.rs/u-srbiji-preko-50-kompjuterski-nepismenih/

Paganini, P. (2015). *New Intel Security study shows that 97% of people can't identify phishing emails*, https://securityaffairs.co/wordpress/36922/cyber-crime/study-phishing-emails-response.html

Palmer, D. (2019). *PC security warning: That out-of-date software is putting you at risk.* https://www.zdnet.com/article/pc-security-warning-that-out-of-date-software-is-putting-you-at-risk/

PC Press. (2019). *Svaka treća mlada osoba u Srbiji trpi digitalno nasilje.* https://pcpress.rs/svaka-treca-mlada-osoba-u-srbiji-trpi-digitalno-nasilje/

Porter, J. (2019a). *Google fined €50 million for GDPR violation in France.* https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil

Porter, J. (2019b, 02 21). *WinRAR patches 19-year-old security vulnerability that put millions at risk*. https://www.theverge.com/2019/2/21/18234448/winrar-winace-19-year-old-vulnerability-patched-version-5-70-beta-1?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19

Porter, J. (2019c). *Facebook admits harvesting 1.5 million people's email contacts without consent.* https://www.theverge.com/2019/4/18/18485089/facebook-email-password-contacts-upload-1-5-million-security-cybersecurity?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19

Ross, A. & Leonard, B. (2019, 06 28). *Ransomware attacks put Florida governments on alert.* https://www.tampabay.com/florida-politics/buzz/2019/06/28/ransomware-attacks-put-florida-governments-on-alert/

Saviano, R. (2019). *Roberto Saviano and Edward Snowden: "I'm fighting for the Internet to be free again. Zuckerberg? He'll repent".* https://www.repubblica.it/esteri/2019/09/13/news/roberto_saviano_edward_snowden_intervi ew-235883649/

Schneier, B. (2015). *RM Education*, https://www.rm.com/support/technicalarticle.asp?cref=tec377232

Schwartz, M. (2019). *Apple iPhones Hacked by Websites Exploiting Zero-Day Flaws,* https://www.bankinfosecurity.com/apple-iphones-hacked-by-websites-exploiting-zero-day-flaws-a-13001

Sputnik International. (2019, 09 14) *Go West? Edward Snowden Hopes France's Emmanuel Macron Will Approve His Asylum Application.* https://sputniknews.com/europe/201909141076804460-go-west-edward-snowden-hopes-frances-emmanuel-macron-will-approve-his-asylum-application/

Stevens, K. (2019). *Children as young as 10 are using sophisticated cyber-attacks to take out opponents on online gaming sensation Fortnite.* https://www.dailymail.co.uk/news/article-6738141/NSW-children-young-10-using-sophisticated-cyber-attacks-opponents-Fortnite.html?utm_medium=email&utm_source=flipboard

Stone, J. (2019). *Google's Triada backdoor demonstrates vulnerabilities in the mobile supply chain.* https://www.cyberscoop.com/android-backdoor-triada-mobile-supply-chain/

Tech Crunch, 29.1.2019.b, https://techcrunch.com/2019/01/29/facebook-project-atlas/

Teiss. (2019.b, 01 21). *15 fake navigation apps on Google Play Store enjoyed 50m downloads.* https://www.teiss.co.uk/fake-navigation-apps-play-store/

Teiss. (2019a, 01 31). *Fake beauty apps on Google Play Store enjoyed millions of downloads.* https://www.teiss.co.uk/fake-beauty-apps-play-store/

Thubron, R. (2019, 09 19). *RuneScape player spends $62,000 on microtransactions.* https://www.techspot.com/news/81968-runescape-player-spends-62000-game-microtransactions.html

Turner, G. (2019). *The Data Big Tech Companies Have On You (Or, At Least, What They Admit To).* https://securitybaron.com/blog/the-data-big-tech-companies-have-on-you-or-at-least-what-they-admit-to/

TVC. (2019, 07 16). Ubiystvo sledovatelya Shishkinoy svyazali s delom "darkneta". https://www.tvc.ru/news/show/id/159580

Vincent, J. (2018). *Don't use Huawei phones, say heads of FBI, CIA, and NSA.* https://www.theverge.com/2018/2/14/17011246/huawei-phones-safe-us-intelligence-chief-fears

Wagenseil, T. (2019). *Hackers Say They've Breached Three Antivirus Companies.* https://www.tomsguide.com/us/antivirus-companies-breached,news-30045.html

Wei, W. (2019). *Hacker Stole Data of Over 70% Bulgarian Citizens from Tax Agency Servers.* https://thehackernews.com/2019/07/bulgaria-nra-data-breach.html

Wei, W. (2019b). *Multiple Code Execution Flaws Found In PHP Programming Language.* https://thehackernews.com/2019/09/php-programming-language.html

Whittaker, Z. (2019, 08 29). *Malicious websites were used to secretly hack into iPhones for years, says Google.* https://techcrunch.com/2019/08/29/google-iphone-secretly-hacked/

Winder, D. (2019). *Windows Users Warned To Update Now As 'Complete Control' Hack Attack Confirmed.* https://www.forbes.com/sites/daveywinder/2019/08/24/windows-users-warned-to-update-now-as-complete-control-hack-attack-confirmed/?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19#31d9f5f45bdb

Wodinsky, S. (2018). *Many Android devices ship with firmware vulnerabilities, researchers find.* https://www.theverge.com/2018/8/10/17677206/android-devices-firmware-security-flaws-kryptowire?utm_source=PCPress&utm_medium=post&utm_campaign=Septembar19

Datum prve prijave: 26.08.2019.
Datum prijema korigovanog članka: 07.09.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

Style – APA Sixth Edition:

Milanović, Z. (2019, 10 15). Zloupotreba novih tehnologija i digitalno nasilje. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 86-98. doi:10.12709/fbim.07.07.02.10

Style – Chicago Sixteenth Edition:

Milanović, Zoran. 2019. "Zloupotreba novih tehnologija i digitalno nasilje." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 86-98. doi:10.12709/fbim.07.07.02.10.

Style – GOST Name Sort:

Milanović Zoran Zloupotreba novih tehnologija i digitalno nasilje [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 86-98.

Style – Harvard Anglia:

Milanović, Z., 2019. Zloupotreba novih tehnologija i digitalno nasilje. *FBIM Transactions,* 15 10, 7(2), pp. 86-98.

Style – ISO 690 Numerical Reference:

Zloupotreba novih tehnologija i digitalno nasilje. **Milanović, Zoran.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 86-98.

FBIM Transactions
DOI 10.12709/fbim.07.07.02.11

PRIMENA RFID TEHNOLOGIJE – NEKI PROBLEMI I PRAVCI RAZVOJA

APPLICATION OF RFID TECHNOLOGY – SOME PROBLEMS AND DEVELOPMENT DIRECTIONS

Lyudmila Prigoda
Maykop State Technological University, Maykop, Russian Federation

Milanka Bogavac
Faculty of Business and Law, „Union – Nikola Tesla“ University, Belgrad, Serbia

Jelena Maletić
Technical School GSB, Belgrade, Serbia

JEL Category: **R41**

Apstrakt

U uslovima savremenog poslovanja i sve veće primene kompjuterskih tehnologija, postavljaju se sve stroža vremenska ograničenja, sve veći zahtevi u pogledu efikasnosti upotrebe mehanizacije, automatizacija tehnoloških procesa, veća pouzdanost i niži troškovi i bolji ekonomski pokazatelji. Kao jedno od pogodnih rešenja, pojavljuje se upotreba RFID tehnologije. RFID sistemi poslednjih desetak godina imaju sve značajnu ulogu u povećanju efikasnosti i smanjenju troškova poslovanja i pored toga što još uvek nisu otkriveni ni iskorišćeni svi potencijali ove tehnologije. RFID tehnologija pruža praktične koristi svakome ko ima potrebe da prati fizičko prisustvo objekata u nekoj sredini. Mnogi unapređuju lance snabdevanja i procese proizvodnje uvođenjem ove tehnologije. Razlozi za korišćenje RFID tehnologije u velikim sistemima su mogućnost potpune automatizacije rada primenom kompjuterskog upravljanja i nadzora, kao i bolja kontrola izdavanja i praćenja stanja u magacinima, uz smanjenje mogućnosti greške kao i krađe i prevare, povećanje profita i kvaliteta, dobijanje izveštaja o izdavanju delova ili goriva (u koje vreme je preuzeto, u kojoj količini...) i dr. U ovom radu je detaljnije prikazano jedno rešenje za kontrolu točenja goriva na stanicama za snabdevanje gorivom na bazi RFID tehnologije. Razmotrene su prednosti i nedostaci ove tehnologije, ekonomski aspekti primene, kao i mogućnosti potpune zaštite od krađe i raznih drugih prevara. Analiza je pokazala da efekti mogu biti: smanjenje ukupnih troškova, optimizacija postojećeg sistema snabdevanja, optimizacija postojećeg sistema praćenja kvantitativnog stanja zaliha goriva na stanicama za snabdevanje gorivom, potrošnja goriva po vozilima i dr. Na kraju rada je analizirana budućnost primene RFID tehnologije, putevi daljeg razvoja i potencijalni rizici primene ove tehnologije.

Adresa autora zaduženog za korespodenciju:
Lyudmila Prigoda
lv_prigoda@mail.ru

***Ključne reči**: Informacione tehnologije, RFID, kontrola, gorivo, nedostaci, napadi*

Abstract
In the conditions of modern business and the increasing use of computer technologies, more time constraints are being imposed to businesses, increasing demands in terms of efficiency of the use of machinery, automation of technological processes, higher reliability, lower costs and better economic indicators. As one of the convenient solutions, the use of RFID technology appears. RFID systems are playing a significant role in increasing efficiency and reducing operating costs in the last dozen years, even though all the potentials of this technology have not yet been discovered or exploited. RFID technology provides practical benefits to anyone who needs to monitor the physical presence of objects in a certain environment. Many improve supply chains and production processes by introducing this technology. The reasons for the use of RFID technology in large systems are the ability to fully automate the work with the use of computer management and control, better control of issuing and monitoring the stock situation, while reducing the possibility of error as well as theft and fraud, increasing profits and quality, obtaining reports on the issue of parts or fuel (at what time it was taken, in what quantity ...) etc. In this paper, one RFID solution for controlling fuel refueling at fuel supply stations is shown in more detail. The advantages and disadvantages of this technology, the economic aspects of the application, as well as the possibilities of complete protection against theft and various other frauds are considered. The analysis has shown that the positive effects can be a reduction of total costs, optimization of the existing supply system, optimization of the existing system for monitoring the quantitative state of the fuel stock at fuel stations, fuel consumption by vehicles, etc. At the end of the paper, the future of RFID technology, the paths for further development, and the potential risks of applying this technology are analyzed.

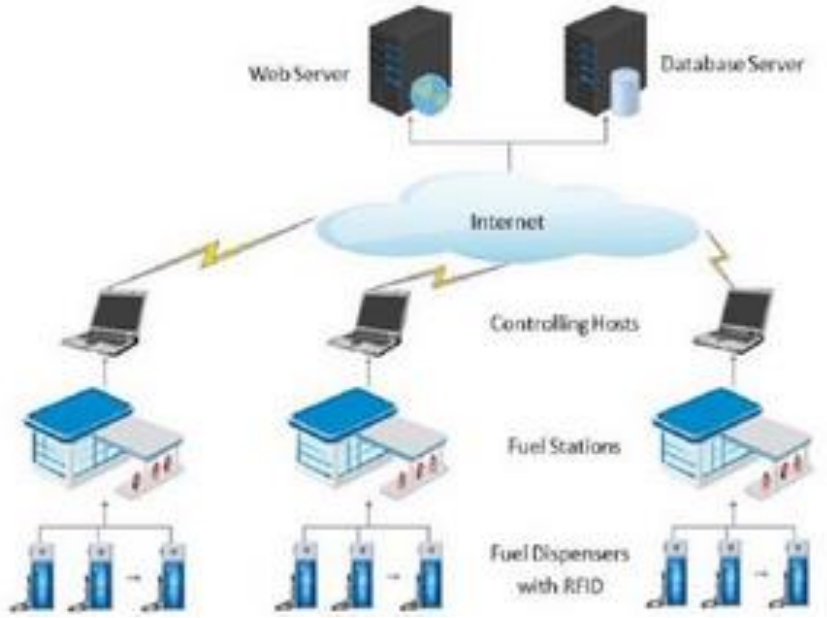
***Keywords:** Information Technologies, RFID, control, fuel, disadvantages, attacks.*

1 GLAVNI ELEMENTI I PRINCIPI RADA RFID TEHNOLOGIJE

Radio Frequency Identification (u daljem tekstu: RFID), što u slobodnom prevodu znači, identifikacija putem radio talasa, je sistem daljinskog slanja i prijema podataka pomoću RFID taga (primo-predajnik/transmiter). RFID tag je komponenta koja se može zalepiti ili ugraditi na željeno mesto proizvoda, pakovanja, teretne jedinice i dr. Svaki RFID tag (pasivan, polu-pasivan i/ili aktivni) sadrži u sebi antenu koja mu omogućava prijem i slanje radio talasa od RFID primopredajnika, preko čitača do objekta i nazad. Proces prikupljanja, odn. prenosa podataka je u osnovi "beskontaktan". Poseduje i niz drugih povoljnih karakteristika, među kojima su i da ne zavisi od operatera, da prevazilazi ograničenja drugih identifikacionih sistema zato što može efektivno raditi u okruženju sa mnogo prašine, prljavštine, sa velikom vlažnošću, lošom vidljivošću, itd. Pored toga, nekim RFID tagovima nije neophodno posebno napajanje električnom energijom, a RFID niskofrekventni sistem funkcioniše i kroz većinu nemetalnih materijala. Aplikacija RFID tehnologije, je sigurna, jedinstvena, dugotrajna i izuzetno pouzdana u smislu identifikacije, nezavisna od specifičnog uticaja okoline i nije joj potrebna optička vidljivost. U većini okruženja, RFID postiže 99,5%-100% očitavanja u prvom skeniranju. Takođe, RFID je bez pokretnih delova ili optičkih komponenti, mada se RFID tagovima mogu pridodati oznake sa bar-kodovima i/ili drugim grafičkim prikazima. Glavna karakteristika RFID tehnologije, je mogućnost očitavanja starih i upis novih podataka u tag dok se teretna jedinica (roba), za koju je tag fiksiran, kreće u transportnom procesu. Ovakav način rada nije moguć sa starijim sistemima za identifikaciju kao što je npr. bar-kod. Čitač i tagovi (transponderi) su programabilni, tako da se može realizovati sistem (kroz integraciju odgovarajućih hardverskih komponenti i razvoj softverskih aplikacija) koji zadovoljava specifične zahteve korisnika.

U svetu se koristi RFID tehnologija za kontrolu točenja goriva (The HID Global identiFUEL™ system, RFACS - RFID Fuel Accounting System Marine/Fleet, OPW Fuel Management Systems, Fuel Shield i dr.), (GASNGO, 2013). Opšta konfiguracija takvog sistema data je na slici 1. U Srbiji je, pre više godina, patentiran jedan takav sistem od strane SDD Informaciono Tehnološka

Grupa (SDD ITG) pod nazivom ITGfdc-01 a primenjen je u JGSP „Novi Sad". Ovaj sistem obezbeđuje da se gorivo može točiti isključivo u posebno identifikovana vozila, uz automatsku akviziciju svih relevantnih podataka u vezi točenja goriva. Detaljnije je prikazan u (Čekerevac, Matic, Djuric, & Čelebić, 2006) i (SDD-ITG, 2017), pa će ovde biti prikazan samo u najkraćim crtama. Glavni elementi ovakvog sistema su: identifikator vozila, identifikacione kartice vozača i točioca goriva, kontrolni kompjuter i neophodne mrežne komponente, i aplikativni softver za kontrolu točenja goriva. U zapisu događaja nalaze se očitani podaci sa sva tri identifikatora, datum i vreme obavljenog točenja, te vrsta i količina preuzetog goriva.



Slika 1. Arhitektura sistema

Izvor: (Fawzi & Mohannad, 2015)

Identifikator vozila je RFID tag, postavljen u blizini ulivnog grla rezervoara za gorivo na vozilu, u dometu antene za identifikaciju vozila. On sadrži podatke o vozilu, kao što su: registarski i/ili garažni broj, vrsta goriva koje vozilo koristi i sl. Identifikator ima svoj nepromenljivi kod (dužine 32 bita) i 256B memorije tipa „piši-briši". Kontroler pumpe za gorivo ITGkp-02 predstavlja namenski kontrolno-upravljački računar, a sastoji se od nekoliko antena i čitača RFID taga.

Tabela 1. Efekti primene sistema za točenje goriva

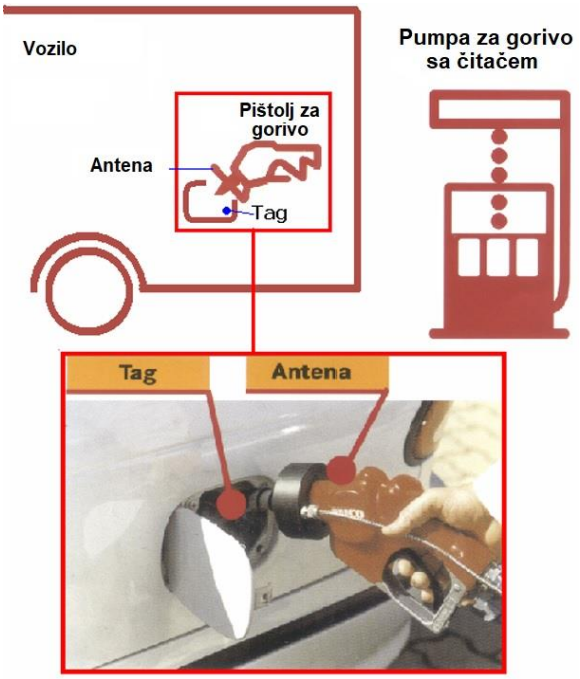
Broj vozila	Orijentaciona cena sistema (u EUR)	Mesečni gubitak (u EUR)	*ROI (u danima) za 2,5 l/vozilu
200	25.000	10.814	69
400	50.000	21.628	69
600	72.000	32.422	67
800	96.000	43.256	67
1.000	115.000	54.070	64

* ROI (Returned of Investment)

Izvor (Jiho & et all, 2007).

Antena za identifikaciju vozila postavlja se oko „pištolja" za točenje goriva, blizu rukohvata. Povezana je sa čitačem pomoću specijalnog kabla. Druga antena, slika 3, služi za čitanje identifikacionih kartica vozača i točioca goriva. Kontroler upravlja radom ovih antena i pumpe, tako što dozvoljava/zabranjuje sipanje goriva, a sve relevantne podatke pamti u svojoj memoriji čak i kada uređaj ostane bez napajanja električnom energijom. Da bi gorivo moglo da se toči neophodno je da sva tri taga budu očitana, s tim što se identifikacija vozila vrši za sve vreme

točenja. Čim identifikator vozila izađe iz dometa antene ulivanje goriva se prekida.



Slika 2. Blok šema sistema za kontrolu točenja goriva i detalj pištolja za gorivo sa antenom za identifikaciju vozila
Izvor: (Čekerevac, Matic, Djuric, & Čelebić, 2006)

Slika 3. Antena čitača ID kartica vozača i točioca

Izvor: (Čekerevac, Matic, Djuric, & Čelebić, 2006) i (SDD-ITG, 2017)

Prvi korisnik sistema ITGfdc-1 je preduzeće JGSP „Novi Sad“ od 2005. godine, a kasnije su ovaj sistem implementirala i druge organizacije (Andrejić, 2001), (Jovanović, 2010). Povratak uloženih sredstava (Return of Investment –ROI) u ovaj sistem, procenjen je od strane proizvođača uređaja na osnovu iskustvenih podataka o nestanku izvesnih količina goriva. U tabeli 1 prikazani su neki efekti primene sistema za kontrolu točenja goriva ITGfdc -1.

Administrativni obrada podataka ne zahteva dokumentaciju o primopredaji goriva u obliku papirnih dokaza, s obzirom na to da su svi podaci u elektronskom obliku poslati i smešteni u administratorovom kompjuteru. Ako neki od podataka iz taga montiranih na vozilu nije validan, ili je obavljena procedura istakanja pogrešne vrste goriva, ili točenje nije dozvoljeno tom vozaču ili vozilu, ili točilac na pumpi nema dozvolu za točenje, uključiće se alarm, u vidu zvučnog i svetlosnog signala. U nepredviđenim situacijama, kada, na primer, gorivo treba istočiti u kanister, bure ili nešto slično, mora biti upotrebljena specijalna identifikaciona kartica od strane autorizovane osobe. Pravila za korišćenje specijalne kartice određuje uprava kompanije.

2 PREDNOSTI I NEDOSTACI RFID TEHNOLOGIJE

Kada se govori o prednostima i nedostacima obično se upoređuju dve tehnologije sličnih karakteristika i funkcija RFID, tradicionalni dvo-dimenzionalni kodovi, bar kodovi, magnetne i/ili IC kartice. Glavne prednosti RFID tehnologije u odnosu na bar kod tehnologiju su:

- nije potrebna optička vidljivost, odnosno prazan prostor između čitača i taga,
- čitanje i pisanje podataka se vrši bez ikakvog kontakta s objektom, sa očitavanjem kada tagovi nisu direktno dostupni čitaču na udaljenosti do 10 m,
- praćenje informacija u procesu kontrole je kvalitetnije sa većom brzinom očitavanja, tako da se u jednoj sekundi može očitati više stotina tagova. Za razliku od bar kodova koji se vrlo lako mogu oštetiti i time izgubiti informaciju,
- nema negativnih posledica uticaja okoline (vlaga, prašina) zahvaljujući komunikaciji preko radio talasa. Voda, sredstva za čišćenje, boja, alkohol, rashladna sredstva, itd., ne oštećuju RFID tagove, a čestice i nemetalne prepreke ne ometaju im rad, vrlo su otporni na fizička opterećenja,
- oblik taga može da bude raznovrstan, prilagođen aplikaciji,

- tag može da bude vrlo mali, i otporan je na refleksiju svetla, a ne ometa ga ni potpun mrak,
- tag ima jako dug životni vek, ponovno korišćenje istog taga (tip za višestruko korišćenje) smanjuje troškove, i ne zahteva nikakvo održavanje,
- u tag mogu da se upisuju informacije (npr. da je određeni komad proizvoda rezervisan ili već plaćen, informacije o uslovima garancije i sl.),
- materijali koji nisu od metala, kao papir, drvo, plastika i sl. ne ometaju komunikaciju između antene i taga, iako nisu transparentni,
- tag može da ima veliki kapacitet memorije za čuvanje podataka.

Kod kontrole goriva, primena RFID svakako pruža dosta prednosti, jer se ostvaruju: potpuna automatizacija rada primenom kompjuterskog upravljanja i nadzora, kontrola izdavanja i praćenja stanja goriva (automatsko merenje nivoa goriva, temperature i indikacije vode u cisternama), nemogućnost nastajanja ljudske greške, prevare ili namernog otuđenja goriva, stalna težnja za povećanjem ekonomičnosti funkcionisanja, profita i kvaliteta usluga, dobijanje automatizovanih pouzdanih izveštaja o preuzetom gorivu (vreme izdavanja, količina goriva, registarski broj vozila i dr.), mogućnost povezivanja programa o izdatim količinama goriva i programa za praćenje troškova transporta.

U postojećim uslovima eksploatacije praćenja kvantitativnog stanja goriva na stanicama za snabdevanje gorivom u velikim sistemima, kod nas ima sledeće nedostatke (Fawzi & Mohannad, 2015), (Ilić & Radosavljević, Unapređenje kvantitativnog stanja mirnodopskih zaliha pogonskog goriva na pumpnim stanicama, 2011), (Ilić, 2009): dobijanje nepouzdanih podataka, usled zastarele opreme za manipulaciju sa gorivom i merne opreme, manuelnog prikupljanja podataka i nastajanje nedozvoljenih manjkova zbog subjektivnih ljudskih grešaka ili namernih prevara. Problemi sa RFID-om mogu se podeliti na nekoliko kategorija:

- tehnički problemi sa RFID, zbog nedostatka standarda opreme i softvera,
- problemi sa privatnošću i etikom korišćenja RFID-a.
- visoki investicijski troškovi,
- mogućnost prekida rada informacionog sistema; kod kvara uređaja potrebna je stručna pomoć,
- rad sistema nije moguć bez električne energije (mada u slučaju nalivanja goriva pri nestanku električne energije neće raditi ni pumpe, pa se ovaj nedostatak u ovoj nameni i ne treba smatrati nedostatkom).

Jedan od značajnih problema je nedostatak standarda, jer se RFID tehnologija na različite načine implementira od strane različitih proizvođača, zbog čega se i dalje radi na globalnim standardima. Ako je, jedna organizacija vlasnik RFID sistema, da bi ga koristila, neka druga mora da plati pristup i da zavisi od prve, što je malo neugodan scenario. S druge strane, ukoliko svaka organizacija ima svoj sistem, kao npr. Mastercard Contactless (ranije brendiran kao Paypass), ExpressPay, payWave (svi bazirani na ISO/IEC 14443), da bi ih koristio kupac bi morao sa sobom da nosi mnogo različitih kartica i uređaja. Domet RFID uređaja je ograničen, što može biti i prednost i nedostatak.

3 MOGUĆNOST SMANJENJA SPOLJNIH UTICAJA NA RFID

Problemi sa sigurnošću, privatnošću i etikom primene RFID tehnologije, zahtevaju prepoznavanje kritičnih situacija iz kojih mogu nastati veći problemi u smislu zaštite imovine i lica. Pitanje sigurnosti RFID-a često se čini paradoksalnim po prirodi, jer upotreba RFID povećava sigurnost u nekim oblastima, dok sama RFID komunikacija predstavlja potencijalni uzrok novih rizika privatnosti i sigurnosti.

Jedan od problema RFID je „Reader Collision", u kojoj je signal jednog čitača ometan od signala iz drugog, tako da se njihova pokrivenost preklapa. Korišćenjem vremenske podele, višestruki pristupi se mogu prevazići, postavljanjem čitača u različite vremenske okvire, kako bi bez ometanja funkcionisali. Međutim, važno je da softver povezan sa čitačem prepoznaje kada su iste RFID oznake pročitane više od jednom u području preklapanja čime se postiže odgovarajuće podešavanje sistema. Sistemi moraju biti pažljivo postavljeni kako bi se izbegao ovaj problem. Mnogi sistemi koriste singularni protokol.

Takođe je prepoznat problem „Tag Collision" kod pasivnih tagova, koji nastaje kada istovremeno čitač RFID tagova prima poruke više tagova i čitač ne može da ih identifikuje istovremeno. Ovaj problem se često vidi kad god se veliki volumen oznaka mora čitati istovremeno u istom RF polju u kom slučaju dolazi do sudara oznaka. Međutim, kako je vreme čitanja veoma kratko, potrebno je a i lakše je, razviti sisteme koji osiguravaju da se oznake odazivaju jedna po jedna, kao što su protokol Queri Tree i ALOHA. Protokol Kueri Tree se koristi za problem sa zadrškom tag-zagušenja i ALOHA za smanjenje sudara pasivnih oznaka (Jiho & et all, 2007).

Postoje i potencijalni problemi od instaliranja RFID-a pored drugih bežičnih sistema, tzv. RFID interferenca, koji mogu sprečiti uspešan rad RFID sistema. Mogu postojati dve grupe smetnji:

- ometanje koje sprečava prenošenje i/ili primanje ispravnih podataka i kao rezultat degradira performanse jednog ili drugih bežičnih sistema; i
- rizici da se signali jednog sistema pogrešno tumače kao važeći podaci kod drugog sistema.

Područja u kojima se najčešće pojavljuju unakrsne smetnje između RFID sistema i bežičnih lokalnih mreža su u oblasti UHF na 2,45GHz. Problemi sa interferencijama za sisteme pasivnih tagova dodatno su smanjeni u Evropi, jer evropski standardi ograničavaju snagu koja se koristi u takvim sistemima na 2W (u poređenju sa 2,4W u SAD). Inače, pored UHF područja, RFID sistemi rade u više frekventnih opsega. Niska frekvencije (LF) je 125-134 kHz. Visoke frekvencije (HF) se kreće od 3 MHz do 30 MHz, pri čemu je 13,56 MHz tipična frekvencija koja se koristi za HF. Tagovi za ultra visoke frekvencije (UHF) rade u područjima od 433 do 915 MHz ili na 2,45 GHz.

Jedna posebna vrsta napada naziva se "Relay Attacks", koja je po svojoj prirodi jedna od vrsta Man-in-the-Miidle napada o kome je bilo reči u (Cekerevac, Dvorak, Prigoda, & Cekerevac, 2017), a predstavlja napad u kome se koriste resursi treće strane. Ove i druge probleme treba pozvati pri forenzičkoj analizi nekog događaja.

4 DALJI RAZVOJ RFID TEHNOLOGIJE

Krajnji domet RFID tehnologije mogao bi da bude učestvovanje u kreiranju „fizički povezanog sveta" u kome bi svaka stvar i/ili čovek bio tagovan, identifikovan (imao bi jedinstveni identifikacioni broj), katalogizovan čime bi bilo omogućeno potpuno i neometeno praćenje.

Kreiranje globalne mreže ili globalnog sistema povlači za sobom razmatranje i postizanje konsenzusa među različitim zemljama. I dok neke kompanije podržavaju i promovišu RFID tehnologiju uglavnom kroz inovacije u ovoj tehnologiji i povećanjem efikasnosti dopreme proizvoda do krajnjih korisnika, druge kompanije se bave razvojem sistema za korišćenje RFID informacija u druge svrhe, kao što su finansijske i/ili informacije o krajnjem korisniku. Te druge aktivnosti mogu predstavljati potencijalni problem za korisnike RFID tehnologije. Evropska Centralna Banka radi na implementiranju RFID čipova u Evro novčanice. Mnoge velike kompanije poput Philip Morris, Procter and Gamble, i Wal-Mart, otpočele su značajne eksperimente sa RFID čipovima radi praćenja svojih proizvoda. Gillette je lider među njima, naručivši još 2003. godine godina 500 miliona RFID tagova. Sa čitačima RFID-a na ključnim lokacijama, kao što su vrata na prodajnim odeljenjima, menadžment može da identifikuje ključne informacije o tajmingu. Takvi podaci pomažu u održavanju tajminga kod osetljivih proizvoda. Rukovodstvo Gillette-a koristi RFID da određuje da li je njihov proizvod blagovremeno otpremljen ili ne. (Evans, 2005) Oko 400 trgovaca opremljenih za korišćenje RFID-a primilo je pošiljke sa oznakama na svakoj paleti i kutiji (O'Connor, 2006).

Nove tehnologije će pomoći da RFID postane pouzdaniji i isplativiji za veći broj aplikacija, koristeći nove tehnologije u štampanoj elektronici sa izuzetno tankim, fleksibilnim RFID oznakama, tankim filmskim fotonaponskim solarnim ćelijama i drugim tehnologijama, biće će omogućeno kompanijama da mogu same da štampaju svoje sopstvene RFID tagove na određenim lokacijama. Postoje i kompanije koje već rade na 3D tehnologiji štampe koja omogućava direktno štampanje čipova na svojim proizvodima.

Vrlo je bitno razviti nove karakteristike antena, radi povećavanja dometa, sa novim memorijama koje će stvoriti smart oznake. Većina RFID sistema sa niskom frekvencijom može čitati oznake od oko jednog metra do nešto dalje. Ultra-visokofrekventni sistemi mogu produžiti domet do 10 metara ili više, u zavisnosti od uslova. Ovi dometi mogu ograničiti veličinu i primena RFID sistema. Očekuju se oznake sa više memorije po nižoj ceni čime bi se omogućile aplikacije za "smart asset". Zajedno sa novim pravcima razvoja, očekuje se napredak u proizvodnji i primeni novih materijala, organskih polimera, nano tehnologija i drugih tehnologija, što će promeniti način integracije RFID-a kod ugradnje u gotove proizvode. Problem će i dalje predstavljati upravljanje podacima sa hiljadama ili milionima oznaka.

Sa svojim aplikacijama RFID, postaje ključni deo celokupnog ekosistema senzora i komunikacionih tehnologija koji će pomoći kompanijama da bolje prate i upravljaju imovinom i pošiljkama. Pasivni senzori za temperaturu, vlagu, pritisak, vibracije i druge uticajne faktore biće kombinovani sa RFID-om.

Iako su radarski i identifikacioni sistemi demonstrirali principe daljinskog nadgledanja objekata i proizvoda, za narednu fazu razvoja u RFID potrebna je senzorska integracija sa drugim informacionim tehnologijama radi poboljšanja poslovanja. Iako je RFID ranije smatrana za tehnologiju nadgledanja, njeno usvajanje i primena u različitim oblastima industrije i života su pokazali da je RFID postala mnogo više od klasične primene. U Americi, su vrlo blizu toga da tagovi imaju funkciju senzora, razvijena je nova UHF tehnologija u kojoj RFID senzorska konfiguracija može da oseti pikove, nedozvoljene granične vrednosti, nekih supstanci hemikalija i gasova u okruženju i bežično prenosi takve informacije do korisnika. Zahteva se da takvi senzori mogu dugo da rade bez potrebe za baterijom ili njihovom zamenom. Kao rezultat, došlo se do toga da antena treba da emituje radio talase do čitača sa karakteristično drugačijom frekvencijom ili jačinom signala.

Uprkos široko rasprostranjenim mrežama, neki uređaji iz nekog od razloga neće biti mrežno povezani ili konfigurisani za određene mreže. Za nepovezane uređaje, nova tehnologija RFID-a preko tagova sa funkcijom senzora, obezbediće prikupljanje podataka i informacija bez obzira na vremenske uslove bez značajnog dodavanja troškova takvom sistemu.

Primena RFID tagova će omogućiti smanjenje falsifikovanja robnih marki. Njihovim publikovanjem u direktorijumu usluga i proizvoda, postavljenom na javnoj platformi RFID na Internetu, krajnji korisnici će moći da, identifikuju autentičnost usluge i/ili proizvoda putem mobilnog telefona sa RFID funkcijama.

5 ZAKLJUČAK

U savremenim uslovima poslovanja koje karakterišu globalizacija tržišta, ubrzan razvoj i primena novih informacionih tehnologija, logističke aktivnosti dobijaju na sve većem značaju. Poslednjih desetak godina je RFID tehnologija imala ključnu ulogu u povećanju efikasnosti i smanjenju troškova poslovanja u logistici, što je pokazano i na primeru kontrole na stanicama za snabdevanje goriva. Iako, još uvek nisu otkriveni ni iskorišćeni svi potencijali ove tehnologije već se ide u hibridne sisteme u kojima se RFID uklapa sa IIoT tehnologijama.

U radu su pokazane mogući problemi primene RFID i neke vrste napada („Reader Collision”, „Tag Collision”, „RFID interferenca“ i „Relay Attacks”), kojima se može ometati rad RFID sistema usled tehničkih problema ili moguće zloupotrebe objekta ili robe. Problem napada na RFID može se osujetiti povećanjem nedostajućih profesionalaca u integraciji RFID sa poslovnim procesima, njihovom većom edukacijom i obučavanjem zaposlenih u pravcu povećanja sigurnosti rada hibridnih tehnologija. Kod RFID-a, sigurnost obuhvata:

- poverljivost ili sigurnost sadržaja poruke,
- integritet sadržaja poruke, i
- autentičnost pošiljaoca i primaoca.

Jedna od ugroženosti RFID sistema može da bude i „man-in-the-middle” napad, pri čemu treća strana može da prati tok podataka između oznake i čitača da bi se dobile odgovarajuće osetljive informacije kroz analizu saobraćaja.

Ukazano je na značaj autentičnosti sopstvenih kodova koje će u narednom periodu ugrađivati sami proizvođači što će uticati na brzinu i uspešnost čitanja poruka. Takođe je ukazano, na

problem privatnosti, jer se u budućnosti planirana potpuna vizuelizacija procesa, objekata, i robe, što će omogućiti neometano i čitanje i praćenje oznaka bez saglasnosti pošiljaoca i primaoca. U vezi sa budućnošću RFID-a, može se zaključiti da kod Ove tehnologije, kao i kod većine drugih, uspeh u implementaciji zavisi od toga koliko će biti uspešno integrisana u postojeće operacije i procese. Ako se RFID jednostavno posmatra kao zamena za bar kodove, ne može se postići veliki uspeh, ali u slučaju redizajniranja poslovnih procesa, mogućnosti su praktično neograničene.

CITIRANA DELA

Andrejić, M. (2001). Metode i tehnike za podršku planiranja u vojnim organizacionim sistemima. *Vojnotehnički glasnik, 49*(1), 36-53.

Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2017). Internet of things and the Man-In-The-Middle attacks – Security and economic risks. *MEST Journal, 5*(2), 15-25. doi:10.12709/mest.05.05.02.03

Čekerevac, Z., Matic, S., Djuric, D., & Čelebić, D. (2006). ITGfdc-1 Fuel Dispenser Control System as the Technical Solution for Preventing of Non-Authorized Fuel Tanking. *Proc. 11th International Scientific Conference devoted to Crises Situations Solution in Specific Environment.* Žilina: FSI.

Evans, B. (2005). *Business Technology: Implementing RFID Is A Risk Worth Taking.* Retrieved from InformationWeek: http://www.informationweek.com/shared/printableArticle.jhtml?articleID=164302282

Fawzi, M. A.-N., & Mohannad, M. H. (2015). Design and Implementation of RFID-based Fuel Dispensing System. *International Journal of Computing and Network Technology, 3*(3).

GASNGO. (2013). *Finally, full real-time fleet control.* Preuzeto sa GASNGO: www.gasngo.com

Ilić, S. (2009). *Praćenje kvantitativnog stanja mirnodopskih zaliha pogonskih sredstava na pumpnim stanicama, magistarski rad.* Beograd: Vojna akademija.

Ilić, S., & Radosavljević, V. (2011). Unapređenje kvantitativnog stanja mirnodopskih zaliha pogonskog goriva na pumpnim stanicama. *Vojnotehnički glasnik, 59*(2), 60-77.

Jiho, R., & et all. (2007). A Hybrid Query Tree Protocol for Tag Collision Arbitration in RFID systems. *ICC 2007 proceedings* (str. 5981-5986). Seoul: School of Computer Science and Engineering. Seoul National University, Seoul, Korea.

Jovanović, V. (2010). *Prednosti RFID tehnologije u logistici i mogućnost njene primene u vojsci – magistarski rad.* Beograd: Ekonomski fakultet u Beogradu.

O'Connor, M. (2006, Mar. 27). Gillette Fuses RFID with Product Launch. *RFID Journal*. Preuzeto sa https://www.rfidjournal.com/articles/view?2222

SDD-ITG. (2017, 11 01). *Sistem za kontrolu točenja goriva ITGfdc-01.* Preuzeto sa SDD ITG: http://www.sdditg.com/2017/11/01/sistem-za-kontrolu-tocenja-goriva-itgfdc-01/

Datum prve prijave: 24.08.2018.
Datum prijema korigovanog članka: 10.04.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

Style – APA Sixth Edition:

Prigoda, L., Bogavac, M., & Maletić, J. (2019, 10 15). Primena RFID tehnologije – Neki problemi i pravci razvoja. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 99-107. doi:10.12709/fbim.07.07.02.11

Style – Chicago Sixteenth Edition:

Prigoda, Ljudmila, Milanka Bogavac, and Jelena Maletić. 2019. "Primena RFID tehnologije – Neki problemi i pravci razvoja." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 99-107. doi:10.12709/fbim.07.07.02.11.

Style – GOST Name Sort:

Prigoda Ljudmila, Bogavac Milanka and Maletić Jelena Primena RFID tehnologije – Neki problemi i pravci razvoja [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 99-107.

Style – Harvard Anglia:

Prigoda, L., Bogavac, M. & Maletić, J., 2019. Primena RFID tehnologije – Neki problemi i pravci razvoja. *FBIM Transactions,* 15 10, 7(2), pp. 99-107.

Style – ISO 690 Numerical Reference:

Primena RFID tehnologije – Neki problemi i pravci razvoja. **Prigoda, Ljudmila, Bogavac, Milanka and Maletić, Jelena.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 99-107.

FBIM Transactions
DOI 10.12709/fbim.07.07.02.12

RADIKALIZACIJA VISOKOTEHNOLOŠKOG TERORIZMA

THE RADICALIZATION OF HIGH-TECH TERRORISM

Ivica Petrović
Akademija za nacionalnu bezbednost, Beograd, Srbija

Dragana Trnavac
Poslovni i pravni fakultet, Univerzitet UNION-Nikola Tesla, Beograd, Srbija

JEL kategorija rada: **L86**

Apstrakt

Visokotehnološki terorizam je rizik još od pojave Interneta. Tehnologija se razvijala brzim tempom samim tim i rizik i uticaj visokotehnološkog terorizma. Važno je da postoje sigurni i ažurirani mehanizmi za ublažavanje rizika visokotehnološkog terorizma, uz međunarodnu saradnju radi daljeg unapređenja istrage i informacija. Ovaj rad govori o mehanizmima kao što su bezbednost aplikacije, bezbednosne politike, razumevanje obrazovanja programi, međunarodna saradnja, nadgledanje i veštačka inteligencija (VI), praćenje, korišćenje i ometanje pristupa. Implementacija svih mehanizama omogućava računarske mreže i sisteme koji su manje ranjivi zato što svaki mehanizam poseduje odvojene funkcije za borbu protiv visokotehnološkog terorizma. Kao rezultat toga, ovo istraživanje dokazuje pozitivnu povezanost između prepoznatih mehanizama i percipiranog rizika od visokotehnološkog terorizma. Bilo je različitih inicijativa, koje su pokrenuli nadležni organi iz celog sveta, kako bi se osiguralo da je pretnja od visokotehnološkog terorizma pod kontrolom. Međutim, pretnja od visokotehnološkog terorizma neprestano raste zbog stalnog razvoja platformi zasnovanih na Internetu. Tako, sprovođenje zakona, politike, prakse i neophodnih mera trebalo bi da se nastavi sa savremenim razvojem kompjuterskih tehnologija.

Ključne reči: *visokotehnološki terorizam, veštačka inteligencija (VI), nadgledanje, korišćenje i ometanje*

Abstract

High-tech terrorism has been a risk since the advent of the Internet. Technology has evolved at a rapid pace, thus the risk and impact of high-tech terrorism. Importantly, there are secure and up-to-date mechanisms to mitigate the risks of high-tech terrorism, with international cooperation to further advance investigations and information. This paper discusses mechanisms such as application security, security policies, education understanding of programs, international collaboration, monitoring and artificial intelligence (VI), monitoring, use and disruption of access. The implementation of all mechanisms is facilitated by computer networks and systems that are less vulnerable because each mechanism has separate functions to

Adresa autora zaduženog za korespodenciju:
Dragana Trnavac
draganatrnavac@gmail.com

counter high-tech terrorism. As a result, the goals for this research prove a positive correlation between the mechanisms identified and the perceived risk of high-tech terrorism. There have been various initiatives, introduced by authorities around the world, to ensure that the threat of high-tech terrorism is under control. However, the threat of high-tech terrorism is steadily rising due to the constant development of Internet-based platforms. Thus, the implementation of the law, policies, practices and necessary measures should continue with the modern development of computer technologies.

***Keywords**: high-tech terrorism, artificial intelligence, surveillance, utilization, interference.*

1 UVOD

Visokotehnološki terorizam je postao popularan poslednjih godina, posebno sa brzo razvijajućom tehnologijom i povećanje zavisnosti ljudskog roda od Interneta i društvenih medija. Iako je visokotehnološki terorizma bilo kog oblika, međunarodno priznat kao glavni rizik, ne postoji glavna definicija, ipak čini se da je opšteprihvaćena ili univerzalna definicija visokotehnološkog terorizma (Dogrul, M., Aslan, A., & Celik, E., 2011) ovu koju navodimo u nastavku. Mnogi istraživači su citirali definiciju Deninga (2000); koji visokotehnološki terorizam opisuje kao "*konvergenciju sajber prostora i terorizma gde su nezakoniti napadi i pretnje napadima protiv računara, mreža i informacija sačuvanih u njima; vrše se zastrašivanjem ili prisiljavanjem vlade ili njenih građana na unapređenje političkih ili društvenih ciljeva koje bi trebalo da rezultira nasiljem nad osobama ili imovini ili bar da nanese dovoljno štete generišući strah*". Iako ovo čini razumnu definiciju visokotehnološkog terorizma u tom trenutku, presudni su međunarodni napori koji preispituju opseg i razvoj mehanizama koji stoje iza visokotehnološkog terorizma da se to osigura zakonima tako da sami po sebi ne stvaraju rupe tj. prostor za visokotehnološkim terorizmom (Denning, & Dorothy E., 2000).

Gore navedena definicija implicira da je visokotehnološki terorizam važi samo ako ošteti poverljivost, integritet i dostupnost (CIA) računara, mreža i informacije koje su sačuvane; kao i radnje koje izazovu nasilje ili neku vrstu šteta. Međutim, u savremenom okruženju i teroristi koristite sajber-prostor i elektronske uređaje za komunikaciju, planiranje, vršenje napade, pribavljanje finansiranja, nabavku oružja, obaveštajno okupljanje i pristalice terorista. 2000. godine pojedinac je hakovao i preuzeo odgovornost za australijski otpad sistem upravljanja, Maroochy Shire i na daljinu ispraznio milione galona sirove kanalizacije (Prasad, 2012). Sve veći broj terorističkih grupa poput islamske Država Irak i Sirije (ISIS) i Al-Kaida, iskoristili su to, Internet kao medij za promociju njihovog uzroka i ponašanja terorističke operacije (Prasad, 2012).. Ove grupe su uspešno privukle veliki broj sledbenika, donatore i pristalice zbog snažne propagande; posebno posezanje za mladima koji žude za avanturama i dokazivanjem. Grupe koriste mnogo različitih frontova da sakriju svoj pravi identitet i aktivnosti, uključujući korišćenje anonimnih zaštita dubokog i mračnog spleta, koja se krije iza verskih i drugih neprofitnih tela itd. Takođe je isprepleteno sa drugim nezakonitim aktivnostima uključujući pranje novca, korupciju i organizovani kriminal. Ovo izaziva dalje dileme odakle se zločin može počiniti odnosno bilo koji deo sveta, skriven ispod mnogih slojeva aktivnosti i pojedinaca. Dakle, neophodno je da svi načini na koji se vrši ovaj zločin nadgleda se i ublažava. Iako su vlade pojačale mere bezbednosti uključujući praćenje putem Interneta, bilo je mnogo prepreka u njihovim nastojanjima. Ali i ostali priznaju da je visokotehnološki terorizam, obično pogrešno tumačen sa drugima slične visokotehnološke pretnje zbog ograničene grane znanja, a ismevanje opasnosti koju predstavlja povećava rizik od visokotehnoloških napada. Sukobni ili suženi zakoni и propisi mogu da poremete istrage i parnice. Odredbe o zaštiti privatnosti i zaštite podataka kompanije kao što su WhatsApp, Apple i druge koje koriste, prouzrokovalo je šifriranje radi zaštite privatnosti njihovih korisnika što mnogo ometa istrage i sudske sporove i proces. Zabrinutosti zbog strogog zakonodavstva takođe mogu izazvati nelagodnost među javnošću. 2017. godine Amber Rudd, državna sekretarka Velike Britanije izrazila je nameru da promeni zakon tako da se poveća kazna od 10 godina na 15 godina zatvora za osobe koje više puta gledaju teroristički sadržaj na mreži, iako sa dovoljnim merama za zaštitu članova javnost uz odbranu razumnog

izgovora (Prasad, 2012). U vestima se navodi i slučaj u kojem osumnjičeni nije mogao biti optužen za terorizam, samo zato što mu je bio potreban materijal da se preuzme i sačuva, dok je kod osumnjičenog pronađen samo striming video snimaka bombi. Isto tako, vesti o povećanom broju korisnika Onion-a Ruter (TOR) u poređenju s drugim pregledačima zbog privatnosti, zabrinutosti i sklonosti anonimnosti, takođe povećavaju rizik visokotehnološkog terorizma. TOR je takođe kapija Mraka i Dubinski web, uključujući aspekte servisa kriminala kao usluge (CaaS) i drugi organizovani zločini. Povećana upotreba kripto valute takođe pomažu kretanje i pranje fondovi. Obrazovanje i izlaganje su neophodni da bi se ublažio rizik. Sve veći broj globalnih prodora interneta, nedostatak bezbednosne svesti kod korisnika i porast broja zavisnost od internet komunikacija smanjuje mogućnosti borbe protiv visokotehnološkog terorizma (Jalil, 2003). Odgovorni organi neprestano su težila tome osigurati, da je pretnja pod kontrolom i da ne utiče na građane ili državu (Prasad, 2012). Vladini sektori iz celog sveta inicirali su nove sisteme, programe, politike, stroge zakone i razne druge akcije u cilju borbe protiv pretnje od visokotehnološkog terorizma. Međutim, to je izazovna bitka koju stalno treba ažurirati nadgledati, kao i same pretnje koje se neprestano razvijaju i rastu. Vlade, kompanije i pojedinci trebaju biti oprezni jer pretnje mogu uticati na njih same, odnosno preduzeća, informacije, privatnost i na kraju njihova sigurnost, koju uzrokuju njihove ranjive računarske mreže i sisteme, kao i zaposleni ili prikriveni prodavci. Stoga ovaj rad procenjuje percepciju dobro upućenih članova javnosti o riziku od visokotehnološkog terorizam u skladu sa raznim naporima i mehanizmima na raspolaganju za borbu protiv ovog zločina. Da bismo pružili više, diskusija je zasnovana na nalazima ovog istraživanja. Ovaj rad je organizovan na sledeći način: Odeljak 2 govori o relevantnoj literaturi, odeljak 3 govori o merama za ublažavanje rizika od visokotehnološkog terorizma, a zatim sledi Odeljak 4 koji govori o akcionom planu Republike Srbije u borbi protiv visokotehnološkog kriminala, odeljak 5 sadrži statističke trendove u oblasti visokotehnološkog kriminala Republike Srbije, odeljak 6 celokupnu perspektivu ovog rada.

2 PREGLED LITERATURE

Percipirani rizik od visokotehnološkog terorizma: Visokotehnološki terorizam leži između tanke linije postajanja virtualne bombe, ali nije tako opasna po život kao stvarna bomba . Rizik od visokotehnološkog terorizma možda neće izgledati ozbiljno, ali u stvari je stvar zaštita nacionalne sigurnosti. Biti više politički motivisan, visokotehnološki terorizam je usmeren ka nanošenju štete kritičnoj infrastrukturi države na koju se indirektno odnosi uticaj na širu javnost u smislu ometanja finansijske pomoći i komercijalnu infrastrukturu, preuzimajući kontrolu odbrane, pa čak i pristup medicinskoj dokumentaciji Zbog političke koordinacije, narod je suočen efektima visokotehnološkog terorizma u stvarnosti. Ovi poremećaji su dovoljni da stvore strah prema javnosti i time omogućava visokotehnološkim terorističkim grupama da daljinski upravljaju operacijama države (Alqahtani, n.d.). Na primer, napadi mogu uzrokovati prekide u snabdevanju vodom ako visokotehnološki teroristi imaju kontrolu nad branama, prouzrokujući nestašicu vode sami tim i patnju građana. Iako možda ne zvuči kao ozbiljno pitanje i prilično je daleko dostignut, ali rizik treba stalno pratiti. Iako je javnost upoznata sa visokotehnološkim terorizmom putem izveštaja u medijima, još uvek nisu toliko obavešteni o poznavanje tehničkih karakteristika i štetu zbog nedostatka informacija i svesti. Studije su pokazale da je percipirani rizik od visokotehnološkog terorizma relativno nizak tokom perioda povišenog visokotehnološkog terorističkog napada. Građani možda nisu svesni (Sjöberg, 2004). upozoravajućih znakova (crvenih zastava) visokotehnološkog terorizma zbog složenosti i brzi razvoj korišćenih metoda. Teško je predvideti gde i kada će se dogoditi napad. Međutim, moguće je smanjiti rizik ispitivanjem područja koja mogu privući visokotehnološke terorističke napade. Zbog toga cilj ove pojave je dobijanje pristupa bez postojanja otkrivanja i izazivanje intenzivnog straha i štete bilo kome namenjeno. Strah je glavni pokretač visokotehnološkog terorizma, on izaziva promene u ponašanju koje destabilizuju političke zemlje i ekonomski sistem, utičući na berze, potrošačke navike i dugoročne finansijske odluke kao što su promene cena nekretnina usled povećanja terorističkih incidenata u određenom području. Dakle, politička nestabilnost može da utiče i na

lokalnu ekonomiju kao globalna investiciona ekonomija, tako da bi stabilnost ekonomskog i političkog sistema neke zemlje trebalo bi da bude manje ranjivija (Murrill, 2011). Rizik visokotehnoloških terorističkih napada prema kritičnoj infrastrukturi države je izuzetno visoka. Zbog svoje ranjivost i složenost, štete nanesene u nacionalnoj infrastrukturi mogla bi uništiti razvoj te zemlje. Vlade su shvatile potrebu da se zaštiti njihov informacioni sistem i kritični infrastrukturni sistemi zbog sve većih pretnji od visokotehnološkog terorizma. Međutim, mnoga ograničenja ne omogućavaju potpuno spuštanje Interneta jer postoje različita pravna pitanja koja su povezana. Anonimnost napadača otežava čak i to identifikovati i procesuirati uljeza kao brojne geografska i zakonska ograničenja koja se dovode u pitanje (Dombe, & Golandsky, 2016).

3 MERE ZA UBLAŽAVANJE RIZIKA OD VISOKOTEHNOLOŠKOG TERORIZMA

Iako je Internet najveća pojedinačna komponenta “cyberspace”-a povezan u gotovo više od 200 zemalja sa više od milijarde korisnika širom sveta, verovatnoća za visokotehnološki terorizam koji se javlja putem interneta raste drastično jer je internet zasnovan na nacionalnim i međunarodnim telekomunikacionim infrastrukturama koje uključuje fiksne, bežične i satelitske komunikacije. Mogli bi ciljne mete visokotehnoloških terorista, biti kritična infrastruktura zemlje kao što su telekomunikacioni sistemi, sistem saobraćaja, elektroenergetski sistem, komunalni sistem i drugi značajni sistemi koji su potrebni za vođenje neke zemlje .Dakle, ako su ovi sistemi uništeni, tada a cela nacija može biti uništena u smislu ekonomskog i socijalno blagostanje. Složenost infrastrukture neke zemlje povećava rizik od visokotehnološkog terorizma ako nije prisutan odbrambeni mehanizam za zaštitu od ovakvih terorističkih napada. Vlade bi trebalo da poboljšaju i usaglase relevantne zakonodavstva u svojim zemljama sa međunarodnim standardima i striktno se pridržavajte politike nulte tolerancije prema visokotehnološkom terorizmu, priznajući potrebu za privatnošću i ljudska prava. Edukacija članova javnosti o visokotehnološkom terorizmu je obavezan, uključujući omogućavanje pristupačnosti i tačne informacije o ranjivosti, pretnjama i incidentima kao i očekivano ponašanje i pružanje pristupa službenicima da se obrate o zabrinutosti ili prijave sumnjiva ponašanja. Ovo nije samo za članove javnost kao pojedinci, nego i za organizacije koje igraju ključnu ulogu u nadgledanju zaposlenih, obavljajući pozadinski pristup i druge politike ljudskih resursa, osim pravovremeno improvizujućih mera zaštite informacijskih manir. Na raspolaganju su i razni mrežni materijali tj. razumevanje pretnje visokotehnološkog terorizma i takođe o tome kako zaštititi računar od napada. Otuda je ključ za borbu protiv visokotehnološkog terorizma obrazovanje i javno-privatna partnerstva (Goodman, 2007).

Bezbednosne politike i sveobuhvatno planiranje za dejstvo mehanizam odbrane od napada visokotehnološkog terorizma trebao bi biti osnovana u organizacijama . Razvijene sigurnosne prakse treba da obuhvate sve aspekte uključene u informacioni sistem koji bi mogao da uradi usvajanje međunarodnih standardnih smernica o informacionoj sigurnosti. Pridržavanjem računarske sigurnosti politike, visokotehnološkog teroriste bilo bi teško probiti u kompjuterski sistem, čime se smanjuje rizik od visokotehnološkog terorizma koji nastaje (Goodman, 2007).

Implementacija sigurnosnih aplikacija u računare otežava da napadi visokotehnološkog terorizma prodiru unutar sistema. Te sigurnosne aplikacije bi trebale ažurirati često, pomoću odbora i uprava razumevanja i priznavanja hitne potrebe i racionaliziranje troškova nastalih na duži rok održivost firme. Međutim, nažalost, mnoge firme to izbegavaju, "vatre za vatru" koje uključuju njihove računarske sisteme za provere rupe u petlji koje mogu privući visokotehnološke terorističke napade jer je skupo i to mora biti urađeno na samostalno rizik.

Ključna karakteristika visokotehnološkog terorizma koja treba biti naglašena je njegovo bezgranično izlaganje, anonimnost i redukovani rizik, koji motiviše terorista. Terorista bi mogao isplanirati napad kilometrima dalje, a da ne napušta dom i smanjiti šanse da bude uhvaćen. Trenutno ograničenje zakonodavstvo unutar nadležnosti je presudni ugao koji treba da se poboljša. Postoji hitna potreba za harmonizacijom zakonodavstva na međunarodnom nivou, a sarađuje više zemalja sporazumima o uzajamnoj pravnoj pomoći i izručivanju. Potrebno je razviti

međunarodnu saradnju u domenu kontrole visokotehnološkog terorizma jer visokotehnološki terorizam je globalno pitanje u koje je uključena vlada zemlje i svetske organizacije koje usvajaju mrežu informacionih sistema. Saradnja sa drugim državama bi mogle biti inicirane ekonomskim alatima od strane formiranje i promovisanje zajedničkih standarda za međunarodne odnose trgovina koja će privući međusobno razumevanje između zemalja, kao i kontrolu rizika od visokotehnološkog terorizma. Vlade, posebno one za koje se zna da su luka ili pružaju sigurno utočište za visokotehnološke teroriste moraju međusobno razvijati jaku međunarodnu saradnju, razmenu informacija i pokrenuti zajedničke obuke za kontrolu rizika od visokotehnološkog terorizma Ovo može biti dodatno omogućeno aktivnijim učešćem iz globalne zajednice institucije. Konvencija Saveta Evrope (SE) od visokotehnološkog kriminala je inicirala prvu međunarodnu izjavu o zločinu počinjenim putem interneta i drugog računara mreže. Evropska unija je takođe preduzela određene korake protiv kontrole ilegalnih sadržaja na Internetu od strane zaštita intelektualne svojine i ličnih podataka, promocija elektronska trgovina i pooštravanje bezbednosti transakcije. Prisustvo aktivnog sistema odbrane kao što je transnacionalni sistem nadzora važan je element ublažavajućeg sistema. To bi moglo pružiti ključne informacije o identitet terorizma, pokretanje mehanizma za suzbijanje i drugi proaktivni koraci za borbu protiv rizika. Međutim, kontroverzno, mada bi to narušilo privatnost prava javnosti, mnogi to i dalje koriste u zemljama i za to je potrebna međunarodna saradnja da u potpunosti funkcionišu. Jedan takav sistem je ECHELON koji koristi zemlje poput Australije, Ujedinjenog Kraljevstva i Novog Zelanda koji ima sposobnost hvatanja inteligencije informacije širom sveta koristeći sistem nadzora dizajniran za filtriranje poruka i telefonskih razgovora putem računarskog sistema koji je u stanju da prepozna ključne reči i fraze. Odbrana Australije, Direkcija za signale (DSD) koristi ovaj sistem nadzora za nadgledanje Indokine, Južne Kine i Indonezije. Komunikacije vlade Ujedinjenog Kraljevstva je Štab (GCHK) koristi ovaj nadzor za nadgledanje Evrope, Rusije i Afrike. Vlada Novog Zelanda Biro za sigurnost komunikacija (GCSB) koristi ovaj sistem za praćenje regiona zapadnog Pacifika. Još jedan pristup koji zahteva međunarodnu saradnju je M.U.D pristup, koji stoji za Monitoring, Korišćenje i Ometanje. Koraci za nadgledanje i korišćenje mogu biti od koristi za analizu procesa radikalizacije terorizma organizacijom da bi se pronašla rešenja za deradikalizaciju situacije. Postupke ometanja mogu koristiti inficiranje terorističkih web lokacija kako bi ih uništili ili promenili sadržaj web stranice. To je više obrnuta radnja kako bi se smanjio rizik od visokotehnoških terorističkih napada. Međutim, pitanja nastaju kada postoje sukobljeni ciljevi zbog kojih neki još uvek žele da nadgledaju blogove, grupe za ćaskanje itd. Ova metoda takođe pomaže u identifikaciji zemalja koje pomažu i podržavaju život teroristi. Zbog pojačanog nadzora i zakonskih propisa, mnogi pojedinci traže mogućnosti da zaštite svoje privatnost iako nije u zločinačkoj nameri. Alati poput tehnika šifrovanja, upotreba pregledača i softver koji štiti njihovu anonimnost samo otežava da zvaničnici nadgledaju stvarne pretnje, posebno sa povećanjem prometa pomoću ovih alata. (Sundaram, 2008).

Isto tako, sa lakim pristupom informacijama visokotehnološki terorizam kao terorističke grupe koriste mrežu i društveni mediji kako bi proširili svoju mrežu, od presudne je važnosti ova istraživanja da se ažuriraju. Preduzeća i pojedinci koji pružaju i dalje Kriminalni softver kao usluge (CaaS) komplikuje postupak otkrivanja. Moguće rešenje bi koristiti veštačku inteligenciju (VI). VI je inovativan i logički pristup koji simulira ljudsku inteligenciju u mašinama, koristeći konvencionalne fiksne algoritme, što im omogućava da donose odluke i prilagođavaju se svom okruženju. VI je u stanju da se samopodešava, samokonfiguriše, samoupravlja, dijagnostifikuje i samoisceljuje. Čini se da metode VI pružaju više obećavajući ishod u smanjenju rizika od visokotehnoloških napada povećavajući sigurnost sajber-prostora. Funkcije VI koje su implementirane u softver koji se bori protiv cyber napada uključuju kompjutersku inteligenciju, prepoznavanje uzoraka, inteligentne agente i neuronske mreže i mogu se primeniti za otkrivanje i sprečavanje upada, odbijanja usluge, neželjene pošte, zloupotrebe i pomoći u forenzičkim ispitivanjima. (Tereshchenko, 2013).

4 AKCIONI PLAN REPUBLIKE SRBIJE U BORBI PROTIV VISOKO-TEHNOLOŠKOG KRIMINALA

Republika Srbija je u obavezi da donese i sprovodi strategiju i akcioni plan za efektivno rešavanje visokotehnološkog kriminala u skladu sa strateškim i operativnim pristupom Evropskoj uniji (EU) u pogledu visokotehnološkog kriminala. Navedena obaveza prevashodno proizilazi iz Pregovaračkih merila za Poglavlje 24 – Pravda, sloboda, bezbednost. Evropska Unija je konstatovala da je Republika Srbija ratifikovala Konvenciju o visokotehnološkom kriminalu (sačinjena u Budimpešti, engl. Budapest Convention) 2009. godine i pozvala Republiku Srbiju da dodatno uskladi svoje zakonodavstvo sa Direktivom 2013/40/EU o napadima na informacione sisteme. Ministarstvo unutrašnjih poslova je, u skladu sa Zakonom o ministarstvima („Službeni glasnik RS", br. 44/14, 14/15, 96/15 – dr. zakon i 62/17) nosilac izrade navedenog strateškog dokumenta u saradnji sa ostalim državnim institucijama, tj. zainteresovanim stranama. U planu za podršku transformacije Zapadnog Balkana u okviru Strategije za verodostojnu perspektivu proširenja i pojačanu saradnju sa državama sa područja Zapadnog Balkana istaknuta je potreba za povećanom podrškom u izgradnji kapaciteta u oblasti visokotehnološkog kriminala, uključujući saradnju sa Evropskom grupom za trening i edukaciju o visokotehnološkom kriminalu i buduće učešće u okviru Agencije za evropsku mrežu i informacionu bezbednost. U okviru Akcionog plana za Poglavlje 24 – Pravda, sloboda i bezbednost, gde je nosilac aktivnosti Ministarstvo unutrašnjih poslova, nalaze se tri preporuke sa osam definisanih aktivnosti, koje Republika Srbija treba da ispuni u okviru pristupnog procesa u EU, sa fokusom na unapređenje organizacionih, kadrovskih i tehničkih kapaciteta, analiziranja trenutnog normativnog i organizacionog okvira i preduzimanja radnji u cilju usaglašavanja sa pravnim tekovinama EU u oblasti visokotehnološkog kriminala i ojačavanje saradnje između državnih organa i institucija. Imajući u vidu da je jedna od glavnih karakteristika dela visokotehnološkog kriminala njihova transnacionalna priroda, od procesa evropskih integracija se očekuje povećanje ekspeditivnosti rada u predmetima visokotehnološkog kriminala, u smislu bržeg protoka informacija potrebnih za otkrivanje i gonjenje učinilaca krivičnih dela, te bržeg odgovaranja po međusobnim zahtevima za pružanje međunarodne pravne pomoći, a sve kroz jačanje kapaciteta državnih organa Republike Srbije, a naročito Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala. Pored navedenih preporuka, Republika Srbija je nakon otvaranja Poglavlja 24 – Pravda, sloboda i bezbednost dobila prelazno merilo koje ima za cilj izradu Strategije za borbu protiv visokotehnološkog kriminala i koje glasi: „Srbija priprema, donosi i sprovodi strategiju i akcioni plan za efektivnu borbu protiv visokotehnološkog kriminala u skladu sa strateškim i operativnim pristupom EU u pogledu visokotehnološkog kriminala. Srbija ojačava svoje operativne kapacitete (u pogledu osoblja i opreme u Jedinici za visokotehnološki kriminal) kako bi rešila problem visokotehnološkog kriminala i usklađuje 2 svoje zakonodavstvo sa relevantnim pravnim tekovinama EU, uključujući u pogledu seksualnog zlostavljanja dece na internetu, obezbeđuje specijalizovane obuke i podiže nivo svesti javnosti i među državnim službenicima po pitanju visokotehnološkog kriminala". Na osnovu navedenih međunarodnih i nacionalnih dokumenata iz ove oblasti Republika Srbija je donela prvu Strategiju za borbu protiv visokotehnološkog kriminala sa pratećim Akcionim planom za njeno sprovođenje. Strategija predstavlja nastavak i proširenje aktivnosti kojima je cilj jačanje efikasnosti svih subjekata u oblasti suzbijanja visokotehnološkog kriminala u Republici Srbiji. Posebno je usmerena na nastavak usklađivanja zakonodavstva s međunarodnim standardima, dalje unapređenje kapaciteta nosilaca borbe protiv visokotehnološkog kriminala, unapređenje preventivnog i proaktivnog pristupa društva u suzbijanju svih oblika kriminala u toj oblasti, unapređenje inter-resorne saradnje u društvu, kao i saradnje Republike Srbije na regionalnom i međunarodnom nivou u oblasti visokotehnološkog kriminala. Ispunjenjem strateških ciljeva i daljim razvojem međunarodne i regionalne saradnje u ovoj oblasti, Republika Srbija će doprineti ne samo sigurnosti u zemlji nego i u regionu. Strategija za borbu protiv visokotehnološkog kriminala predstavlja dokument kojim Vlada utvrđuje institucionalni odgovor na pojavne oblike visokotehnološkog kriminala, definiše uloge i

nadležnosti državnih organa, identifikuje ciljeve i utvrđuje osnovne pravce delovanja na suzbijanju svih vidova visokotehnološkog kriminala. U ovoj strategiji određene imenice navedene su u muškom rodu, a koriste se kao neutralne za muški i ženski rod. Strategija se donosi na period od 2019. do 2023. godine. Akcioni plan 2019-2020. za sprovođenje Strategije za borbu protiv visokotehnološkog kriminala za period 2019-2023. godine čini njen sastavni deo.

5 STATISTIČKI TRENDOVI U OBLASTI VISOKOTEHNOLOŠKOG KRIMINALA

Prema podacima Posebnog odeljenja za borbu protiv visokotehnološkog kriminala u proteklih pet godina na teritoriji Republike Srbije (period 2013-2017. godina) stopa kriminala je u porastu. Pregled broja predmeta Posebnog tužilaštva za visokotehnološki kriminal zaključno sa 31.12.2017. godine. 2019-2023 . godine čini njen sastavni deo.

U periodu od 1. januara 2013. godine do 31. decembra 2017. godine, Posebnom tužilaštvu za visokotehnološki kriminal podnete su krivične prijave protiv ukupno 1.318 poznatih punoletnih lica, dok je optužni akt podnet protiv ukupno 280 poznatih punoletnih lica. Ministarstvo unutrašnjih poslova je u periodu od 2013. do 2017. godine, podneo krivične prijave zbog izvršenja ukupno 3.824 krivičnih dela visokotehnološkog kriminala.

Krivična dela protiv bezbednosti računarskih podataka – ukupno 91 krivično delo i to: oštećenje računarskih podataka i programa iz člana 298. Krivičnog zakonika (5 krivičnih dela ili 5,5 % od ukupnog broja), računarska sabotaža iz člana 299. Krivičnog zakonika (7 ili 7,7%), pravljenje i unošenje računarskih virusa iz člana 300. Krivičnog zakonika (4 ili 4,4%), računarska prevara iz člana 301. Krivičnog zakonika (40 ili 43,9%), neovlašćen pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka iz člana 302. Krivičnog zakonika (34 ili 37,4%) i Krivična dela protiv intelektualne svojine - ukupno 328 krivičnih dela i to: povreda-sprečavanje i ograničavanje pristupa javnoj računarskoj mreži iz člana 303. Krivičnog zakonika (1 ili 1,1%). moralnih prava autora i interpretatora iz člana 198. Krivičnog zakonika (1 ili 0,3%), Ostala krivična dela – ukupno 3.405 krivičnih dela i to: prikazivanje, pribavljanje i neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199. Krivičnog zakonika (316 ili 96,3%), povreda pronalazačevog prava iz člana 201. Krivičnog zakonika (1 ili 0,3%) i neovlašćeno korišćenje tuđeg dizajna iz člana 202. Krivičnog zakonika (10 ili 3,1%). posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju iz člana 185. stav 4. Krivičnog zakonika (128 ili 3,8%), iskorišćavanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu iz člana 185 b Krivičnog zakonika (14 ili 0,4%), falsifikovanje i zloupotreba platnih kartica iz člana 225. Krivičnog zakonika (2.412 ili 70,8%), pravljenje, nabavljanje i davanje drugom sredstava za falsifikovanje iz člana 227. stav 2. Krivičnog zakonika (18 ili 0,5), neovlašćena upotreba tuđeg poslovnog imena i druge posebne oznake robe ili usluga iz člana 233. Krivičnog zakonika (827 ili 24,3%), odavanje poslovne tajne iz člana 240. Krivičnog zakonika (6 ili 0,2%).

6 ZAKLJUČAK

Može se zaključiti da je pretnja od visokotehnološkog terorizma napadi koji će se stalno povećavati kako ljudi postaju zavisni od interneta i zato povećavaju mogućnosti visokotehnoloških terorističkih napada. Teroristi poput ISIS uspešno stvaraju snažnu sliku prema percepciji javnosti na globalnom nivou. Pretnja napadima kontinuirano raste kako je rasprostranjenost korisnika na mreži neprestano u porastu. Rizik da dođe do visokotehnološkog terorističkog napada raste zajedno sa brzim rastom računarskih tehnologija. Dakle, sprovođenje zakona, politike, prakse i potrebne mere bi trebalo da se i dalje razvijaju kao što se i računarska tehnologija kontinuirano razvija. To je odgovornost službenika za razvoj sigurne tehnologije koji je sposoban da utvrdi sumnjive aktivnosti analizom javnih i privatnih podataka. Implementacija svih ovih mehanizama omogućava računar, da su mreža i sistemi manje ugroženi i upravljajući njima smanjuje rizik od visokotehnološkog terorizma zato što svaki mehanizam poseduje odvojene funkcije za borbu protiv visokotehnološkog terorizma, čak iako su već postojali različiti odbrambeni mehanizmi. Zbog stalnog razvoja Internet platforme pretnja od visokotehnološkog terorizma je i dalje u stalnom porastu.

CITIRANA DELA

Alqahtani, A. (n.d.). The Potential Threat of Cyber-terrorism on National Security of Saudi Arabia. 1st ed. [ebook] Department of Politics and International Studies the University of Hull - UK. Available at: http://www.academia.edu/8951385/The_Potential_Threat_of_Cyberterrorism_on_National_Security [Accessed 19 Sep. 2016].

Aly, A., Macdonald, S., Jarvis, L. and Chen, T. (2016). Violent Extremism Online: New Perspectives on Terrorism and the Internet. 1st ed. [ebook] New York: Routledge, pp.18-21. Available at: https://www.book2look.com/embed/9781317431879 [Accessed 5 Sep. 2016].

Balkhi, S. (2013). 25 Biggest Cyber Attacks In History. [online] Available at: http://list25.com/25-biggest-cyber-attacks-in-history/ [Accessed 24 Dec. 2016].

Bogdanoski, M. and Petreski, D. (2013). CYBER TERRORISM– GLOBAL SECURITY THREAT. 1st ed. [ebook] Research Gate. Available at: http://file:///C:/Users/Win%208.1/Downloads/CYBER%20TERRORI SM-%20GLOBAL%20SECURITY%20THREAT%20- %20Mitko%20Bogdanoski.pdf [Accessed 24 Dec. 2016].

Casciani, Dominic (2017), Longer Jail Terms for Viewing Terror Content Online. BBC Available at https://www.bbc.com/news/uk41479620 [Accessed on 27th Sept 2018)

Che, E. (2007). Securing a Network Society Cyber-Terrorism, International Cooperation, and Transnational Surveillance. [online] Available at: http://rieas.gr/images/RIEAS113ELIOTCHE.pdf [Accessed 10 Sep. 2016].

Cyber terrorism Defense Initiative. (2016). [online] Cyberterrorismcenter.org. Available at: http://www.cyberterrorismcenter.org/ [Accessed 23 Nov. 2016].

Dawson, M., Omar, M. and Abramson, J. (2015). Understanding the Methods behind Cyber Terrorism. Research Gate, [online] 3, pp.1539-1549. Available at: http://www.saintleo.edu/media/972036/understanding_the_methods_ behind_cyber_terrorism.pdf [Accessed 5 Sep. 2016].

Dilek, S., Cakır, H. and Aydın, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications, [online] 6(1), pp.21-39. Available at: http://aircconline.com/ijaia/V6N1/6115ijaia02.pdf [Accessed 17 Dec. 2016].

Denning, Dorothy E. (2000). Cyberterrorism: Testimony given to the House Armed Services Committee Special Oversight Panel on Terrorism

Dogrul, M., Aslan, A. and Celik, E. (2011). Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism. 3rd ed. [ebook] Istambul: CCD COE Publications. Available at: https://ccdcoe.org/ICCC/materials/proceedings/dogrul_aslan_celik.pd f [Accessed 5 Sep. 2016].

Dombe, A. and Golandsky, Y. (2016). A Review and Analysis of the World of Cyber Terrorism. 1st ed. [ebook] Available at: http://www.cyberisk.biz/cyber-terrorism-review-and-analysis/ [Accessed 23 Nov. 2016].

Goodman, S. (2007). Science and Technology to Counter Terrorism: Proceedings of an Indo-U.S. Workshop. Chapter 5. Cyberterrorism and Security Measures. [online] Available at: https://www.nap.edu/read/11848/chapter/6 [Accessed 5 Sep. 2016].

Hoffman, A. and Schweitzer, Y. (2015). Cyber Jihad in the Service of the Islamic State (ISIS). [online] www.inss.org.il. Available at:

http://www.inss.org.il/uploadImages/systemFiles/adkan18_1ENG%2 0 (5) _Hoffman-Schweitzer.pdf [Accessed 5 Sep. 2016].

Hyde, O. (2011). Machine Learning for Cybersecurity at Network Speed & Scale. 1st ed. [ebook] AIOne Inc. Available at: http://www.academia.edu/1026724/Machine_Learning_for_Cyber_Security_at_Network_Speed_and_Scale [Accessed 14 Dec. 2016].

Jalil, S. (2003). Countering Cyber Terrorism Effectively: Are We Ready to Rumble? 1st ed. [ebook] SANS Institute. Available at: https://www.giac.org/paper/gsec/3108/countering-cyber-terrorismeffectively-ready-rumble/105154 [Accessed 4 Sep. 2016].

Janczewski, L. and Colarik, A. (2008). Cyber Warfare and Cyber Terrorism. 1st ed. [ebook] New York and Hershey: Information Science Reference. Available at: https://books.google.com.my/books?hl=en&lr=&id=XWK9AQAAQ BAJ&oi = fnd&pg = PA1&dq = cyber + terrorism + cases&ots = 27XIC8yu mj&sig = 4r2Npu9JU4yVd8U70t8cYkVQaE&redir_esc = y#v = onepage&q&f = false [Accessed 14 Aug. 2016].

Murrill, R. (2011). The Question of Cyber Terrorism. [online] Forensic Focus - Articles. Available at: https://articles.forensicfocus.com/2011/07/23/the-question-of-cyberterrorism/ [Accessed 5 Sep. 2016].

Prasad, K. (2012). Cyber terrorism: Addressing the Challenges for Establishing an International Legal Framework. 1st ed. [ebook] Perth: Edith Cowan University. Available at: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1016&context=act [Accessed 5 Sep. 2016].

Santiago, J. (2015). Top countries best prepared against cyber-attacks. [online] World Economic Forum. Available at: https://www.weforum.org/agenda/2015/07/top-countries-bestprepared-against-cyberattacks/ [Accessed 24 Dec. 2016].

Sjöberg, L. (2004). THE PERCEIVED RISK OF TERRORISM. [online] Available at: http://swoba.hhs.se/hastba/papers/hastba2002_011.pdf [Accessed 19 Dec. 2016].

Službeni glasnik RS, br. 44/14, 14/15, 96/15 – dr. zakoni 62/17

Sundaram, S. (2008). Cyber Terrorism: Problems, Perspectives, and Prescription. [online] Academia.edu . Available at: http://www.academia.edu/812094/Cyber_Terrorism_Problems_Perspectives_and_Prescription [Accessed 5 Sep. 2016].

Tereshchenko, N. (2013). US Foreign Policy Challenges: Cyber Terrorism & Critical Infrastructure. [online] E -International Relations. Available at: http://www.e-ir.info/2013/06/12/us-foreignpolicy-challenges-of-non-state-actors-cyber-terrorism-against-criticalinfrastructure/ [Accessed 9 Sep. 2016].

Vlada R.S. (2018). Strategija za borbu protiv visokotehnološkog kriminala za period 2019-2023. godine http://www.mup.rs/wps/wcm/connect/7b8500bb-171c-4ba3-b61a-b3772d5feaf8/PDF_LAT_Strategija+za+borbu+protiv+VTK+2019-2023.pdf?MOD=AJPERES&CVID=mtm2sqy 2019.

Datum prve prijave: 23.09.2019.
Datum prijema korigovanog članka: 08.10.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

Style – APA Sixth Edition:

Petrović, I., & Trnavac, D. (2019, 10 15). Radikalizacija visokotehnološkog terorizma. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 108-117. doi:10.12709/fbim.07.07.02.12

Style – Chicago Sixteenth Edition:

Petrović, Ivica, and Dragana Trnavac. 2019. "Radikalizacija visokotehnološkog terorizma." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 108-117. doi:10.12709/fbim.07.07.02.12.

Style – GOST Name Sort:

Petrović Ivica and Trnavac Dragana Radikalizacija visokotehnološkog terorizma [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 108-117.

Style – Harvard Anglia:

Petrović, I. & Trnavac, D., 2019. Radikalizacija visokotehnološkog terorizma. *FBIM Transactions,* 15 10, 7(2), pp. 108-117.

Style – ISO 690 Numerical Reference:

Radikalizacija visokotehnološkog terorizma. **Petrović, Ivica and Trnavac, Dragana.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 108-117.

FBIM Transactions
DOI 10.12709/fbim.07.07.02.13

DA LI SU PROBLEMI U IT VEŠTINAMA REŠIVI ILI OSTAJU DA BUDU UVEK PRISUTNI?

ARE THE PROBLEMS IN INFORMATION TECHNOLOGY SKILLS SOLVABLE, OR WILL STAY FOREVER?

Hana Rizqallah Qananah
Univerzitet ''UNION – Nikola Tesla'', Beograd, Fakultet za informacione tehnologije i inženjerstvo, Beograd, Srbija

Khalefa Altaher Mohamed Alnagasa
Univerzitet ''UNION – Nikola Tesla'' Beograd, Fakultet za informacione tehnologije i inženjerstvo, Beograd, Srbija

Mohamed Salem Almabrouk
Univerzitet ''UNION – Nikola Tesla'', Beograd, Fakultet za poslovne studije i pravo, Beograd, Srbija

Nada Živanović
Univerzitet ''UNION – Nikola Tesla'' Beograd, Poslovni i pravni fakultet, Beograd, Srbija

JEL kategorija rada: **A29, I21, J24**

Apstrakt

Četvrta svetska revolucija nauke i prakse pripada primeni novih IT informacionih tehnologija i njihovoj velikoj mogućnosti primene u svim sferama poslovanja. Polazeći od najrazvijenije društvene mreže – Interneta, gde je otvorena javna upotreba ove mreže, ali kako podaci pokazuju, postoje primeri u svetu koji dokazuju suprotno, odnosno da priroda Interneta kroz njegovu upotrebu ugrožava zatvorene informativne mreže, npr. koje je razvila finansijska industrija krajem 20. veka. Problemi koji su rezultirali ovom konfliktu, u prvom redu najbolje se objašnjavaju u bankama. To govori, da su te tehnologije dominirale u formi, kao tehnologije za razmenu informacija i za sigurnost informacija. Prema podacima, evolutivni razvoj on-line komercijalne transakcije počeo je još 1995. godine, a do 1998. godine preko Internet mreže je obrađeno više od 50 milijardi dolara transakcija. U 21-om veku, godišnja vrednost internet transakcija je značajno porasla što se shodno tome, zahteva više mreža, više

Adresa autora zaduženog za korespodenciju:
Hana Rizqallah Qananah
hana.gananah@gmail.com

računara i više programa sigurnosti. Tako su uglavnom finansijske institucije usmerene na razvoj i sticanje više veština u korišćenju IT tehnologija da bi se mogle takmičiti. Jasna koncepcija primene IT preferira preciznost odnosno, ne mogu se finansijske institucije takmičiti bez široke i sigurne informacione mreže što govori, da su informacione tehnologije od suštinskog značaja za poslovne procese i dugoročni uspeh. Šta podrazumeva, termin "Globalno finansiranje"? To se u modernom finansijskom svetu praktično objašnjava na sledeći način: da informacione tehnologije omogućavaju, posmatrano na globalnom nivou, da finansiranje funkcioniše na osnovu poslovne sintagme koja strukturira koncepciju u IT sektoru za finansije na sledeći način: "da se finansijska tržišta mogu smatrati prvim organizovanim globalnim informacionim tržištima koja rade preko umreženih računara". (n.d., Investment planning, 2019) Suština je, da se spozna u informacionom svetu, da većina ljudi ne planira neuspeh. (Beckley, 2009) Iako su nekada troškovi visoki, veštine u IT okruženju treba da napreduju, jer ne treba čekati da se zaradi novac pa da se snize troškovi. Kako podaci govore, to zvuči dobro, ali nikada se realno tako ne događa. Finansijski plan koji se temelji na ciljevima pomaže, da se učini ono što je najbolje za uspešno poslovanje. Cilj je, da se proces finansijskog planiranja pojednostavi, i da se eliminišu sve pretpostavke ili nagađanja, šta može da bude. U suštini, u pogledu usredsređivanja pažnje na korišćenje sopstvenih veština prilikom primene IT tehnika i tehnologija, treba uraditi sledeće: 1. Upoznati planove i odrediti prioritete. 2. Minimizirati razlike u ostvarivanju uspeha. 3. Definisati strategiju primene veština. 4. Razvijati i primenjivati fleksibilnost primene tih veština. 5. Spremno odgovoriti na potrebe i fluktuacije na tržištu.

Ključne reči: *Problemi u nedostatku veština, IT tehnologije, rizici, komunikacije, promene, liderstvo, poslovanje*

Abstract

The fourth world revolution of science and practice belongs to the application of new IT information technologies and their great application in all spheres of business. Starting from the most developed social network - the Internet, where the public use of this network is open, but as the data show, there are examples in the world that prove otherwise, that is, the nature of the Internet through its use threatens closed information networks, e.g. developed by the financial industry in the late 20th century. The problems that have resulted in this conflict are primarily explained by banks. That said, these technologies have dominated form, as information-sharing and information-security technologies. According to the data, the evolutionary development of online commercial transactions began back in 1995, and by 1998, more than $ 50 billion in transactions had been processed through the Internet. In the 21st century, the annual value of Internet transactions has increased significantly, which consequently requires more networks, more computers and more security programs. Thus, it is mainly financial institutions that are focused on developing and acquiring more skills in using IT technologies to compete. A clear conception of implementing IT prefers precision, that is, financial institutions cannot compete without a broad and secure information network, which is to say that information technologies are essential for business processes and long-term success. What is meant by the term "Global Financing"? In the modern financial world, this is practically explained as follows: that information technologies enable, globally, financing to operate on the basis of a business syntax that structures the conception in the IT sector for finance as follows: "that financial markets can be considered as the first organized global information markets to operate over networked computers." The bottom line is to realize in the information world that most people do not plan to fail. Although sometimes costs are high, skills in the IT environment need to thrive because you don't have to wait for money to be made and costs reduced. As the data say, it sounds good, but it never really happens. A goal based financial plan helps to do what is best for a successful business. The goal is to streamline the financial planning process, and to eliminate all assumptions or speculations, which may be. Basically, in order to focus on using your own skills when applying IT techniques and technologies, the following should be done: 1. Know the plans and prioritize. 2. Minimize the chances of success. 3. Define a strategy for applying skills. 4. Develop and apply the flexibility of applying these skills. 5. Ready to respond to market needs and fluctuations.

Keywords: *Skills problems, IT technologies, risks, communications, change, leadership, business*

1 UVOD

Poslovanje kompanija na globalnom nivou govori, da bez informacionih tehnologija, finansijska tržišta ne mogu da reaguju uspešno, na globalna kretanja, i da finansijske kompanije ne mogu dosledno da stiču relevantne informacije istovremeno sa svojim konkurentima. Kako primeri pokazuju u svetu, Internet omogućava neprekidan pristup bonitetnim ocenama (prema ekonomskim naukama, to je skup objektiviziranih i standardizovanih podataka koji obuhvataju celokupno poslovanje jednog privrednog subjekta. Utvrđuje se na osnovu posebne metodologije koja obuhvata finansijsku i ekonomsku analizu poslovanja u prethodnoj godini) (Kljun, 2019), i kreditnim rejtinzima svim zajmodavcima, osiguravajućim društvima i preduzećima kojima su potrebni finansijski odgovorni klijenti.

Postavlja se pitanje, da li uvek mora da postoji "Jaz veština"?

Primeri u svetu govore, da se mnogo raspravlja o jazu veština u IT-u (n.d., Marketing Automation, 2019), ali u suprotnom – postoje u svetu tehnološki lideri koji sada problem smatraju više samo-prisutnim u svakodnevnom poslu, nego nerešivim.

Naime, IT sektori mogu u tome uspeti, tako što će „pokazati svoje veštine prisutnim zaposlenima".

Većina IT grupa za zapošljavanje istražuje, analizira i procenjuje prisutnu različitost ljudskih resursa na holistički način, što omogućava da se otvori šire polje veština prisutnih pojedinaca, što za posledicu toga može da se ostvari veći nivo produktivnosti.

2 JAZ IZMEĐU IT VEŠTINA – PRIKAZ ČINJENICA U ODNOSU NA FIKCIJE

Kada se danas govori o IT tehnologijama, njihovoj primeni i razvoju, misli se na:

- neprekidno stvaranje inovacija,
- na primenu digitalne transformacije,
- na poslovne lidere koji u svojim kompanijama žele da ubrzaju digitalnu transformaciju (prema podacima njih je oko 2/3 u poslovnom svetu), da se ne bi suočili sa gubitkom pozicije pred konkurentima,
- na alate za postizanje prioriteta koji su kritični za misiju kompanije,
- na donošenje ispravnih odluka, veštinama kojima se predviđa budućnost,
- na istraživanja i merenje podataka pomoću mreže stručnjaka i dr. (n.d., Marketing Automation, 2019)

Pored ostalih karakteristika kvaliteta primenom IT tehnologija u poslovanju, važno je razvijati sledeće veštine:

1. **Analitičke veštine.** Struktura rada zaposlenih odnosi se na procenu kvaliteta mreža i sistema. To se sprovodi u cilju osiguranja pouzdanog rada i predviđanja novih zahteva za potrebe klijenata koji se često podložni menjanju.
2. **Komunikacijske veštine.** Sprovode se u cilju opisivanja problema i iznalaženja njihovih rešenja.
3. **Potrebne višegodišnje inovativne veštine.** Sprovode se istovremeno na mnogim problemima i zadacima.
4. **Veštine rešavanja problema.** Sprovodi se brzo u cilju efikasnog rešavanja problema koji nastaju kod računarskih mreža. Ključnu ulogu u tome ima *radno okruženje.*

3 STRATEŠKI TREND U IT TEHNOLOGIJAMA

Kada se govori o preduzeću kao sistemu koji pokreće nove promene u IT sektoru, prema analizi (Cearley & Burke, 2019), to se odnosi prvenstveno na digitalnu transformaciju, gde se time podstiču organizacije na stalno osvežavanje svojih poslovnih modela ka tehnološkom napretku. Praksa u svetu govori, da nova IT tehnologija stalno pojačava promene i to sa sve većom brzinom. Lideri tehnoloških inovacija moraju da se usmere na:

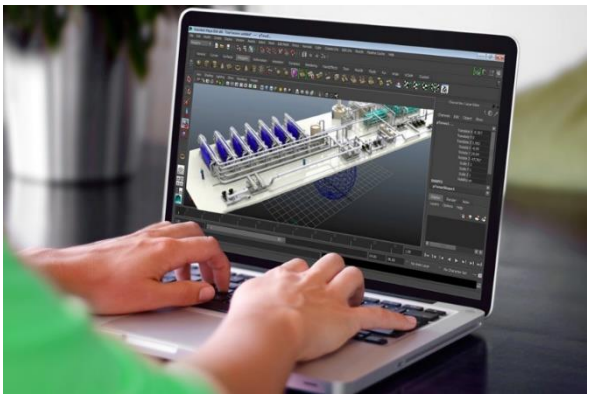
- spoznaju, saznanja i prihvatanje takvih promena,

- prihvatanje strategije „ContinuousNext“ koja se odnosi na postizanje uspeha u svetu koji se stalno kreće unapred,
- pozicioniranje svoje organizacije koje podstiču stalne inovacije, integraciju i isporuku.

Kako bi se u poslovnoj arhitekturi preduzeća i tehnološkim inovacijama uspešno identifikovali strateški trendovi u IT tehnologijama, lideri (vođe) moraju proceniti korist pri njihovoj implementaciji i razvoju u sopstvenom preduzeću, kako bi:

1. Shodno tome uporedili svoje mogućnosti
2. Prevazišli moguće pretnje
3. Stvorili konkurentsku prednost i
4. Realizovali najvažnije inicijative.

Prednosti novih strateških trendova su, što se omogućava preduzeću da testira širok spektar hipoteza, otvarajući tako nove mogućnosti za obradu i analizu podataka (slika 1). Naime, automatizovani uvid u primenu proširenih analitika doprinosi ugradnji adekvatne poslovne aplikacije kako bi se optimizirale odluke i postupci svih zaposlenih. Proširena analitika uključuje:



Slika 1. Novi strateški trendovi

- Pripremu podataka koristeći automatizaciju mašinskog učenja za proširenje, profilisanje i kvalitet podataka, usklađivanje, modeliranje, manipulaciju, obogaćivanje, razvoj metapodataka (u digitalnom smislu to su strukturirani podaci koji opisuju, objašnjavaju, lociraju ili na neki drugi način omogućavaju lakše upravljanje resursima) i katalogiziranje.
- Poslovnu inteligenciju koja omogućava poslovnim korisnicima i naučnicima da automatski pronađu informacije, vizualiziraju i predstavljaju relevantne nalaze bez izrade modela ili pisanja algoritama.
- Proširenje nauke o podacima i mašinsko učenje koje koriste AI za automatizaciju AI modeliranja i njihovih ključnih aspekata, kao što su inženjering, izbor modela, operacionalizacija, objašnjenje, podešavanje i upravljanje. (Gartner, 2019)

4 STRATEŠKE POSLOVNE MOGUĆNOSTI VEZANE ZA IT POTROŠNJU

Poslovanje savremenih kompanija se usmerava ka cilju, odnosno većem korišćenju IT potrošnju za strateške poslovne mogućnosti, kako bi bile spremne da odgovore na pitanje, koje su sopstvene mogućnosti za veću konkurentnost.

U praksi se javljaju rizici autsorsinga (korišćenje spoljašnjih usluga). To znači da zbog nedostatka veština kod sopstvenih zaposlenih mnoge će organizacije potražiti pomoć spolja. Treba izgraditi svoj ugled i posao na ovoj kritičnoj stvari.

Svaki potez u poslovanju nosi i određene rizike. Neki IT procesi su suviše komplikovani. IT utiče na celo preduzeće od jednostavnih dokumenata do veoma komplikovanih procedura. Rešenje se traži u:

1. **Pristupu savremenim tehnologijama.** Lideri shvataju da nove tehnologije brzo osvajaju razne industrijske oblasti. Oni prate trendove i žele da budu u korak sa konkurencijom i novim tehnologijama.
2. **Visokoj stručnosti zaposlenih.** Kod kompanija čija je to jedina delatnost - IT kompanije, zapošljavaju veoma stručan personal koje već imaju bogato iskustvo u informacionim tehnologijama
3. **Fleksibilnost.** Specijalizovane IT kompanije imaju mnogo više mogućnosti za sticanje novih znanja i iskustava od pojedinaca. (Smith, 2019)

5 ZAKLJUČAK

Novi strategijski trendovi poslovanja kompanija u IT okruženju iniciraju veštine kao značajnu karakteristiku zaposlenih u ovom sektoru. Kako govore podaci, to je posebno važno, kod rešavanja danas sve kompleksnijih poslovnih zadataka i sve složenijih postavljenih ciljeva za koje se nije lako izboriti. Sa druge strane, IT stručnjaci su specifični kad je u pitanju ’’IT komunikacija’’. Podaci govore, da će u zemljama sa padom broja stanovnika ove tehnologije doneti

ekonomski prosperitet i uspešno zameniti opadajući ljudski rad (Japan, Južna Koreja). Trendovi su usmereni na pažnju koju privlače novi programi javnog i privatnog sektora kako bi se ljudi osposobili za potrebne veštine.

U svetu dominira uspeh ostvaren računarskim inženjerstvom i elektrotehnikom. Shodno, najefikasnijim komunikativnim programima u oblasti interneta, ovi programi uključuju svetske klase koje se odnose na programiranje računara, umrežavanje ili dizajn sistema. Praksa u svetu govori, da se mrežna tehnologija neprestano menja, a to znači da zaposleni administratori – programeri i sl. moraju stalno učestvovati u razvoju IT tehnologija kako bi pratili najnovija dostignuća.

Svako radno okruženje obuhvata interne i eksterne faktore razvoja internet tehnologija kako bi se ostvarilo efikasno poslovanje u tom sektoru.

Radno okruženje čine sledeći faktori:

- Dizajniranje računarskih sistema i srodnih usluga
- Informacije
- Obrazovne usluge – edukacija, trening
- Finansije i osiguranje
- Državni, lokalni i privatni sektor
- Upravljanje preduzećima IT tehnologijom i dr.

Danas Internet tehnologija ima sposobnost da prenosi informacije i podatke preko različitih servera i sistema. Internet tehnologija je važna u mnogim različitim industrijama, jer omogućava ljudima da komuniciraju jedni sa drugima putem sredstava net mreže i da posluju uspešno.

CITIRANA DELA

Beckley, J. J. (2009). *National Register Information System.* National Register of Historic Places.

Cearley, D., & Burke, B. (2019). *Vrhunski tehnološki trendovi Gartner-a.* Gartner, Inc.

Gartner. (2019, May 14). *Top technology trends of 2019 by Gartner*. Preuzeto sa NNTC: https://www.nntc.digital/blog/digital-transformation/top-technology-trends-of-2019-by-gartner/

Kljun, M. (2019). *Company Wall d.o.o.* Preuzeto sa Kratki Opis: https://www.ogledalofirme.com/company/22091.Company%20Wall%20d.o.o.?ignoreTouch=1

n.d. (2019). *Investment planning*. Preuzeto sa VINN Financial: https://www.vinnfinancial.com/investment-planning/

n.d. (2019). *Marketing Automation*. Preuzeto sa Sales Manago: https://www.salesmanago.com/info/requestpricing.htm?plan=B2C_ENTERPRISE

Smith, B. (2019). *Information Technology* (T. Published on January). Microsoft Corporation, SAD.

Datum prve prijave: 09.09.2019.
Datum prijema korigovanog članka: 08.10.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

Style – APA Sixth Edition:

Rizqallah Qananah, H., Altaher Mohamed Alnagasa, K., Salem Almabrouk, M., & Živanović, N. (2019, 10 15). Da li su problemi u it veštinama rešivi ili ostaju da budu uvek prisutni? (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 118-123. doi:10.12709/fbim.07.07.02.13

Style – Chicago Sixteenth Edition:

Rizqallah Qananah, Hana, Khalefa Altaher Mohamed Alnagasa, Mohamed Salem Almabrouk, and Nada Živanović. 2019. "Da li su problemi u it veštinama rešivi ili ostaju da budu uvek prisutni?" Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 118-123. doi:10.12709/fbim.07.07.02.13.

Style – GOST Name Sort:

Rizqallah Qananah Hana [et al.] Da li su problemi u it veštinama rešivi ili ostaju da budu uvek prisutni? [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE , 10 15, 2019. - 2 : Vol. 7. - pp. 118-123.

Style – Harvard Anglia:

Rizqallah Qananah, H., Altaher Mohamed Alnagasa, K., Salem Almabrouk, M. & Živanović, N., 2019. Da li su problemi u it veštinama rešivi ili ostaju da budu uvek prisutni?. *FBIM Transactions,* 15 10, 7(2), pp. 118-123.

Style – ISO 690 Numerical Reference:

Da li su problemi u it veštinama rešivi ili ostaju da budu uvek prisutni? **Rizqallah Qananah, Hana, et al.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE , 10 15, 2019, FBIM Transactions, Vol. 7, pp. 118-123.

FBIM Transactions
DOI 10.12709/fbim.07.07.02.14

NEVIDLJIVE TRANSAKCIJE U DARK WEB-U

STEALTH TRANSACTIONS IN THE DARK WEB

Sergej Uljanov
Fakultet za poslovne studije i pravo Univerztiteta „UNION – Nikola Tesla“, Beograd, Republika Srbija

Đorđe Milošević
Kriminalističko-policijski univerzitet, Beograd, Republika Srbija

JEL Kategorija rada: **E49, F38, L86**

Apstrakt

Autori u ovom radu razmatraju mogućnosti vršenja novčanih transakcija skrivenih u okruženju dark web-a. Kao ključne komponente ovakve aktivnosti autori ističu fenomenološki tripod, koji čine pojmovi kripto valute, blockchain tehnologije i virtuelnog novčanika (web wallet). S tim u vezi, autori će prikazati u radu, u posebnim poglavljima, pojmove i vrste virtuelnog novca, web wallet-a i način funkcionisanja blockchain razmene podataka odnosno jedinica kripto valute. Poseban osvrt biće napravljen u odnosu na pitanja anonimnosti i skrivanja tragova novčanih tokova u Darknetu. Autori teže da objasne razloge zbog kojih nosioci transakcija virtuelnog novca insistiraju na svojoj anonimnosti i nemogućnosti praćenja njihove aktivnosti od strane drugih subjekata prisutnih u tamnom vebu, bez obzira na to da li je reč o hakerima ili organima za primenu zakona. Takođe, autori smatraju značajnim obuhvatno posmatranje želje za anonimnim delovanjem, koja ne podrazumeva uvek i isključivo kriminalnu intenciju. U radu su otvorena pitanja stvarne anonimnosti virtuelnih novčanika, kao i ranjivosti blockchain modusa u odnosu na sajber napade i zloupotrebu radi skrivanja novčanih transakcija u kriminalne svrhe, te „pranje“ kripto valuta. Autori u radu nastoje da iznesu najnovije podatke koji se odnose na navedenu problematiku, kako bi istraživani fenomen mogao biti sagledan u svojoj aktuelnosti. Namera autora je da svoje zaključke temelje na punoj voluminoznosti ključnih pojmova, čiji značaj predstavlja okosnicu ovog rada.

Ključne reči: *dark web, kripto valuta, blockchain, web wallet, kripto novčanik, „pranje“ virtuelnog novca, transakcija kripto valute*

Abstract

The authors of this article deem possibilities of doing money transactions covered by the network of the dark web. As key components of such activity the authors highlight phenomenological tripod made of terms relate to cryptocurrency, blockchain technology and virtual wallet (known as web wallet). Thereby, the authors are about to present in this article, as chaptered, terms and kinds of

Adresa autora zaduženog za korespodenciju:
Đorđe Milošević
djodjolos@gmail.com

virtual money, web wallets and the way of running, both, blockchain exchanging of data and of cryptocurencies units. The special overview is to be done considering questions of anonymity and hiding traces of money transactions in the Darknet. The authors tend to explain the reasons why subjects of cryptocurencies transactions insist to remain stealth and anonymized having their activities untraceable to other subjects presented in the dark web, no matter if it is up to hackers or law enforcement. Also, the authors consider as important to make a broader view to the phenomenon of having need for anonymized way of doing transactions, which is not always to be solely connected to criminal intention. There are issues of virtual wallets anonymity and blockchain modus vulnerability relate to cyber attacks and misuse of stealth money transactions, both, for illegal purpose and for criptocurrencies money laundering, to be mattered in this article. The authors strive to express the most recent data on the above-mentioned challenges, to make researched phenomenon to be perceived as actual one. Intention of the authors is to base their conclusions on full-scale volume of essential terms which importance represents framework to this article.

Keywords: *the dark web, cryptocurrency, blockchain, web wallet, dark wallet, cryptocurrency money laundering, cryptocurrency transaction*

1. UVOD

Digitalna era prekinula je i gotovo prevazišla tradicionalno organizovanje baza podataka u svakoj oblasti poslovanja uvodeći standarde koji podrazumevaju njene produkte, kao što su elektronsko trgovanje, društvene mreže, kripto valute, cloud computing i obrada kompleksnih setova podataka. Brz napredak u razvoju i inovacijama digitalnih proizvoda otovorio je mogućnosti za neovlašćen pristup zaštićenim podacima i sajber krađe. Zbog ovakvih pretnji, korisnici se sve više opredeljuju za informatičke proizvode koji štite privatnost i podižu nivo sajber bezbednosti. Korisnici koji se kreću u prostorima digitalnih tržišta, upotrebljavaju elektronski način plaćanja i razmenjuju informacije na grupnim forumima zahtevaju veći stepen anonimnosti za svoje prisustvo i svoje aktivnosti na globalnom vebu, a naročito u njegovom nevidljivom delu Deep Web-u u kome se odvija intentzivna online komunikacija i realizuju novčane transakcije. Platforme koje omogućuju anonimnost podataka, svakako, čine rešenje za ovakav problem korisnika. Ove platforme postoje u formi web wallet odnosno virtuelnog novčanika, poznatog i kao dark wallet, te skrivenih mreža za komunikaciju u dubokom vebu, posebno u njegovoj Darknet zoni. Jedna od ovakvih mreža je, prvenstveno, izraz kapaciteta pretraživača TOR, čija eksploatacija ne eksponira identitet korisnika. Kao ulaznica u polje dark web-a, TOR je značajna karika u lancu kretanja korisnika kroz neprozirne slojeve nevidljivog veba.

Darknet je popularniji nego posećeniji, jer samo manja populacija korisnika poznaje načine njegovog funkcionisanja. Za ogromnu većinu korisnika tamni veb je misteriozni deo dubokog veba, povodom koga i dalje ima više pitanja nego odgovora. U njegovom okruženju, pored ostalih diskretnih aktivnosti, kripto valute svojim tokovima doprinose održavanju i razvoju ilegalnog prometa i jačanju kriminalnih tržišta. Nevidljive transakcije pomoću blockchain tehnologije privlače brojne korisnike da plasiraju svoj virtuelni novac na „crna“ tržišta Darkneta i tako anonimno dođu do zabranjenih proizvoda odnosno nelegalnih informatičkih sadržaja, usluga i servisa.

Da bi anonimna transakcija kripto valute na kriminalnom tržištu tamnog veba bila ostvariva neophodna je sinergija tripoda njenih komponenti: kripto valuta, blockchain tehnologije i web wallet-a, kojima posvećujemo sledeće redove.

2. KRIPTOVALUTE

Bitcoin je digitalni fenomen koji je imao iznenađujuće brz razvoj kao monetarni entitet sposoban da očuva vrednost, ali i kao sredstvo razmene. Međutim, rame uz rame sa porastom njegove popularnosti, ovaj virtuelni novac postao je učestala meta krađe i izuzetno tražena platežna jedinica za potrebe ilegalnog poslovanja. S tim u vezi, napomenućemo da kao način odbrane anonimnosti i privatnosti učesnika u transakciji kripto valute, može da posluži dark wallet koji je vrsta web wallet-a odnosno kripto novčanika zaštitnika virtuelnog novca od sajber napada i krađe.

Najveći protivnik kripto valute je nedovoljna obaveštenost javnosti o njenoj svrsi, s obzirom na to da se ovaj digitalni novac predstavlja kao činilac privatnosti korisnika koji se ne može kontrolisati. Ipak, koncept virtuelnog novca nije shvaćen u potpunosti jer je mreža za razmenu bitcoin-a dostupna na javnom registratoru što smanjuje garanciju potpune anonimnosti korisnika.

Bitcoin nije samo fenomen koji je postavio trend upotrebe virtuelnog načina plaćanja roba i usluga, već je činjenicom svoje upotrebljivosti u decentralizovanoj peer-to-peer mreži (u kojoj su svi učesnici jednaki) postao standard za kreiranje kripto valuta i kao takav izazov i inspiracija za mnoge dizajnere virtuelnog novca.

Pre upoznavanja sa drugim vrstama kripto valuta, koje se uslovno rečeno mogu posmatrati kao alternative bitcoin-u, neophodno je najpre sagledati smisao virtuelnog novca uopšte. Naime, reč je o digitalnom novcu, koji ima oblik kovanica. Dok su neke vrste kripto valuta dostupne u fizičkom svetu posredstvom kreditnih kartica, velika većina ovakve vrste novca ostaje potpuno neopipiljiva (Bajpai, 2019).

Tajnost kripto valuta odnosi se na diskretnost složenog postupanja sa digitalnim kovanicama, koje se odnosi na njihovo generisanje, čuvanje i bezbednu transakciju, uz prerogativ anonimnosti. Uz tajnost, kao ključnu karakteristiku, kripto valute odlikuje i decentralizovanost načina upotrebe jer su nastale timskim radom, koji je kodirao proces njihovog izdavanja (često nazivan „iskopavanje rude“) i kontrole tokova njihovog plasiranja (Bajpai, 2019). Kripto valute su dizajnirane na načine koji ih skrivaju od kontrole državnih organa, zbog čega su često izložene javnoj kritici.

Pored bitcoin-a, sve druge vrste virtuelnog novca nazivaju se alternativne kripto valute i njihovi kreatori nastoje da ih predstave kao izmenjenu ili unapređenu verziju bitcoin-a. Neke od ovih digitalnih valuta se „iskopavaju“ jednostavnije od bitcoin-a, ali mogu biti manje likvidne, manje prihvatljive i zato manje vrednosti jer način njihovog generisanja uslovljava njihov kvalitet (Bajpai, 2019).

Nije moguće obuhvatno predstaviti jedinstvenom listom sve postojeće kripto valute jer neprestano nastaju nove. Danas ima više od 1.600 virtuelnih moneta i mnoge od njih su popularne u različitim grupama sponzora i ulagača (Bajpai, 2019). Polje kripto valuta se stalno uvećava, pa se bitcoin već uveliko posmatra kao inicijalna pionirska moneta u odnosu na koju se određuju parametri za kreiranje novih virtuelnih valuta (Bajpai, 2019). Uobičajeno je da se rejting kripto valuta uspostavlja prema njihovoj tržišnoj vrednosti, što je *inter alia* uzeto u obzir prilikom narednog redosleda njihovog izlaganja.

2.1. Vrste kripto valuta

U odnosu na veliki broj postojećih alernativnih kripto valuta, od kojih su među najpopularnijima: ethereum, ripple, bitcoin cash, litecoin, cardano, neo, eos, iota, dash, monero, ark, nem, vechain, tether, lisk, gas, qtum, aelf, icon, zcash, waves, steem, verge, ardor, ox, nano, tron, stellar, dent, salt i dr., podrobnije ćemo razmotriti značaj sledećih virtuelnih moneta:

1. Litecoin, nastala 2011. godine, bila je jedna od prvih virtuelnih valuta koje su pratile uzor bitcoin-a i često je karakterisana kao srebrna verzija bitcoin-ovog zlatnika. Ova kripto valuta koncipirana je na globalnoj otvorenoj platnoj mreži, koja nije pod centralizovanom kontrolom. Litecoin kao verifikator koristi algoritamsku šifru čije dekodiranje izvodi glavni procesor na korisničkom nivou. Premda litecoin u velikoj meri podseća na bitcoin, ipak ima veću brzinu u generisanju digitalnih podataka i nudi bržu potvrdu transakcije. U porastu je broj sajber trgovaca koji su prihvatili ovaj kripto novac, kao i onih koji doprinose njegovom razvoju. Početkom februara, 2019. godine, litecoin je imao tržišnu vrednost od 2.630.000.000 američkih dolara, uz pojedinačnu vrednost kovanice u iznosu od 43,41 američka dolara (Bajpai, 2019).
2. Nastala tokom 2015. godine, ethereum je decentralizovana softverska platforma koja omogućuje izradu protokola neposrednih transakcija i mrežnih softvera bez radnog diskontinuiteta angžovanih umreženih računarskih jedinica, mogućnosti prevare, kontrole ili mešanja treće strane. Aplikacije se pokreću na ovoj platformi na svakoj kovanici kripto valute. Kovanice nalikuju vozilima koja se kreću po platformi, pa ulagači svoja

potraživanja drugih kripto valuta obavljaju posredstvom ethereum-a. Tokom 2014. godine, ethereum je plasirao pretprodaju kovanica, koja je naišla na neočekivano veliki odgovor korisnika. Prema devizi svojih kreatora, ova kripto valuta može biti upotrebljena za organizovanje, decentralizovanje, obezbeđivanje i trgovinu svega i svačega. Posle hakerskog napada 2016 godine, od ethereum-a je izdvojen ethereum classic, kao poseban vid ove virtuelne monete. Početkom 2019. godine, tržišna vrednost ethereum-a iznosila je 12.490.000.000 američkih dolara, a vrednost pojedinačne kovanice bila je 118,71 američki dolar (Bajpai, 2019).

3. Zcash je decentralizovana kripto valuta otvorenog tipa, koja je plasirana krajem 2016. godine. Kreatori tvrde da bitcoin svojom važnošću predstavlja http (glavni protokol) za finansije, ali da zcash u tom smislu predstavlja https (obezbeđen glavni protokol). Ova kripto valuta nudi privatnost i selektivnu transparentnost transakcija. Tako, poput https-a, zcash može da obezbedi izuzetan stepen bezbednosti ili privatnosti u slučajevima gde se sve transakcije registruju i izdaju u blockchain modusu, ali da pri tom podaci o pošiljaocu, primaocu i visini iznosa ostaju u sferi privatnosti. Zcash omogućuje svojim korisnicima zaštićene transakcije, čiji sadržaj je kriptovan upotrebom napredne kriptrografske tehnike sa nazivom zk-SNARK, koju kreira isti tim tvoraca ove virtuelne valute. U prva dva meseca 2019. godine, zcash je ima tržišnu vrednost od 291.500.000 američkih dolara, dok je pojedinačna vrednost kripto kovanice iznosila 49,84 američka dolara (Bajpai, 2019).
4. Dash je kripto moneta, poznata i kao darkcoin, koja je diskretnija verzija bitcoin-a. Dash nudi veći stepen anonimnosti jer funkcioniše preko decentralizovane mreže glavnog koda koja gotovo sasvim onemogućava praćenje tragova transakcije. Ova kripto moneta nastala je 2014. godine i za kratko vreme dobila je veliki broj korisnika. U prvom tromesečju 2015. godine darkcoin je promenio ime u dash, što je skraćenica od digital cash odnosno digitalne gotovine. Ova izmena nije uticala na funkcionalnost informatičkih alata, kao što su DarkSend za mešanje kovanica radi povećanja njihove anonimnosti i InstantX koji omogućava brze digitalne transakcije u rasponu od 3 američka centa do 3.000 američkih dolara. Početkom 2019. godine, tržišna vrednost dash-a bila je 640.760.000 američkih dolara, uz pojedinačnu vrednost kovanice od 74,32 američka dolara (Bajpai, 2019).
5. Ripple je globalna mreža koja u realnom vremenu nudi brzu, pouzdanu i jeftinu mogućnost vršenja uplata na međunarodnom nivou. Nastala je 2012. godine. Njeno potvrđivanje konsenzusom korisnika ne zahteva generisanje „iskopavanjem“ zbog čega se ripple kripto novac odvojio od bitcoina i drugih altrenativnih virtuelnih moneta. S obzirom da ripple ne zahteva „iskopavanje“, to umanjuje angažovanje računarskih jedinica i minimizira usporenost mreže. Ideja tvoraca ripple-a je da distribucijom vrednosti motivišu razvoj poslovnosti, podignu nivo likvidnosti provajdera i prodaju ovu kripto valutu institucionalnim kupcima zainteresovanim da investiraju plasiranjem ovog virtuelnog novca. Do sada, ripple je imao uspeha sa ovim modelom funkcionisanja, te je ostao privlačan kao digitalna valuta tradicionalnim finansijskim subjektima, koji traže načine za unapređivanje prekograničnog načina isplate. Na početku 2019. godine, ripple je imao tržišnu vrednost od 12.690.000.000 milijardi američkih dolara, a pojedinačna vrednost njegove kovanice bila je 0,308 američkog dolara (Bajpai, 2019).
6. Monero je bezbedna i anonimna kripto valuta, čije tragove nije moguće pratiti. Ovaj virtuelni novac, otvorenog tipa, nastao je 2014. godine i brzo pobudio interesovanje kriptografske zajednice i entuzijasta. Njegov razvoj je u potpunosti doniran i timski usmeravan. Monero je produkt potrebe za decentralizovanom upotrebom i promenljivom veličinom blokova podataka, što omogućava potpunu privatnost uz upotrebu posebne tehnike zvane prstenasti potpis. Ovo podrazumeva postojanje grupe validnih potpisa, od kojih bar jedan pripada postojećem korisniku, ali se on ne može izdvojiti jer ga krije grupa. Zbog takvog izuzetnog mehanizma zaštite, monero je kao virtuelni novac stekao lošu reputaciju jer se

dovodi u vezu sa kriminalnim operacijama širom sveta. Nebitno da li se ova kripto valuta koristi u dobre ili loše svrhe, ne može se poreći da je njenim nastankom u svet virtuelnih moneta uveden značajni tehnološki pomak. Na početku 2019. godine, tržišna vrednost monera iznosila je 808.500.000 američkih dolara, a vrednost njene kovanice bila je 48,18 američkih dolara (Bajpai, 2019).

7. Bitcoin cash kao kripto moneta zauzima značajno mesto u istoriji alternativnog virtuelnog novca jer je prvi uspešno odvojen od originalnog bitcoin-a razdvajanjem blockchain modusa, do kog je došlo usled neslaganja unapređivača ovog kripto novca i onih koji su ga „iskopavali“. Zbog decentralizovane prirode digitalnog novca, obuhvatne promene esencijalnog koda u kovanici moraju biti rezultat konsenzusa svih članova u zajednici korisnika. Ovaj mehanizam varira u zavisnosti od tipa konkretne kripto valute kod koje je došlo do protokolarnog neslaganja u blockchain-u. Bitcoin je, tako, nastao 2017. godine kao rezultat navedenog razdvajanja. Dok je kod bitcoin-a limit veličine blokova sa podacima striktan i iznosi 1 megabajt, kod bitcoin cash-a se kreće od 1 do 8 megabajta sa idejom da će veći blokovi doprineti bržem odvijanju transakcije. Ovo je dovelo i drugih promena, kao što je uklanjanje protokola Segregated Witness koji se odnosi na veličinu blokova sa podacima. Početkom 2019. godine, bitcoin cash je imao tržišnu vrednost od 2.230.000.000 američkih dolara, uz pojedinačnu vrednost kovanica od 126,49 američkih dolara (Bajpai, 2019).
8. Neo je nastao 2014. godine pod svojim prvim nazivom AntShares. Do sada, ovo je najzastupljenilja kripto valuta koja se pojavila u Kini zbog čega se naziva i kineskim ethereum-om, uzevši u obzir njenu sličnu upotrebu kod ostvarivanja neposrednih transakcija. Tokom 2017. godine, neo je ostvario uspeh sa skokom tržišne vrednosti od 0,16 do čak 162 američka dolara po kovanici, što iznosi uvećanje od neverovatnih 111%. Jedan od razloga za ovakav strelovit uspon leži u podršci koju je ova kripto valuta ostvarila u odnosu na razvoj programskih jezika, kao što su Go, Java, C++ i drugi. Smatramo ključnim afirmativan odnos kineske Vlade prema ovom virtuelnom novcu, imajući u vidu njen rigidan stav prema kripto valutama. Na početku 2019. godine, neo je vredeo na tržištu 492.480.000 američkih dolara, a po kovanici 7,58 američkih dolara (Bajpai, 2019).
9. Cardano je virtuelna moneta kreirana u drugoj polovini 2017. godine, nudeći sve prednosti platforme ethereum u vezi sa neposrednim transakcijama i mobilnim aplikacijama. Tendencija tvoraca ove kripto valute je rešavanje problema interoperabilnosti i veličine blokova podataka u nizu blockchain modusa. Cardano kripto novac, takođe, je usmeren na prevazilaženje problema međunarodnih isplata, koje su skupe i vremenski zahtevne. Zahvaljujući tako usmerenim naporima kreatora putem ove kripto valute međunarodna isplata bila je realizovana u vremenskom intervalu od nekoliko sekundi. Početkom 2019. godine, cardano-va tržišna vrednost iznosila je 1.160.000 američkih dolara, dok je pojedinačna vrednost kovanica bila 0,041 američkog dolara (Bajpai, 2019).
10. Eos spada u najmlađe kripto valute. Nastala je 2018. godine prema dizajnu ethereum-a, tako da nudi platformu za razvoj decentralizovanih aplikacija. Prvi plasman ovog virtuelnog novca doneo je 4.000.000.000 američkih dolara od usluga upućenih masovnom broju korisnika. Eos funkcioniše prema distribuiranom konsenzusu na svojoj mreži u kojoj se razmenjue prema blockchain modusu, pri čemu je svaki sledeći blok podataka izabran slučajnom kombinacijom promenljivih faktora, kao što su imovinska vrednost ili starosna dob. Ovo je razlog zašto eos upotrebljava blokove podataka promenljive veličine. Ova kripto valuta ima svoj operativni sistem, koji igra ulogu blockchain mreže za razmenu eos kovanica. Eos je izuzetno napredan kripto novac jer ne zahteva „iskopavanje“ da bi se proizvodile njegove kovanice. Umesto toga, proizvođači blokova podataka bivaju nagrađeni eos kovanicama u zavisnosti od dostignutog stepena ostvarene proizvodnje. Eos podrazumeva složen sistem pravila koja se odnose na upravljanje navedenim procesom, sa ciljem da mreža ovog virtuelnog novca bude više

decentralizovana od sistema rivalskih kripto moneta. Krajem 2018. godine, tržišna vrednost eos-a bilaje 2.490.000.000 američkih dolara, dok je pojedinačna vrednost njegove kovanice iznosila 2,47 američkih dolara (Bajpai, 2019).

Bitcoin nastavlja da predvodi ostale kripto valute, prema kriterijumima tržišne vrednosti, baze podataka korisnika i popularnosti. Ipak, virtualne monete kao što su ethereum i ripple, koje se više koriste u preduzetničke svrhe, postaju sve zastupljenije. Vreme će pokazati da li će i koje kripto valute, zbog revolucionarnosti svojih performansi, potisnuti konkurentske alternativne virtuelne monete i prevazići rešenja koja za sada nudi bitcoin. Prema nekim mišljenjima bitcoin nije anoniman zbog čega je podesan za ilegalne aktivnosti i „pranje“ virtuelnog novca (Canellis, 2018), dok ima i tvrdnji koje afirmativno ocenjuju prednosti bitcoin-a jer omogućava izbegavanje sporosti protokola tradicionalnih finansijskih institucija (Nakamoto, 2009).

2.2. „Pranje” novca zloupotrebom kripto valute

Nasuprot opštem uverenju, nije teško slediti tragove transakcija bitcoin-a i otkriti podatke onih koji su ih izvršili. Očigledno, blockchain modus je transparentan, tako da se akteri kriminalnih transakcija bitcoin-a mogu otkriti. Bitcoin nije anoniman. Za ostale kripto valute i dalje veliki problem predstavlja skrivanje podataka njihovih pošiljaoca, primaoca i potrošača (Canellis, 2018). Ostaje pitanje na koji način nosioci kriminalnih aktivnosti kripto novac, koji potiče iz nezakonite delatnosti, „peru“ i plasiraju u regularne tokove virtuelnih valuta.

Prema nekim mišljenjima ilegalno stečena kripto moneta može se „oprati“ tzv. preturanjem i slobodnom razmenom (Canellis, 2018). Preturanje podrazumeva rasturanje kovanica bitcoin-a, radi njihovog ponovog skupljanja. Bitcoin-i se najpre upućuju na različite adrese, da bi se potom u celokupnom iznosu sve kovanice našle u kripto novčaniku (dark wallet) postavljenom u tamnom vebu (Canellis, 2018). Ovaj postupak ne iziskuje previše pažljivosti, ali nije besplatan. Uobičajeni troškovi iznose 1% do 3% vrednosti virtuelne valute koja se „čisti“ mešanjem. Potrebno je imati jedan web wallet postavljen u regularnoj zoni Interneta, a zatim još dva ili više wallet-a (u ovom slučaju dark wallet-a) koji funkcionišu u okruženju Darkneta. Dalji postupak nalaže da se bitcoin-i iz web wallet-a pošalju u skrivene dark wallet-e. Ovakva transakcija naziva se „skok“ i može se izvesti više puta u samom tamnom vebu. Svakim „skokom“ više se zameću tragovi transakcije. Kada se niz takvih transakcija završi, bitcoin-i se prevrću u mešalici odnosno u naročitom informatičkom servisu koji rastura i skuplja kovanice kripto novca, kako bi se još više obezbedio stepen anonimnosti njihovog korisnika. Rasturanje kovanica realizuje se brojnim transakcijama, koje se vrše u nasumičnom intervalu prema bitcoin adresama u TOR-ovoj mreži. Posle mešanja, pretpostavlja se da je kripto valuta „oprana“ odnosno da se ne mogu otkriti podaci njenog korisnika. Takve kovanice razmenjuju se za druge bitcoin-e, kovanice drugih kripto moneta ili čak legalno izdat nekonvertibilni papirni novac. Neki autori smatraju da ni prikazani postupak ne garantuje bezbednost i privatnost korisnika kripto novca koje se „pere“ jer se ovakvi servisi za preturanje i mešanje virtuelnih valuta koriste u kriminalne svrhe i mogu oštteti bez kontrole inicijatora navedenih transakcija (Canellis, 2018), dok postoje i osporavanja funkcionalnosti dark wallet-a u TOR-ovoj mreži uz isticanje prevaziđenosti takvog načina postupanja (Khatwani, 2019).

Kao jednostvaniji način „pranja“ virtuelnog novca može poslužiti slobodna razmena (Canellis, 2018). Ova razmena se vrši mimo protokola know-your-customer i anty-money-laundering, u kojima je identifikacija korisnika obavezna. Postupak razmene vrši se bez mešanja kripto valute. Potrebno je trgovati bitcoin-ima na različitim tržištima više puta. Tako korisnik može da izvši razmenu bitcoin-a za kovanice alternativnog virtuelnog novca. Svaki put kada se kripto valuta razmeni za drugu virtuelnu monetu povećava se stepen privatnosti, slično „skokovima“ na wallet adrese u Darknetu. Efektivnost razmene uslovljena je kapacitetom informatičkog servisa koji obavlja uslugu, tako da i ovaj način „pranja“ virtuelnih kovanica nije potpuno siguran. Nakon razmene, korisnik može svoj kripto novac uputiti u dark wallet posredstvom još jedne anonimne transakcije. Naposletku razmenjen virtuelni novac može biti

zamenjen i sa „čistom“ nekonvertibilnom legalnom valutom, ali to je ređi slučaj zbog nepostojanosti i kratkotrajnosti održavanja ovakvih tržišta za razmenu kripto valuta sa legalnim novcem. Nesumnjivo, „perači“ kripto moneta opredeljuju se za skrovita peer-to-peer tržišta i ilegalne usluge u TOR-ovoj mreži, kako bi svoje kriminalno stečene virtuelne kovanice pretvnorili u legalnu gotovinu.

Holandska policije je 2016. godine je upala u međunarodni lanac za „pranje“ novca, kojom prilikom je zaplenjeno više bankovnih računa, bitcoin kovanice, luksuzna vozila visoke klase i sastojci za pravljenje sintetičke droge. Utvrđeno je da je u ovom slučaju kripto valuta „čišćena“ slobodnom razmenom i to preko država gde gotovo i da se ne primenjuju protokoli za sprečavanje „pranja“ novca, te da je 97% „opranih“ kovanica završilo u državama koje imaju izuzetno blag režim ograničavajućih protokola (Canellis, 2018).

Postoji, takođe, mogućnost „pranja“ kripto novca, možda manje nedozvoljena ali i dalje u sferi sumnjivih aktivnosti, koja podrazumeva mešanje kovanica i dovodi se u vezu sa zabranjenim sajtovima za kockanje virtuelnim novcem (Canellis, 2018). Ovi sajtovi su pod nadzorom Coinbase servisa za vršenje regularnih razmena. U ovom slučaju, digitalni novac dospeva u blockchain kockarnica pre nego što se plasira u Coinbase zbog čega pruža mogućnost za „pranje“ virtuelnog novca proisteklog iz kriminalne aktivnosti (Canellis, 2018).

Naposletku, navešćemo još jedan modalitet „pranja“ virtelnih moneta putem zloupotrebe kripto kartica. U aprilu 2019. godine, Coinbase je ostvario partnerstvo sa Paysafe i Visa provajderima, te svojim korisnicama omogućio snabdevanje kripto karticama (Kaminska, 2019). Posrednici u „čišćenju“ digitalnih kovanica, sada mogu da svojim klijentima predaju kripto kartice i pin brojeve. Time se narušava zadari režim korišćenja kripto kartica, ali tome se ne pridaje poseban značaj. Ključna je činjenica da su kripto kartice i pin brojevi bezlični i ne podrazumevaju kontaktiranje ličnim podacima korisnika u ovakvom mehanizmu za „pranje“ kripto novca zbog čega kripto kartice predstavljaju ozbiljan izvor rizika za savesne nosioce (Kaminska, 2019).

3. BLOCKCHAIN MODUS

U suštini blockchain je lanac blokova, u kome „blokovi“ predstavljaju grupu digitalnih podataka, koji su pohranjeni u „lance“ odnosno baze podataka. Preciznije, blokovi su sačinjeni od digitalnih delova informacija i imaju tri osnovna dela. U prvom segmentu bloka, nalaze se podaci o datumu, vremenu, te iznosu novca poslednje realizovane nabavke izvršene preko Interneta. U drugom segmentu, blok sadrži podatke o učesnicima transakcije koji su prikazani kroz digitalni potpis, a nisu navedeni doslovno. U trećem segmentu bloka, pohranjen je identifikacioni jedinstveni kod, poznat kao hash, koji omogućuje međusobno razlikovanje blokova zbog čega nije moguće napraviti istu porudžbinu dva puta. Jedan blok u blockchain-u ima kapacitet do 1 megabajta podataka, što bi značilo da u odnosu na veličinu transakcije, u jednom bloku može biti smešteno nekoliko hiljada transakcija.

Primera radi prikazaćemo javni ključ: 1EHYa6X4Jz2uvNExL504nE41pwXhwL6kWn. Ovaj ključ povezan je sa privatnim ključem kojim se pristupa glavnom kripto novčaniku učesnika u transakciji (Khatwani, 2019). Uvidom u blockchain pretraživač doći ćemo do saznanja da je na ovoj adresi obavljeno više hiljada transakcija, te da je na njoj istovremeno pozicionirano 7 bitcoin-a (Khatwani, 2019).

Kada se u blok smeste novi podaci, oni se dodaju i celom lancu. Blockchain obuhvata veći broj blokova zbog čega predstavlja zbir njihovih kapaciteta za pohranjivanje podataka. Da bi jedan blok bio prihvaćen u blockchain moraju biti ispunjeni sledeći uslovi. Najpre mora doći do transakcije. Potom ona podleže verifikaciji. U slučaju transakcije bitcoin-a, oko 5.000.000 računarskih jedinica u svetu mrežno će obaviti kontrolu novih podataka, koji se odnose na vreme transakcije, novčani iznos i učesnike. Sledi pakovanje podataka o transakciji u blok, koji će se pridružiti hiljadama drugih takvih blokova u blockchain-u. Na kraju, svaki blok dobija svoj jedinstveni hash kod kojim se razlikuje od drugih blokova, ali i hash koji ga označava kao poslednjeg u nizu blockchain-a. Po dodavanju novog bloka lancu, njegov sadržaj postaje javno dostupan. Moguće je ostvariti uvid u podatke koji su predmet transakcije, kao što su oni koju

ukazuju na vreme, mesto i korisnika koji je dodao blok u blockchain.

Blokchain je javni registar na kome počiva kompletna mreža za razmenu Bitcoin-a. Sve potvrđene transakcije nalaze se u blockchain-u. On dozvoljava kripto novčanicima da vrše kalkulaciju svog platnog kapaciteta, tako da nova transakcija može biti verifikovana jer pripada potrošaču koji je pokrenuo. Integritet i hronološki poredak u blockchain-u su kriptografski zaštićene kategorije jer se poruke i transakcije kreću kroz različite blockchain mreže na bezbedan i matematički pouzdan način (Khatwani, 2018).

Sama transakcija je transfer vrednosti koji se odvija između kripto novčanika sa bitcoin-ima, koji su uvršteni u blockchain. Web wallet sadrži i tajni deo podatka, koji se zove tajni ključ ili seme. Ovaj ključ se koristi za potpisivanje transakcije i predstavlja matematičku činjenicu da potiče od vlasnika kripto novčanika kome i pripada. Potpis štiti transakciju od neovlašćenog pristupa jer samo vlasnik tajnog ključa može vršiti transfer podataka na bitcoin adrese koje želi (Khatwani, 2019). Ne treba smetnuti s uma da se podaci kodirani i prikazani kao numerički niz (Khatwani, 2019). Sve transakcije u mreži obično se potvrđuju u roku od 10 do 20 minuta postupkom koji se naziva „iskopavanje“. Ovaj postupak je distribuirani sistem koji počiva na konsenzusu radi potvrde transakcije i njenog upakivanja u blockchain. Time je naložen i hronološki red postavljanja blokova u lanac, kojim se štiti neutralnost mreže blockchain-a i odobrava različitim računarskim jedinicama da jednoglasno svoje slaganje sa stanjem u sistemu. Svaki blok podleže strogim kriptografskim pravilima, čije poštovanje verifikuje mreža blockchain-a. Ova pravila sprečavaju izmenu u blokovima koji su već postavljeni u lanac jer bi to oštetilo sve naredne blokove. Postupak „iskopavanja“ podseća na takmičarsku lutriju, koja ne dozvoljava dodavanje novih blokova u blockchain bez poštovanja navedene procedure. Na ovaj način ne može doći do mogućnosti da grupa ili pojedinac ostvare kontrolu nad sadržajem bloka i lanca, niti da izvrše zamenu delova blockchain-a kako bi nedozvoljeno povratili svoja sredstava već namenjena realizovanju transakcije.

U svoj svojoj složenosti, blockchain kao decentralizovani oblik registrovanja podataka ima gotovo neograničeni potencijal. Tehnologija blockchain-a uz reduciranje troškova obezbeđuje veću privatnost korisnicima i viši stepen bezbednosti, uz manju mogućnost greške u svojoj mreži. Prednosti blockchain-a svakako su: pojačana preciznost, izostavljanje faktora ljudskog uticaja u procesu verifikacija, smanjivanje troškova zbog eliminisanja treće strane kao verifikatora, decentralizovan sistem koji limitira mogućnost neovlašćenog pristupa i izmene podataka, bezbedno i efikasno obavljanje transakcija uz očuvanje privatnosti učesnika, te transparentna tehnologija. Nedostaci blockchain-a mogli bi biti: značajni tehnološki troškovi u vezi sa postupkom „iskopavanja“ bitcoin-a, usporenost transakcija po sekundi, mogućnost ostvarivanja uvida u hronologiju nelegalnih aktivnosti i osetljivost na hakerske napade. Obzirom da je svaka transakcija registrovana u digitalnom javno dostupnom registratoru, lako se mogu uočiti tragovi koji su zabeleženi u istoriji transakcije i vode do bitcoin adrese korisnika (Vladimir, 2019). Ovo naravno može biti iskorišćeno kao međuprostor u kome privatna korporacija ili određeni državni organ mogu diskretno pratiti aktivnosti učesnika transakcije anulirajući njihovu privatnost (Greenberg, 2014).

4. WEB WALLET

Kripto novčanik je namenjen čuvanju virtuelnog novca i prevashodno služi da zaštiti privatnost korisnika. Dark wallet je kripto novčanik koji je vrsta web wallet-a posebno kreirana da omogući anonimnost svog korisnika (Vladimir, 2019). Njemu mogu pristupiti sve kategorije korisnika jer je dobro dizajniran i dostupan. Ipak, zbog imperativa da garantuje anonimnost korisnika rašireno je verovanje da dark wallet najviše upotrebljavaju prekršioci zakona. Postoje mišljenja da je upravo dark wallet-om omogućeno da se u sajber prostoru vrše brojne kriminalne aktivnosti zbog čega je kritikovan u oblasti kriptozaštite (Vladimir, 2019). Bez obzira na različite stavove o ulozi dark wallet-a, činjenica je da se njime nedvosmisleno doprinosi vršenju nevidljivih isplata, te da bez njega mešanje radi „pranja“ virtuelnih kovanica u CoinJoin servisu ne bi bilo moguće. Neki autori navode da je kripto novčanik softver namenjen „pranju“ novca (Greenberg, 2014). Ima tvrdnji da „perači“ novca mešalicama digitalnih moneta neprestano

eksploatišu nove adrese wallet-a, koje se generišu automatski, što pogoduje organizatorima sive ekonomije i kriminalnih tržišta da koordiniraju transakcijama u tamnom vebu radi „čišćenja“ kripto valuta (Kaminska, 2019). Prisutna je i opasnost da se kripto novac poslat radi „čišćenja“ u nečiji virtuelni novčanik, nikada ne vrati pošiljaocu (Kudlovich, 2018).

Kripto novčanik je digitalni alat za zaštitu privatnosti, koji pojačava anonimnost tako što transakcije bitcoin-a čini nevidljivim. Struktura njegovog dizajna podrazumeva tri obavezna podsegmenta tzv. džepova, koje korisnik može za svoje potrebe kreirati u većem broju. Ovi podsegmenti odnose se na potrošnju, poslovanje i uštedu. Svaki od njih ima svoj poseban „nevidljivi“ mod u kome korisnik može da obavlja privatne transakcije virtuelnim novcem. Međutim i pored navedenih karakteristika dark wallet-a, postoje kritike na račun ne obaziranja njegovih provajdera na potrebe privatnosti, koja bi u dovoljnom stepenu obezbedila samostalno finansijsko delovanje korisnika (Reutzel, 2016).

Dark wallet od ostalih kripto novčanika razlikuju sledeće performanse, koje ga odlikuju. Reč je najpre o modu za skrivanje adrese. On maskira svaku transakciju bitcoin-a, koja se vrši iz kripto novčanika, što ometa napore praćenja tragova transakcije koji vode do njenog inicijatora. Svaka transakcija je enkriptovana, pa nijedan od učesnika u transakciji ne može znati adrese drugih učesnika. Postoji i opcija mešanja digitalnih kovanica iz najmanje dve transakcije zbog čega se otežava otkrivanje njihovih korisnika, koji te transakcije realizuju. Kad god neki od korisnika pošalje iznos virtuelnih kovanica na određenu adresu, kripto novčanik izabere drugu transakciju koja se vrši istovremeno i meša virtuelni novac iz obe transakcije radi izbegavanja identifikacije korisnika. Neki autori smatraju da je dark wallet, kao TOR-ov kripto novčanik, zastareo, nefunkcionalan i prevaziđen (Khatwani, 2019). Postoje i druge vrste wallet-a za koje se tvrdi da su najefektivniji u 2019. godini (Khatwani, 2019). Reč je o sledećim vrstama kripto novčanika sa ključnim odlikama navedenim u zagradi: Ledger Nano X (anonimni hardver wallet), Ledger Nano S (anonimni hardver i veb wallet), Samourai Wallet (anonimni mnobilni wallet), PINT Wallet (anonimni mnobilni wallet), Bitcoinpaperwallet.com (anonimni papirni wallet), BitLox (anonimni hardver wallet) i Electrum (desktop i mobilni wallet).

Dark wallet se konstantno unapređuje. Njegova usluga je stalno dostupna za preuzimanje sa zvaničnog veb sajta. Korisnici su obavezni da otvore fajl iz zip moda i sačuvaju ga na radnoj površini svoje računarske jedinice. Posle preuzimanja i otvaranja fajla, korisnik koristi Chrome pretraživač i iz menija usluga se opredeljuje za ekstenzije. Posle pokretanja razvojnog moda iz postavki i njegovog unošenja u otvoreni fajl, korisnik unosi svoje korisničko ime i lozinku u wallet. Od pošiljaoca se zahteva da za dekodiranje upotrebi jednokratnu šifru kako bi otvorio adresu primaoca, što je podatak koji je poznat samo primaocu. Prema nekim shvatanjima, kripto novčanik je softverska kombinacija javnog i tajnog ključa, te ukoliko je registrovana na papiru opredeljuje wallet kao papirni, a ako se nalazi na mobilnom uređaju određuje wallet kao mobilni (Khatwani, 2019).

Oprečna su mišljenja o prirodi dark wallet-a, od onih koja ističu prednost njegovih informatičkih karakteristika koje doprinose očuvanju anonimnosti i privatnosti korisnika, do drugih koja kritikuju njegov potencijal za skrivanje kriminalnih aktivnosti i ometanje kapaciteta organa za primenu zakona. Ove zabrinutosti su realne, ali ipak ne može se poreći zaštitna uloga kripto novčanika koju ostvaruje jačanjem stepena privatnosti učesnika transakcija i pravljenjem brane prema sajber kradljivcima digitalnih privatnih dobara.

5. ZAKLJUČCI

Paradoks kripto valute je njena dihotomna priroda, zbog čega je bitcoin istovremeno i javan i anoniman (Kudlovich, 2018). Sve transakcije u mrežama tamnog veba ostavljaju svoje tragove, iako javni kjučevi ne ukazuju na podatke svojih vlasnika. Kritičan trenutak kada kripto valuta gubi plašt anonimnosti jeste kada korisnik vrši plaćanje ili razmenu odnosno kada bitcoin napušta okrilje dark wallet-a radi plasiranja u tokove transakcije.

Ipak, postoje razni načini zaštite privatnosti korisnika u blockchain modusu. Jedan od njih je mešalica kripto valute, koja održava anonimnost korisnika virtuelnog novca. Algoritam je jednostavan i podrazumeva da korisnik uputi svoj

virtuelni novac na adresu mešalice koja se se za svakog korisnika vodi posebno. Potom se jedinice kripto valute mešaju sa jedinicama iz transakcija drugih korisnika ili se distribuiraju na pozicije stotine hiljada drugih web wallet-a koji su povezani sa određenom mešalicom. Kada se ovaj postupak okonča, „čisti" bitcoin-i se prenose u web wallet koji pripada njihovom prethodnom ili novom vlasniku. Alternativan način ovom postupku predstavljaju posebni web wallet-i, koji obezbeđuju visok stepen privatnosti, kao što je Electrum. Zatim, postoje i wallet-i sa ugrađenim opcijama za mešanje virtuelnog novca (Kudlovich, 2018). Jedan od web wallet-a, dark wallet, ima svoju integrisanu performansu pod nazivom CoinJoin, koja omogućuje da se sve jedinice kriptovalute u transaciji mešaju, te nije moguće otkriti inicijalnog vlasnika plasiranog virtuelnog novca. Više korisnika wallet-a podiže stepen anonimnosti transacija u Dark Web-u (Kudlovich, 2018).

Kao uspešan primer primene anonimnih kripto valuta za potrebe transakcija u tamnom vebu, navešćemo Z-Pay, kao platni sistem velikog potencijala sa aktivnim razvojem mehanizma za zaštitu privatnosti. Ključna karakteristika ovog sistema je izdavanje i transfer anonimnih računa odnosno čekova, kojima se vrši plaćanje roba i usluga (Kudlovich, 2018).

I pored svih prednosti i mana načina i informatičkih usluga i alata za obezbeđivanje anonimnosti i privatnosti u delovanju korisnika komunikacionih mreža u nevidljivim slojevima dubokog veba, a posebno u njegovom tamnom delu, dark web-u, činjenica je da pokretački impuls za gotovo sva „crna" tržišta Darkneta predstavljaju prevashodno kriminalna poslovanja bazirana na nevidljivim transakcijama kripto valuta (Report-CAML-20190812, 2019), koje se vrše i radi „pranja" virtuelnog novca koji potiče iz ilegalnih aktivnosti.

CITIRANI RADOVI

Bajpai, P. (2019). The 10 Most Important Cryptocurrencies Other Than Bitcoin. *Cryptocurrency*. Dostupno na: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/, preuzeto 12.08.2019.

Canellis, D. (2018). Here's how criminals use Bitcoin to launder dirty money. *Hard Fork*. Dostupno na: https://thenextweb.com/hardfork/2018/11/26/bitcoin-money-laundering-2/, preuzeto 04.08.2019.

Cryptocurrency Anti-Money Laundering Report, 2019 Q2. (2019). Report-CAML-20190812, *Cipher Trace Cryptocurrency Intelligence*, July 2019, p. 6.

Greenberg, A. (2014). 'Dark Wallet' is about to make Bitcoin money laundering easier than ever. *Wired*. Dostupno na: https://www.wired.com/2014/04/dark-wallet/, preuzeto 05.08.2019.

Kaminska, I. (2019). Why money laundering risk is very real with crypto cards. *Financial Times*. Dostupno na: https://ftalphaville.ft.com/2019/05/31/1559275247000/Why-money-laundering-risk-is-very-real-with-crypto-cards/, preuzeto 01.08.2019.

Khatwani, S. (2018). Private Key vs Public Key: Understanding The Two & Their Importance In Crypto. *The Money Mongers*. Dostupno na: https://themoneymongers.com/private-key-vs-public-key/, preuzeto 17.08.2019.

Khatwani, S. (2019). Anonymous Bitcoin Wallets To Use In 2019. *The Money Mongers*. Dostupno na: https://themoneymongers.com/anonymous-bitcoin-wallets/, preuzeto 05.08.2019.

Khatwani, S. (2019). Bitcoin Private Key: Noob To Expert Guide. *The Money Mongers*. Dostupno na: https://themoneymongers.com/bitcoin-private-key/, preuzeto 15.08.2019.

Kudlovich, Y. (2018). How Cryptocurrency Mixers and Anonymous Wallets Work. *De Center*. Dostupno na: https://decenter.org/en/how-cryptocurrency-mixers-and-anonymous-wallets-work, preuzeto: 06.08.2018.

Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. *Coindesk*. Dostupno na: https://www.coindesk.com/bitcoin-peer-to-peer-electronic-cash-system, preuzeto 14.08.2019.

Reutzel, B. (2016). Report: Bitcoin Wallet Providers Failing to Make Privacy a Priority. *Coindesk*. Dostupno na: https://www.coindesk.com/bitcoin-wallet-providers-failing-privacy-obpp, preuzeto 11.08.2019.

Vladimir C. (2019). The Ultimate Dark Wallet Review. *Blockchain Analyzes & Reviews*. Dostupno na: https://coindoo.com/the-ultimate-dark-wallet-review/, preuzeto 23.08.2019.

Datum prve prijave: 11.09.2019.
Datum prijema korigovanog članka: 08.10.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

Style – APA Sixth Edition:

Uljanov, S., & Milošević, Đ. (2019, 10 15). Nevidljive transakcije u dark web-u. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 124-134. doi:10.12709/fbim.07.07.02.14

Style – Chicago Sixteenth Edition:

Uljanov, Sergej, and Đorđe Milošević. 2019. "Nevidljive transakcije u dark web-u." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 124-134. doi:10.12709/fbim.07.07.02.14.

Style – GOST Name Sort:

Uljanov Sergej and Milošević Đorđe Nevidljive transakcije u dark web-u [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 124-134.

Style – Harvard Anglia:

Uljanov, S. & Milošević, Đ., 2019. Nevidljive transakcije u dark web-u. *FBIM Transactions,* 15 10, 7(2), pp. 124-134.

Style – ISO 690 Numerical Reference:

Nevidljive transakcije u dark web-u. **Uljanov, Sergej and Milošević, Đorđe.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 124-134.

FBIM Transactions
DOI 10.12709/fbim.07.07.02.15

PREVARE PUTEM INTERNETA: SAJBER ZABAVA KOJA „PRAZNI" RAČUNE ŠIROM SVETA

INTERNET FRAUD: CYBER ENTERTAINMENT THAT "CLEANS" BANK ACCOUNTS WORLDWIDE

Vida M. Vilić
Klinika za stomatologiju Niš, Niš, Srbija

JEL Kategorija rada: **L86**

Apstrakt

Postoje različiti oblici prevara putem Interneta, a kako najveći broj izvršilaca ovog dela pripada mlađoj populaciji, stiče se utisak da je ova vrsta kriminalne aktivnosti postala sve češća zabava mlađih ljudi koji su vešti u poznavanju informaciono-komunikacionih tehnologija. Pojavni oblici prevara su mnogobrojni i zbog različitih načina njihovog izvršenja nemoguće ih je u potpunosti sagledati. U praksi se javljaju kako primitivne i grube prevare tako i one prevare kod kojih učinioci ispoljavaju visok stepen veštine. Kao česti oblici Internet prevara javljaju se „Valentino" prevare, „lančana pisma", piramidalne šeme, „lutajući" trgovci, transfer novca u dobrotvorne svrhe i lutrijske prevare, dok je svakako jedan od najčešće viđenih oblika sa kojim se svako od nas susreo u svom poštanskom sandučetu tzv. "Nigerijska prevara". Prevare putem Interneta u Republici Srbiji još uvek nisu pravno regulisane. U toku 2008. i 2009. godine na teritoriji Republike Srbije prijavljeno je devet krivičnih dela prevare sa elementima „nigerijskih" prevara protiv nepoznatih učinilaca, dok je na svetskom nivou procena da su Internet prevare dostigle svoj vrhunac 2009. godine. Pored definisanja i klasifikacije najčešćih pojavnih oblika prevara putem Interneta, u radu su dati i neki praktični saveti kako sprečiti viktimizaciju od prevarnog ponašanja na Internetu.

Ključne reči: *Prevare putem Interneta, računarske prevare, nigerijska prevara, krivično delo prevare*

Abstract

There are various forms of Internet frauds, and since most of the perpetrators belong to the younger population, it seems that this type of criminal activity has become even more and more fun for younger people with great knowledge and practical skills in the field of information and communication technologies. There are many forms of this act, because of the many different modus operandi, so it is almost impossible to

Adresa autora:
Vida M. Vilić
e-mail: vila979@gmail.com

fully understand and to explain them, or even harder to prevent them. Common forms of Internet scams include so-called "Valentine" scams, "chain letters", pyramidal schemes, "wandering" merchants, charity transfers and lottery scams, while certainly one of the most commonly seen form we've encountered are so-called "Nigerian scams". In the Republic of Serbia, Internet fraud is not yet legally regulated as criminal acts. During 2008 and 2009, nine criminal offenses with elements of "Nigerian scam" were reported in the territory of the Republic of Serbia against unknown perpetrators, while at the global level, it is estimated that this particular kind of Internet fraud reached its top in 2009. In addition to defining and classifying the most common forms of Internet frauds, this paper also provides some practical tips on how to prevent victimization from fraudulent behavior on the Internet.

***Keywords**: Internet scams, computer fraud, Nigerian scam, fraud*

1 UVOD

Dosadašnja proučavanja i postojeća zakonska regulativa na međunarodnom i nacionalnom planu odnose se uglavnom na zloupotrebu računarskog hardvera i softvera, koji prilikom izvršenja krivičnih dela mogu da budu sredstvo izvršenja ili objekat napada (npr. kompjuterske krađe, prevare, oštećenje računarskih podataka i programa, sabotaža, pravljenje i unošenje računarskih virusa). Jedan od oblika devijantnog ponašanja koje još uvek nije regulisano krivičnim zakonodavstvom Republike Srbije jesu prevare putem Interneta. Transnacionalno posmatrano, ovaj fenomen je sve više prisutan u sajber prostoru, njegove žrtve su sve brojnije a pretrpljene materijalne štete sežu i do nezamisliih razmera. Postoje različiti oblici prevara putem Interneta, a kako najveći broj izvršilaca ovog dela pripada mlađoj populaciji, stiče se utisak da je ova vrsta kriminalne aktivnosti postala sve češća zabava mlađih ljudi koji su vešti u poznavanju informaciono-komunikacionih tehnologija.

2 ŠTA SU PREVARE PUTEM INTERNETA

Prevara, kao krivično delo, stara je koliko I ljudski rod, i za sve vreme nisu se promenili ni pojam prevare ni efekat koji prevara ima na žrtvu (Koong, Liu & Wei, 2012: 442). Prevare putem Interneta predstavljaju najrašireniji oblik sajber kriminaliteta, o kome se prvi put govori još 1996. godine ali sa veoma malo konkretnih detalja o pojavnim oblicima. Ova dela treba razlikovati od računarskih prevara kada se u računar unose netačni podaci ili se propušta unošenje tačnih podataka ili se na bilo koji drugi način računar koristi za ostvarivanje prevare putem prikrivanja ili lažnog prikaza podataka, a sve u cilju sticanja protivpravne materijalne koristi kojom se drugome prouzrokuje imovinska šteta (Vilić, 2016, str. 203).

Krivični zakonik Republike Srbije (2005) sadrži propise materijalnopravnog karaktera, koji se odnose na kompjuterski kriminalitet, predviđajući krivična dela protiv bezbednosti računarskih podataka, ali i druga krivična dela koja se na osnovu Konvencije o visokotehnološkom kriminalu (čl. 8) i pozitivnopravnih zakonskih propisa smatraju krivičnim delima kompjuterskog kriminaliteta (Vilić, 2017, str 118). U okviru krivičnih dela kompjuterskog kriminaliteta koja se odnose na bezbednost računarskih podataka (Glava XXVII), predviđeno je krivično delo "računarska prevara" (čl. 301).

Radnje izvršenja ovog krivičnog dela sastoje se svakom umišljajno učinjenom delu unošenja, menjanja, brisanja ili prikrivanja kompjuterskih podataka ili ometanju funkcionisanja kompjuterskih sistema kojim se drugim licima nanosi veća imovinska šteta, a u nameri pribavljanja veće imovinske koristi sebi ili drugom licu. Za pravilnu kvalifikaciju krivičnog dela i dokazivanje računarske prevare potrebno je, pored ostalog, tačno utvrditi radnju koja je preduzeta, način unošenja neistinitog podatka, u čemu se neistinitost ogleda i kakav je bio uticaj na rezultat elektronske obrade i prenosa podataka.[1]

[1] U domaćoj sudskoj praksi zabeleženo je nekoliko slučajeva procesuiranja krivičnog dela računarske prevare. Tužilaštvo za borbu protiv visokotehnološkog kriminala pokrenulo je istragu protiv osumnjičenog Č. A. zbog osnovane sumnje da je tokom 2007. i 2008. godine u dva navrata koristeći računar ulazio u sisteme banaka u Australiji i Švajcarskoj i izdavao lažne naloge za transfer sredstava, čime je pribavio protivpravnu

Krivično delo računarske prevare treba razlikovati od klasičnog krivčnog dela prevare (čl. 208 KZ RS) koje pripada imovinskom kriminalitetu, odnosno grupi krivičnih dela protiv imovine. Iako u zakonu nije izričito naglašeno, krivično delo prevare može se izvršiti i korišćenjem računarskih tehnologija. Pojava Interneta otvorila je široke mogućnosti za vršenje krivičnog dela prevare, povećala broj potencijalnih žrtava i skoro sasvim otklonila troškove potrebne za izvršenje krivičnog dela. Načini izvršenja prevara korišćenjem kompjutera i Interneta su različiti, izvršioci su potpuno anonimni, a žrtva može da postane svako ko koristi računarsku tehnologiju.

Prevara putem Interneta nije uvek i obavezno računarska prevara, jer neke Internet prevare odgovaraju klasičnim prevarama koje za sredstvo izvršenja imaju Internet bez nekog posebnog uticaja na elektronsku obradu podataka ili rad računara. Prevarom putem Interneta obmanjuju se ljudi, dok se računarskom prevarom „obmanjuje“ računar i elektronska obrada navodi na pogrešan rezultat koji je usmeren na sticanje protivpravne imovinske koristi (Babović, 2004, str. 749-750).

Prevara putem Interneta ili Internet prevara odnosi se na bilo koju prevaru pri čijem izvršenju lice koje u nameri pribavljanja protivpravne imovinske koristi za sebe i drugoga, iskoristi jednu ili više komponenti Interneta, kao što su sobe za ćaskanje, veb stranice ili elektronska pošta, 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 (sprovođenje finansijske transakcije, prenošenje podatka finansijskoj instituciji koja je meta napada i sl.) (Matijašević, Spalević & Ignjatijević, 2012, str. 563).

3 NAJČEŠĆI POJAVNI OBLICI INTERNET PREVARA

Raznolikost i obim različitih vrsta mrežnih prevara teško je odrediti iz više razloga. Pojavni oblici prevara su mnogobrojni, zbog različitih načina njihovog izvršenja nemoguće ih je u potpunosti sve sagledati jer se u praksi javljaju kako primitivne i grube prevare tako i one prevare kod kojih učinioci ispoljavaju visok stepen veštine. Takođe, prevare putem Interneta se retko prijavljuju, a mnoge prevare putem Interneta koriste kombiacije različitih vrsta krivičnih dela (Button, McNaughton Nicholl, Kerr.& Owen, 2014, str. 396).

Kao čest oblik Internet prevara javljaju se: „valentino“ prevare, „lančana pisma“, piramidalne šeme, „lutajući“ trgovci, transfer novca u dobrotvorne svrhe i lutrijske prevare.

- „Valentino“ prevare su povezane sa „uslugama“ koje se pružaju usamljenim osobama koje žele da sklope brak ili da stupe u kontakt sa nekom osobom radi druženja. Posle određene pripreme, koja obuhvata komuniciranje mejlovima i razmenu fotografija, prevarant predlaže lični kontakt sa žrtvom pod uslovom da mu uplati određenu sumu novca kako bi doputovao do mesta susreta. Posle transfera novca, svaki kontakt sa žrtvom prestaje.
- „Lančana pisma“ sadrže zahtev upućen mejlom da se dobijeni mejl prosledi određenom broju prijatelja i ukoliko se to ne učini, osobu će zadesiti neka nesreća. Ovakva pisma sadrže kriptovane informacije, koje će licu koje je poslalo lančano pismo omogućiti da sazna lične podatke velikog broja lica i da ih zloupotrebi.
- Piramidalne šeme predstavljaju takvu vrstu prevara kod kojih se žrtvi obećava isplata određene svote novca za „privlačenje“ određenog broja ljudi i uključivanje u rad „piramide“.
- „Lutajući trgovci“ se bave prodajom nepostojeće robe, robe lažnog kvaliteta, koja može biti opasna po zdravlje, traže mejlovima isplatu novca, ali nikad ne izvrše isporuku.
- Kod prevare transferom novca u dobrotvorne svrhe od žrtve se traži da za određenu proviziju primi na svoj bankovni račun

imovinsku korist u iznosu od 51.990 CHF, odnosno da je pokušao da iz jedne švajcarske banke neovlašćeno izvrši transfer sredstava u iznosu od 19.000 USD. Takođe je zabeleženo više slučajeva zloupotrebe računarskih sistema računarskih mreža u sportskim kladionicama. Izvršioci na različite načine pokušavaju da utiču na rezultat elektronske obrade podataka i koristeći softverska rešenja falsifikuju odigrane tikete. Više o tome: Nikolić, K. i dr., 2010, str.102-103 i Prlja, D., Ivanović, Z. & Reljanović, M., 2011, str. 173.

određenu sumu novca, podigne ga sa računa i uplati na neki račun u inostranstvu, sa obrazloženjem da će novac biti iskorišćen u dobrotvorne svrhe. Provizija za ovakvu transakciju se ne dobija, a ovakvim transferom se prikriva poreklo novca („pranje novca“).

- Lutrijske prevare se sastoje u tome što žrtvi stiže obaveštenje da je dobitnik neke premije i da pošalje određenu svotu novca u cilju dobijanja te nagrade ili se traži da žrtva navede broj svog bankovnog računa i određene lične podatke, što će svakako biti zloupotrebljeno.

Prema istraživanju Američkog udruženja za zaštitu potrošača za otkrivanje najčešćih Internet prevara (National consumers league – NCL), koje je sprovedeno 2006. godine (The top 10 Internet Frauds, 2017, *n.d.*), najčešće Internet prevare su navedene u tabeli 1.

Tabela 1. Vrste i frekvencija pojave Internet prevara

Mesto / zastupljenost u ukupnom broju	Internet prevare		
	Naziv prevare	**% žalbi u odnosu na ukupan broj**	**Prosečan gubitak u USD**
1.	Internet aukcije	34%	1.331
2.	Prodaja preko Interneta	33%	1.197
3.	Plaćanje lažnim čekovima	11%	4.053
4.	„Nigerijske prevare“	7%	3.741
5.	Lažne lutrije	4%	1.750
6.	Lažni zajmovi	3%	1.515
7.	Fišing	2%	/
8.	Nagradne igre	1%	2.447
9.	Prevare provajdera	1%	920
10.	Investicije	1%	4.759

Isto udruženje je i narednih godina analiziralo vrste najčešćih Internet prevara, a 2019.godine je u okviru projekta „Fraud.org“ objavilo podatke koje su bile najzabeleženije vrste Internet prevara tokom 2018. godine (Top ten scams of 2018, 2019, *n.d.*), Tabela 2.

Tabela 2. Najčešćih 10 Internet prevara tokom 2018. godine

Mesto / zastupljenost u ukupnom broju	Internet prevare	
	Naziv prevare	**% žalbi u odnosu na ukupan broj**
1.	Prodaja preko Interneta	31,25%
2.	Nagradne igre i besplatne stvari	16,97%
3.	Plaćanje lažnim čekovima	13,09%
4.	Lažni zajmovi koji se daju pravnim licima	7,63%
5.	Lažni zajmovi i krediti	7,37%
6.	Fišing/Spufing	4,84%
7.	Prevare iskorišćavanjem virtuelnih prijateljstava	2,81%
8.	Oprema za kompjutere i kompjuterski softver	2,23%
9.	Stipendije i donacije	1,63%
10.	Iznuđivanje i ucenjivanje porodice ili prijatelja	1,41%

Prevare prilikom različitih Internet prodaja postale su tokom 2018. godine najčešće vršene Internet prevare, čija se radnja izvršenja dela sastoji u tome da žrtva naruči i plati robu koja mu/joj nikada ne bude isporučena. Primećen je porast prevara koje su zasnovane na zloupotrebi ličnih odnosa žrtve i učinioca (rođački odnosi, prijateljski ili intimno partnerski odnosi), pri čemu se radnja izvršenja sastoji u zadobijanju nečijeg poverenja, razvijanju veze između žrtve i učinioca i ubeđivanju žrtve da učiniocu pošalje novac. Ipak, najveći porast je primećen u broju slučajeva fišinga. Krađa identiteta putem elektronske pošte (fišing, eng. phishing) sastoji se u slanju e-mail poruke korisniku u kojoj se navodi da poruku šalje legitimno pravno lice ili ovlašćena osoba tražeći lične podatke i privatne informacije (Vilić, 2019, str. 46). Navodi u poruci su lažni, a ukoliko primalac napiše podatke koji se traže, oni će kasnije biti iskorišćeni za krađu identiteta.

U najčešće vršene Internet prevare spadaju i prevare putem Internet promocija, kreditnih kartica, piramidalne novčane prevare putem multi level marketinga, poslovne ponude i pogotovo rad od kuće, investicione prevarne šeme poput „kako se lako obogatiti”, prevare sa putovanjima kao i prevare korišćenjem tuđih brojeva zdravstvenog osiguranja (Computer Crime Research Center: Fraud in the Internet, 2005). Među često vršene

prevare spadaju prevare prilikom Internet kupovine automobila i aukcijske i maloprodajne novčane prevare preko Interneta.

Prilikom kupovine automobila preko Interneta, prevarant oglašava da se po veoma pristupačnoj ili čak niskoj ceni prodaje nepostojeće vozilo, najčešće luksuzan ili skup sportski auto, čija regularna cena može da bude i nekoliko puta veća od tražene. Detalji o vozilu su najčešće preuzeti sa drugih sajtova koji se bave prodajom automobila preko Interneta i deluju vrlo primamljivo, pa zainteresovani kupci nadajući se povoljnoj kupovini kontaktiraju prevaranta, koji daje instrukcije žrtvi prevare da pošalje depozit ili celu uplatu preko elektronskog transfera kako bi pokrenuo proces „špedicije“, pošto se traženi automobil obično nalazi u inostranstvu. Prevarant može takođe da nabavi podatke o vozilu koje navodno pokušava da proda preko Interneta tako što će kontaktirati nekoga ko zaista pokušava da proda vozilo preko Interneta, pitajući ga za broj šasije vozila kako bi proverio zapise o nesrećama sa tim vozilom. Prevarant će zapravo taj broj iskoristiti da upotpuni sliku o vozilu koje navodno on prodaje.

Kod aukcijske i maloprodajne novčane prevare preko Interneta prevarant započinje prodaju po veoma povoljnoj ceni preko Interneta na sajtovima koji su za to specijalizovani. Najčešće su u pitanju skuplje i vrednije stvari ili ponekad i kolekcionarski primerci. Prevarant prihvata uplatu od pobednika virtuelne aukcije ili kupca u Internet prodavnici, ali mu uopšte ne isporučuje stvar za koju je dobio novac ili mu isporučuje predmet čija je realna vrednost znatno manja od one za koju je žrtva dala novac (npr. falsifikat ili korišćen predmet umesto novog).

Za izvršenje navedenih dela, prevaranti najčešće koriste fišing tehnike kako bi „oteli“ podatke sa naloga legitimnih korisnika ili naloge sa veoma pozitivnom reputacijum na Internetu i koriste ih da postave lažne virtuelne prodavnice. Prevarant ovakvim postupkom istovremeno sakuplja novac za sebe, a dok žrtva prevare shvati da nije dobila ono za šta je dala novac, za krivično delo prevare će biti optužen pravi nosilac naloga čiji je identitet prevarant preuzeo.

4 „NIGERIJSKA PREVARA” ILI „PREVARA 419”

Jedna od najpoznatijih svetskih, tzv. investicionih Internet prevara (engl. Advance-fee fraud) je „Nigerijska prevara” ili „Prevara 419”. Radnja ovog dela sastoji se u pribavljanju imovine putem prevarnih radnji, a koja može da podrazumeva ulaganje određene svote novca u određeni „posao“, uz obećanje da će se kao benefit ostvariti znatno veća suma novca od uložene (Matijašević, Spalević & Ignjatijević, 2012, str. 563).

Nekoliko nezaposlenih studenata sa nigerijskog univerziteta počelo je ranih osamdesetih godina XX veka da prevarom uzima novac od poslovnih ljudi sa zapada. Izraz „prevara 419” dobila je naziv po članu broj 419 Nigerijskog krivičnog zakona koji definiše i sankcioniše krivično delo prevare. Iako je po samom nazivu dela vezana za Nigeriju, ova vrsta prevare vezuje se i za sledeće zemlje iz kojih potiču izvršioci ovog dela: Togo, Burkina Faso, Gana, Benin, Obala Slonovače, ali i Južna Afrika, Španija, Holandija i Velika Britanija

Kriminalna aktivnost izvršilaca sastoji se u slanju elektronske poruke koja je tako osmišljena da izgleda kao da je namerno poslata primaocu poruke, a počinje ubeđivanjem potencijalne žrtve prevare da učestvuje u podeli novčanih fondova ako unapred uplati određeni iznos koji je, u najvećem broju slučajeva, neuporedivo manji od onog iznosa koji bi trebalo da dobije kao korist od tog fonda. Elektronskom porukom se od potencijalne žrtve traži pomoć za transfer velikih novčanih iznosa, a ona će zauzvrat dobiti određeni procenat kao nagradu. U porukama se takođe navodi da je reč o izuzetno velikoj sumi novca, da je pošiljalac poruke član nigerijske vlade ili vojske, da je spreman da podeli novac sa osobom koja mu pomogne da se transfer izvrši i da je neophodno da ceo postupak ostane u najstrožijoj tajnosti. Ukoliko žrtva pristane da učestvuje u sprovođenju ove transakcije, dostavljaju joj se falsifikovani dokumenti, na osnovu kojih će žrtva uplatiti određeni novčani iznos prema instrukcijama koje je dobila. Nakon toga, počinje odlaganje novčanih transakcija, povećanje troškova transakcija, vrši se pritisak na žrtvu, koja posle dužeg vremena shvata da je prevarena.

Pisma sa elementima "Nigerijske prevare" su se 2016. godine u Srbiji pojavila i na lošem srpskom jeziku, pa čak i na ćiriličnom pismu, jer izvršioci ovog dela, korišćenjem usluge *Google translate,* pokušavaju da dođu do što šireg kruga ljudi koje bi prevarili, a koji ne poseduju dovoljno znanja engleskog jezika kako bi sledili postupak koji je u originalnom prevarnom pismu naveden. Kako ovaj alat za prevođenje tekstova nije baš najpouzdaniji i najprecizniji u prevodu na srpski jezik, moguće je lako uočiti da poruka nije verodostojna i da ima potencijalni prevarni karakter.

Model pisma „Nigerijske prevare“ (Model 1):

“INVESTMENT ASSISTANCE

Sir,

With due respect, trust and humility I write you this proposal which I believe would be of great interest to you. I am MRS TINA GOGO the wife of late DR. DONALD GOGO of blessed memory. Before my husband was killed by rebel forces loyal to Major JOHN PAUL KOROMAH. He was the Director General Gold and Diamond Mining Corporation (G.D.M.C.) of Sierra Leone.

Two days before his death, he managed to sneak a written message to me, explaining his condition and concerning trunk box of valuables containing money and diamonds, which he concealed under the roof. He instructed me to take our children and move out of Sierra Leone immediately to any neighbouring country. Eventually it resulted into full war, I became a widow overnight, helpless in this hopeless situation.

Daughter and I my son managed to escape to Abidjan, Ivory Coast through the help of my husband’s friend. The cash inside the box was USD $ 25.5 MILLION (TWENTY FIVE MILLION FIVE HUNDRED THOUSAND US DOLLARS), and DIAMOND, due to fear and limit right as a refugee I deposited the items with private security company with my son’s name MR. JOGO GOGO (JR). Be informed that the real content of the boxes were not disclosed to the security company as these were deposited as personal effects for security reasons. Meanwhile I want to travel out of Ivory Coast entirely with this money for investment in your country because of the unsuitable political situation and mostly for the future benefit of my children. I want you to assist us get the money out of the Security Company and transferred into your nominated private account in your country. You shall also source for good investment, so that we can invest the money wisely.

*Concerning the money, we are prepared to give you 20% of the total sum and 5% mapped out for expenses. For the interest of this business do not hesitate to call my son MR JOGO GOGO (JR) on telephone number ********** or email address: ********** immediately you receive this message for more information to enable us proceed in earnest towards concluding all arrangements, no other person knows about this money expect I, my son and you.*

Awaiting your most urgent response.
Thanks for your co-operation and GOD bless you.”

Model pisma „Nigerijske prevare“ (Model 2):

“Poštovani,

Treba mi hitna pomoć,

Dobar dan. Znam da vam ova pošta može doći kao iznenađenje. Molim vas, nemojte se ljuti na mene što ste primili moju poštu. Uzmite me kao svoju kćerku ili kao sestru. Videla vašu adresu e-pošte putem online poslovnog imenika tokom moje pretrage. Poštena sam osoba i kontaktirala sam te lično, jer sam ozbiljno trebala vašu pomoć.

Moje ime je Mari Frank. Ja imam 20 godina i jedina sam dete mojih pokojnih roditelja Mr. and Mrs Frank. Moj otac je dugi niz godina radio sa preduzećem za naftu i gas i deponovao je ukupno dva miliona evra u moje ime pre nego što je umro 2014. godine. Tokom ovog depozita, moj otac je imao saglasnost sa bankom da mi novac neće biti direktno dat sve do 25 godina ili više. Molim vas, hoćete da mi pomognete da prebacim ovaj novac na vaš bankovni račun za investicije i da vam pomognem da dođem u vašu zemlju da nastavim sa školovanjem, jer moj ujak želi da me ubije i sakupi moj novac za nasleđe, jer sam ja mala devojčica.

Prijavila sam ga u lokalnoj policiji moje zemlje, Obale Slonovače, ali policija nije učinila ništa da mi pomogne. Od tada i moj život je u velikom riziku ovde u mojoj zemlji. Pišem vam ovu poštu

iz lokalnog hotela u kome se trenutno krijem za moju sigurnost dok ne odem iz svoje zemlje nakon prenosa. Ja sam voljna da vam ponudim 20 odsto ukupnih sredstava kao nadoknadu za vašu pomoć nakon transfera i želim da mi hitno odgovorite ako prihvatite da mi pomognete da vam pošaljem više detalja.

Hvala i Bog blagoslovio,

Gospođica Mari Frank"

„Nigerijske prevare" dostigle su na globalnom nivou svoj vrhunac 2009. godine, kada su žrtve prevara, prema podacima holandske kompanije Ultrascan (Ultrascan Advanced Global Investigations, 2018, *n.d.*), izgubile gotovo 50% više novca nego 2008. godine. 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 2008. godine (*Ibid.*). Ukupno 51.761 prevara je počinjena iz 69 svetskih zemalja, dok je ostalih 250.000 prevara počinjeno iz Nigerije (*Ibid.)*.

U Srbiji je, prema podacima Tužilaštva za visokotehnološki kriminal, prvi slučaj jednog od oblika "Nigerijske prevare" prijavljen 2009. godine, kad je jedan građanin ostao bez 2.500 dolara (Brkić, 2017), dok je kasnije prijavljena i slična aktivnost, čija se radnja izvršenja dogodila 2008. godine. Ukupno, tokom 2008. i 2009. godine na teritoriji Republike Srbije izvršeno je i prijavljeno devet krivičnih dela prevare sa elementima „nigerijskih prevara" protiv nepoznatih učinilaca, pri čemu je ukupna imovinska šteta iznosila preko 60.000 evra (Urošević, 2009). Oštećena lica su novac izvršiocima krivičnih dela slala preko servisa Western Union i MoneyGram, uglavnom preko besplatnih naloga za elektronsku poštu koja je otvarana na Internet servisima koji omogućuju besplatne naloge elektronske pošte. Nakon što se prevara prijavi, neophodno je prikupiti sve elektronske dokaze koji ukazuju na ostvarenu komunikaciju između izvršilaca krivičnog dela i oštećenih, kao i podatke o finansijskim transakcijama koje je oštećeni izvršio prema instrukcijama koje je dobio od izvršilaca. Pokušava se da se pronađe IP adresa i locira server sa koga su izvršioci krivičnog dela slali elektronske poruke oštećenom, prikuplja se pregled celokupne elektronske pošte koju je oštećeni primio, a zatim se preko Interpola vrše provere korisnika kome je ova adresa bila dodeljena u trenutku vršenja krivičnog dela (*Ibid.)*. Korišćene su lažne Internet adrese, Internet portali, falsifikovana dokumentacija državnih organa i preduzeća Nigerije, Gane i drugih država sa teritorije Zapadne Afrike. Izvršioci su najčešće svu korespodenciju obavljali sa javnih mesta, kao što su Internet kafei, kako ne bi moglo da im se uđe u trag.

Interesantan slučaj "Nigerijske prevare" dogodio se mladiću (23) iz Beograda, koji je 2012. godine na jednom Internet sajtu objavio oglas da prodaje kuću. Na oglas se javio navodno državljanin Velike Britanije, koji je rekao da želi da se preseli u Srbiju, da želi da dođe da pogleda svoj budući stambeni prostor i od prodavca je zahtevao da mu pošalje svoju adresu, kopiju lične karte i adresu na kojoj se nalazi kuća, kako bi od službenika carine dobio neophodna dokumenta, vizu i putne isprave za preseljenje i ocarinjenje svog pokućstva koje bi doneo u Srbiju prilikom navodnog preseljenja. Kupac je prodavcu slao svoje fotografije i fotografije svoje porodice, kako bi sa njim uspostavio prisnu prijateljsku vezu, autentične dokumente nadležnih institucija, troškovnike i različite sertifikate. Jednog dana, ovaj navodni kupac je prodavca obavestio da je kupio avionske karte, ali, da bi ocarinio svoje stvari, prodavac treba da reguliše plaćanje slanja i preuzimanja ovih stvari, kao i angažovanja carinika. Prodavac je to učinio na način na koji je od njega kupac tražio, uplaćujući na račune koje mu je takođe kupac davao, čime je izgubio oko 640.000 dinara. Sam prodavac je naveo kako mu ništa nije delovalo sumnjivo i kako je celokupan ovaj postupak trajao skoro dve godine. Shvatio je da je prevaren tek kada je shvatio da mu mejlove ne šalju nadležne službe na koje se kupac pozivao, kada se konačno obratio policiji i Upravi za visokotehnološki kriminal. Prijava je prosleđena Višem sudu u Beogradu, koji je pokrenuo pretkrivični postupak, dok Interpol dalje procesuira slučaj (Čuvajte se – Nigerijska prevara u Srbiji, 2014, *n.d.*).

Drugačija vrsta "Nigerijske prevare" zabeležena je 2018. godine u Kosjeriću, kada su se u ulozi žrtava našla dva oženjena muškarca iz Kosjerića, koji su, iako su bili dobro nasamareni i oštećeni

za 550 evra, ipak skupili hrabrosti i policiji prijavili šta im se dogodilo. Naime, obojica su preko društvenih mreža dobili zahteve za prijateljstvo od navodnih profila atraktivnih devojaka bele puti pod imenima Seli i Monika. Kako su obojica ušli sa njima u prepisku koja je prerasla u otvoreni flert i slanje nagih fotografija intimnih delova tela i video snimaka istih, ubrzo su im stigle poruke da ukoliko ne uplate po 1000 EUR, ove slike i video snimci će biti prosleđeni njihovim porodicama i prijateljima. Uz poruku je bila napisana i adresa za transfer novca, a zahtevani rok za isplatu bio je pola sata. Ova avantura je jednog od dvojice muškaraca koštala 300, a drugog 250 EUR, jer su im ucenjivači poverovali da nemaju više od toga da plate (Čuvena nigerijska prevara opet hara Srbijom, 2018).

Tokom 2016. godine, "Nigerijske prevare" su se u Srbiji raširile i na društvene mreže i na sajtove za masovnu trgovinu. Jedna od meta napada bio je i sajt za trgovinu *Limundo*, čiji su administratori odmah detektovali pokušaj prevare, obavestili regtistrovane članove ovog portala i dali im smernice o poželjnom ponašanju u slučaju viktimizacije od ove vrste Internet prevare (Divković, 2018). Radnje napada su se sastojale u pokušaju prevare prodavaca na ovom sajtu, ostavljanju ličnih poruka sa molbom da se uplati novac zbog neke nesreće koja je nastala, pokušaju dopisivanja radi ostvarivanja bliske I emotivne veze kako bi se zatim tražio novac, lažnim zahtevima za odobravanje kredita kojima bi se prikupljali detaljni lični podaci registrovanih korisnika sajta koji bi potom bili zloupotrebljeni u nekoj drugoj Internet prevari I sl. Tokom 2017. godine samo na sajtu *Limundo* zabeleženo je 28 pokušaja ovakvih prevara (Ibid.). Svi ti pokušaji su brzo detektovani, nalozi su suspendovani, pa oštećenih korisnika ovog sajta nije bilo.

Veliki broj prevara putem Interneta omogućen je društvenom interakcijom preko društvenih mreža (Vilić, 2013, str. 188), pri čemu svi oblici krivičnih dela i devijantnih ponašanja koja se na njima pojavljuju mogu da imaju oblik bilo kog tradicionalnog krivičnog dela. U istraživanju koje je sprovedeno 2014. godine u kome je učestvovalo 612 ispitanika i ispitanica starosti od 9 do 65 godina (Vilić, 2018, str. 16-17), korisnici društvenih mreža su prepoznali visok stepen rizika od Internet prevara ali je najveći broj (533 tj. 87,1%) izjavio da nije direktno bio/bila žrtva Internet prevare ili krađe (Vilić, 2016, str. 369).

5 ZAKLJUČCI – KAKO SE ZAŠTITITI?

Kompjuterski kriminalitet je postao jedan od najvećih transnacionalnih problema koji se prostire daleko van granica samo jedne države, pa samim tim se i nameće zaključak da mehanizmi borbe protiv ovog vida kriminaliteta moraju da obuhvataju preduzimanje odgovarajućih mera tehničkog, strukturalnog i obrazovnog karaktera (Vilić, 2015, str. 12).

Preporuke Saveta ministara Evropskog saveta (Recommendations to the European Council “Europe and the global information society”, 1994) predstavljaju jedan od bitnih napora preventivnog delovanja međunarodne zajednice na suzbijanju komjuterskog kriminaiteta i prevarnog ponašanja u sajber prostoru, i koje se, između ostalog, odnose na poboljšanje tehničkih mogućnosti za autentifikaciju korisnika podataka, poboljšanje tehničkih mogućnosti praćenja komunikacija preko Interneta i poboljšanje tehnologija kojima bi se zaštitile novčane transakcije preko Interneta (Vilić & Žunić, 2018, str. 93).

Svako od korisnika Interneta, a posebno korisnika društvenih mreža, može da doprinese borbi prevarnog ponašanja na Internetu, kako bi se izbegla ovakva vrsta viktimizacije ili bar smanjila mogućnost da do nje dođe. Korisnicima se savetuje da (The FBI – Common Fraud Schemes: Internet Fraud, 2018):

- ukoliko učestvuju u Internet aukcijama, dobro prouče kako se aukcije zaista sprovode, koje su obaveze prodavaca pre nego što proda određenu stvar i koje su obaveze kupca; da se što bolje raspitaju i da saznaju sve o prodavcu i njegovom poslovanju, kao i o načinu dostave kupljene stvari;
- korisnici dobro provere da li prilikom Internet kupovine nema još nekih dodatnih i nepredviđenih troškova;
- nema potrebe da za ovakav vid transakcija nigde upisuju broj zdravstvenog osiguranja ili vozačke dozvole, jer su to podaci koji se mogu zloupotrebiti i za krađu identiteta i izvršenje različitih krivičnih dela;

- kako bi se izbegla zloupotreba kreditnih kartica, korisnik ne sme da ukucava njen broj ukoliko nije uveren da je sajt zaštićen i pod sigurnom vezom;
- prilikom Internet kupovine, neophodno je proveriti da li prodavac zaista postoji (proveriti pozivom na telefonski broj prodavca, poslati eletronsku poruku da se vidi da li je adresa aktivna i da li se zaista koristi i sl.);
- kada je reč o tzv. "nigerijskim prevarama", korisnici moraju da budu skeptični po pitanju svih osoba koji im se obraćaju kao zvaničnici iz Nigerije a traže pomoć u novcu koja mora da se uplati u neku stranu banku, da ne veruju obećanjima o velikim sumamam novca koje će im biti isplaćene i da veoma pažljivo čuvaju lozinku svog naloga kako ga neko ne bi zloupotrebio.

U svim ovim mogućim situacijama, od korisnika se očekuje da kontaktiraju administratora sajta preko koga su dobili sumnjivu poruku, kako bi sprečili da dođe do nastanka bilo kakve štete i eventualnog izvršenja krivičnog dela.

Pored preduzimanja odgovarajućih tehničkih mera koje bi umanjile mogućnost zloupotreba u virtuelnom svetu Interneta i korigovanja ponašanja samih korisnika, veoma je bitno i stvaranje međunarodnog pravnog okvira, kako bi se sprečilo vršenje krivičnih dela kompjuterskog kriminaliteta, otkrili i procesuirali izvršioci ovih krivičnih dela i kako bi se stvorili mehanizmi pomoću kojih bi se žrtvama ovih dela nadoknadila pretrpljena šteta, koja je kod dela Internet prevara velika i u materijalnom i u nematerijalnom smislu. Postojeće krivično zakonodavstvo u Republici Srbiji žrtvama prevare na Internetu omogućava pokretanje postupka podnošenjem prijave Odeljenju za visokotehnološki kriminal Ministarstva unutrašnjih poslova Republike Srbije ili Odeljenju za visokotehnološki kriminal javnog tužilaštva pred Višim sudom u Beogradu, ali i različitim udruženjima za zaštitu potrošača ili servisima koji se bave zaštitom na Internetu.

CITIRANI RADOVI

Babović, M. (2004). Hakerska subkultura i kompjuterski kriminal. *Pravni život – časopis za pravnu teoriju i praksu,* 9/2004, godina LIII, knjiga 485, 749-750, Udruženje pravnika Srbije, Beograd.

Brkic, M. (2017). *Nova Internet prevara u Srbiji.* Preuzeto na https://www.blic.rs/vesti/hronika/nova-Internet-prevara-u-srbiji-da-bi-vam-novac-legao-kao-i-meni-javite-se-ovom-coveku/lz1rpnm, dana 29.08.2019.

Button, M., McNaughton Nicholl, C.C., Kerr, J. & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian and New Zealand Journal of Criminology 47*(3):391-408, DOI: 10.1177/0004865814521224

Divković, A. (2018). *Nigerijska prevara – koje su vrste i kako ih prepoznati.* Preuzeto sa https://blog.limundograd.com/2018/01/nigerijska-prevara-vrste-i-kako-se-zastiti/, dana 26.08. 2019.

Koong, S. K., Liu, L.C. & Wei, J. (2012). *An Examination of Internet Fraud Occurrences,* Preuzeto sa https://www.researchgate.net/publication/228460925_An_Examination_of_Internet_Fraud_Occurrences, dana 30.08. 2019.

Krivični zakonik Republike Srbije („Službeni glasnik RS" br.85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012 i 104/2013)

Matijašević, J., Spalević, Ž. & Ignjatijević, S. (2012). *Vrste Internet prevara - pojam, značaj i uticaj na ekonomske i moralne aspekte društvene zajednice.* INFOTEH-JAHORINA Vol. 11, 562-565

n.d. (1994). *Recommendations to the European Council "Europe and the global information society".* Preuzeto sa http://channelingreality.com/Digital_Treason/Brussels_1995/Bangemann_report.pdf, dana 31.08.2019.

n.d. (2005). *Computer Crime Research Center: Fraud in the Internet.* Preuzeto sa http://www.crime-research.org/articles/Internet_fraud_0405/, dana 02. 09. 2019.

n.d. (2014). *Čuvajte se – Nigerijska prevara u Srbiji*. Preuzeto na https://srbin.info/pocetna/aktuelno/nigerijska-prevara-u-srbiji-hteo-da-proda-kuca-a-ostao-bez-para/, dana 12.08.2019.

n.d. (2017). *The top 10 Internet Frauds - National Fraud Information Center*. Preuzeto sa http://www.nclnet.org/, dana 14. 08. 2018.

n.d. (2018). *Čuvena nigerijska prevara opet hara Srbijom.* Preuzeto na https://www.kurir.rs/vesti/drustvo/3168527/cuvena-nigerijska-prevara-opet-hara-srbijom-ozenjeni-muskarac-iz-kosjerica-dobio-poruku-od-nepoznate-devojke-na-fejsbuku-tog-trenutka-pocela-je-njegova-nocna-mora-ovako-ga-je-opeljesila, dana 23.08.2019.

n.d. (2018). *Nigerijska prevara i dalje živi: Lažni naslednici lakoverne Srbe vrebaju i na ćirilici.* Preuzeto sa https://www.telegraf.rs/vesti/ekonomija/2986678-nigerijska-prevara-i-dalje-zivi-lazni-naslednici-lakoverne-srbe-vrebaju-i-na-cirilici, dana 23.08.2019.

n.d. (2018). *The FBI – Common Fraud Schemes: Internet Fraud.* Preuzeto sa http://www.fbi.gov/scams-safety/fraud/_fraud , dana 23. 01. 2018.

n.d. (2018). *Ultrascan Advanced Global Investigations.* Preuzeto sa http://www.ultrascan-agi.com/, dana 03.02. 2018.

n.d. (2019). *Top ten scams of 2018 – Fraud.org.* Preuzeto sa https://www.fraud.org/2018_top_ten, dana 31.08.2019.

Nikolić, K., Gvozdenović, L., Radulović, R., Milosavljević, S., Jerković, A., Živković, R., Živanović, V., Reljanović, M. & Aleksić, I. (2010). *Kratak prikaz razvoja pravne regulative o visokotehnološkom kriminalitetu na međunarodnom nivou.* Suzbijanje visokotehnološkog kriminala, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd.

Prlja, D., Ivanović, Z. & Reljanović, M. (2011). *Krivična dela visokotehnološkog kriminala*. Institut za uporedno pravo, Beograd.

Urošević, V. (2009). Nigerijska prevara u Republici Srbiji. *Časopis Bezbednost.* (3).

Vilić, V. (2013). *Possibilities of privacy rights abuses in social networks and practical protective measures.* International scientific and practical conference „Internet – Government – Politics“, Kemerovo, 2013, 187-192, ZAKAZ No.458

Vilić, V. (2015). *Mechanisms for Protecting the Right to Privacy and Personal Data on Social Networks.* INTERNATIONAL Scientific Conference of IT and Bussiness – Related Research Synthesis Univerzitet Singidunum Beograd 2015, 10-13. DOI: 10.15308/Synthesis-2015-10-13, ISBN 978-86-7912-595-8

Vilić, V. (2016). *Povreda prava na privatnost zloupotrebom društvenih mreža kao oblik kompjuterskog kriminaliteta, Doktorska disertacija,* Pravni fakultet Univerziteta u Nišu, 535. COBISS.SR-ID 1026747809

Vilić, V. (2017). *CYBERCRIME: Basic criminological characteristics and legislation.* LAP - LAMBERT Academic Publishing – International Book Market Service Ltd. member of OmniScriptum Publishing Group. -166. ISBN 978-620-2-01800-5

Vilić, V. (2018). *Users' considerations about possibilities of self-protection on social networks.* Center for Open Access in Science - Open Journal for Legal Studies, 2018, 1(1), 9-24. ISSN (Online) 2620-0619 ▪ DOI: 00.00000/ojls.2017.00000a

Vilić, V. & Žunić, N. (2018). *Prevencija i mere zaštite od kompjuterskog kriminaliteta (Prevention and measures of protection against computer crime).* III međunarodna naučna konferencija „Društvene devijacije: NE NASILJU – jedinstven društveni odgovor“, Banja Luka 25-27.05.2018, Centar modernih znanja, Banja Luka, 92-100, UDK: 004,738,5:316,472,4, DOI: 10.7251/CMZ1803092V

Vilić, V. (2019). Phishing and pharming as forms of identity theft and identity abuse. *Balkan Social Science Review, 13*(13), 43-57.

Datum prve prijave: 08.09.2019.
Datum prijema korigovanog članka: 08.10.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

Style – APA Sixth Edition:

Vilić, V. (2019, 10 15). Prevare putem Interneta: Sajber zabava koja „prazni" račune širom sveta. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 135-145. doi:10.12709/fbim.07.07.02.15

Style – Chicago Sixteenth Edition:

Vilić, Vida. 2019. "Prevare putem Interneta: Sajber zabava koja „prazni" račune širom sveta." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 135-145. doi:10.12709/fbim.07.07.02.15.

Style – GOST Name Sort:

Vilić Vida Prevare putem Interneta: Sajber zabava koja „prazni" račune širom sveta [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 135-145.

Style – Harvard Anglia:

Vilić, V., 2019. Prevare putem Interneta: Sajber zabava koja „prazni" račune širom sveta. *FBIM Transactions,* 15 10, 7(2), pp. 135-145.

Style – ISO 690 Numerical Reference:

Prevare putem Interneta: Sajber zabava koja „prazni" račune širom sveta. **Vilić, Vida.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 135-145.

FBIM Transactions
DOI 10.12709/fbim.07.07.02.16

DIGITALIZATION OR ICT IN TOURISM

Slavoljub M. Vujovic
Institute of Economics, Belgrade, Serbia

JEL Category: **O3, O31, O32, O33, Z3,Z32.**

Abstract

The research presented in the paper is theoretical, focused on analyzing and clarifying the role and importance of using information technology for tourism development as an economic activity. It also seeks to point out that the use of the term "digitalization of tourism" (or digitization of business in the tourism economy) is unnecessary. Research is not focused on information technology as a new discipline, but on the practical use of technologies to process and transfer data and information, technologies for communications, to enable faster flow of capital and services, and so on. The special purpose of the research is the analysis of the benefits of the use of information and communication technologies from the aspect of the providers of tourism supply, carriers of tourist demand and intermediary factors. The work is part of the research on the project "Development and application of new and traditional technologies in the production of competitive food products with added value for the domestic and world markets - Let's create wealth from the wealth of Serbia" (MPNTR RS, No. 046001).

Keywords: *tourism development, information technology, tourism digitalization.*

1 INTRODUCTION

When it comes to economics and tourism, the increasing use of vague (unnecessary) terms or concepts in scientific research and writing the scientific paper.

Specifically, quite vague terms are used in tourism such as: “creative tourism, digitization of tourism, green tourism, dark tourism, ecotourism, equestrian tourism, rural tourism, children, youth, etc.”?

Based on previous research into similar problems in tourism and discussions with experienced researchers, what causes this phenomenon, a unique conclusion is uncritical retrieval of terms from foreign authors, then, the consequences of translation, ignorance, etc.!

However, here the focus is specifically on the notion of "digitization", which is unnecessary when it comes to tourism, that is, the tourism economy.

Based on the literature focused on the application and importance of information technology in economics and management, there is no need to introduce the term "digitization" when the more concrete and clearer term is application information technology in tourism (Shanker, 2008 and Mihajlovic, 2015).

The expansion of the use of modern information and communication technologies (ICT) or "digitalization" in all walks of life is increasingly intense, so this is one of the reasons for the use of the term digitalization in the literature related to tourism research, and therefore connection, also appears here in the paper.

Address of the author
Slavoljub Vujović
kelovic1967@yahoo.com

The term information-communication technology means a wide range of technologies - the Internet, GPS, wireless, digital radio, mobile phone applications, digital cameras and the like. (Turban, Mclean, & Wetherbe, 2003).

Of the many definitions of IT as relevant, the following "information technologies include all forms of technology that are used to create, store and share information in various forms (business data, speech, sound, images, multimedia, etc.)". (Mitic, 2019).

In the broad sense of information technology, some theorists consider the set of computer systems an organization uses (Turban, Meclean, & Wetherbe, 2003).

In order to emphasize the broader aspect of information technology through the use of communications, especially electronic, some authors refer to information and communication technologies as "technologies such as desktops and laptops, software, peripherals, and Internet connectivity devices designed for information processing and communication" (Mitic, 2019).

In tourism and economy, the application of ICT brings a number of benefits for different participants or entities, while the paper explains the application of information technology or digitization in light of the interests of tourism demand factors and tourism supply factors.

From a broader point of view, when it comes to digitization in tourism, two approaches to the analysis of the benefits of digitization are indispensable: the digitization of processes or activities on the part of the driving factors of tourism (demand factors) and the digitization of processes on the side of the providers of tourism supply.

However, it should be noted that in addition to the interests of the two groups of factors (supply-side and demand-side factors), there are other parties or stakeholder groups interested in introducing and implementing new information and communication technologies, where factors deserve special attention. of the environment.

Some, well-known authors in the world, link the fate of tourism development in the future to the natural environment and humanity, stating: "*Tourism has a future only if the goal of its development is more humanity. Tourism is invented and created for man's sake, not man for tourism's sake. It is important to bring tourism back to people and thus make it more humane*" (Krippendorf, 1986, 121).

The fact that certain jobs in tourism, especially on the supply side (e.g. the work of cooks), can not be replaced by an apparatus or machine, indicates the specificity of tourism in the introduction of new information and communication technologies or digitization in relation to other activities.

In a nutshell, digitization from the perspective of time and money providers should contribute to reducing costs, shortening the processing time and maximizing profits, while contributing to higher quality services at the lowest cost and in the planned time from the demand side.

Many authors (Dickson and DeSannctis, 2001; Gill, 1996; Tapscott et al., 2000) consider information technology (IT) to be a major factor in facilitating business in all sectors, while some (Dertouzos, 1997) emphasize that (IT) is a major catalyst fundamental changes in business and management processes.

In accordance with the specificities of the tourist market, the use of information and communication technologies or "digitalization" is particularly pronounced with a strong contribution to marketing activities. Thanks to the application of ICT, tourism providers have more flexibility to offer a wider range of products and services in the global market in a shorter time (Chaffey, 2009).

In addition to a number of benefits, some authors point to the importance of implementing information technology or digitizing the tourism business, in order to improve service quality and increase consumer satisfaction (Law, Leung & Buhalis 2009). The benefits of ICT are particularly visible in data processing, both in terms of time and scope, where ICTs are far more successful than human factors.

In addition to the aforementioned aspects, indispensable in analyzing the importance of ICTs or "digitalization" in tourism, factors in space or security and ecology are also very important, however, broader explanations are directed at the interests of tourism providers and holders of tourism demand, in short, factors demand and supply.

In all EU countries, information security is governed by specific laws and technical standards to achieve IS security standards within the EU (Boc, Dvorak, & Cekerevac, 2019).

2 IMPACT OF DIGITIZATION AND CAPTIVE CAPITAL ON TOURISM DEVELOPMENT

Given that the development and use of new information technologies require capital, and that financial capital is always strictly controlled by certain circles and individuals, the title "*Impact of digitization and captive capital on tourism development*" is defined.

Confirming the importance of digitalization is the focus of the United Nations World Tourism Organization (UNWTO) on the *five pillars* of development in 2018-2019: *innovation and digital transformation, investment and entrepreneurship, education and employment, travel safety and social, cultural and environmental sustainability*.

In order to adequately address new challenges and trends in tourism and improve the business environment for the sector, UNWTO paid particular attention to boosting innovation and digitization in the sector, contributing to the creation of new business opportunities, increased investment in the tourism economy, and increased competitiveness and sustainability sectors.

In the context of the application of ICT in order to increase tourism demand, that is, to increase tourism traffic and tourism revenues, it is necessary to work on animating a part of the population with increasing material wealth, to travel, to spend money visiting attractive destinations. Travel and vacation certainly contribute to better psycho-physical fitness and health, while information and communication technologies directly stimulate an increase in tourist demand, enabling potential tourists to reach information very quickly and easily.

One of the burning problems of economic and tourism development, and thus the use of ICT (digitalization) and their benefits, is captured capital.

In the context of the developmental aspects of tourism, captive capital has obstructive (negative) effects.

The importance of information and communication technologies for the development of tourism can, to a large extent, be understood thanks to the well-known economic theories: mercantilism, physiocratism, comparative advantages, Samuelson's theory, Leonti's paradox, etc., however, they cannot completely shed light on tourism with all its specificities.

It has already been pointed out that the development aspects of tourism as an economic activity can best be understood through consumption.

Through the consumption of individuals, there is an overflow of money from one country to another, or through the export of services, if viewed through the balance of payments of a particular country. It is interesting to note here that one of the world's greatest economists, A. Smith, in his famous work Exploring the Nature and Causes of Wealth of Nations, pointed to the importance of the individual's interests in the function of the development of the overall economic system (Adam, 1998).

From an economic point of view, it is inevitable to analyze the benefits of digitalization in the light of time and money as inevitable economic factors, directed towards consumption.

Earlier, before the advent and application of information technology, for example, in the tourism market, carriers offered their services and products using with the help of postal (PTT) services (paper offers), later by telephone and fax, which required more staff and more time (higher costs). however, the introduction of new ICTs reduces costs and time. Now the providers of service providers and service providers simply thanks to the Internet, through their own sites, offer a single offer to all potential users of the world their services and products.

Consumption is at the heart of the benefits of digitalization, that is, the development processes of tourism and overall economic development have been argued by the world's greatest economists - Smith and John Maynard Keynes.

"Adam Smith believed that goods, people and institutions were the real causes of prosperity. Therefore, he also believed that consumption was the basis for economic growth. Keynes believed that in addition to consumption, production was

also important to the economy and that in the modern economy, state intervention was necessary, which was the viewpoint and mercantilist" (Beslać, M., 2013, 31).

Economic or economic and social inequalities and the capture of capital by individuals and groups are certainly negatively affected by tourism. These inequalities and the volume of tourist trips are in reverse proportion.

It is precise because of the large-scale continued capture of capital by the minority, at the expense of the majority, in order to control capital (and thus of work and life), that these inequalities are deepening.

Today, as J-J. Rousseau, the main stumbling block of the economy, beginning from the individual to the largest corporations (e.g. Agrokor in Croatia, Port of Belgrade and Azotara Pancevo in Serbia, etc.).

The question is, did the technological and technological progress of the whole twentieth century lead to the progress and wealth of the population or, to put it better, the progress aimed at creating inequality.

There is no inequality without the state, in the sense that the state does not function as it should function, because it selectively applies the law, thus enabling individuals to make enormous riches by abusing the law and taking it from others.

The control of material wealth by the minority, through corporations and the irregular use of leverage by the state, has contributed to the current 1% of Americans in the US prosper and 99% enslave (Stiglic, 2011).

"Through the process of globalization, national economic structures are destroyed (national producers with all their specificities are either destroyed or bought and then unified under" international standards") and subjugation of the world economy to the interests of the world oligarchy and transnational capital (by sphere of activity and by origin basically American). As a rule, the contradictions between the interests of the transnational and national capital are resolved by recruiting the latter into the service of international corporations and creating a domestic comprador elite that is included in the peripheral layer of the world oligarchy (Dusanic, 2009, 29)".

Perhaps here, in order to counteract these inequalities, Malthus's theory (Malthus, 1978) holds that after a certain time of development, societies also necessarily need wars and large-scale natural disasters ?!

Economic cycles are inevitable, sometime after twenty-thirty and at most fifty years, as Kondratyev wrote (Michael, 2002). Particularly important here is Kondrat's fifth cycle, which began in the 1970s and was initiated by computer information technology. The industrial society has transformed into an information society, which has transformed the world into a global village. In this cycle, the information technology sector has become a major driver of economic growth. This cycle is said to have been completed at the beginning of the 21st Century.

Inequalities in favor of the minority at the expense of the majority diminish the travel opportunities of the majority. Inequalities as a result of corruption and crime, that is, the non-functioning of the state, are the antithesis to the overriding need and guidelines for the emergence of the state, as explained by Jean Jacques Rousseau (Rousseau, 2011) in the Social Contract! In discussing inequality, Rousseau discusses the causes that put a person in an unworthy position. In the aforementioned part, by analyzing all possible forms of government, he wants to affirm the model of society without inequality.

Controlling 85% of material wealth by 15% of the wealthy in the 1990s, the first decade of the twenty-first century changed that 10% of wealthy individuals controlled more than 85% of the wealth.

It is interesting that all of the above does not stop (but negatively affects the volume of tourist traffic) the further development of tourism, while the negatives are reflected through greater pressure on the natural environment.

Captive capital means capital excluded from creative - investment activities and consumption (factory in the hands of an incapacitated owner, money taken abroad, black population funds, time or unlimited money in various accounts, purchase of various expensive vessels without putting them into the commercial function, etc.).

3 APPLICATION OF INFORMATION TECHNOLOGY OR DIGITIZATION IN TOURISM

It has already been mentioned that the terms: digitalization, digital transformations, digital economy, digital tourism are increasingly being used in practice, which is unnecessary from the aspect of use and purpose of using information technologies.

"*Tourism and Digital Transformation*" was the theme of 2018 World Tourism Day celebrated on September 27 (http://wtd.unwto.org/content/world-tourism-day-2018).

The combination of digital platforms, user-generated content and feedback, social media integration, global positioning and use of big data and artificial intelligence has changed the way people perceive, consume and share information. *This is the result of successive advances in telecommunications, computers, databases, networks, the Internet, mobile and wireless technology, global positioning systems and smartphones, among others*.

Tourism, as one of the complex economic activities, is inevitably part and opposite of these changes. For tourism, public and private sector entities, ICTs provide - the necessary and very powerful tools for management, logistics, distribution, and marketing. This has led to a digital tourist who is autonomous, hyper-connected and increasingly demanding, expecting personalized customer service (https: //www.iznajmljivači.hr/digitalni-turizam/, 10.03.2019).

Shifts in customer expectations and global trends are forcing the tourism sector to adapt business and operational models in the pursuit of increased customer satisfaction and operational performance. This creates opportunities for new entrants to the value chain of tourism, especially digital "hosts" such as internet travel aggregators. At the same time, private tourism platforms (the so-called sharing economy) are on the rise. In addition, the heterogeneous nature of the tourism sector extends its level of responsibility for the use of technological change and digitization to help create an economically and socially sustainable, inclusive and environmentally sound future. (http://wtd.unwto.org/content/wtd-2018-tourism-digital-era).

All participants in the tourism market, especially employees of three groups of factors: supply factors, demand factors, and intermediary factors, obtain the necessary information through information and communication technologies using available electronic networks, primarily the Internet. Whether you want to book a hotel room in Macau, an apartment in Greece, or a campsite in the US, you will do so digitally, that is, through your computer or smartphone, and of course the internet. You will use an app or a popular website to book and pay for the tourist service you want. This is why digital tourism is actually everyday tourism, at least as far as the search, booking, and booking of tourist services is concerned (https: //www.iznajmljivači.hr/digitalni-turizam/, 10.03.2019).

Personal contact between the users of the service (tourists) and the service provider during the realization or consumption of the service, as an exceptional peculiarity and specificity of the mechanisms of supply and demand in the tourist market, comes to the full in the application of information and communication technologies in tourism. “Consumption of tourist services is not digital, however. You will experience the hotel room or apartment in person, in immediate reality, and you will have such impressions accordingly. Perhaps staying in a destination will be extremely interesting, fun, relaxing, enchanting and more. You may not, and you will be disappointed with the hotel room facilities, the poor quality of the tourist offer, the lack of amenities, etc. In any case, it all depends on your subjective impression based on the experience of non-virtual reality” (https: //www.iznajmljivači.hr/digitalni-tourism/10.03.2019).

In contrast to personal attendance at the realization of the service offered and personal (hedonism and epicureanism) experiences (spa pool, snow skiing, bed comfort), the experiences can be virtually based on digital technologies that allow users to experience certain services at home, in the place of residence.

There are also views in the literature that digital tourism is a segment of the tourist offer that enables interested users to digitally, remotely, without a physical presence, virtually experience

and feel artificially created values, especially values from the ancient past due to their cultural and historical interest (https : //www.iznajmljivači.hr/digitalni-turizam/).

Due to the importance of information technologies and how they are applied in the business process, especially in decision-making, some authors, emphasizing the importance of business intelligence, emphasize that these business intelligence systems are "predominantly based on modern information technologies (IT) and do not depend on the field of work or level decision making" (Borovcanin, Cerovic, and Knezevic, 2017, 416).

Many tourism industry researchers place a system of information in the context of markets and communications (Macura, 2000), some emphasize a communication system, some a marketing information system (Rakic, 2003), while the essence of all of them is about the application of information technology and their importance as infrastructures providing data and information flow. Even complex systems such as the marketing system would not be able to function without the constant supply of the right information and enabled by information technology (Macura, 2000, 36).

The overall marketing system as a system of information flow between producers and consumers in order to satisfy their own desires and goals (Galogaza, 1998), is based on information and communication technologies.

Internationally renowned marketing researchers (Rakic, 2003) point out that information needs have contributed to the "development of impressive new information technologies such as computers, microfilm, cable television, photocopiers, fax machines, video recorders, CD-ROMs, the internet, etc." (Rakic, 2003, 104).

It is the definition of business intelligence that these authors distinguish as the most acceptable and comprehensive "business intelligence is: 1) system, concept, method, process and structure 2) continuous, defined and organized collection, storage, processing and access to data 3) about customers, products, financial indicators, business operations, etc. 4) for the purpose of obtaining accurate and timely information necessary for making accurate, timely, strategic, operational and tactical decisions 5) with the aim of improving business performance" (Borovcanin et al., 2017, 417) can also be accepted as an explanation and definition of information technology.

Some authors, pointing to the importance of the dynamics of development and application of new information and communication technologies for the business of tourism industry entities, emphasize that they influence the forms of the organizational structure of large tour operators (multinational, vertically integrated companies, small specialist tour operators, etc.), (Djurasevic, 2008, 119).

The necessity of development and implementation in the tourism economy of new information technologies is confirmed by certain basic economic principles and rules: the necessity of creating new economic values, profit maximization, minimization of investments (costs), shortening of the work process, etc.

Analysis of the above concepts: application of information technology, digitalization, business systems, information systems, marketing information system, suggests that these are synonyms for the use of information and communication technologies in the business process.

Based on the analysis of the literature and the opinions of many authors on what a marketing information system is, especially its role and importance when it comes to tourism, citing only the definition of the well-known world expert Kotler "*Marketing information system is made up of people, tools and procedures that enable collection , sorting, analyzing, evaluating and distributing the necessary timely and accurate information to marketing decision-makers*" (Kotler, 2000, 169), it can be concluded that tourism digitalization is just another name for the marketing information system.

4 CONCLUSION

The role and importance of information, especially information and communication technologies for doing business in the tourism economy and developing tourism as an economic activity is direct and fundamental.

Indirectly, the importance of other new technologies is certainly important and contributes to the constant positive growth and development of tourism, however, the existing level of development, in addition to the human factor, has reached tourism thanks to information and communication technologies.

Based on the analysis of the role and importance of marketing information systems in companies, tourism, and society in general, it can be concluded that digitalization of tourism is just another name (wrong) for the application of marketing information systems in tourism.

WORKS CITED

Adam, S. (1998). Istraživanje prirode i uzroka bogatstva naroda, Novi Sad: Global book.

Beslać, M. (2013). Međunarodna ekonomija. Beograd: Visoka škola za poslovnu ekonomiju i preduzetništvo.

Boc, K., Dvorak, Z., Čekerevac, Z. (2019). Security of information and communication technologies. FBIM Transactions, Vol. 7 No. 1 pp.29-37. DOI: 10.12709/fbim.07.07.01.04

Chaffey, D. (2009). E-Business and E-Commerce Management: Strategy, Implementation, and Practice, 4th Edition, Chapter 8. Edinburgh: Pearson Education Limited.

Dertouzos, M. (1997). What Will Be: How the New World of information will change our lives. San Francisco: Harper Edge.

Dickson, G.W., DeSanctis, G. (2001). Information technology and the future enterprise: New models for managers. Upper Saddle River, N.J.: Prentice-Hall.

Digital Transformation in Tourism: Evolving Travel with Technology. Preuzeto s http://wtd.unwto.org/content/wtd-2018-tourism-digital-era (16.09.2018).

Digitlni turizam: povratak izgubljenih svetova. Preuzeto s https://www.iznajmljivači.hr/digitalni-turizam/, (10.03.2019).

Galogaza, M. (1998). Principi marketinga, knjiga prva. Novi Sad: Autorsko izdanje.

Gill, K.S. (ed.) (1996). Information society. London: Springer Publishing.

Kotler, P. (2000). Marketing management, New Jersy: Prentice –Hall International Inc.

Krippendorf, J. (1986). The new tourist - a turning point for leisure and travel, *Tourism Management, 7*(2), pp. 131-135.

Law, R., Leung, R. & Buhalis, D. (2009). Information technology applications in hospitality and tourism: A review of publications from 2005 to 2007. Journal of Travel & Tourism Marketing, 26(5-6), pp. 599-623.

Macura, P. (2000). Sistem informacija promocije. Banja Luka: Glas Srpski.

Malthus, T.R. (1798). An Essay on the Principle of Population, Sixth Edition. London: Ward Lock.

Mitić, Mirjana Informaciono-komunikacione tehnologije. Retrieved from http://miticmirjana.weebly.com/ (06.09.2019).

Michael, A. (2019). The Kondratiev Cycle: A generational interpretation. Dostupno na https://www.amazon.com/dp/059521 (06.06.2019).

Mihajlović, I. (2015). Značaj informaciono-komunikacionih tehnologija u poslovanju turističkih i hotelijerskih preduzeća, Beograd: Univerzitet Singidunum.

Rakić, B. (2000). Marketing. Beograd: Megatrend univerzitet primenjenih nauka.

Rousseao, J-J. (2011). Društveni ugovor: o poreklu i osnovama nejednakosti među ljudima-rasprava o naukama i umetnosti, Beograd: Filip Višnjić.

Shanker, D. (2008). ICT and Tourism: challenges and opportunities. In Conference of Tourism in India - Challenges Ahead (Vol. 15, p.17).

Stiglic, J., (10. novembar 2011). Ideološka ostrašćenost MMF-a. Politika, str. 11.

Tapscott, D., et al. (2000). Digital capital. Boston: Harvard Business School Press.

Tourism and the digital transformation. Retrieved from http://wtd.unwto.org/content/wtd-2018-tourism-digital-era (06.09.2019)

Turban, E., Meclean, E., i Wetherbe, J. (2003). Informaciona tehnologija za menadžment-transformacija poslovanja u digitalnu ekonomiju. Beograd: Zavod za udžbenike i nastavna sredstva.

Turizam i digitalna transformacija. Svjetski dan turizma, 27. septembra 2018. Retrieved from http://wtd.unwto.org/content/world-tourism-day-2018

UNWTO. 63 Sjednica Komisije za Evropu, Prag, 11-13. jun 2018. Retrieved from http://www.mrt.gov.me/vijesti/185937/UNWTO-U-fokusu-digitalizacija-u-turizmu.html, (20.12.2018)

UNWTO. U fokusu digitalizacija u turizmu. Retrieved from http://www.mrt.gov.me/vijesti/185937/UNWTO-U-fokusu-digitalizacija-u-turizmu.html, (02.10.2019).

Datum prve prijave: 09.09.2019.
Datum prijema korigovanog članka: 08.10.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

Style – APA Sixth Edition:

Vujovic, S. M. (2019, 10 15). Digitalization or ICT in tourism. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 146-153. doi:10.12709/fbim.07.07.02.16

Style – Chicago Sixteenth Edition:

Vujovic, Slavoljub M. 2019. "Digitalization or ICT in tourism." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 146-153. doi:10.12709/fbim.07.07.02.16.

Style – GOST Name Sort:

Vujovic Slavoljub M Digitalization or ICT in tourism [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 146-153.

Style – Harvard Anglia:

Vujovic, S. M., 2019. Digitalization or ICT in tourism. *FBIM Transactions,* 15 10, 7(2), pp. 146-153.

Style – ISO 690 Numerical Reference:

Digitalization or ICT in tourism. **Vujovic, Slavoljub M.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 146-153.

Reviewers of the FBIM Transactions – alphabetically

1. Dr. **Svetlana Anđelić**, Prof.v.s., Information Technology School - ITS, Belgrade, Serbia
2. **Dragan Anucojić**, Mgr., Fakultet za pravne i poslovne studije, Novi Sad, Serbia
3. Dr. **Dragutin Ž Arsić**, Assoc. Prof., Faculty of Business and Law of the "Union - Nikola Tesla" University Belgrade, Belgrade, Serbia
4. Dr. **Suat Askin**, Asst. Prof., Adiyaman University, Adıyaman Merkez/Adıyaman, Turkey
5. **Olga Artemenko**, PhD, Bukovinian University, Faculty of Computer Sciences and Technologies, Chernivtsi, Ukraine
6. Dr. **Daniel Badulescu**, Assoc. Prof., Faculty of Economic Sciences, University of Oradea, Romania
7. Prof. Dr. **Milan Beslać**, Faculty of Business Economy and Entrepreneurship in Belgrade, Belgrade, Serbia
8. Dr. sc. **Mario Bogdanović**, research associate, Faculty of Economics, University of Split, Croatia
9. Dr. **Nikola Bračika**, Assoc. Prof., Business School Čačak, Belgrade, Serbia
10. Mr **Nemanja Budimir**, Agency for Bookkeeping "Budimir", Banja Luka, Bosnia and Herzegovina
11. CSc. **Anastasia Bugaenko**, "Ukrgasbank", Kyiv, Ukraine
12. Prof. Dr. **Ana Čekerevac**, University Belgrade Faculty of Political Sciences, Belgrade, Serbia
13. Prof. Dr. **Zoran Čekerevac**, Faculty of Business and Law of the "Union - Nikola Tesla" University Belgrade, Belgrade, Serbia
14. **Sanja Čukić**, MA, Faculty of Business and Law, "Union - Nikola Tesla" University, Belgrade, Serbia
15. Dr. **Dražen Ćućić**, Assistant Professor, Faculty of Economics in Osijek, Osijek, Croatia
16. Dr. **Radmila Ćurčić**, Ass. Prof., Faculty of Business and Law, "Union - Nikola Tesla" University, Belgrade, Serbia
17. Prof. Dr. **Sreten Ćuzović**, Faculty of Economics, University of Niš, Niš, Serbia
18. Prof. Dr. **Predrag Damnjanović**, Business School Čačak, Belgrade, Serbia
19. Prof. Dr. **Branko Davidović**, Technical College, Kragujevac, Serbia
20. Dr. **Derya Dispinar**, Asst. Prof., Istanbul University, Metallurgical and Materials Engineering, Avcilar, Istanbul, Turkey
21. Prof. Ing. **Zdenek Dvorak**, PhD, Faculty of Special Engineering University of Žilina, Žilina, Slovakia
22. **Bela Yu. Dzhamirze**, PhD, Assoc. Prof., Maykop State Technological University, Maykop, Russia
23. Prof. Dr. **Branislav Đorđević,** Emeritus, Belgrade, Serbia
24. Prof. Dr. **Branko Đurović**, Medical Faculty, University of Belgrade, Belgrade, Serbia
25. **Ljupčo Eftimov**, PhD, Asst. Prof., Faculty of Economics - Skopje, Skopje, R. Macedonia
26. Prof. **Valeriy Eudokymenko**, DrSc, Bukovinian State Finance and Economics University, Chernivtsi, Ukraine
27. Ing. **Stanislav Filip**, PhD, Assoc. Prof., School of Economics and Management in Public Administration in Bratislava, Slovakia
28. **Jelena Fišić**, MA, "Pro-elektro" doo, Belgrade, Serbia
29. **Milena Gajic-Stevanovic**, DMD, MSc.SM, PhD, Institute of Public Health of Serbia, Belgrade, Serbia
30. **Bogdan Gats**, Chernivtsy Trade and Economics Institute of the Kyiv National Trade and Economics University, Chernivtsy, Ukraine
31. Prof. Dr. **Sonja T. Gegovska-Zajkova**, Ss Cyril and Methodius University, Faculty of Electrical Engineering and Information Technologies, Skopje, Macedonia
32. **Mariya P. Hristova**, PhD, Assoc. Prof., "Todor Kableshkov" University of Transport, Sofia, Bulgaria
33. Dr. **Miroljub Ivanović**, Prof.v.s., Higher School of Vocational Studies in Education of Tutors in Sremska Mitrovica, Sremska Mitrovica, Serbia
34. Dr. **Aleksandra M. Izgarjan**, Assoc. Prof., Faculty of Philosophy, University of Novi Sad, Novi Sad, Serbia
35. Dr. **Miloje Jelić**, Preduzeće za proizvodnju “Klanica“d.o.o. Kraljevo

36. Prof. Dr. **Zoran Jerotijević**, Faculty of Business and Law of the "Union - Nikola Tesla" University in Belgrade, Belgrade, Serbia
37. Dr. **Bisera S. Jevtić**, Assoc. Prof., University of Niš - Faculty of Philosophy, Niš, Serbia
38. Prof. Dr. **Natalija Jolić**, Faculty of Transport and Traffic Sciences, University of Zagreb, Zagreb, Croatia
39. Prof. Dr. **Svetlana Kamberdieva**, North Caucasian Institute of Mining and Metallurgy (State Technological University), NCIMM (STU), Vladikavkaz, Republic of North Ossetia – Alania, Russia
40. Prof. Dr. **Zvonko Kavran**, Faculty of Transport and Traffic Sciences, University of Zagreb, Zagreb, Croatia
41. Prof. **Antoaneta Kirova**, PhD, "Todor Kableshkov" University of Transport, Sofia, Bulgaria
42. Ing. **Jozef Klučka**, PhD, Assoc. Prof., Faculty of special engineering University of Žilina, Žilina, Slovakia
43. Prof. **Petar Kolev**, Dr, "Todor Kableshkov" University of Transport, Sofia, Bulgaria
44. **Oksana Koshulko**, PhD, Assoc. Prof., Polotsk State University, Novopolotsk, Republic of Belarus
45. Prof. Dr. **Boris Krivokapić**, Faculty of Business and Law of the "Union - Nikola Tesla" University Belgrade, Belgrade, Serbia
46. Dr. **Evelin Krmac**, Asst. Prof., University of Ljubljana, Faculty of Maritime Studies and Transportation Portorož, Slovenia
47. Prof. Dr. **Adil Kurtić**, University of Tuzla - Faculty of Economics, Tuzla, Bosnia and Herzegovina
48. Dr. **Aleksandar Lebl**, Iritel AD, Beograd, Serbia
49. Prof. Dr. **Branko Ž. Ljutić**, certified auditor, University Business Academy, Novi Sad, Serbia
50. Ing. **Maria Luskova**, PhD, Faculty of special engineering University of Žilina, Žilina, Slovakia
51. CSc. **Elena S. Maltseva**, Assoc. Prof., Maykop State Technological University, Maykop, Russia
52. Dr. **Dubravka Mandušić**, University of Zagreb - Faculty of Agriculture, Zagreb, Croatia
53. **Milorad Markagić**, University of Defense - Military Academy, Belgrade, Serbia
54. **Željko Mateljak**, PhD, University of Split, Faculty of Economics, Split, Croatia
55. Prof. Dr. **Dobrivoje Mihailović**, University of Belgrade, Faculty of Organizational Sciences, Belgrade, Serbia
56. Prof. Dr. **Božidar Mihajlović**, College of Business Economics and Entrepreneurship in Belgrade, Belgrade, Serbia
57. Dr. **Ivo Mijoč**, Assistant Professor, Faculty of Economics in Osijek, Osijek, Croatia
58. Dr. **Živanka Miladinović Bogavac**, Asst. Prof., Faculty of Business and Law of the "Union - Nikola Tesla" University Belgrade, Belgrade, Serbia
59. Dr. **Zoran Milenković**, Prof.v.s., College of Tourism, Belgrade, Serbia
60. Dr. **Živorad Milić**, Prizma, Kragujevac, Srbija
61. Dr. **Milorad Milošević**, Prof.v.s., Business School Čačak, Belgrade, Serbia
62. Dr. **Aleksandar Miljković**, Assoc. Prof., Faculty of Business and Law of the "Union - Nikola Tesla" University Belgrade, Belgrade, Serbia and FORKUP, Novi Sad, Srbija
63. **Piotr Misztal**, PhD, Assoc. Prof., Jan Kochanowski University in Kielce, Kielce, Poland
64. Prof. Dr. **Dragan M Momirović**, Faculty of Business and Law of the "Union - Nikola Tesla" University Belgrade, Belgrade, Serbia
65. Dr. **Saša Muminović**, Julon d.d. Ljubljana, Slovenia
66. Prof. Dr. **Predrag M. Nemec**, Faculty of Management in Sport, "Alfa" University, Belgrade, Serbia
67. Prof. Dr. **Nevenka Nićin**, Faculty of Business and Law of the "Union - Nikola Tesla" University Belgrade, Belgrade, Serbia
68. Ing. **Ladislav Novak**, PhD, Assoc. Prof., Faculty of special engineering University of Žilina, Žilina, Slovakia
69. Dr. **Srećko Novaković**, Assistant Prof., High Business and Technical School Doboj, Bosnia and Herzegovina and College of Vocational Studies for Education of Tutors and Coaches, Subotica, Serbia
70. Prof. Dr. **Saša Obradović**, Fakultet za ekonomiju i inženjerski menadžment, Novi Sad, Serbia
71. Dr. **Milorad Opsenica**,Assistant Prof.,Traffic Engineering Faculty of the International University, Brcko District, Bosnia and Herzegovina

72. CSc. **Tatiana Paladova**, Assoc.Prof., Maykop State Technological University, Maykop, Russia
73. Prof. Dr. **Yurij Vasylyovych Pasichnyk**, Cherkassy State Technological University, Cherkassy, Ukraine
74. Prof. **Dinara Peskova**, PhD, Bashkir Academy of Public Administration and Management under the Auspices of the Republic of Bashkortostan, Ufa, Russia
75. Prof. Dr. **Šemsudin Plojović**, University of Novi Pazar, Novi Pazar, Serbia
76. Prof. Dr. **Lyudmila Prigoda**, Maykop State Technological University, Maykop, Russia
77. Prof. Dr. **Vlado N. Radić**, Faculty of Business Economics and Entrepreneurship, Belgrade, Serbia
78. Dr. **Dragan Radović**, Assoc. Prof., Faculty of entrepreneurial business and management of real estate of the "Union - Nikola Tesla" University, Belgrade, Serbia
79. Prof. Dr. **Dušan Regodić**, Faculty of Business and Law, "Union - Nikola Tesla" University, Belgrade, Serbia
80. Dr. **Bojan Ristić**, Prof., Information Technology School, Belgrade, Serbia
81. Dr. **Slobodan Ristić**, University Belgrade, Faculty of Organizational Sciences, Belgrade, Serbia
82. **Muzafer Saračević**, PhD, Assistant Prof., University in Novi Pazar, Novi Pazar, Serbia
83. Dr. **Drago Soldat**, Prof.v.s., Technical College, Zrenjanin, Serbia
84. Prof. Dr. **Dragan Dj. Soleša**, Faculty of Economics and Engineering Management, University Business Academy, Novi Sad, Serbia
85. Ing. **Katarina Stachova**, PhD, School of Economics and Management in Public Administration in Bratislava, Slovakia
86. **Jasmina Starc**, PhD, Assistant Prof., School of Business and Management Novo Mesto na Loko, Novo Mesto, Slovenia
87. **Bohdana Stepanenko-Lypovyk**, MA, Institute for Economics and Forecasting of the Ukrainian National Academy of Sciences, Kyiv, Ukraine
88. Ing. **Eva Sventekova** , PhD, Assoc. Prof.,Faculty of Special Engineering, University of Žilina, Žilina, Slovak Republic
89. Prof. Dr. **Radomir Šalić**, "Metropolitan" University in Belgrade, Belgrade, Serbia, and "Synergy" University in Bijeljina, Bijeljina, Bosnia and Herzegovina
90. Prof. Dr. **Dubravka Škunca**, Faculty of Business and Law, "Union - Nikola Tesla" University, Belgrade, Serbia
91. **Daniela Todorova**, PhD, Assoc. Prof., "Todor Kableshkov" University of Transport, Sofia, Bulgaria
92. Prof. Dr. **Miomir Todorović**, Faculty of Business and Law, "Union - Nikola Tesla" University, Belgrade, Serbia
93. Prof. Dr. **Zoran Todorović**, "Mediteran" University Podgorica – MTS "Montenegro Tourism School", Bar, Montenegro
94. Dr. **Janusz Tomaszewski**, Assoc. Prof., Eugeniusz Kwiatkowski University of administration and business, Gdynia, Poland
95. **David Ramiro Troitino**, Assoc. Prof., Tallinn University of Technology, Tallinn, Estonia
96. Dr. **Kristian Ujvary**, Ministry of Interior of the Slovak Republic, Bratislava, Slovak Republic
97. Dr. **Detelin Vasilev**, Assoc. Prof., "Todor Kableshkov" University of Transport, Sofia, Bulgaria
98. Prof. Dr. **Dragan Vučinić**, Higher school of modern business, Belgrade, Serbia
99. **Branko Vujatović**, Center for Applied Mathematics and Electronics - Belgrade, Serbia
100. Prof. **Yaroslav Vyklyuk**, DSc, Bukovinian University, Chernivtsi, Ukraine
101. Dr. hab. Eng. **Zenon Zamiar**, Assoc. Prof., Wroclaw University of Environmental and Life Sciences, Wroclaw, Poland
102. Prof. Dr. **Nada Živanović**, Faculty of Business and Law, "Union - Nikola Tesla" University, Belgrade, Serbia
103. Prof. Dr. **Dragan R. Životić**, Faculty of Management in Sport, "Alfa" University, Belgrade
104. **. . . You? . . . . . To apply, please, visit webpage:**
http://fbim.meste.org/FBIM_2_2019/Recenzenti_eng.html
click the button **Reviewer**, fill up the form, and return it to **meste@meste.org**

Recenzenti časopisa FBIM Transactions – po abecednom redu

1. dr **Svetlana Anđelić**, prof.s.s, Visoka škola strukovnih studija za informacione tehnologije – ITS, Beograd, Srbija
2. mr **Dragan Anucojić**, Fakultet za pravne i poslovne studije, Novi Sad, Srbija
3. dr **Dragutin Ž. Arsić**, v. prof., Poslovni i pravni fakultet, „Union – Nikola Tesla" Univerzitet u Beogradu, Beograd, Srbija
4. dr **Suat Askin**, docent, Adiyaman University, Adıyaman, Turska
5. **Olga Artemenko**, PhD, Bukovinski Univerzitet, Černivci, Ukrajina
6. Dr. **Daniel Badulescu**, Assoc. Prof., Faculty of Economic Sciences, University of Oradea, Romania
7. Prof. dr **Milan Beslać**, Visoka škola za poslovnu ekonomiju i preduzetništvo, Beograd, Srbija
8. dr **Mario Bogdanović**, dipl. oec., prof. psih., naučni saradnik, Ekonomski fakultet Sveučilišta u Splitu, Hrvatska
9. dr **Nikola Bračika**, v. prof., Visoka poslovna škola Čačak, Beograd, Srbija
10. mr **Nemanja Budimir**, Agencija za knjigovodstvene poslove „Budimir“, Banja Luka, Bosna i Hercegovina
11. CSc. **Anastasia Bugaenko**, "Ukrgasbank", Kijev, Ukrajina
12. prof. dr **Ana Čekerevac**, Univerzitet u Beogradu, Fakultet političkih nauka, Beograd, Srbija
13. prof. dr **Zoran Čekerevac**, Poslovni i pravni fakultet, „Union – Nikola Tesla" Univerzitet u Beogradu, Beograd, Srbija
14. **Sanja Čukić**, MA, Poslovni i pravni fakultet, „Union – Nikola Tesla" Univerzitet u Beogradu, Beograd, Srbija
15. dr **Dražen Ćućić**, Ekonomski fakultet u Osijeku, Osijek, Hrvatska
16. dr **Radmila Ćurčić**, docent, Poslovni i pravni fakultet, „Union – Nikola Tesla" Univerzitet u Beogradu, Beograd, Srbija
17. prof. dr **Sreten Ćuzović**, Ekonomski fakultet Univerziteta u Nišu, Niš, Srbija
18. prof. dr **Predrag Damnjanović**, Visoka poslovna škola Čačak, Beograd, Srbija
19. Prof. dr **Branko Davidović**, Visoka tehnička škola strukovnih studija, Kragujevac, Srbija
20. dr **Derya Dispinar**, docent, Istanbul University, Metallurgical and Materials Engineering, Avcilar, Istanbul, Turkey
21. prof. Ing. **Zdenek Dvorak**, PhD, Fakultet sigurnosnog inženjerstva Žilinskog Univerziteta u Žilini, Žilina, Slovačka
22. **Bela. Ju. Džamirze**, Ph.D., v. prof., Državni tehnološki univerzitet Majkop, Majkop, Rusija
23. prof. dr **Branislav Đorđević,** Emeritus, Beograd
24. prof. dr **Branko Đurović**, Medicinski fakultet Univerziteta u Beogradu, Beograd, Srbija
25. **Ljupčo Eftimov**, PhD, docent, Ekonomski fakultet Skopje, Skopje, Makedonija
26. Prof. **Valeriy Eudokymenko**, DrSc, Bukovinski državni univerzitet za finansije i ekonomiju, Černivtci, Ukraina
27. Ing. **Stanislav Filip**, PhD, docent, Visoka škola ekonomije i menadžmenta državne uprave u Bratislavi, Bratislava, Slovačka
28. **Jelena Fišić**, MA, "Pro-elektro" doo, Beograd, Srbija
29. **Milena Gajic-Stevanovic**, DMD, MSc.SM, PhD, Institut za javno zdravlje Srbije "Dr Milan Jovanović Batut", Beograd, Srbija
30. **Bogdan Gats**, Chernivtsy Trade and Economics Institute of the Kyiv National Trade and Economics University, Chernivtsy, Ukraine
31. prof. dr **Sonja T. Gegovska-Zajkova**, Ss Cyril and Methodius University, Faculty of Electrical Engineering and Information Technologies, Skopje, Macedonia
32. **Mariya P. Hristova**, PhD, Assoc. Prof., "Todor Kableshkov" University of Transport, Sofia, Bulgaria
33. dr **Miroljub Ivanović**, prof. s.s., Visoka škola strukovnih studija za obrazovanje vaspitača u Sremskoj Mitrovici, Sremska Mitrovica, Srbija
34. dr **Aleksandra M. Izgarjan**, v. prof., Filozofski fakultet, Univerzitet u Novom Sadu, Novi Sad, Srbija
35. dr **Miloje Jelić**, Preduzeće za proizvodnju “Klanica“d.o.o. Kraljevo

36. prof. dr **Zoran Jerotijević**, Poslovni i pravni fakultet „Union – Nikola Tesla“ Univerziteta u Beogradu
37. dr **Bisera S. Jevtić**, v. prof., Filozofski fakultet Univerziteta u Nišu, Niš
38. Prof. dr **Natalija Jolić**, Fakultet prometnih znanosti Sveučilišta u Zagrebu, Zagreb, Hrvatska
39. Prof. dr **Svetlana Kamberdieva**, Severnokavkaski institut za rudarstvo i metalurgiju (Državni tehnološki univerzitet), SKGMI (GTU), Vladikavkaz, Republika Severna Osetija – Alania, Rusija
40. prof. dr **Zvonko Kavran**, Fakultet prometnih znanosti Sveučilišta u Zagrebu, Zagreb, Hrvatska
41. Prof. **Antoaneta Kirova**, PhD, "Todor Kableškov" Univerzitet transporta, Sofija, Bugarska
42. Ing. **Jozef Klučka**, PhD, docent, Fakultet sigurnosnog inženjerstva Žilinskog Univerziteta u Žilini, Žilina, Slovačka
43. Prof. dr **Petar Kolev** "Todor Kableškov" Univerzitet transporta, Sofija, Bugarska
44. **Oksana Koshulko**, PhD, v. prof, Polotsk State University, Novopolotsk, Republic of Belarus
45. Prof. dr **Boris Krivokapić**, Poslovni i pravni fakultet, „Union – Nikola Tesla“ Univerzitet u Beogradu, Beograd, Srbija
46. dr **Evelin Krmac**, docent, Univerzitet u Ljubljani, Fakultet za pomorstvo i promet, Portorož, Slovenija
47. prof. dr **Adil Kurtić**, Ekonomski fakultet Univerziteta u Tuzli, Tuzla, BiH
48. dr **Aleksandar Lebl**, Iritel AD, Beograd, Srbija
49. Ing. **Maria Luskova**, PhD, Fakultet sigurnosnog inženjerstva Žilinskog Univerziteta u Žilini, Žilina, Slovačka
50. prof. dr **Branko Ž. Ljutić**, ovlašćeni revizor, Univerzitet Privredna akademija, Novi Sad, Srbija
51. CSc. **Elena S. Maltseva**, v. prof., Državni tehnološki univerzitet Majkop, Majkop, Rusija
52. dr **Dubravka Mandušić**, naučni saradnik, Agronomski fakultet, Zagreb, Hrvatska
53. **Milorad Markagić**, Univerzitet odbrane - Vojna akademija, Beograd, Srbija
54. dr **Željko Mateljak**, Sveučilište u Splitu, Ekonomski fakultet, Split, Hrvatska
55. prof. dr **Dobrivoje Mihailović**, Univerzitet u Beogradu, Fakultet organizacionih nauka, Beograd, Srbija
56. prof. dr **Božidar Mihajlović**, Visoka škola za poslovnu ekonimiju i preduzetništvo Beograd, Beograd, Srbija
57. dr **Ivo Mijoč**, docent, Ekonomski fakultet Sveučilišta u Osijeku, Osijek, Hrvatska
58. dr **Živanka Miladinović Bogavac**, Poslovni i pravni fakultet, „Union – Nikola Tesla" Univerzitet u Beogradu, Beograd, Srbija
59. dr **Zoran Lj. Milenković**, prof.s.s.,Visoka turistička škola strukovnih studija, Beograd, Srbija
60. dr **Živorad Milić**, Prizma, Kragujevac, Srbija
61. dr **Milorad Milošević**, prof.s.s., Visoka poslovna škola Čačak, Beograd, Srbija
62. dr **Aleksandar Miljković**, v. prof., Poslovni i pravni fakultet „Union – Nikola Tesla“ Univerziteta u Beogradu, Beograd i FORKUP, Novi Sad, Srbija
63. **Piotr Misztal**, PhD, Assoc. Prof., Jan Kochanowski University in Kielce, Kielce, Poland
64. prof. dr **Dragan M. Momirović**, Poslovni i pravni fakultet, „Union – Nikola Tesla" Univerzitet u Beogradu, Beograd, Srbija
65. dr **Saša Muminović**, Julon d.d. Ljubljana, Slovenija
66. prof. dr **Predrag M. Nemec**, Fakultet za menadžment u sportu, "Alfa" Univerzitet, Beograd, Srbija
67. prof. dr **Nevenka Nićin**, Poslovni i pravni fakultet, „Union – Nikola Tesla" Univerzitet u Beogradu, Beograd, Srbija
68. Ing. **Ladislav Novak**, PhD, docent, Fakultet sigurnosnog inženjerstva Žilinskog Univerziteta u Žilini, Žilina, Slovačka
69. dr **Srećko Novaković**, docent, Visoka poslovno tehnička škola Doboj, BiH i Visoka škola strukovnih studija za obrazovanje vaspitača i trenera, Subotica, Srbija
70. prof. dr **Saša Obradović**, Fakultet za ekonomiju i inženjerski menadžment, Novi Sad, Srbija
71. dr **Milorad Opsenica**, docent, Saobraćajni fakultet Internacionalnog univerziteta, Brčko-distrikt, BiH
72. CSc. **Tatiana Paladova**, v. prof., Državni tehnološki univerzitet Majkop, Majkop, Rusija
73. prof. dr **Yurij Vasylyovych Pasichnyk**, Čerkaski državni tehnološki univerzitet, Čerkasi, Ukrajina

74. prof. **Dinara Peskova**, PhD, Bashkir Academy of Public Administration and Management under the Auspices of the Republic of Bashkortostan, Ufa, Russia
75. Prof. Dr. Šemsudin Plojović, Internacionalni Univerzitet u Novom Pazaru, Novi Pazar, Srbija
76. prof. dr **Ljudmila Prigoda**, Državni tehnološki univerzitet u Majkopu, Majkop, Rusija
77. prof. dr **Vlado N. Radić**, Visoka škola za poslovnu ekonomiju i preduzetništvo, Beograd, Srbija
78. dr **Dragan Radović**, v. prof., Fakultet za menadžment Sremski Karlovci Univerziteta "Alfa" Beograd, Srbija
79. Prof. dr **Dušan Regodić**, Poslovni i pravni fakultet, „Union – Nikola Tesla" Univerzitet u Beogradu, Beograd, Srbija
80. Dr. **Bojan Ristić**, Prof., Visoka škola strukovnih studija za informacione tehnologije, Beograd, Serbia
81. dr **Slobodan Ristić**, Fakultet organizacionih nauka Univerziteta u Beogradu, Beograd, Srbija
82. **Muzafer Saračević**, MSc, Univerzitet u Novom Pazaru, Novi Pazar, Srbija
83. dr **Drago Soldat**, prof.s.s., Visoka tehnička škola strukovnih studija u Zrenjaninu, Zrenjanin, Srbija
84. prof. dr **Dragan Đ. Soleša**, Fakultet za ekonomiju i inženjerski menadžment, Univerzitet Privredna akademija, Novi Sad, Srbija
85. Ing. **Katarina Stachova**, PhD, Visoka škola ekonomije i menadžmenta državne uprave u Bratislavi, Bratislava, Slovačka
86. **Jasmina Starc**, PhD, docent, Visoka šola za upravljanje in poslovanje Novo mesto, Novo Mesto, Slovenija
87. **Bohdana Stepanenko-Lypovyk**, MA, istraživač saradnik, Institut za ekonomiku i prognoziranje Ukrajinske nacionalne akademije nauka, Kyiv, Ukrajina
88. Ing. **Eva Sventekova**, PhD, docent, Fakultet sigurnosnog inženjerstva Žilinskog Univerziteta u Žilini, Žilina, Slovačka
89. prof. dr **Radomir Šalić**, Univerzitet "Metropolitan" u Beogradu, Beograd, Srbija i Univerzitet "Sinergija" Bijeljina, Bijeljina, Bosna i Hercegovina
90. dr **Dubravka Škunca**, vanredni profesor, Poslovni i pravni fakultet "Union - Nikola Tesla" Univerziteta u Beogradu, Beograd, Srbija
91. prof. **Daniela Todorova**, PhD, "Todor Kableškov" Univerzitet transporta, Sofija, Bugarska
92. Prof. dr **Miomir Todorović**, Poslovni i pravni fakultet, „Union – Nikola Tesla" Univerzitet u Beogradu, Beograd, Srbija
93. prof. dr **Zoran Todorović**, Univerzitet Mediteran Podgorica, Fakultet za turizam Bar – MTS "Montenegro Tourism School", Bar Crna Gora
94. dr **Janusz Tomaszewski**, v. prof., Eugeniusz Kwiatkowski Univerzitet administracije i biznisa, Gdynia, Poljska
95. **David Ramiro Troitino**, PhD, Assoc. Prof., Tallinn University of Technology, Tallinn, Estonia
96. dr **Kristian Ujvary**, Ministarstvo unutrašnjih poslova Republike Slovačke, Bratislava, Slovačka
97. dr **Detelin Vasilev**, docent, "Todor Kableškov" Univerzitet transporta, Sofija, Bugarska
98. prof. dr **Dragan Vučinić**, Visoka škola modernog biznisa, Beograd, Srbija
99. **Branko Vujatović**, MSc, Centar za primenjenu matematiku i elektroniku - Beograd, GŠ VS, Beograd, Srbija
100. prof. dr **Yaroslav Vyklyuk**, Bukovinski Univerzitet, Černivci, Ukrajina
101. dr hab. ing. **Zenon Zamiar**, v. prof., Univerzitet prirodnih nauka i ekologije u Vroclavu, Wroclaw, Poljska
102. prof. dr **Nada Živanović**, Poslovni i pravni fakultet, „Union – Nikola Tesla" Univerzitet u Beogradu, Beograd, Srbija
103. prof. dr **Dragan R. Životić**, Fakultet za menadžment u sportu, "Alfa" Univerzitet, Beograd, Srbija
104. **. . . Vi? . . . . Da biste se prijavili, molimo vas da posetite veb stranicu:**
http://fbim.meste.org/FBIM_2_2019/Recenzenti_srb.html
kliknite dugme **Izjava recenzenta,** popunite formular i vratite ga popunjenog na adresu meste@meste.org

Editorial procedure

Peer review

All manuscripts submitted to FBIM Transactions journal will be reviewed by up to three experienced reviewers. At least two of reviewers must recommend the article for publication. The selection of reviewers for each of submitted works will be carried out by the editor-in-chief. In cases where the editor-in-chief is the author or coauthor, for submitted work reviewers will be selected by the deputy chief editor or one of the members of the Scientific Committee. The names of the reviewers will be published in the journal in the special list without specifying the titles of the papers that were reviewed. For the purpose of the reviewing, authors are requested to submit all documents at once at the time of their submission with the following structure:

— A title page, which includes:
  - The title of the article
  - The name(s) of the author(s) with the concise and informative title(s)
  - The affiliation(s) and address(es) of the author(s)
  - The e-mail address, telephone and fax numbers of the corresponding author
  - Abstract (The abstract should be in the range of 150 to 250 words and should not contain any undefined abbreviations or unspecified references.
  - Keywords (4 to 6 keywords which can be used for indexing purposes)
— A blinded manuscript without any author names and affiliations in the text or on the title page. Self-identifying citations and references in the article text should either be avoided or left blank.

Authors must honor peer review comments in order of the manuscript improvement. All changes must be elaborated, and improved manuscript should be submitted to the Editor-In-Chief. Of course, authors can argue peer review comments by giving reasons/references to counter peer review comments. After receiving of resubmitted manuscript Editor-in-Chief will choose whether the manuscript will be published or sent to the old/new reviewers.

Manuscript submission

FBIM JOURNAL accepts only manuscript use the template MEST_Template.docx from the web address: http://www.meste.org/fbim/documents/FBIM_Template.docx with un-modified format only.

Submission of a manuscript implies that corresponding author responsible declares:

— that the submitted article is an original work and has not been published before;
— that it is not under consideration for publication anywhere else;
— that its publication has been approved by all co-authors, if any; and
— that there are no any legal obstacles for the article publishing.

The publisher will not be held legally responsible should there be any claims for compensation.

Permissions

Authors, who wish to insert figures, tables, or passages of text that have previously been published elsewhere, are required to obtain permission from the copyright owner(s), and to attach the evidence that such permission has been granted when submitting their papers. Any material received without such evidence will be considered as authors'.

Submission

Authors should submit their manuscripts by e-mail to the address: mest.submissions@meste.org .

E-mail should contain the following items:

1. Declaration and copyright transfer, which should include that:
   - the submitted article is an original work and has not been published before;
   - the submitted article is not under consideration for publication anywhere else;(s)
   - the submitted article publication has been approved by all co-authors, if any; and
   - there are not any legal obstacles for the article publishing.
2. Title Page, which should include:
   - Full title of the article (no more than 12 words)
   - The name(s) of the author(s)
   - The affiliation(s) and address(es) of the author(s)
   - The short title (a concise and informative title, no more than 50 characters with spaces)
   - The e-mail address, telephone and fax numbers of the corresponding author
   - **Abstract** (The abstract, paper summary, should be in the range of 150 to 200 words, and should not contain any undefined abbreviations or unspecified references. Summary needs to hold all essential facts of the work, as the purpose of work, used methods, basic facts and specific data if necessary. It must contain review of underlined data, ideas and conclusions from text, as well as recommendation for a group of readers that might be interested in the subject matter. Summary has no quoted references.)
   - **Keywords** (4 to 6 keywords which can be used for indexing purposes need to be placed below the text)
3. **Manuscript,** which should be prepared as a camera ready, but without any data that can make a connection between author and the submitted article, such as: author(s) name(s) and affiliation(s). Author(s) should avoid self-identifying citations and references. Manuscripts should be submitted in MS Word, in accordance with the template MEST_Template.docx, which can be downloaded from MEST_Template.docx (105 kB). Manuscripts are not limited in length, but precise and concise writing should result with the article length of 8 to 14 pages, prepared according the proposed FBIM JOURNALtemplate.

   Authors have to:
   - use a normal, plain 10-point Arial font for text;
   - Italics for emphasis;
   - use the automatic page numbering function to number the pages;
   - use tab stops or other commands for indents, not the space bar;
   - use the table function, not spreadsheets, to make tables;
   - use the equation editor or MathType for equations;
   - save their manuscript in .docx format (Word 2007 or higher);
   - use the decimal system of headings with no more than three levels;
   - define abbreviations at their first mention and use them consistently thereafter;
   - avoid footnotes, but, if necessary, footnotes can be used to give additional information about some term(s). Footnotes should not be used to referee citation, and they should never include the bibliographic details of a reference. Footnotes have not to contain figures or tables. Footnotes to the text are numbered consecutively, automatically by text editor. Endnotes are not intended for use in the article.
   - avoid the use of "the above table" or "the figure below";
   - use SI system of units as preferable.

References – Works Cited (New up-to-date information should be used and referenced. References should be cited in the text by name and year in parentheses, according to the APA Sixth Edition.

Citation should be made using *References --> Citations & Bibliography* in MS Word®©, and we strongly recommend that the ***Work Cited*** list should be made automatically using MS Word®© option: *References --> Citations & Bibliography --> Bibliography --> Works Cited*. More detailed explanation can be found in the tutorial at: http://office.microsoft.com/en-us/word-help/create-a-bibliography-HA010067492.aspx .

4. **Acknowledgments** (All acknowledgments, if exist, should be placed in a separate page after the **Works Cited** list. The names of funding organizations or people should be written in full, unambiguously.)

5. **Tables** (All tables should be sent as the separate files in .docx or .xlsx format.)
   - All table files must be named with "Table" and the table number, e.g., Table 1.
   - All attached tables have to be numbered using Arabic numerals, and for each table, a table caption (title explaining the components of the table) should be provided.
   - Tables should always be lined in text in consecutive numerical order.
   - Previously published material should be identified by giving a reference to the original source. The reference should be placed at the end of the table caption.
   - Footnotes to tables (for significance values and other statistical data) should be indicated by asterisks and placed beneath the table body.

6. **Photographs, pictures, clip arts, charts and diagrams** should be numbered and sent as the separate files in the .JPEG, .GIF, .TIFF or .PNG format in the highest quality. MS Office files are also acceptable, but font sizes and the size of the figure must suite to the size in the published article. The quality of submitted material directly influences to the quality of published work, so the FBIM JOURNALmay require of authors to submit figures of the higher quality. All figure files must be named with "Fig" and the figure number, e.g., Fig1.

   Remarks:
   - All figures can be made as colored and will be published free of charge as colored in the online publication.
   - Paper version of the document will be published as the gray scale document (black-white) so authors are kindly asked to check how their contributions look like printed on black-white printers.
   - All lines should be at least 0.1 mm (0.3 pts) tick.
   - Scanned figure should be scanned with a minimum resolution of 1200 dpi.
   - For lettering, it is best to use sans serif fonts Helvetica or Arial.
   - Variance of font size within an illustration should be minimal (the sizes of characters should be 2–3 mm or 8-12 pts).
   - To increase clarity author(s) should avoid effects such as shading, outline letters, etc.
   - Titles and captions should not be included within illustrations.

FBIM Journal does not provide English language support

Manuscripts that are accepted for publication will be checked by MESTE lectors for spelling and formal style. This may not be sufficient if English is not authors' native language. In most cases, these

situations require substantial editing. FBIM JOURNAL suggests that all manuscripts are edited by a native speaker prior to submission. A clear and concise language will help editors and reviewers to concentrate on the scientific content of the submitted paper. Correct language may allow faster and smoother review process.

Authors are not obliged to use a professional editing service. Also, the use of such service is not a guarantee of acceptance for publication.

Copyright transfer

By submitting a paper, authors, transfer copyright of the article to the Publisher (or, authors grant the publication and dissemination rights exclusively to the Publisher). This ensures the widest possible protection and dissemination of information under copyright laws.

Under this copyright transfer authors can:

- use part of the work as a basis for a future publication
- send copies of the work to colleagues
- present the work at conference or meeting and give copies of the work to attendees
- use a different or extended version of the work for a future publication
- make copies of the work for personal use and educational use
- self-archive the work in an institutional repository
- use graphs, charts, and statistical data for a future publication
- post the work on a laboratory or institutional website
- use the work for educational use such as lecture notes or study guides
- deposit supplemental data from the work in an institutional or subject repository
- place a copy of the work on electronic reserves or use for student course-packs
- include the work in future derivative works
- make an oral presentation of the work
- include the work in a dissertation or thesis
- use the work in a compilation of works or collected works
- expand the work into a book form or book chapter
- retain patent and trademark rights of processes or procedures contained in the work

Proofreading

After the decision that the paper will be published, processed article will be returned to the author for an approval. The aim of the approval is that author checks if some incorrectness appeared during the processing. Also, author checks the completeness and accuracy of the text, tables and figures. Any change must be noted and returned to MEST. After online publication, further changes can be made only in the form of an Erratum, which will be hyperlinked to the article. All changes must be specified and returned to MEST. Any substantial change can be done only with the approval of the Editor.

Procedura publikovanja

Recenzija

Svi prijavljeni radovi, u slučaju da su tematski i po veličini prihvatljivi za publikovanje u FBIM Transactions, biće recenzirani po principu "peer" recenzije od strane dva ili tri recenzenta. Najmanje dva recenzenta moraju da preporuče članak za publikovanje. Izbor recenzenata za svaki od prijavljenih radova vrši Glavni i odgovorni urednik. U slučajevima kada je Glavni i odgovorni urednik autor ili koator prijavljenog rada, izbor recenzenata vrši zamenik glavnog urednika ili jedan od članova Naučnog odbora. Imena recenzenata biće publikovana u časopisu u okviru posebne liste bez navođenja naziva radova koje su recenzirali. Autori treba da postupe u skladu sa preporukama recenzenata kako bi poboljšali svoj članak. Sve izmene u radu treba da budu obeležene i korigovani rad (sa obeleženim izmenama) treba dostaviti Uredništvu povratnim e-mejlom. Naravno, autori imaju pravo i da ne prihvate preporuke recenzenata ako smatraju da za to imaju valjani razlog. Uredništvo će odlučiti da li će rad posle korekcije biti publikovan, ili upućen starim ili drugim recenzentima na ponovnu recenziju.

Prijavljivanje radova

FBIM Transactions prihvata samo radove koji su urađeni u skladu sa modelima koje je propisao. Autor zadužen za korespodenciju treba kompletan rad da dostavi jednim e-mejlom, sa prilozima, na adresu: **fbim.submissions@meste.org**. Molimo da pogledate stranicu: **Prijavljivanje rada**. Zbog potreba recenzije od autora se traži da prijavljuju svoje radove jednom i kompletno sa svim potrebnim prilozima, prema sledećem redosledu:

1. Izjavu o originalnosti rada i o prenosu autorskih prava na izdavača. Izjava se može pruzeti na adresi: http://fbim.meste.org/FBIM_1_2019/documents/Declaration_srb_docx.docx
2. Naslovnu stranicu, koja se može preuzeti na adresi: http://fbim.meste.org/FBIM_1_2019/documents/FBIM_Naslovna_stranica.docx
   a koja treba da sadrži:
   - Pun naziv članka (ne više od 12 reči)
   - Ime(na) i prezime(na) autora sa titulama
   - Kratak naziv rada (koncizan i informativan naslov, ne više od 50 karaktera sa razmacima)
   - Naziv i adresu(e) institucije(a) u kojoj/kojima je/su autor(i) zaposlen(i)
   - Ime autora zaduženog za korespodenciju sa FBIM Transactions
   - E-mail adresu i broj telefona autora koji je zadužen za korespodenciju sa FBIM
   - Apstrakte - Apstrakti, rezimei rada, prvo na srpskom (ili srodnom jeziku), a zatim i na engleskom jeziku, treba da budu u obimu od 150 do 250 reči, i ne bi trebalo da sadrži nikakve nedefinisane skraćenice ili nespecificirane reference. Apstrakt treba da sadrži sve bitne činjenice o radu, kao i cilj rada, korišćene metode, osnovne činjenice i, eventualno, konkretne podatke ako je potrebno. Apstrakt mora da sadrži pregled najvažnijih podataka, ideja i zaključaka iz teksta, kao i preporuku za grupu čitalaca koji bi mogli biti zainteresovani za tematiku koju članak obrađuje. U apstraktu se ne navode citirane reference.
   - Ključne reči - četiri do deset ključnih reči koje se mogu koristiti za indeksiranje, treba postaviti ispod apstrakata, prvo na srpskom jeziku (ili srodnim jezicima), a potom na engleskom jeziku.)

3. Manuskript, koji treba da bude pripremljen kao „spreman za kopiranje“, po modelu koji se može pruzeti na web adresi:
   http://fbim.meste.org/FBIM_2_2019/Instructions_for_authors_srb.html
   klikom na FBIM_Template.docx (105 KB), ali bez podataka koji mogu da naprave vezu između autora i dostavljenog članka, kao što su: ime (imena) autora i mesto zaposlenja. Autor(i) treba da izbegava/ju samo-identifikujućih citata i referenci. Rukopisi se dostavljaju u MS Wordu, u skladu sa šablona FBIM.docx, koji se može preuzeti sa FBIM_Template.dock (83 KB). Rukopisi nisu ograničeni dužinom, ali precizan i koncizan način pisanja treba da rezultira člankom dužine od 8 do 14 stranica, pripremljeno prema predloženom FBIM modelu.

   Autori treba da koriste:
   - normal, čist 10-point Arial font za tekst;
   - *Italik, kurziv* za naglašavanje;
   - automatsko numerisanje stranica za numerisanje stranica;
   - tabulator ili druge komande za uvlačenje teksta, a da za uvlačenje teksta ne koriste razmaknicu;
   - funkciju tabele (Insert > Table) za kreiranje tabela i da ne unose tabele iz programa za tabelarnu obradu podataka;
   - „Equation editor“ za jednačine;
   - .docx format za konačnu verziju manuskripta (Word 2007 ili noviji);
   - decimalni sIstem za označavanje naslova i podnaslova sa ne više od tri nivoa;
   - SI sistem jedinica.

   Autori treba da:
   - definišu skraćenice odmah, pri njihovom prvom pojavljivanju u tekstu, a zatim da ih dosledno primenjuju u tekstu, u istom značenju;
   - izbegavaju fusnote, ali, ako je neophodno, fusnote se mogu koristiti za davanje dodatnih informacija o pojedinim pojmovima. Fusnote se ne koriste za citiranje i ne treba da sadrže bibliografske podatke o referenci. Fusnote ne treba da sadrže slike i/ili tabele. Fusnote se u tekstu obeležavaju brojevima, automatski tekst editorom. Endnote nisu predviđene za upotrebu u članku;
   - izbegavaju upotrebu fraza "iz gornje tabele" ili "na donjoj slici" i slično;
   - brojeve manje od 10 pišu **slovima.**

   Reference – Citirani radovi (Treba koristiti, pre svega, nove, aktuelne, informacije a citirane informacije treba referencirati. Citiranu literaturu treba navesti u tekstu u zagradi u obliku prezime i godina (prezime, godina), prema APA šesto izdanje.

   Za citiranje treba koristiti alate tekst editora, npr. *References → Citations & Bibliography* u slučaju korišćenja programa MS Word®©, a za formiranje konačne liste citiranih radova preporučujemo upotrebu alata tekst editora, npr, u slučaju korišćenja programa MS Word®©: *References → Citations & Bibliography → Bibliography → Works Cited* .

   Detaljnije uputstvo o primeni ove opcije nalazi se na:
   http://office.microsoft.com/en-us/word-help/create-a-bibliography-HA010067492.aspx

4. **Zahvalnice** - Sve zahvalnice, ako postoje, treba da budu prikazane na posebnoj stranici, posle lista Citirani radovi. Imena ljudi ili organizacija treba da budu pisana u celosti, jednoznačno.

5. **Tabele** - Sve tabele treba dostaviti kao posebne fajlove u .docx ili .xlsx formatu.

- Svi fajlovi moraju biti imenovani sa "Tabela_" uz dodavanje broja tabele, na primer: Tabela_1; Tabela_2 itd.
- Sve priložene tabele moraju biti numerisane arapskim brojevima, i za svaku tabelu treba dati naslov (naslov objašnjava sadržaj tabele).
- Tabele u tekstu moraju da budu postavljene po redosledu prema rastućem broju tabele.
- Prethodno publikovani materijal treba identifikovati davanjem odgovarajuće reference na originalni izvor. Reference treba postaviti na kraju naziva tabele.
- Fusnote za delove tabele (za značajne vrednosti i statističke podatke) treba označiti zvezdicama i postaviti **odmah ispod tela tabele.**

6. **Fotografije, slike, grafikoni i dijagrami** treba da budu numerisani i poslati kao posebni fajlovi u JPEG formatu, GIF, TIFF ili PNG formatu u najvišem kvalitetu. MS Office datoteke su takođe prihvatljive, ali veličina korišćenog fonta za prikazivanje teksta na slici mora da odgovara veličini ostalog teksta u objavljenom članku. Kvalitet dostavljenog materijala direktno utiče na kvalitet objavljenih radova, tako da FBIM može zahtevati od autora da dostave slike, grafikone i dijagrame višeg kvaliteta. Sve datoteke sa slikama moraju biti imenovane sa "Slika" i broj, na primer, Slika_1, Slika_2 itd.
   - Sve slike mogu biti rađene u koloru i kao takve biće publikovane u elektronskoj, onlajn, verziji časopisa FPIB Transactions.
   - Štampana verzija časopisa biće štampana kao crno-bela, pa se autori umoljavaju da provere kako njihovi radovi izgledaju štampani na laserkom, crno-belom štampaču.
   - Sve linije moraju da imaju debljinu od najmanje 0,1 mm (0,3 pt).
   - Skenirane slike treba da budu skenirane u rezoluciji od najmanje 600dpi, a preporučuje se rezolucija od 1200 dpi.
   - Kao font za natpise slika koristiti Calibri ili Arial kurzivom (Italik).
   - Varijacija veličine fonta unutar ilustracija treba da bude minimalna (razlika veličine slova treba da bude unutar 2 – 3 mm ili 6 – 9 pt).
   - U cilju povećanja jasnosti, autor(i) treba da izbegavaju efekte kao što su senčenje, prikazivanje slova kao kontura itd.
   - Naslovi i nazivi **ne treba da budu prikazani u ilustracijama.**

FBIM Transactions ne obezbeđuje usluge prevođenja na engleski jezik

Radovi objavljeni na srpskom (ili srodnim jezicima), pored Rezimea, sadrže i apstrakt na engleskom jeziku. Od autora se očekuje da priloženi apstrakt bude kvalitetno urađen. FBIM Transactions od autora ne zahteva da dostavljaju profesionalno preveden tekst, ali preporučuje da tekst bude preveden od strane osobe kojoj je engleski jezik prirodni jezik izražavanja. Jezički korektno napisan rad može da omogući bržu i jednostavniju recenziju rada i njegovo brže publikovanje.

Saglasnosti i odobrenja

Autori koji žele da u svoj rad umetnu slike, tabele, grafikone ili pasuse teksta koji su ranije već objavljivani na nekom drugom mestu (časopis, zbornik radova itd.), ukoliko ne raspolaže autorskim pravom na njih, mora da obezbedi i uz prijavu rada dostavi saglasnost za publikovanje od vlasnika autorskog prava na dati materijal. Svaki materijal dostavljen u FBIM Transactions, bez takve saglasnosti, smatraće se autorovim delom.

Prenos autorskih prava

Prijavljivanjem rada, autor/i prenosi/e sva autorska prava na članak izdavaču, FBIM Transactions. Drugim rečima, autor/i odobrava/ju ekskluzivno izdavaču da publikuje i distribuira prihvaćeni rad. Na

ovaj način se obezbeđuje maksimalna zaštita i diseminacija informacija prema Zakonu o autorskim pravima.

U okviru ovog prenosa autorskog prava autori mogu:

- upotrebiti rad kao osnovu za buduće publikacije
- slati kopije rada kolegama
- predstavljati rad na konferencijama ili skupovima i davati kopije rada prisutnima
- koristiti drugu ili proširenu verziju rada za buduće publikacije
- napraviti kopije rada za ličnu upotrebu i obrazovne svrhe
- arhivirati rad u institucionalnom repozitorijumu
- koristiti grafikone, dijagrame, i statističke podatke za buduće publikacije
- postaviti rad na laboratorijskom ili institucionalnom sajtu
- koristiti rad za obrazovne svrhe
- postaviti dopunske materijale iz rada u institucionalnom repozitorijumu
- postaviti kopiju rada u elektronske arhive ili koristiti ga kao materijal koji će dati studentima kao materijal za učenje
- uključiti rad u buduće radove, disertacije ili teze
- usmeno prezentovati rad
- koristiti rad u kompilacijama radova ili u okviru sabranih dela
- proširiti rad do nivoa poglavlja knjige ili knjige
- zadržati patentni prava za procese i procedure sadržane u radu

Korektura – Proofreading

Posle donošenja odluke da će članak biti publikovan FBIM Transaction će dostaviti autoru zaduženom za korespodenciju obrađeni članak, kako bi autor mogao da prekontroliše da li je pri obradi članka došlo do nekih nepravilnosti. Takođe, autor zadužen za korespodenciju treba da proveri tačnost i kompletnost teksta, tabela i slika. Svaka eventualno uočena nepravilnost mora da bude notirana i dostavljena Uredništvu. Svaka značajnija promena može biti učinjena isključivo uz saglasnost Urednika. Posle onlajn publikovanja izmene rada nisu moguće, osim u obliku Errata - Spisak štamparskih grešaka.

Before manuscript submission, please, check if you prepared all your attachments.

http://fbim.meste.org/FBIM_1_2019/Submit_a_manuscript.html

Submission Checklist:

☐ **The declaration and copyright transfer that:**

- the submitted article is an original work and has not been published before;
- the submitted article is not under consideration for publication anywhere else;
- the submitted article publication has been approved by all co-authors, if any; and
- there are no any legal obstacles for the article publishing.

☐ **Title Page, which should include:**

- Full title of the article (no more than 12 words)
- The name(s) of the author(s)
- The affiliation(s) and address(es) of the author(s)
- The e-mail address, telephone and fax numbers of the corresponding author
- The short title (a concise and informative title, no more than 50 characters with spaces)
- Abstract
- Keywords

☐ **Manuscript,** prepared as a camera ready, but without any data that can make a connection between author and the submitted article.

☐ **Acknowledgements** (if any)

☐ **All tables** – Each table has to be saved as a separated .docx file and attached to the e-mail. All table files must be named with "Table_" and the table number, e.g., Table_1, Table_2 etc.

☐ **All figures –** Each figure has to be saved as a separated .jpg, .gif, .tif or .png file and attached to the e-mail. All graphic files must be named with "Figure_" and the table number, e.g., Figure_1, Figure_2 etc.

If everything is checked, you can send your article to us to the address:

fbim.submissions@meste.org

Pre prijavljivanja svog rada, molimo vas da proverite da li ste pripremili sve priloge.

http://fbim.meste.org/FBIM_1_2019/Submit_a_manuscript_srb.html

Ček lista dokumenata koje treba dostaviti:

☐ **Izjava** o originalnosti rada i o prenosu autorskih prava na izdavača da:
- je priloženi rad originalan i da nije ranije publikovan;
- priloženi rad nije u razmatranju za publikovanje ni u jednom drugom časopisu;
- za publikovanje rada postoji saglasnost svih koautora, ako ih ima;
- nema zakonskih i bilo kojih drugih prepreka da rad bude publikovan.

Na veb stranici http://fbim.meste.org/FBIM_2_2019/Submit_a_manuscript_srb.html kliknite na jedno od dugmadi ***Declaration*** da biste preuzeli model izjave u zavisnosti od željenog formata dokumenta.

☐ **Naslovna stranica**, koja treba da sadrži:
- Pun naziv članka (ne više od 12 reči)
- Ime i prezime autora, odn. imena i prezimena autora ako ih ima više
- Mesto zaposlenja autora i adresa/e poslodavca/poslodavaca
- E-mail edresa i broj telefona autora zaduženog za korespodenciju sa FBIM Transactions
- Kratak naziv rada (sažet i informativan naslov, ne duži od 50 karaktera sa razmacima)
- Rezime i Abstract
- Ključne reči i Keywords

Na veb stranici http://fbim.meste.org/FBIM_2_2019/Submit_a_manuscript_srb.html kliknite na jedno od dugmadi Title page da preuzmete model za naslovnu stranicu.

☐ **Manuscript**, pripremljen za publikovanje, ali bez podataka koji mogu da autora/e dovedu u vezu sa radom koji prijavljuju. Kliknite na jedno od dugmadi Template da preuzmete model po kome treba formatirati rad.

☐ **Zahvalnice** (ako postoji potreba za njima)

☐ **Sve tabele** – Svaka od tabela treba da bude sačuvana kao poseban *.docx* ili *.doc* fajl i pridodata e-mejl poruci kojom se prijavljuje rad. Svi fajlovi sa tabelama moraju da budu označeni kao "Tabela_" sa rednim brojem tabele u radu, npr. Tabela_1, Tabela_2 itd.

☐ **Sve slike i ostali grafički prilozi** - Sve slike i drugi grafički prikazi treba da budu priloženi kao posebni fajlovi (*.jpg, .gif, .tif* ili *.png*. Svi grafički fajlovi moraju da budu označeni sa "Slika_" i pridodatim rednim brojem slike u radu, npr., Slika_1, Slika_2 itd.

Ako je svaka kućica čekirana, vaš rad je spreman za prijavljivanje na adresu:

fbim.submissions@meste.org

Review FBIM- M_…

PART A:

SECTION I

Name and surname of reviewer	
ORCID Identifier of the reviewer	https://orcid.org/____-____-____-____
E-Mail	
Phone	
Manuscript No.	**M_...**
Title	
Author / Authors	-
Sent to reviewer	
The expected date of receipt of reviews	

PART B: Reviewer only

SECTION II: Comments of manuscript

General comment	
Introduction	
Methodology	
Results	
Discussion	
Findings	

SECTION II (continue) (Click on the box next to the appropriate answer and check in one of the categories, or delete unnecessary in the event that you are unable to check the desired box)

Bibliography / References	**Literature is relevant** **Citation is in accordance with the requirements**	**Yes** ☐ **Yes** ☐	**No** ☐ **No** ☐
Figures	**Figures are appropriate**	**Yes** ☐	**No** ☐
Tables:	**Tables are appropriate**	**Yes** ☐	**No** ☐

SECTION III
Please rate it from one of: *(1 = Excellent) (2 = Good) (3 = Correct) (4 = Poor)*

Originality	
Scientific contribution	
Technical quality of the article	
Clarity of presentation	
Depth of study	

SECTION IV – Recommendations for publication:
(Please select one of the options with an *X*)

Accept the article "as it is"	
The work requires minor repairs	
The work requires small-scale changes	
The work requires large-scale changes	
The work is good but it is not for publishing in the MEST Journal. It could be published in another journal, for example (make the proposal)	
Work has to be rejected because (please specify particular reason)	

SECTION V: Additional comments

This part of the review is confidential and will be available only to editors of the FBIM Transactions. If you have any special comment to the editors you can enter it here.

Recenzija FBIM-

DEO A

SEKCIJA I

Ime recenzenta	
ORCID identifikator recenzenta	https://orcid.org/____-____-____-____
E-mail	
Manuscript br.	**M_...**
Naslov rada	
Autor/Autori	-
Datum slanja recenzentu	
Očekivani datum prijema recenzije	

DEO B: Samo recenzent

SEKCIJA II: Komentari manuskripta

Opšti komentar	
Uvod	
Metodologija	
Rezultati	
Diskusija	
Zaključak	

SEKCIJA II (Nastavak) (Kliknite na kvadratić uz odgovarajući odgovor i čekirajte po jednu od ponuđenih opcija, ili obrišite suvišno u slučaju da niste u mogućnosti da čekirate željeni kvadratić)

Bibliografija/Reference	**Literatura je relevantna**	**Da ☐**	**Ne ☐**
	Citiranje je u skladu sa zahtevima	**Da ☐**	**Ne ☐**
Slike	**Slike su odgovarajuće**	**Da ☐**	**Ne ☐**
Tabele:	**Tabele odgovarajuće**	**Da ☐**	**Ne ☐**

SEKCIJA III

Molimo ocenite jednom od ocena: ***(1 =Odličan) (2 = Dobar) (3 = Korektno) (4 = Slabo)***

Originalnost	
Naučni doprinos	
Tehnička obrada članka	
Jasnoća izlaganja	
Dubina istraživanja:	

SEKCIJA IV – Preporuka za publikovanje: (Molimo vas da označite jednu od opcija sa *X*)

Prihvatiti rad ovakav kakav je:	
Rad zahteva sitnije popravke:	
Rad zahteva izmene manjeg obima:	
Rad zahteva izmene velikog obima:	
Rad je dobar ali nije za objavljivanje u FBIM Transactions. Mogao bi se publikovati u nekom drugom časopisu, npr. (dati predlog):	
Rad se odbija zbog (Molimo navesti konkretan razlog):	

SEKCIJA V: Dodatni komentari

Ovaj deo recenzije je poverljiv i biće dostupan samo uredništvu FBIM Transactions-a. Ukoliko imate neke posebne napomene Uredništvu možete ih upisati ovde.

Templates

All templates for the FBIM Transactions articles preparing and submission can be found at the web address:
http://fbim.meste.org/FBIM_2_2019/Submit_a_manuscript.html

Šabloni

Svi formulari za pripremu i prijavljivanje radova časopisu FBIM Journal mogu se preuzeti sa veb adrese:
http://fbim.meste.org/FBIM_2_2019/Submit_a_manuscript_srb.html

4D414E4147454D454E54

454455434154494F4E

534349454E4345

544543484E4F4C4F47

45434F4E4F4D494353