



ISSN 2334-718X

ISSN 2334-704X (Online)

DOI 10.12709/issn.2334-704X

FBIM Transactions

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

**Edited by
Zoran Čekerevac**

MESTE

Year VII Vol. 7

No. 1

April 2019

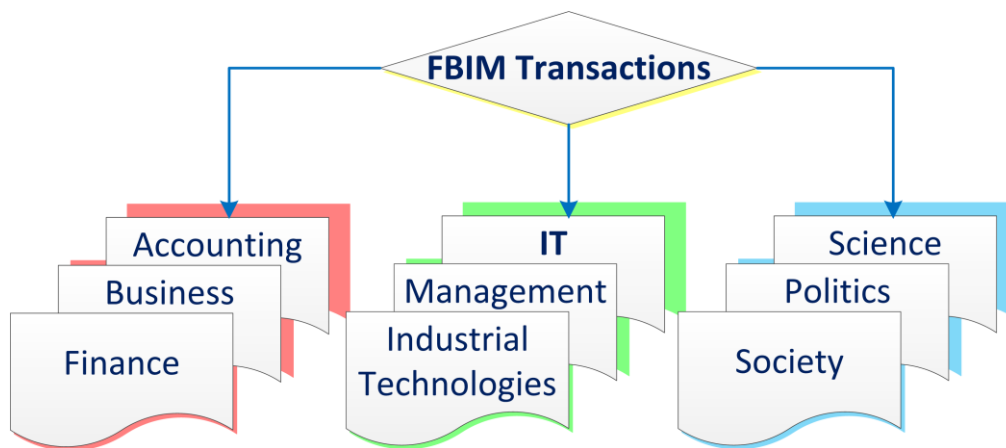
Intentionally left blank – Namerno ostavljeno prazno



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

This issue:
DOI: 10.12709/fbim.07.07.01.00

FBIM Transactions



Edited by
Zoran Čekerevac

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. 1 (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.07.07.01.00**

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

Editorial staff – Production:

Prof. Dr. **Zoran Čekerevac**, Editor-in-chief, Faculty of Business and Law, Belgrade, Serbia
Prof. Dr. **Milija Bogavac**, Deputy chief editor, Faculty of Business and Law, Belgrade, Serbia
Slavko Zdravković, MSc, Editor, SZ & Assoc.- Toronto, Canada
Damjan Čekerevac, MSc, Technical editor, University of Coimbra, Coimbra, Portugal
Prof. Dr. **Ljiljana Jovković**, Proofreader, Faculty of Business and Law, Belgrade, Serbia
Sanja Čukić, MA, Lecturer, Proofreader, Faculty of Business and Law, Belgrade, Serbia
Milanka Bogavac, MA, Manager, Faculty of Business and Law, Belgrade, Serbia

Editorial board – Scientific Board:

Prof. Dr. **Milija Bogavac**, Faculty of Business and Law of the "Union - Nikola Tesla" University in Belgrade, Serbia
Prof. Dr. **Ana Čekerevac**, University of Belgrade Faculty of Political Sciences, Serbia
Prof. Dr. **Zoran Čekerevac**, Faculty of Business and Law of the "Union - Nikola Tesla" University in Belgrade, Serbia
Prof. Ing. **Zdenek Dvorak**, PhD, Faculty of Special Engineering of the University of Žilina, Žilina, Slovakia
Prof. Dr. Sc. **Zvonko Kavran**, Faculty of Transport and Traffic Engineering, University of Zagreb, Croatia
Prof. Dr. **Petar Kolev**, "Todor Kableshev" University of Transport, Sofia, Bulgaria
Prof. **Iouri Nikolski**, PhD, National University "Lvivska Polytechnica", Lviv, Ukraine





Prof. Dr. **Lyudmila Prigoda**, Maykop State Technological University, Maykop, Russia
Prof. Ing. **Ladislav Šimak**, PhD, Faculty of Special Engineering of the University of Žilina, Žilina, Slovakia
Prof. **Daniela Todorova**, PhD, "Todor Kableshev" University of Transport, Sofia, Bulgaria
Prof. **Yaroslav Vyklyuk**, DSc, Bukovinian University, Chernivtsi, Ukraine
Ing. **Stanislav Filip**, PhD, Assoc. Prof., School of Economics and Management in Public Administration in Bratislava, Slovakia
Dr. hab. **Ladislav Hofreiter**, Assoc. Prof., Andrzej Frycz Modrzewski, Krakow University, Poland
CSc. **Irina Ivanova**, Assoc. Prof., State University of Food Technologies, Mogilev, Belarus
Col. Ing. **Veroslav Kaplan**, CSc., Assoc. Prof., Faculty of Military Technology, University of Defence in Brno, Czech Republic
Tatiana Paladova, PhD, Assoc. Prof., Maykop State Technological University, Maykop, Russia
Denis Vasilievich Kapski, PhD, Assoc. Prof., Belarussian National Technical University, Minsk, Belarus
Ing. **Radovan Soušek**, PhD, Assoc. Prof., University of Pardubice Jan Perner Transport Faculty, Pardubice, Czech Republic
Dr. hab. Eng. **Zenon Zamiar**, Assoc. Prof., Wrocław University of Environmental and Life Sciences, Wrocław, Poland
Dr. sc. **Mario Bogdanović**, Assoc. Prof., Faculty of Economics, University of Split, Croatia
Dr. **Evelin Krmac**, Assoc. Prof., University of Ljubljana, Faculty of Maritime Studies and Transportation Portorož, Slovenia
Dr. **Svetlana Andjelić**, Prof. v.s., Information Technology School - ITS, Belgrade, Serbia

Printed by: **ICIM+, Belgrade**

Circulation: 100 copies

The journal was published online at URL: http://fbim.meste.org/FBIM_1_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.07.07.01.00**

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 Toronto - 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

Suizdavači

- **MESTE** - Beograd
- **Poslovni i pravni fakultet** – “Union – Nikola Tesla” Univerziteta iz Beograda
- **SZ & Associates** – Toronto, Kanada

Uredništvo - Redakcija:

prof. dr **Zoran Čekerevac**, Glavni i odgovorni urednik, Poslovni i pravni fakultet, Beograd

prof. dr **Milija Bogavac**, Zamenik glavnog urednika, Poslovni i pravni fakultet, Beograd

mr **Slavko Zdravković**, Urednik, SZ & Assoc.- Toronto, Kanada

Damjan Čekerevac, MSc, Tehnički urednik, University of Coimbra, Coimbra, Portugal

prof. dr **Ljiljana Jovković**, Lektor, Poslovni i pravni fakultet, Beograd

Sanja Čukić, MA, Lektor, Poslovni i pravni fakultet, Beograd

Milanka Bogavac, MA, Organizator, Poslovni i pravni fakultet, Beograd

Izdavački savet - Naučni odbor:

prof. dr **Milija Bogavac**, Poslovni i pravni fakultet "Union - Nikola Tesla" Univerziteta, Beograd, Srbija

prof. dr **Ana Čekerevac**, Fakultet političkih nauka Univerziteta u Beogradu, Beograd, Srbija

prof. dr **Zoran Čekerevac**, Poslovni i pravni fakultet "Union - Nikola Tesla" Univerziteta, Beograd, Srbija

prof. Ing. **Zdenek Dvorak**, PhD, Fakultet specijalnog inženjerstva Univerziteta u Žilini, Žilina, Slovačka

Prof. dr. sc. **Zvonko Kavran**, Fakultet prometnih znanosti Sveučilišta u Zagrebu, Zagreb, Hrvatska

prof. dr **Petar Kolev**, "Todor Kableškov" Univerzitet transporta, Sofija, Bugarska

prof. **Iouri Nikolski**, PhD, Nacionalni Univerzitet "Lvivska Polytechnica", Lviv, Ukrajina





prof. dr. **Ljudmila Prigoda**, Državni tehnološki univerzitet Majkop, Majkop, Rusija
prof. Ing. **Ladislav Šimak**, PhD, Fakultet specijalnog inženjerstva Univerziteta u Žilini, Žilina, Slovačka
prof. **Daniela Todorova**, PhD, "Todor Kableškov" Univerzitet transporta, Sofija, Bugarska
prof. **Yaroslav Vykylyuk**, DSc, Bukovinski Univerzitet, Černivci, Ukrajina
v. prof Ing. **Stanislav Filip**, PhD, Visoka škola ekonomije i menadžmenta državne uprave, Bratislava, Slovačka
dr hab. **Ladislav Hofreiter**, v. prof., Andrzej Frycz Modrzewski Univerzitet, Krakov, Poljska
v. prof. **Irina Ivanova**, CSc., Državni univerzitet tehnologije hrane, Mogilev, Belorusija
Puk. docent inž. **Veroslav Kaplan**, CSc., Fakultet vojne tehnologije Univerziteta Odbrane, Brno, Češka Republika
v. prof. **Tatiana Paladova**, PhD, Državni tehnološki univerzitet Majkop, Majkop, Rusija
Ph.D. **Denis Vasilievich Kapski**, v. prof., Beloruski Nacionalni Tehnički Univerzitet, Minsk, Belorusija
Doc. Ing. **Radovan Soušek**, PhD, Saobraćajni fakultet Jan Perner Univerziteta u Pardubicama, Pardubice, Češka Republika
dr hab. Eng. **Zenon Zamiar**, v. prof., Univerzitet prirodnih nauka i zaštite životne sredine, Vroclav, Poljska
dr. sc. **Mario Bogdanović**, docent, Ekonomski fakultet Univerziteta u Splitu, Split, Hrvatska
dr **Evelin Krmac**, docent, Fakultet za pomorstvo i transport Univerziteta u Ljubljani, Portorož, Slovenija
dr **Svetlana Anđelić**, prof. s.s., ITS - Visoka škola strukovnih studija za informacione tehnologije, Beograd, Srbija

Štampa: **ICIM+, Beograd**

Tiraž: 100 primeraka

Žurnal je publikovan i onlajn na URL adresi: http://fbim.meste.org/FBIM_1_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 1
DOI: 10.12709/fbim.07.07.01.00

Editorial on FBIM Transactions 2019-1

Prof. Dr. Dr. h. c. Zoran Čekerevac¹

(1) Faculty of Business and Law, "Union - Nikola Tesla" University, Knez Mihailova 33, Belgrade, Serbia
Email: zoran@cekerevac.eu

Belgrade
April 15th, 2019
(Without Abstract)

Welcome to the April 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. Twenty papers have been published in this issue, two of which have been classified as original scientific papers, and eighteen as review articles. 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 1
DOI: 10.12709/fbim.07.07.01.00

Reč urednika kao predgovor za FBIM Transactions 2019-1

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
15.04.2019.

(Bez apstrakta)

Dobrodošli 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 dvadeset radova od kojih su dva svrstana u grupu originalnih naučnih radova, a osamnaest u grupu preglednih 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
- Entrepreneurship
- Innovation 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
- Bihevioralne 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 informacijski 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

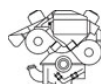
- Politika i društvo
- Menadžment javne uprave
- Javna uprava
- Pravni aspekti menadžmenta
- Menadžment u poljoprivredi
- Menadžment u kriznim situacijama
- Menadžment u ekologiji
- Menadžment u ekonomiji
- Menadžment u obrazovanju
- Menadžment u industriji
- Menadžment u transportu
- Tehnologije i alati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

Article No.	Category Name(s) of the author(s) TITLE OF THE ARTICLE DOI	Pages From - to
#1	Review article Hatidza Berisa, Katarina Jonev CHALLENGES OF INFORMATION SECURITY IN THE DEFENSE SYSTEM OF THE REPUBLIC OF SERBIA DOI 10.12709/fbim.07.07.01.01	1-9
#2	Review article Nenad Bingulac THE UNAUTHORIZED PROCESSING OF PERSONAL DATA AND MISDEMEANOR LIABILITY UNDER THE LAW OF PERSONAL DATA PROTECTION DOI 10.12709/fbim.07.07.01.02	10-19
#3	Review article Srdjan Blagojevic SOCIAL ENGINEERING AND PERSONAL DATA DOI 10.12709/fbim.07.07.01.03	20-28
#4	Review article Kamil Boc, Zdenek Dvorak, and Zoran Cekerevac SECURITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES DOI 10.12709/fbim.07.07.01.04	29-37
#5	Review article Boris Bursac ORIGINS AND HISTORY OF ISLAMIC STATE DOI 10.12709/fbim.07.07.01.05	38-49
#6	Review article Zoran Cekerevac, Zdenek Dvorak, and Lyudmila Prigoda MODERN COMPUTER FORENZICS AND FORENZIC TOOLS DOI 10.12709/fbim.07.07.01.06	50-60
#7	Review article Aleksandar Gracanac, Vladimir Stojanovic, and Nada Zivojinovic TECHNICAL SPECIALISM OF HUMAN RESOURCES AS CONDITION FOR DEVELOPMENT OF SMES IN SERBIA DOI 10.12709/fbim.07.07.01.07	61-66
#8	Review article Haris Hamidovic OBLIGATION TO IMPLEMENT TECHNICAL MEASURES FOR DATA PROTECTION BASED ON EU GDPR DOI 10.12709/fbim.07.07.01.08	67-73



Article No.	Category Name(s) of the author(s) TITLE OF THE ARTICLE DOI	Pages From - to
#9	Research paper Goran Jovanov, Nemanja Jovanov, and Radovan Radovanovic IDENTIFICATION OF FAILURE SCENARIO AND THE CONCEPTION OF MATHEMATICAL TOOLS IN NUMERIC RISK ASSESSMENT DOI 10.12709/fbim.07.07.01.09	74-84
#10	Review article Mario Lukinovic CRYPTOCURRENCY, BLOCKCHAIN, AND BITCOIN DOI 10.12709/fbim.07.07.01.10	85-90
#11	Review article Branka Mijic INFORMATION SECURITY IN BOSNIA AND HERZEGOVINA DOI 10.12709/fbim.07.07.01.11	91-99
#12	Review article Zivanka Miladinovic Bogavac LEGAL REGULATION OF CHILDREN'S PORNOGRAPHY ON THE INTERNET DOI 10.12709/fbim.07.07.01.12	100-109
#13	Research paper Zoran Milanovic INFORMATION-SECURITY CULTURE OF YOUTH IN SERBIA DOI 10.12709/fbim.07.07.01.13	110-118
#14	Review article Ljubomir Miljkovic, Dragana Trnavac, and Kristijan Ristic CRYPTOCURRENCIES - A NEW MODEL OF BUSINESS DOI 10.12709/fbim.07.07.01.14	119-124
#15	Review article Zeljko Nikac ADOPTION OF THE LAW ON NATIONAL DNA REGISTER IN THE REPUBLIC OF SERBIA DOI 10.12709/fbim.07.07.01.15	125-133
#16	Review article Dusan Regodic, Marija Matotek, and Radomir Regodic APPLICATION OF INTELLIGENT TECHNOLOGIES IN THE MANAGEMENT OF SUPPLY CHAINS DOI 10.12709/fbim.07.07.01.16	134-151





Article No.	Category Name(s) of the author(s) TITLE OF THE ARTICLE DOI	Pages From - to
#17	Review article Bosko Rodic IT COURT EXPERT BETWEEN SCYLLA AND CHARYBDIS DOI 10.12709/fbim.07.07.01.17	152-158
#18	Review article Miroslav D. Stevanovic and Dragan Z. Djurdjevic CHALLENGE OF THE ABUSE OF INFORMATION TECHNOLOGIES FOR PUBLIC INFORMATION DOI 10.12709/fbim.07.07.01.18	159-169
#19	Review article Salih Sutkovic, Nebojsa Zakic, and Aleksandra Tornjanski THE IMPACT OF TRANSFORMATIONAL AND CHANGE LEADERSHIP ON CHANGE READINESS AND COMMITMENT TO CHANGE DOI 10.12709/fbim.07.07.01.19	170-180
#20	Review article Slobodan Vuksanovic MANAGEMENT IN THE TEACHING PROCESS - THE ROLE OF TEACHERS DOI 10.12709/fbim.07.07.01.20	181-184
	Reviewers	185-187
	Recenzenti	188-190
	Instrucions for authors	191-194
	Uputstva za autore	195-198
	Manuscript submission	199
	Prijavljivanje radova	200
	Reviewer's report	201-202
	Izveštaj o recenziji	203-204
	Templates	
	Šabloni	205



Rad broj	Kategorija rada Autor(i) NASLOV RADA DOI	Stranice Od - do
#1	Pregledni rad Hatidža Beriša, Katarina Jonev IZAZOVI INFORMACIONE BEZBEDNOSTI U SISTEMU ODBRANE REPUBLIKE SRBIJE DOI 10.12709/fbim.07.07.01.01	1-9
#2	Pregledni rad Nenad Bingulac NEDOZVOLJENOST OBRADJE PODATAKA O LIČNOSTI I PREKRŠAJNA ODGOVORNOST PO OSNOVU ZAKONA O ZAŠTITI LIČNOSTI DOI 10.12709/fbim.07.07.01.02	10-19
#3	Pregledni rad Srđan Blagojević SOCIJALNI INŽENJERING I LIČNI PODACI DOI 10.12709/fbim.07.07.01.03	20-28
#4	Pregledni rad Kamil Boc, Zdenek Dvorak, Zoran Čekerevac BEZBEDNOST INFORMACIONIH I KOMUNIKACIONIH TEHNOLOGIJA DOI 10.12709/fbim.07.07.01.04	29-37
#5	Pregledni rad Boris Bursać POREKLO ISLAMSKJE DRŽAVE DOI 10.12709/fbim.07.07.01.05	38-49
#6	Pregledni rad Zoran Čekerevac, Zdenek Dvorak, Lyudmila Prigoda SAVREMENA RAČUNARSKA FORENZIKA I FORENZIČKI ALATI DOI 10.12709/fbim.07.07.01.06	50-60
#7	Pregledni rad Aleksandar Gračanac, Vladimir Stojanović, Nada Živanović KOMUNIKACIJA I PERFORMANSE POSLA DOI 10.12709/fbim.07.07.01.07	61-66
#8	Pregledni rad Haris Hamidović OBAVEZA PODUZIMANJA TEHNIČKIH MJERA ZAŠTITE PODATAKA TEMELJEM EU UREDBE O ZAŠTITI PODATAKA DOI 10.12709/fbim.07.07.01.08	67-73





Rad broj	Kategorija rada Autor(i) NASLOV RADA DOI	Stranice Od - do
#9	Originalni naučni rad Goran Jovanov, Nemanja Jovanov, Radovan Radovanović IDENTIFIKACIJA SCENARIJA OTKAZA I KONCEPIRANJE MATEMATIČKIH ALATKI U NUMERIČKOM PROCENJIVANJU RIZIKA DOI 10.12709/fbim.07.07.01.09	74-84
#10	Pregledni rad Mario Lukinović KRIPTOVALUTE, BLOKČEJN I BITKOIN DOI 10.12709/fbim.07.07.01.10	85-90
#11	Pregledni rad Branka Mijić INFORMACIJSKA SIGURNOST U BOSNI I HERCEGOVINI DOI 10.12709/fbim.07.07.01.11	91-99
#12	Pregledni rad Živanka Miladinović Bogavac PRAVNA REGULATIVA DEČIJE PORNOGRAFIJE NA INTERNETU DOI 10.12709/fbim.07.07.01.12	100-109
#13	Originalni naučni rad Zoran Milanović INFORMACIONO-BEZBEDNOSNA KULTURA MLADIH U SRBIJI DOI 10.12709/fbim.07.07.01.13	110-118
#14	Pregledni rad Ljubomir Miljković, Dragana Trnavac, Kristijan Ristić KRIPTOVALUTE – NOVI MODEL POSLOVANJA DOI 10.12709/fbim.07.07.01.14	119-124
#15	Pregledni rad Željko Nikač USVOJEN ZAKON O NACIONALNOM DNK REGISTRU U REPUBLICI SRBIJI DOI 10.12709/fbim.07.07.01.15	125-133
#16	Pregledni rad Dušan Regodić, Marija Matotek, Radomir Regodić PRIMENA INTELIGENTNIH TEHNOLOGIJA PRI UPRAVLJANJU LANCIMA SNABDEVANJA DOI 10.12709/fbim.07.07.01.16	134-151



Rad broj	Kategorija rada Autor(i) NASLOV RADA DOI	Stranice Od - do
#17	Pregledni rad Boško S. Rodić IT VEŠTAK IZMEĐU SCILE I HARIBDE DOI 10.12709/fbim.07.07.01.17	152-158
#18	Pregledni rad Miroslav D. Stevanović, Dragan Ž. Đurđević IZAZOV ZLOUPOTREBE INFORMACIONIH TEHNOLOGIJA ZA JAVNO INFORMISANJE DOI 10.12709/fbim.07.07.01.18	159-169
#19	Pregledni rad Salih Šutković, Nebojša Zakić, Aleksandra Tornjanski UTICAJ TRANSFORMACIONOG LIDERSTVA I LIDERSTVA PROMENE NA SPREMNOST ZA PROMENU I PREDANOST PROMENI DOI 10.12709/fbim.07.07.01.19	170-180
#20	Pregledni rad Slobodan Vuksanović MENADŽMENT U NASTAVNOM PROCESU ULOGA NASTAVNIKA DOI 10.12709/fbim.07.07.01.20	181-184
	Reviewers Recenzenti	185-187 188-190
	Instructions for authors Uputstva za autore	191-194 195-198
	Manuscript submission Prijavljivanje radova	199 200
	Reviewer's report Izveštaj o recenziji	201-202 203-204
	Templates Šabloni	205







IZAZOVI INFORMACIONE BEZBEDNOSTI U SISTEMU ODBRANE REPUBLIKE SRBIJE

CHALLENGES OF INFORMATION SECURITY IN THE DEFENSE SYSTEM OF THE REPUBLIC OF SERBIA

Hatidža Beriša

Univerzitet odbrane, Vojna akademija, Beograd, Srbija

Katarina Jonev

Fakultet bezbednosti, Univerzitet u Beogradu, Beograd, Srbija

©MESTE

JEL Category: **D82, F52**

Apstrakt

Informaciona bezbednost je aspekt bezbednosti koji se odnosi na bezbednosne rizike povezane sa upotrebom informaciono-komunikacionih tehnologija, uključujući bezbednost podataka, uređaja, informacionih sistema, mreža, organizacija i pojedinaca. Razvoj novih tehnologija donosi nesumnjive koristi za društvo, ali paralelno sa tehnološkim razvojem dolaze i novi bezbednosni izazovi. Visokotehnološki kriminal i hakerski napadi na informacione sisteme mogu bitno da ugroze kako funkcionisanje državne infrastrukture i nacionalnu bezbednost, tako i sistem odbrane Republike Srbije. Napadi na informacione sisteme mogu da bitno ugroze funkcionisanje sistema odbrane Republike Srbije, kao što je bio slučaj u Estoniji 2007. godine, kada je izvršen sajber napad na IKT sisteme državnih organa, kada je došlo do blokade informacionih sistema. Poznat je i slučaj unošenja računarskog virusa „Staksnet” u nuklearnu elektranu u Iranu 2010. godine, sa namerom da se izvrši sabotaža industrijskih sistema. Pored toga, postoje pretnje po odbranu koje se po međunarodnom pravu ne mogu svrstati u oblike oružane agresije, ali su prisutne u međunarodnim odnosima. Prema podacima Ministarstva unutrašnjih poslova, broj prijavljenih krivičnih dela iz oblasti visokotehnološkog kriminala raste 50% godišnje. Napadi na servere državnih organa sve su učestaliji i napredniji. U radu će sagledati sa kojim se izazovima informaciona bezbednost u sistemu odbrane Republike Srbije, Takođe u radu će se razmatrati neki od načina ugrožavanja savremenih komunikacionih i računarskih sistema i mreža.

Ključne reči: bezbednost, sistem odbrane, informaciona bezbednost, izazovi, Republika Srbija, ugrožavanje, mreža

Abstract

Information security is an aspect of security related to the security risks associated with the use of information and communication technologies, including the security of data, devices, information systems, networks, organizations and individuals.

Adresa autora zaduženog za korespondenciju:

Hatidža Beriša

berisa.hatidza@gmail.com



The development of new technologies brings undoubted benefits to society, but parallel to technological development, new security challenges are coming. High-tech crime and hacking attacks on information systems can significantly jeopardize the functioning of state infrastructure and national security, as well as the defense system of the Republic of Serbia. Attacks on information systems can significantly jeopardize the functioning of the defense system of the Republic of Serbia, as it was the case in Estonia in 2007, when cyber-attack on the ICT systems of state authorities was carried out, when information systems were blocked. The case of the introduction of a computer virus "Stuxnet" in the nuclear power plant in Iran in 2010 to sabotage industrial systems is also known. In addition, there are threats of defense that cannot be classified under international law as forms of armed aggression but are present in international relations. According to the Ministry of Internal Affairs, the number of reported criminal offenses in the field of high-tech crime is growing 50% annually. Attacks on state authority servers are even more frequent and advanced. The paper will discuss the challenges of information security in the defense system of the Republic of Serbia. Also, in this paper will be considered some of the threats of using modern communication and computer systems and networks.

Keywords: security, defense system, information security, challenges, Republic of Serbia, threats, network

1 UVOD

Kineski filozof Konfučije (551-479. pre n. e.) rekao je „Upoznaj sebe i upoznaj protivnika, pa ćeš biti nepobediv“. Nemamo nameru apsolutizirati ovu izjavu, ali želimo istaći onaj deo koji govori o značaju upoznavanja neprijatelja.

Sigurno je da su, od kada je ratova, zaraćene strane još u pripremi ratnih dejstava, a u toku oružanog sukoba naročito, nastojale da o protivniku saznaju što više - s jedne strane i da prikriju što više podataka o sebi - s druge strane. Ova nepobitna činjenica i bitan preduslov uspeha u ratu i dobija na značaju sve više u savremenim kao i u eventualnim budućim ratovima.

U savremenim uslovima posedovanje informacija ima veliki značaj za sve oblike društvenih delatnosti, a posebno u oblasti bezbednosti i odbrane. Mnoge zemlje u svetu danas pridaju izuzetan značaj bezbednosti informacija i informacionih sistema.¹

Jedan od zadataka osiguranja bezbednosti informacija kojima raspolaže neka organizacija je i zaštita od preuzimanja informacija o strane neovlašćenih lica i službi. Za preuzimanje na daljinu aktuelne su informacije koje cirkulišu posredstvom sredstava telekomunikacionog i informatičkog sistema. To su poverljivi podaci i informacije u vidu usmenih saopštenja u telefonskim razgovorima, video-konferencijama, radio i radio telefonskim vezama, dokumenta sa poverljivim sadržajima, podaci i informacije koje se obrađuju na računarima kao i razni podaci u računarskim mrežama, iz kojih protivnici mogu izvući korisne informacije za sebe.

Moguće je razmatrati tri aspekta sigurnosti informacija (Pleskonjić, Maček, Đoršević, & Carić, 2007, str. 2):

- napad na sigurnost - (engl. security attack) bilo koja akcija koja ugrožava sigurnost informacija;

¹ U okviru Saveta bezbednosti Ruske Federacije postoji Odeljenje za upravljanje informacionom bezbednošću. Saveznim zakonom o zaštiti podataka iz 1972. godine u SR Nemačkoj bile su definisane obaveze nadležnih u vezi sa bezbednošću informacionih sistema, na osnovu kojih je u Nemačkoj osamdesetih godine na poslovima referenata bezbednosti u informacionim sistemima radilo oko 10 hiljada ljudi.

U Americi je 1960. godine formirana DCA (Defense Communications Agency), kao agencija za "odbranu" komunikacija. Od 1991. godine DCA je prerasla u agenciju za odbranu informacionih sistema DISA

(Defense Information Systems Agency), i kao ogranak NSA, zadužena je za pomoć u komandovanju, upravljanju, komunikacijama i informacionim sistemima predsedniku i potpredsedniku SAD, ministru odbrane i najvišim vojnim komandantima, odeljenjima Ministarstva odbrane u svim mirnodopskim i ratnim uslovima. U februaru 2003. godine, predsednik SAD, Džordž Buš potpisuje Nacionalnu strategiju bezbednosti "sajberspejsa" (National Strategy to Secure Cyberspace) kojom se stvaraju okviri za zaštitu informatičke infrastrukture od izuzetne važnosti za ekonomiju i uopšte bezbednost života.

- sigurnosni mehanizam - (engl. security mechanism) mehanizam koji treba da detektuje i predupredi napad ili da sistem oporavi od napada;
- sigurnosna usluga (engl. security service) - usluga koja povećava sigurnost sistema za obradu i prenos podataka. Sigurnosna usluga podrazumeva upotrebu jednog ili više sigurnosnih mehanizama.

2 IZAZOVI BEZBEDNOSTI INFORMACIONE DIMENZIJE

Složenost sajber prostora i njegove karakteristike, neminovno utiču i na informacionu dimenziju u kojoj savremeno društvo uspostavlja sve informacione tokove i obavlja svoje aktivnosti. Široka primena savremenih IKT uvećala je ranjivost društva, koje je u informacionoj dimenziji izloženo mnogim opasnostima i pretnjama, što je nekada bila karakteristika, isključivo, fizičkih domena ljudske delatnosti. Tehnološki razvoj, ekspanzija IKT i sajber prostor doneli su nove opasnosti po bezbednost u informacionom ambijentu – sajber pretnje. Informacioni ambijent povezan je sa skoro svim bezbednosnim izazovima koji se navode u strateškim razmatranjima nacionalne bezbednosti većine savremenih država, vojnih i bezbednosnih saveza i organizacija (Slavković, Kršljanin, 2015, str. 341).

Internet, kao osnova sajber prostora, nema centralizovano upravljanje, samim tim nema ni centralizovanu kontrolu, svačiji i ničiji, postao je zanimljiv za mnoge interesne grupe sa različitim pretenzijama. Danas, IKT čine osnovu infrastrukture svih esencijalnih sistema u jednoj državi. Energetski, transportni, finansijski, telekomunikacioni, bezbednosni i odbrambeni sistemi direktno su zavisni od funkcionisanja IKT. Time je savremeni svet doveden u paradoksalnu situaciju: baziranost na informacionim tehnologijama predstavlja i glavnu slabost zbog zavisnosti od tehnologija. Glavnu opasnost po sisteme zasnovane na IKT predstavljaju napadi na informacionu i telekomunikacionu (kritičnu) infrastrukturu.

Države, koje se oslanjaju na IKT, izloženije su i ranjivije na sajber napade, prekide rada ili uništenje informacionih dobara i tehnologije. Direktna zavisnost informacionih tokova od IKT čini industrijska društva ranjivijim, dok su zemlje

sa nižim nivoom zavisnosti od IKT manje ranjive i mogu da iskoriste ranjivost razvijenijih zemalja za ostvarenje svojih strateških ciljeva.

Mogućnost izvršavanja destruktivnih akcija, sa ekonomskog, bezbednosnog i vojnog aspekta, sasvim je realna. Razvijanje ofanzivnih strategija u informacionom ambijentu ne zahteva visoke investicije kao za konvencionalno ratovanje, što ih čini dostupnim velikom broju aktera. Sajber oružje mogu razvijati pojedinci ili grupe, a za to su im potrebni jedino znanje i motivacija. Državama ili akterima, kojima do sada nije pridavan značaj u strateškom kontekstu, to omogućava drugačiju poziciju u sajber prostoru, jer ravnotežu moći određuje pre znanje nego količina vojnog arsenala.

Trend ispoljavanja pretnje u sajber prostoru ukazuje na stalni razvoj sposobnosti napadača za ugrožavanje IKT, napade na računarske mreže, ispoljavanje nasilja i nanošenje štete. Opasnosti su, pre svega, zasnovane na tehničkim i tehnološkim karakteristikama i ranjivostima Interneta i sajber prostora. Znatan uticaj na bezbednost Interneta ostvaruju i tradicionalne forme društvenih konflikata i sukoba jer su eskalirali u sasvim nove forme u globalnoj računarskoj mreži.

Sajber napadom se prevashodno ciljaju informaciona dobra, a prekid ili uništavanje kritične informacione infrastrukture i informacionih tokova, predstavlja značajnu ranjivost društvenih vrednosti, koja može dovesti do širokog dijapazona posledica i štete po društvo. Konvergencija fizičkih napada sa sajber napadima na kritične infrastrukture, opasne terorističke aktivnosti usmerene na ugrožavanje elektronskih i automatizovanih sistema, kojima su podržani energetski, komunikacioni, komercijalni i odbrambeni sektor, predstavljaju samo deo mnogobrojnih ranjivosti društva u informacionoj dimenziji. Sajber napadi na sisteme kontrole, koji su osnova kritične infrastrukture i pružaju povezanost između realnog i virtuelnog sveta, mogu rezultirati u velikim materijalnim gubicima i ljudskim žrtvama. Sajber napad na sisteme za prikupljanje podataka, nadzor, praćenje i upravljanje - SCADA sisteme (engl. Supervisory Control And Data Acquisition) može imati dramatične posledice po društvo. Trend povećanja međupovezanosti sistema kontrole

unutar Interneta, uz upotrebu standardnih protokola iz ekonomskih razloga i zbog povećanja uzajamne operativnosti, znatno povećavaju rizike i ugrožavaju IKT i društvene aktivnosti.

Koliko god se pretnja sajber napada činila kao precenjena, mere koje se danas preduzimaju radi suprotstavljanja nisu gubici ni vremena, ni energije, ni novca. Preventivne aktivnosti u polju zaštite od potencijalne sajber pretnje svakako da osnažuju mere koje se preduzimaju u borbi protiv onoga što je trenutno najveća pretnja informacionom ambijentu – zloupotreba sajber prostora u kriminalne svrhe.

2.1 Načini ugrožavanja informacione bezbednosti u računarskim mrežama i IKT sistemima

U osnovi napada su akcije koje su usmerene na ugrožavanje sigurnosti informacija u računarskim mrežama i telekomunikacionim sistemima. Postoje različite vrste napada, ali se one generalno mogu klasifikovati u četiri osnovne kategorije:

- **Presecanje**, tj. prekidanje (engl. interruption) predstavlja napad na raspoloživost (engl. availability). Presecanjem se prekida tok informacija, tj. onemogućava se pružanje neke usluge ili funkcionisanje nekog sistema. Ovakav napad je aktivan.
 - **Presretanje** (engl. interception) predstavlja napad na poverljivost (engl. confidentiality). Presretanje može biti u praksi sprovedeno kao prisluškivanje saobraćaja, nadziranje njegovog intenziteta, uvid u osetljive informacije ili slično. Kao pasivan napad, teško se otkriva jer ne menja podatke tj. ne utiče na unutrašnje funkcionisanje sistema. Ovakav tip napada ponekad je pripremna faza za neku drugu vrstu napada.
 - **Izmena** (engl. modification), predstavlja napad na integritet (engl. integrity). Po svojoj prirodi, to je aktivan napad. Ukoliko se dešava na prenosnom putu, može se, na primer, ispoljiti kao napad "čovjek u sredini" (engl. man in the middle). Napad se može obaviti i unutar nekog računarskog sistema - u tom slučaju se radi o izmeni podataka, pristupnih prava, načina funkcionisanja programa ili sistema i slično. Iako menja podatke ili sistem, često ostaje neprimećen izvesno vreme, kako zbog nepažnje, tako i zbog složenih tehnika koje se pri ovom napadu koriste.
 - **Fabrikovanje** (engl. fabrication), predstavlja napad na autentičnost (engl. authenticity). Napadač izvodi ovaj aktivan napad tako što generiše lažne podatke, lažni saobraćaj ili izdaje neovlašćene komande. Veoma često se koristi i lažno predstavljanje korisnika, usluge, servera, Web strane ili nekog drugog dela sistema.
- Ako se razume osnovni pristup koji napadači koriste da "osvoje" neki sistem ili mrežu, lakše će se preduzimati odbrambene mere znajući šta je promenjeno i protiv čega.
- Osnovni koraci napadačeve metodologije (Pleskonjić, Maček, Đoršević Carić, 2007, str. 4) su:
- a. **Ispitaj i proceni**. Prvi korak koji napadač preduzima jeste istraživanje potencijalne mete i identifikovanje i procena njenih karakteristika. Te karakteristike mogu biti podržani servisi, protokoli s mogućim ranjivostima i ulaznim tačkama. Napadač koristi informacije prikupljene na ovaj način kako bi napravio plan za početni napad.
 - b. **Eksplatiši i prodri**. Nakon što je istražio potencijalnu metu, napadač pokušava da eksploatiše ranjivost i da prodre u mrežu ili sistem. Ako su mreža ili umreženi računari (obično server) potpuno osigurani, aplikacija postaje sledeća ulazna tačka za napadača - napadač će najlakše upasti u sistem kroz isti ulaz koji koriste legitimni korisnici. Na primer, može se upotrebiti stranica za prijavljivanje ili stranica koja ne zahteva proveru identiteta.
 - c. **Povećaj privilegije**. Nakon što napadač uspe da ugrozi aplikaciju ili mrežu - na primer ubacivanjem koda u aplikaciju ili uspostavljanjem legitimne sesije na operativnom sistemu - odmah će pokušati da poveća svoja prava. Posebno će pokušati da preuzme administratorske privilegije tj. da uđe u grupu korisnika koji imaju sva prava nad sistemom. Definisanje najmanjeg nužnog skupa prava i usluga koji je neophodno obezbediti korisnicima aplikacije, primarna je odbrana od napada povećanja privilegija.
 - d. **Održi pristup**. Kad prvi put uspe da pristupi sistemu, napadač preduzima korake da olakša buduće napade i da prikrije tragove.

Čest način olakšanja budućih pristupa jeste postavljanje programa sa zadnjim vratima (engl. back door), ili korišćenje postojećih naloga koji nisu strogo zaštićeni. U prikrivanje tragova često spada brisanje dnevnčkih datoteka (engl. log files) i skrivanje napadačevih alata. Uzevši u obzir da su dnevničke datoteke jedan od objekata koje napadač želi da modifikuje kako bi prikrio tragove, one treba da budu osigurane i da se redovno analiziraju. Analiza dnevnčkih datoteka često može otkriti rane znakove pokušaja upada u sistem, i pre nego što nastane šteta.

- e. **Odbij uslugu.** Napadači koji ne mogu da pristupe sistemu ili računarskoj mreži i da ostvare svoj cilj često preduzimaju napad koji prouzrokuje odbijanje usluge (engl. Denial of Service attack, DoS), kako bi sprečili druge da koriste aplikaciju. Za druge napadače DoS napad je cilj od samog početka.

Problemi bezbednosti i zaštite podataka u širokopojasnim telekomunikacionim mrežama mogu se uspešno rešavati samo ako su unapred poznate, ili realno procenjene pretnje kojima mreže mogu biti ugrožene.

2.2 Ugrožavanja informacione bezbednosti putem kompromitujućeg elektromagnetnog zračenja

Kompromitujuće elektromagnetno zračenje (KEMZ) računara i telekomunikacione opreme je takođe jedan od mogućih načina za ugrožavanje sigurnosti podataka i informacija. Mikročipovi, monitori, štampači i bilo koji drugi elektronski

uređaji i komponente emituju elektromagnetne talase. Kao posledica ove emisije može da se desi, zahvaljujući interferenciji, da na TV prijemniku uhvatite sliku sa monitora računara u susednoj prostoriji. Ova pojava je izuzetno važna za sve institucije i organizacije koje imaju poverljive podatke i informacije na svojim računarima i poznata je pod nazivom kompromitujuće elektromagnetno zračenje (KEMZ)². Koristeći TEMPEST (Transient Electromagnetic Pulse Emanation Standard) tehnologiju³ informacija sa bilo koje digitalne mašine može da bude sinuta i rekonstruisana obaveštajno korisno. Ova tehnologija je posebno korisna za prihvatanje podataka i informacija koje se nalaze na računaru, prikazuju na monitoru, štampaču, kucaju na tastaturi i prenose kroz kablove iz kompleta računara.

Teško je doći do konkretnih dokaza o slučajevima skidanja podataka i informacija sa računara koristeći KEMZ, a posebno utvrditi nivo i udaljenost sa koje se može signal rekonstruisati. Kod nas je ta mogućnost dokazana još davne 1988. godine na savetovanju u Institutu za bezbednost pod nazivom „Elektromagnetska kompatibilnosti i protivelektronska zaštita računara i računarskih mreža“ (Rodić, Đorđević, 2004, str. 35-37).

2.2.1 Računarski virusi kao oblik ugrožavanja

Od rizika koji nastaju korišćenjem mogućnosti koje pruža IKT sistem izdvajaju se rizici koji nastaju korišćenjem računarske tehnologije kao okosnice IKT sistema. Od savremenih zlonamernih (malicioznih) aktivnosti usmerenih prema IKT sistemu koji dovode do degradacije funkcionisanja

² KEMZ - Kompromitujuće Elektromagnetno Zračenje - predstavlja nenamerne elektromagnetne emisije prilikom prenosa, obrade ili čuvanja podataka, čijim prijemom i analizom se može otkriti sadržaj tih podataka (član 2. stav 1. tačka 18. Zakona o informacionoj bezbednosti).

³ TEMPEST je skraćenica od Transient Electromagnetic Pulse Emanation Standard - privremeni standard za emisiju pulsno modulisanog signala. Ovaj pre svega defanzivni standard je skup stavova o elektromagnetnom zračenju preko kog uređaji mogu da zrače bez kompromitacije informacija koje se nalaze u njima. TEMPEST istovremeno definiše opremu i uslove koji određuju procese koji imaju za cilj da preveniraju kompromitujuće zračenje. Uređaji koji su usklađeni sa ovim standardom nazivaju se TEMPEST sertifikovani

uređaji. M TEMPEST (Transient Electromagnetic Pulse Surveillance Technology) je program američke vlade za evaluaciju elektronske opreme za prisluškivanje. Može se reći da su uređaji za vojne i državne primene (bezbednost) testirani u skladu sa strožim standardima. Navodno dva tipa standarda: NACSIM 5100 A (SAD) i AMSG 720 B (NATO). Oba standarda su primenljiva na svim delovima računarskog sistema, a ne samo na video jedinice ili terminale. Merne metode i standardi NACSIM nisu poznati izvan Amerike. AMSG standard je specijalan slučaj korišćenja vojnih i državnih aplikacija u zemljama NATO-a. Američki standard u vezi sa kompromitujućim elektromagnetnim zračenjem (KEMZ), naziva se memorandum o nacionalnoj bezbednosti komunikacija (direktiva za TEMPEST bezbednost) - NACSIM 5100 (National Communications Security Information Memorandum).

i bezbednosti sadržaja pohranjenih u informacionim sistemima izdvajaju se:

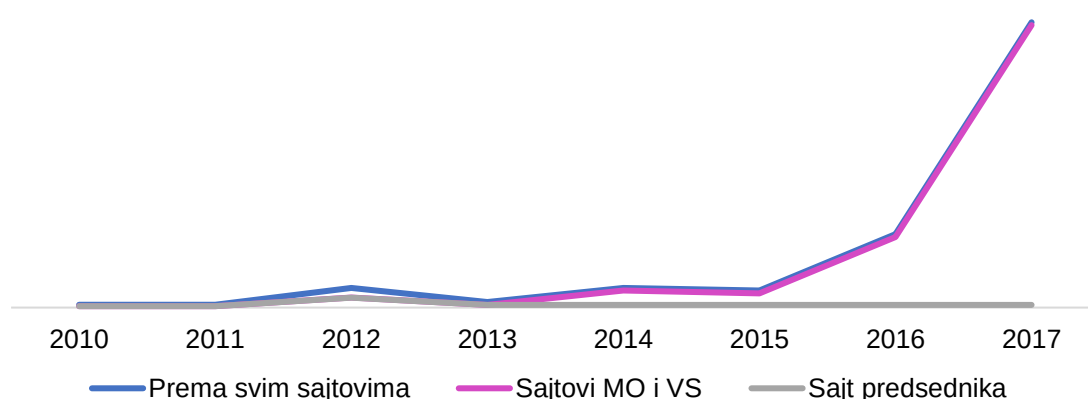
1. Crv (engl. worms) je program kreiran da se samostalno kreće i prebacuje sa računara na računar. Tipičan crv je dizajniran tako da može da otkrije druge kompjutere u okruženju sa specifičnim osobinama koje mu omogućuju da uspešno napadne sledeći računar i samostalno se instalira na isti. Nakon toga crv skenira neposredno okruženje novoosvojenog domaćina i ciklus se ponavlja dokle god ima novih računara pogodnih za osvajanje.
2. Trojanski konj (trojanac) je drugi tip štetnog softvera. Za razliku od crva, trojanac zahteva intervenciju čoveka da bi se prebacivao sa sistema na sistem. Trojanski konj je dobio ime jer liči na nešto bezopasno. Može da bude ugrađen u kompjuterski program kao da je igrara, čuvar ekrana ili neki drugi program. Ali jednom aktiviran trojanac će napraviti štetu za koju je dizajniran. Može to da bude skeniranje okolne mreže u cilju pronalaženja nove žrtve, skeniranje sistema u cilju pronalaženja važnih podataka ili instalacija drugog malicioznog softvera.
3. Napadi zagušenja bafera je specifična vrsta napada gde je napad dizajniran tako da izvršavanjem instrukcija napadača zbuni napadnuti IKT sistem. Napadački program uspostavlja komunikacionu sesiju sa specifičnim komponentama za napadnuti IKT sistem i šalje specijalno napravljene poruke za isti. Takve poruke namerno šalju veliku količinu podataka u ulazni bafer napadnutog IKT sistema. Tako velika količina podataka u programima osetljivim na ovu vrstu napada može da dovede do izvršavanja napadačevih instrukcija umesto izvornih. Takve nove instrukcije obično sadrže kod kojim se „otvara“ napadnuti IKT sistem i dozvoljava delimično ili potpuno preuzimanje kontrole nad napadnutim sistemom. Ova vrsta napada je komplikovana za razvoj i pretpostavlja detaljno znanje o internoj arhitekturi ciljanog IKT sistema (hardver i softver) kao i detaljno znanje o programu ili servisu koji se napadaju. Crvi, trojanci, virusi i drugi maliciozni softveri veoma često koriste ovu vrstu napada radi ubacivanja u novi sistem žrtve.
4. Špijunski softver (engl. spyware) je odeljen širokoj grupi tehnika koje se koriste da na skriven način dobiju informacije sa računara. Špijunski softver najčešće uzima oblik računarskog koda koji je instaliran na računar korisnika bez njegovog znanja i pristanka, koji sakuplja određene informacije i šalje ih nekom centralnom izvoru. Ovakav softver može izmeniti ponašanje korisnikovog računara.
5. Pecanje (phising - igra reči sa reči fishing - pecanje) je napada na korisnike računara u pokušaju da ih prevari da učine radnju koja je predviđena da ih ošteti. Ta šteta može, na primer, imati oblik bilo koje vrste prevare ili instalacije malvera ili špijunskog softvera na računar korisnika.
6. Synchronization poplava je napad na ciljani IKT sistem, konkretno napad na ključne projektne karakteristike TCP/IP mrežnog protokola. U SYN poplavi, napadač šalje hiljade SYN paketa ciljanom IKT sistemu. SYN paket je obično poruka poslata sa drugog računara koji želi da ustanovi mrežnu konekciju sa metom. Nakon prijema SYN paketa, ciljani IKT sistem odgovara sa SYN/ACK (engl. acknowledgement - potvrda) i u tom trenutku počinje komunikacija.
7. Napad za odbijanje usluge (engl. Denial of Service attacks - DoS napad) je napad na ciljani IKT sistem pri čemu je cilj da se isti delimično ili potpuno onesposobi. Svrha DoS napada jeste da predstavi ciljani sistem beskorisnim za legitimne namene. Radi efikasnije prikrivenosti napada napadači koriste razne tehnike za izbegavanje detekcije. U malver ekonomiji, autori malvera smatraju da su njihovi proizvodi uspešni ukoliko su u stanju da izbegnu detekciju.
8. „Napad nultog dana“ je ime novih napada na prethodno nepoznatoj ranjivosti napadnutog IKT sistema, ili potpuno nova vrsta napada na postojeće slabosti IKT sistema. Izraz „nulti dan“ potiče od broja dana upozorenja od vremena kada je ranjivost objavljena i kada je zloupotrebljena. Drugim rečima, ovo su ranjivosti za koje ne postoje zakrpe. Napredne istrajne pretnje (engl. Advanced Permanent Threat - APT) su podigle dosta buke i uzrok su mnogim dezinformacija u stručnim krugovima. Od ove vrste napada trenutno ne postoji adekvatna odbrana.
9. Brutal-force attack je vrsta napada koja za cilj ima razbijanje lozinki za pristup IKT sistemu. Napad se izvodi od strane zlonamernog

korisnika ili softvera na računar (server) ili operativni sistem da bi se došlo do tajne lozinke ili simetričnog ključa za enkripciju. Najčešće se vrši pogađanjem lozinke ili ključa dok se ne otkriju.

10. SQL injection predstavlja napad na bilo koju vrstu baze podataka, uključujući i Oracle baze podataka.
11. Cross-site scripting (XSS) predstavlja tip ranjivosti računarskih mreža u IKT sistemu i tipično se javlja u veb aplikacijama. U ovoj vrsti napada napadač ubacuje client-side skript u veb strane koje su pregledali drugi

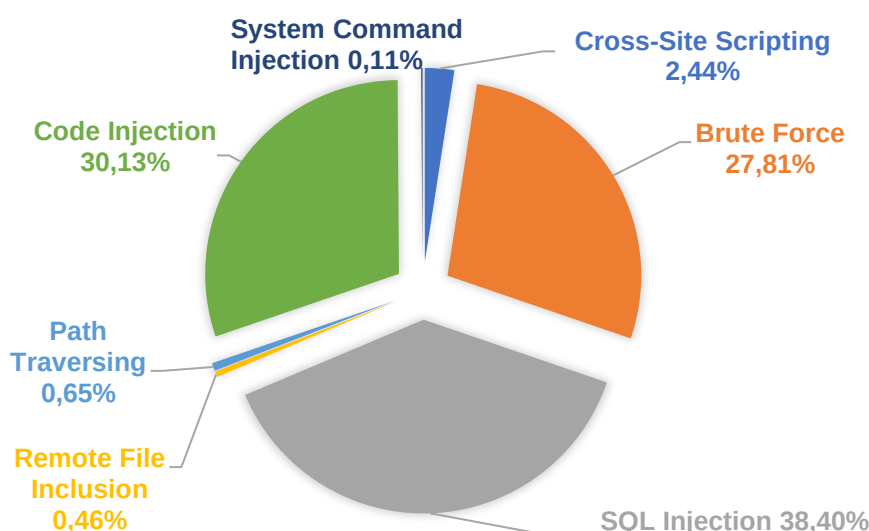
korisnici. XSS ranjivosti mogu se koristiti od strane napadača radi zaobilaženja kontrole pristupa određene politikom sajta. Ovi napadi čine oko 80% napada koji su izvršeni na veb sajtovima. Uticaj ovakvog napada može biti u rasponu od male smetnje do ozbiljnog bezbednosnog rizika.

12. Root.kit napadi se izvode infiltriranjem zlonamernog softvera u ciljani IKT sistem. Dizajniran je tako da skriva sebe u okviru ostalih resursa (direktorijuma, fajlova, procesa i sl.). Pri tome svoje delovanje sve vreme zadržava u napadnutom IKT sistemu.



Slika 1: Maliciozne aktivnosti na hostovanim Internet prezentacijama po godinama (CKISIP)

Izvor: Statistički podaci preuzeti iz periodičnog izveštaja CKISIP



Slika 2: Maliciozne aktivnosti prema servisima MO i VS na internetu (KISIP)

Izvor: Statistički podaci preuzeti iz periodičnog izveštaja CKISIP

Iz svega navedenog može se zaključiti da je IKT sistem stalno izložen raznim rizicima koji prete da degradiraju njegovu funkciju i učine ga osetljivim na gubitak poverljivih informacija. Njegov značaj za sistem odbrane Republike Srbije i Republiku

Srbiju u celini nameće potrebu sveobuhvatne procene rizika. Procena rizika u području informacione bezbednosti IKT sistema podrazumeva sistematičan proces organizovanja informacija i znanja u cilju donošenja odluka u

okviru šireg procesa upravljanja rizikom u kome se na sveobuhvatan način i na svim nivoima moraju identifikovati pretnje i analizirati i proceniti rizici asocirani sa izloženostima delovanju tih pretnji. Zbog toga se proces procene rizika mora sprovesti na svim nivoima komandovanja i rada i u svim sistemima od značaja za operativne i funkcionalne sposobnosti.

Pregled malicioznih aktivnosti na hostovanim internet prezentacijama prikazan je na slici 1.

U pogledu napada na servise MO i VS na Internetu, zastupljenost pojedinih malicioznih aktivnosti je data na slici 2.

Prikazani podaci pokazuju da je IKT sistem MO i VS konstantno pod napadima različitog tipa, a takođe može se uočiti trend povećanja ispoljavanja zlonamernih aktivnosti u 2017. godini u odnosu na 2016. godinu, prema svim Internet sajtovima.

3 ZAKLJUČAK

Sagledavanjem izazova, rizika i pretnji odbrani Republike Srbije, složenosti i kompleksnosti sistema odbrane, kao i aktivnosti na planiranju i pripremama odbrane Republike Srbije, uviđa se ogroman značaj pravovremenih, sigurnih, proverenih, zaštićenih, odnosno bezbednih informacija. Složenost i kompleksnost sistema odbrane, kako njegove strukture, tako i sistema upravljanja, rukovođenja i komandovanja sistemom, prouzrokuje i niz mera i aktivnosti koje

treba preduzeti u pogledu informacione bezbednosti.

Planiranje priprema civilnog društva za odbranu treba da bude stalan, planski, organizovan, sveobuhvatan, racionalan i efikasan proces, zasnovan na realnim mogućnostima i usklađen sa postojećim i potencijalnim izazovima, rizicima i pretnjama po bezbednost i odbranu Republike Srbije. Jedinstvenom metodologijom pripremanja, izrade, usvajanja, usklađivanja i ažuriranja planova obezbediće se maksimalan stepen povezivanja subjekata sistema odbrane u ostvarivanju i iznalaženju optimalnih rešenja za planirane ciljeve i stvaranje preduslova za efikasno izvršavanje postavljenih zadataka i preuzetih obaveza iz Plana odbrane u ratnom i vanrednom stanju.

Zbog mnogih ranjivosti, direktno i stalno su ugrožena informaciona dobra i primenjene savremene tehnologije, a posredno se pretnja ispoljava i prema korisnicima i čitavom društvu. Iako se pretnja, ostvarivanjem ispoljava kao sajber napad u virtuelnom prostoru, može imati dalekosežne posledice u materijalnom svetu i može ugroziti tradicionalne društvene aktivnosti, u koje spadaju i aktivnosti odbrambenog sistema. Većina savremenih armija, bez obzira na stepen društvenog i ekonomskog razvoja matične zemlje, vojni savezi i organizacije intenzivno su prisutni i svoje aktivnosti u sajber prostoru i dalje povećavaju.

CITIRANA DELA

Pleskonjić, D., Maček, N., Đoršević, B. i Carić, M. (2007). *Sigurnost računarskih sistema i mreža*. Beograd: Mikro knjiga.

Rodić, B, G. Đorđević, Da li ste sigurni da ste bezbedni, monografska publikacija, Produktivnost AD, Beograd, 2004. godina, strana 35-37.

Slavković, R., Kršljanin, D. (2015). Uticaj operativnog okruženja na sajber pretnje. *Vojno delo*, (5). Beograd: Medija centar „Obrana“.

Stajić, Lj. (2003). *Osnovi bezbednosti*. Beograd: Policijska akademija, str.16.

Datum prve prijave:	19.08.2018.
Datum prijema korigovanog članka:	20.11.2018.
Datum prihvatanja članka:	22.11.2018.

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

Style – **APA Sixth Edition:**

Beriša, H., & Jonev, K. (2019, 04 15). Izazovi informacione bezbednosti u sistemu odbrane Republike Srbije. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 1-9. doi:10.12709/fbim.07.07.01.01

Style – **Chicago Sixteenth Edition:**

Beriša, Hatidža, i Katarina Jonev. 2019. „Izazovi informacione bezbednosti u sistemu odbrane Republike Srbije.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 1-9. doi:10.12709/fbim.07.07.01.01.

Style – **GOST Name Sort:**

Beriša Hatidža and Jonev Katarina Izazovi informacione bezbednosti u sistemu odbrane Republike Srbije [Journal] // *FBIM Transactions* / ed. Čekerevac Zoran. - Beograd : MESTE, 04 15, 2019. - 1 : Vol. 7. - pp. 1-9.

Style – **Harvard Anglia:**

Beriša, H. & Jonev, K., 2019. Izazovi informacione bezbednosti u sistemu odbrane Republike Srbije. *FBIM Transactions*, 15 04, 7(1), pp. 1-9.

Style – **ISO 690 Numerical Reference:**

Izazovi informacione bezbednosti u sistemu odbrane Republike Srbije. **Beriša, Hatidža and Jonev, Katarina.** [ed.] Zoran Čekerevac. 1, Beograd : MESTE, 04 15, 2019, *FBIM Transactions*, Vol. 7, pp. 1-9.



NEDOZVOLJENOST OBRADJE PODATAKA O LIČNOSTI I PREKRŠAJNA ODGOVORNOST PO OSNOVU ZAKONA O ZAŠTITI LIČNOSTI

THE UNAUTHORIZED PROCESSING OF PERSONAL DATA AND MISDEMEANOR LIABILITY UNDER THE LAW OF PERSONAL DATA PROTECTION

Nenad Bingulac

Pravni fakultet za privredu i pravosuđe u Novom Sadu,
Privredna akademija Novi Sad, Novi Sad, Srbija

©MESTE

JEL kategorija: **K14, K24, K42**

Apstrakt

Zaštita ličnih podataka usled značajnog tehnološkog iskoraka i sve masovnijih korišćenja društvenih mreža, online usluga i sličnih savremenih pogodnosti, postaje sve teža, kako u doslovnom smislu, tako i u zakonodavnom pogledu, posebno onda kada ne postoji informisanost o tome koji se lični podaci u kojim slučajevima mogu zahtevati, a koji ne mogu. Po ovom pitanju pojedina istraživanja ukazuju na to da značajni procenat ljudi nije upoznat sa prethodno pomenutom tematikom, ali i da mnogi od njih nemaju ni neku posebnu volju da se o tome informišu. Upravo ovo dovodi do dodatne problematike posebno kada se radi o raznim mogućim oblicima zloupotreba ličnih podataka. U ovom istraživanju fokus će biti na dva centralna pitanja i to na nedozvoljenoj obradi podataka na osnovu zakona o zaštiti ličnosti, dok će se drugo pitanje odnositi na prekršajnu odgovornost koja proizilazi iz kršenja pomenutog zakona, a sve kako bi se postigla generalna i specijalna prevencija. Značaj razmatranja ove problematike nije samo u sagledavanju koji su to podaci čija obrada nije dozvoljena i razmatranju prekršajne odgovornosti usled kršenja pomenutog zakona, već je i u podizanju svesti o pomenutoj problematici, preventivnim merama zaštite, a posredno će se ukazati i na pribavljanje podataka o ličnosti na zakonom predviđen način.

Ključne reči: nedozvoljenost obrade podataka, prekršajna odgovornost, zakon o zaštiti ličnosti, obrada podataka

Adresa autora:

Nenad Bingulac

nbingulac@pravni-fakultet.info

Abstract

The protection of personal data due to significant technological breakthroughs and the growing use



of social networks, online services and similar modern conveniences is becoming increasingly difficult, both in the literal sense and in the legislative sense, especially when there is no information on which personal data in which cases can be requested and which can not. In this regard, some research indicates that a significant percentage of people are not familiar with the above-mentioned topic, but also that many of them have no special will to inform themselves. This is exactly what leads to additional issues, especially when it comes to various forms of misuse of personal data. In this research, the focus will be on two central issues, namely the unauthorized processing of data on the basis of the personal data protection, while the second question will relate to misdemeanor liability arising from violation of the mentioned law, all in order to achieve general and special prevention. The importance of considering this issue is not only in considering which data are not permitted and consideration of misdemeanor responsibility due to violation of the mentioned law, but also in raising awareness of the mentioned issue, preventive measures of protection, and indirectly it will be pointed to the collection of personal data on the law envisaged way.

Keywords: unauthorized processing of data, misdemeanor liability, law of personal data protection, data processing

1. UVOD

Razvoj društvene svesti i mnogobrojne potrebe uslovljavale su, ali i podsticale mnoge tehnološke razvoje. Neki od njih imali su kratkotrajnu primenu usled brzog prevazilaženja ili usled nedovoljne praktične primene ili zbog nemogućnosti za masovno primenjivanje usled raznih uslova npr. troškova održavanja, eksplataisanja i sl. Upotreba računara koncizno posmatrano imala je u pojedinim fazama oscilacije u volji i potrebi za njihovom (masovnom) primenom, ali ipak usavršavanjem mnogih tehnologija dovelo je do toga da se danas jednostavno ne može zamisliti svakodnevni život bez korišćenja računara.

Moglo bi se reći da postoji skoro potpuna zavisnost od upotrebe računara u privatne i poslovne svrhe, počevši od međusobne korespondencije, korišćenja i pružanja usluga, dok je posebno izražena upotreba računara u domenima razonode, edukacije i sl. (Bingulac, 2016: 125)

Pomenuta neminovnost se može posmatrati sa pozitivnog i negativnog aspekta. Nesporno je da kada se pitanje tehnološkog razvoja u ovoj sferi posmatra iz pozitivnog ugla najčešće se ističe brzina obrade podataka i informacija, zatim izuzetna mogućnost pretrage traženih informacija posebno kada radi o „snazi i širini“ interneta, mogućnost instant komunikacije sa apsolutnih udaljenosti, posebnosti cloud tehnologije, i dr. Pozitivna primena do te mere dominira da se često, a možda bi preciznije bilo napisati, najčešće, upotpunosti zanemaruju sve negativne moguće posledice koje mogu da izazovu razne

oblike šteta. Kao i mnoga druga tehničko i tehnološka dostignuća u istoriji čovečanstva, ne postoji odstupanje ni kod upotrebe savremenih tehnologija, npr. informacionih, koje mogu da budu korišćene i izložene različitim vidovima zloupotrebe. Tendencija razvoja tehnologija, a samim tim i novih načina upotrebe računara i računarskih sistema, je u uzlaznoj skali, te je stoga jasno da će načini i razni oblici zloupotreba nastaviti uporedni razvoj, posebno kada te nove tehnologije budu dostupne širem krugu korisnika.

Posmatrano sa aspekta pravne zaštite, tehnološki razvoj je neuporedivo brži i fleksibilniji u odnosu na stvaranje, preciziranje ili dopunjavanje postojeće zakonodavne politike zaštite. Dodatno, a realno je, da stanje se i sa postojanjem zakone zaštite ne može očekivati niti obezbediti sveobuhvatna sigurnost korisnika računarskih sistema, iako nije sporno da se apsolutna bezbednost ne može postići

Rizik da nove tehnologije ugroze postojeće bezbednosne mere, sve dok se ne razviju novi načini zaštite u fizičkom i zakonodavnom smislu, uvek postoji.

Jasno je da sa razvojem računarskih tehnologija paralelno se razvija obučavanje i usavršavanje lica koji će ih koristiti posebno ako se radi o nekim specijalizovanim rešenjima koja nisu predviđenja za masovnu upotrebu. Pomenuto ostavlja prostor da se iskoristi pomenuto za razne oblike zloupotreba.

Ne predstavlja nikakvu retkost da pojedinci ili manje organizovane grupe nezakonito pristupaju

nekom važnom javnom ili privatnom računarskom sistemu, ili kućnim računarima, iz raznih pobuda (sticanje protivpravne imovinske koristi, razni oblici krađe podataka, narušavanje privatnosti, iz drugih niskih pobuda i sl.). Ovaj oblik savremenog kriminaliteta ne poznaje granice, posebno kada se zloupotrebe ili napadi na neki računarski sistem vrše preko interneta. (Bingulac, 2016: 126)

Posebno osetljivo pitanje odnosi se na obradu podataka, tj. koji se podaci mogu i na koji način prikupljati i obrađivati. Prikupljanje podataka o ličnosti nužno ne mora da ima oblike koji će kod lica koje ih pruža stvoriti sumnju da se radi o nekoj zakonom ne dozvoljenoj radnji, npr. prikupljanje ličnih podataka potrošača od strane nekog prodajnog lanca a sa ciljem informisanja o nekim proizvodima ili sa ciljem usmerenog marketinga.

Upravo zbog pomenutog, cilj ovog istraživanja je da se razmotri ovo veoma kompleksno pitanje i da se ukaže na zakonsku zaštitu i prekršajnu odgovornost prilikom elektronskog prikupljanja i obrade podataka o ličnosti jer nesporno se radi o osetljivoj problematici posmatrano iz ugla mogućih zloupotreba.

Ozakonjenje ovog pravnog pitanja počinje još 1998. godine. Tada je u Saveznoj Republici Jugoslaviji usvojen Zakon o zaštiti podataka o ličnosti (Službeni list SRJ, broj 24/98). Isti zakon nastavio da važi i u pravnom poretku Državne zajednice Srbije i Crne Gore, a potom i Republike Srbije.

U svom trajanju od oko deset godina nije bilo njegove praktične primene niti su korišteni predviđeni mehanizmi zaštite, navode autori koji su se bliže bavili ovom problematikom u tom periodu. (Mišljenović, Nedić, Toskić, 2013: 20)

Novi Zakon o zaštiti podataka o ličnosti Republike Srbije, donešen je 2008. godine, njegova primena je otpočela 2009. godine.

Pomenutom je prethodilo usklađivanje domaćeg zakonodavstva sa evropskim te stoga je od značaja je ukazati da je Republika Srbija potpisala i ratifikovala Konvenciju Saveta Evrope broj 108 o zaštiti lica u odnosu na automatsku obradu podataka o ličnosti 2005. godine i da je potpisala je i ratifikovala Dodatni protokol uz Konvenciju 108 u vezi sa nadzornim organima i prekograničnim protokom podataka 2008. godine, a sve sa ciljem harmonizacije domaćeg

zakonodavstva sa evropskim. (Bingulac, 2016: 126)

2. OSVRT NA ZAČETKE PRAVNOG REGULISANJA ZAŠTITE PODATAKA O LIČNOSTI U EVROPSKOJ UNIJI

Zaštita podataka o ličnosti je pitanje koje ne može da izađe iz domena aktuelnosti isključivo iz razloga svakodnevnog uticaja na život.

Suštinski posmatrano, čovekovo pravo na zaštitu podataka o ličnosti proizilazi iz prava na privatn život koji se direktno odnosi na domen ljudskih prava i njihove garancije i zaštite posebno od strane evropskih institucija.

Upravo na osnovu brzog razvoja tehnologija posebno informacionih tehnologija postoji opravdana bojaznost da usled automatske obrade podataka se ugroze pomenuta prava pojedinca.

Posmatrano iz ugla evropskog zakonodavstva predviđa se da „svako ima pravo na zaštitu podataka o svojoj ličnosti. Takvi podaci moraju biti obrađeni pošteno za tačno određenu svrhu, na osnovu pristanka lica na koje se podaci odnose ili po nekom drugom osnovu utvrđenom zakonom. Svako ima pravo da pristupi prikupljenim podacima o svojoj ličnosti i pravo da zatraži njihovu ispravku.” Citirano se predviđa Poveljom o osnovnim pravima Evropske unije u Poglavlju II, članu 8.

Iz iznetog proizilazi da svako lice na osnovu zaštite podataka o ličnosti ima pravo da bude upoznato sa podacima koji se prikupljaju o njemu. Zatim da zna na koji način će se ti podaci obraditi obrađuju. Lice takođe ima pravo na uvid u prikupljene podatke, kao i na njihovu izmenu ako ima za tim potrebe.

Lice ima pravo da zna na koji su način podaci zaštićeni i gde se prenose. Pored pomenutog, postoji i obaveza davanja pristanka lica čiju su podaci za korišćenje tih podataka od strane drugog lica, vlasti ili nekog drugog subjekata. Pojedini autori još preciziraju da vrednosti zaštite podataka ne odnose se samo na privatnost. Ovim vrednostima, kako ih isti autori nazivaju, se ne može pristupiti isključivo sa stanovišta privatnosti, jer u pitanju su samostalne vrednosti koje pružaju

osnovna prava, odnosno pravo na zaštitu podataka. (Musar & Mišić, 2018: 12)

Kompleksnost i specifičnost sprovedena regulativa koje se odnose na zaštitu podataka o ličnosti ispoljila se na samom početku primene. Rezultati istraživanja početnih faza primene pomenute regulative pokazali su da je zakonodavni okvir Evropske unije bio konfuzan i diskutabilno primenljiv jer Direktive koje uređuju oblast zaštite podataka i to Direktiva 95/46/EZ, Direktiva 2002/58/EZ i Direktiva 2002/20/EZ su se preklapale u regulisanju i predviđanju, a pored toga što su uređivale ista pravna pitanja, pojedine sadržine bile su nejasne. (Musar & Mišić, 2018: 13)

Za posledicu je bilo da nije bio najjasniji pravni odnos između korisnika i davaoca usluga iz razloga što prava korisnika neće biti na kvalitetan i jedinstven način zaštićena. Postojao je opravdani strah od mogućnosti da upravo zbog novonastalih problema usled nepoznavanja i razumevanja regulativa usledi smanjenje pružanja usluga, a možda čak i potpunog prestanka pružanja usluga korisnicima. (Musar & Mišić 2018: 13)

Kao i u mnogim drugim slučajevima tako je i ovde došlo do „uplitanja” precedentnog prava.

Prva presuda Evropskog suda pravde koja se odnosila na ovu oblast proistekla je iz slučaja C-101/01, Bodil Lindqvist, a odnosila se na zaštitu podataka. Konkretno posmatrano, postupak koji je vođen pred sudom ticao se pitanja davanja pristanka lica čiji su podaci prikupljeni od strane kompanije i dalje njihovo korišćenje i zaštita. Ova presuda postigla je podizanje svesti o zaštiti ličnih podataka, ali i da je konačno započeta praktična primena direktiva. Značaj presude, u smislu da su podaci o ličnosti zaštićeni i da niko ne može da ih koristi bez prethodnog odobrenja, manifestovao se kod svih onih koji su do tada prikupljali i brađivali lične podatke. Zatim na osnovu pokazatelja moglo se videti da postepeno zemlje Evropske unije počinju da „pravilno” primenjuju Direktivu 95/46/EZ jer se po pojedinim autorima ova presuda koristila i kao neki oblik objašnjenja pomenute presude u smislu da su podaci zaštićeni ne samo sa stanovišta privatnosti, već i kao lično pravo. (Manolescu, 2010: 3 ; Musar & Mišić, 2018: 13)

3. OBRADA PODATAKA U SKLADU SA ZAKONOM O ZAŠTITI PODATAKA O LIČNOSTI

Poslednje izmene i dopune Zakona o zaštiti podataka o ličnosti načinjene su 2012. godine, a podsećanja radi usvojen je 2008. godine iako je primena usledila tek naredne.

Predmet Zakona je uređivanje uslova za prikupljanje i obradu podataka o ličnosti, prava lica i zaštita prava lica čiji se podaci prikupljaju i obrađuju. Zatim Zakonom se još uređuju pitanja ograničenja zaštite podataka o ličnosti, postupak pred nadležnim organom za zaštitu podataka o ličnosti, obezbeđenje podataka, evidencija, iznošenje podataka iz Republike Srbije i nadzor nad izvršavanjem ovog zakona.

U skladu sa evropskim vrednostima u članu 1 stavu 2 predviđa se da se zaštita podataka o ličnosti obezbeđuje svakom fizičkom licu, bez obzira na državljanstvo i prebivalište, rasu, godine života, pol, jezik, veroispovest, političko i drugo uverenje, nacionalnu pripadnost, socijalno poreklo i status, imovinsko stanje, rođenje, obrazovanje, društveni položaj ili druga lična svojstva.

Zakonodavac je pod terminom podatak o ličnosti podrazumeva svaku informaciju koja se odnosi na fizičko lice, bez obzira na oblik u kome je izražena i na nosač informacije npr. papir, traka, film, elektronski medij i sl, po čijem nalogu, u čije ime, odnosno za čiji račun je informacija pohranjena, datum nastanka informacije, mesto pohranjivanja informacije, način saznavanja informacije, a što može biti neposredno, putem slušanja, gledanja i sl, odnosno posredno, putem uvida u dokument u kojem je informacija sadržana i sl.

Pod obradom podataka smatra se na osnovu Zakona, svaka radnja koja je preduzeta u vezi sa podacima počevši od prikupljanja podataka, beleženja, prepisivanja, umnožavanja, kopiranja, prenošenja, pretraživanja, razvrstavanja, zatim pohranjivanja podataka, razdvajanja, ukrštanja, objedinjavanja, upodobljavanja, menjanja, obezbeđivanja, korišćenja, stavljanja na uvid, otkrivanja, objavljivanja, širenja, snimanja, organizovanja, čuvanja, prilagođavanja, otkrivanja putem prenosa ili na drugi način činjenje dostupnim, prikriivanja, izmeštanja i na

drugi način činjenje nedostupnim, kao i sprovođenje drugih radnji u vezi sa navedenim podacima, bez obzira da li se vrši automatski, poluautomatski ili na drugi način. Definisanje obrade podataka na ovaj zakonodavac je predvideo članom 3, stavom 1, tačkom 3. Zakona o zaštiti podataka o ličnosti.

Zakonom se predviđa nekoliko načina obrade podataka i to: obrada sa pristankom, obrada bez pristanka i obrada od strane organa vlasti. Zakonom se još predviđa i obrada naročito osetljivih podataka, ali o tome će biti više reči u nastavku rada.

Zakonodavac predviđa da punovažan pristanak za obradu podataka može dati lice, nakon što ga rukovalac tj. fizičko ili pravno lice, odnosno organ vlasti koji obrađuje podatke prethodno obavesti o obradi.¹

Punovažan pristanak se može dati pismeno ili usmeno na zapisnik ili preko punomoćnika. Kada se punovažan pristanak daje preko punomoćnika, punomoćje mora biti overeno, izuzev ako zakonom nije propisano drukčije.

U posebnim slučajevima pristanak može da da zakonski zastupnik ili staralac za lica koja nisu sposobna za davanje pristanka.

Punovažni pristanak može se dati i za lice koje je umrlo i to od strane supružnika, deca sa navršених 15 godina života, roditelja, braća i sestre, odnosno zakonski naslednik ili lice koje je za to odredio umrli.²

Zakonodavac je predvideo i mogućnost opoziva pristanka. Punovažan opoziv se može dati pismeno ili usmeno na zapisnik. U slučaju opoziva, lice koje je dalo pristanak dužno je da rukovaocu naknadi opravdane troškove i štetu, u skladu sa propisima koji uređuju odgovornost za štetu. Bilokakva dalja obrada podataka nakon opoziva je nedozvoljena. Zakonodavac je opoziv pristanka predvideo članom 11.

Obrada bez pristanka dozvoljena je: 1) da bi se ostvarili ili zaštitili životno važni interesi lica ili

drugog lica, a posebno život, zdravlje i fizički integritet; 2) u svrhu izvršenja obaveza određenih zakonom, aktom donetim u skladu sa zakonom ili ugovorom zaključenim između lica i rukovaoca, kao i radi pripreme zaključenja ugovora; 3) u svrhu prikupljanja sredstava za humanitarne potrebe. Zakonodavac dodatno još predviđa da rukovalac može podatke o ličnosti, koje već obrađuje u određene svrhe na osnovu zakonskog ovlašćenja, da obrađuje i u svrhu prikupljanja sredstava za humanitarne potrebe i 4) u drugim slučajevima koji su predviđeni zakonom, radi ostvarenja pretežnog opravdanog interesa lica, rukovaoca ili korisnika.³

Naredni način je obrada podataka od strane organa vlasti. Organ vlasti obrađuje podatke bez pristanka lica, ako je obrada neophodna radi obavljanja poslova iz svoje nadležnosti određenih zakonom u cilju ostvarivanja interesa nacionalne ili javne bezbednosti, odbrane zemlje, sprečavanja, otkrivanja, istrage i gonjenja za krivična dela, ekonomskih, odnosno finansijskih interesa države, zaštite zdravlja i morala, zaštite prava i sloboda i drugog javnog interesa, a u drugim slučajevima na osnovu pismenog pristanka lica.⁴

Potrebno je naznačiti da postoji mogućnost automatizovane obrade podataka i tada odluka koja proizvodi pravne posledice za lice ili pogoršava njegov položaj, ne može biti isključivo zasnovana na podacima koji se obrađuju automatizovano i koji služe oceni nekog njegovog svojstva, kao što su radne sposobnosti, pouzdanosti, kreditne sposobnosti i sl. Odluka na osnovu automatizovane obrade moguća je isključivo u slučajevima kada je to zakonom izričito određeno, odnosno kada se usvaja zahtev lica u vezi sa zaključenjem ili ispunjenjem ugovora, uz sprovođenje odgovarajućih mera zaštite, a pri čemu lice mora biti upoznato sa postupkom automatizovane obrade i načinom donošenja odluke.⁵

Zakonodavac prikupljanje podataka predviđa članom 14 i to na način da se podaci prikupljaju

¹ Obaveštavanje o obradi Zakon o zaštiti podataka o ličnosti (ZZPL) predviđa u članu 15. koji će se u radu detaljnije razmotriti.

² Obrada sa pristankom predviđa se članom 10. ZZPL

³ Obrada bez pristanka predviđa se članovima 12 i 12a ZZPL

⁴ Obrada podataka od strane organa vlasti predviđa se članom 13. ZZPL

⁵ Odluka pomoću automatizovane obrade predviđa se članom 9. ZZPL

od lica na koje se odnose i od organa uprave koji su zakonom ovlašćeni za njihovo prikupljanje. Predviđa se istim članom da se podaci mogu prikupljati i od drugog lica ako: 1) je to predviđeno ugovorom zaključenim sa licem na koje se podaci odnose; 2) je to propisano zakonom; 3) je to neophodno s obzirom na prirodu posla; 4) prikupljanje podataka od samog lica na koje se odnose zahteva prekomerni utrošak vremena i sredstava; i ako 5) se prikupljaju podaci radi ostvarenja ili zaštite životno važnih interesa lica na koje se odnose, posebno života, zdravlja i fizičkog integriteta.

Naročito osetljivi podaci predstavljaju podatke koji se odnose na nacionalnu pripadnost, rasu, pol, jezik, veroispovest, pripadnost političkoj stranci, sindikalno članstvo, zdravstveno stanje, primanje socijalne pomoći, žrtvu nasilja, osudu za krivično delo i seksualni život. Ovi podaci se mogu obrađivati na osnovu slobodno datog pristanka lica, osim kada zakonom nije dozvoljena obrada ni uz pristanak.

Pored pomenutog, zakonodavac predviđa da se podaci koji se odnose na pripadnost političkoj stranci, zdravstveno stanje i primanje socijalne pomoći, mogu se obrađivati bez pristanka lica, samo ako je to zakonom propisano.

Obrada ovih podataka mora biti posebno označena i zaštićena merama zaštite. Poverenik ima pravo uvida u podatke i provere zakonitosti obrade po službenoj dužnosti ili po zahtevu lica, odnosno rukovaoca. Način arhiviranja i mere zaštite podataka uz prethodno pribavljeno mišljenje Poverenika, uređuje Vlada.

Pristanak za obradu naročito osetljivih podataka daje se u pismenom obliku, koji sadrži oznaku podatka koji se obrađuje, svrhu obrade i način njegovog korišćenja.

Ako davalac pristanka nije pismen ili iz drugog razloga nije u stanju da pristanak svojeručno potpiše, pristanak je punovažan ako dva svedoka svojim potpisima potvrde da pismeno sadrži izjavu volje davaoca pristanka.

Opoziv pristanka za obradu naročito osetljivih podataka, predviđa se na način kao i u

slučajevima opšteg opoziva pristanka o kojem je već bilo reči.⁶

Na kraju ovog dela istraživanja nužno je ukazati i na pitanje obaveštavanja o obradi ličnih podataka, koje se predviđa članom 15.

Rukovalac koji podatke prikuplja od lica na koje se odnose, odnosno od drugog lica, pre prikupljanja ima obavezu da upozna lice na koje se podaci odnose, odnosno drugo lice o: 1) svom identitetu, odnosno imenu i adresi ili firmi, odnosno identitetu drugog lica koje je odgovorno za obradu podataka u skladu sa zakonom; 2) svrsi prikupljanja i dalje obrade podataka; 3) načinu korišćenja podataka; 4) identitetu lica ili vrsti lica koja koriste podatke; 5) obaveznosti i pravnom osnovu, odnosno dobrovoljnosti davanja podataka i obrade; 6) pravu da pristanak za obradu opozove, kao i pravne posledice u slučaju opoziva; 7) pravima koja pripadaju licu u slučaju nedozvoljene obrade i o 8) drugim okolnostima čije bi nesaopštavanje licu na koje se odnose podaci, odnosno drugom licu bilo suprotno savesnom postupanju.

Pomenuta obaveza ne postoji kada je upoznavanje, s obzirom na okolnosti slučaja, nije moguće ili je očigledno nepotrebno, odnosno neprimereno, a naročito ako je lice na koje se odnose podaci, odnosno drugo lice već poznato sa time ili ako lice na koje se podaci odnose nije dostupno.

Zakonodavac dodatno predviđa da rukovalac koji je podatke o licu prikupio od drugog lica, upoznaće sa pomenutim uslovima lica na koje se podaci odnose, bez odlaganja ili najkasnije pri prvoj obradi, osim kada takvo upoznavanje, s obzirom na okolnosti slučaja, nije moguće, odnosno zahteva prekomerni utrošak vremena i sredstava ili je očigledno nepotrebno. Rukovalac je dužan da obavesti lice na koje se podaci odnose čim to postane moguće, odnosno ako lice to zahteva. Upoznavanje potrebno ako je lice na koje se odnose podaci već poznato sa time, odnosno ako lice na koje se podaci odnose nije dostupno ili ako je prikupljanje i dalja obrada podataka od drugog lica propisana zakonom. Zatim, rukovalac je dužan da obavesti lice na koje

⁶ Naročito osetljivi podaci, pristanak za obradu naročito osetljivih podataka i opoziv pristanka za obradu

naročito osetljivih podataka predviđaju se članovima 16,17 i 18. ZZPL

se podaci odnose čim to postane moguće, odnosno ako lice to zahteva.

Upoznavanje lica vrši se u pismenom obliku u slučaju kada se za pristanak za obradu daje u pismenom obliku, osim ako lice na koje se podaci odnose, odnosno drugo lice, pristane na usmeno upoznavanje.

Na kraju, zakonodavac je još predvideo da će rukovalac obavestiti lice na koje se podaci odnose i korisnika o izmeni, dopuni ili brisanju podataka bez odlaganja, a najkasnije u roku od 15 dana od dana izmene, dopune ili brisanja podataka.

4. NEDOZVOLJENOST OBRADE LIČNIH PODATAKA

Zakonom o zaštiti podataka o ličnosti članom 8. predviđa se nedozvoljenost obrade ličnih podataka.

Zakonodavac je predvideo da obrada nije dozvoljena ako: 1) fizičko lice nije dalo pristanak za obradu, odnosno ako se obrada vrši bez zakonskog ovlašćenja; 2) se vrši u svrhu različitu od one za koju je određena, bez obzira da li se vrši na osnovu pristanka lica ili zakonskog ovlašćenja za obradu bez pristanka, osim ako se vrši u svrhu prikupljanja sredstava za humanitarne potrebe; 3) svrha obrade nije jasno određena, ako je izmenjena, nedozvoljena ili već ostvarena; 4) je lice na koje se podaci odnose određeno ili određivo i nakon što se ostvari svrha obrade; 5) je način obrade nedozvoljen; 6) je podatak koji se obrađuje nepotreban ili nepodesan za ostvarenje svrhe obrade; 7) su broj ili vrsta podataka koji se obrađuju nesrazmerni svrsi obrade; 8) je podatak neistinit i nepotpun, odnosno kada nije zasnovan na verodostojnom izvoru ili je zastareo.

U pojedinim komentarima Zakona o zaštiti podataka o ličnosti može se videti stavovi koji ukazuju na neke posebnosti koje se odnose na nedozvoljenost obrade podataka.

Indirektno se može zaključiti da član 8. predstavlja „mini rezime” onoga šta se mora ispuniti da bi obrada podataka bila dozvoljena.

Ako se započne sa stanovišta da se ne sme odstupiti od načela zabrane diskriminacije, srazmernosti i načela tačnosti i ažurnosti, obrada podataka o ličnosti nije dozvoljena jedino kada

fizičko lice nije dalo pristanak za obradu, odnosno ako se obrada vrši bez zakonskog ovlašćenja; kada se vrši u svrhu različitu od one za koju je određena, bez obzira da li se vrši na osnovu pristanka lica ili zakonskog ovlašćenja za obradu bez pristanka; kada svrha obrade nije jasno određena, ako je izmenjena, nedozvoljena ili već ostvarena; kada je lice na koje se podaci odnose određeno ili određivo i nakon što se ostvari svrha obrade i kada je način obrade nedozvoljen. (Baković Tamburković et al., 2014: 26)

Isti autori su još ukazali i na to da je nužno prethodno određivanje svrhe podataka, u kontekstu svrhe koja je određena zakonom ili koja se jasno može videti na osnovu pristanka pojedinca. Kao izuzetak se predviđa obrada za istorijske, statističke i naučno-istraživačke svrhe. Podaci, koji su već prikupljeni i obrađeni za druge svrhe, mogu obrađivati u istorijske, statističke i naučno-istraživačke svrhe. Zatim, pored određivanja svrhe, mora biti precizno opredeljena, nepromenjena i dozvoljena. Ako do promene iz nekih razloga i dodje rukovalac morad za promenu obezbediti novi tj. ponovni pristanak lica. (Musar, 2009: 25)

Boljim razmatranjem može se uočiti da postoji i vremensko ograničenje obrade podataka, kako to navode autori koji su se bavili znatno preciznije analizom Zakona o zaštiti podataka o ličnosti. Naime, radi se o tome da obrada podataka, nije dozvoljena u slučaju kada je svrha obrade već postignuta. Zatim, obrada podataka o ličnosti, takođe nije dozvoljena kada je svrha obrade postignuta. Znači, podaci o ličnosti, nakon ispunjenja svrhe obrade moraju se izbrisati ili uništiti. Isti autori još dodaju da ispunjenje svrhe obrade podataka o ličnosti i rok čuvanja podataka ne spadaju uvek u isti vremenski period, iz razloga jer drugi zakon može odrediti rok čuvanja određenih podataka o ličnosti, bez obzira na to što je svrha obrade već bila ispunjena. (Musar, 2009: 25)

Pored pomenutog, uočena je i jedna praktična posebnost koja se odnosi na konkretnu obradu podataka i to u smislu da je obrada podataka o ličnosti jedino dozvoljena na način na koji je to predviđeno zakonom. Najbolje se to može sagledati kroz primer: fotokopiranje lične karte i čuvanje fotokopije u fizičkom obliku je dozvoljeno od strane pojedinca, a usled nekih tehničkih

okolnosti izvršeno je skeniranje lične karte i čuvanje u elektronskom obliku, što pojedinac nije dozvolio. Iz ovoga proizilazi da podatke o ličnosti pojedinca su obrađivani na način koji nije dozvoljen jer za takav način obrade nije bila data saglasnost pojedinca. (Musar, 2009: 30)

Po poslednjim dostupnim podacima, samo u mesecu avgustu 2018. godine služba Poverenika primila je 572 predmeta koji se odnose na zaštitu podataka o ličnosti. Iz prethodnog perioda je preneto 642 predmeta. Preciznije posmatrano pripremljeno je 88 mišljenja u vezi sa zaštitom podataka o ličnosti. Rešeno je 7 žalbi zbog povrede prava, na sledeći način; okončano je 186 inspekcijskih nadzora nad sprovođenjem i izvršavanjem Zakona o zaštiti podataka o ličnosti. U okviru inspekcijskog nadzora Poverenik je doneo: 52 upozorenja rukovaocima podataka kojima je ukazano na nepravilnosti u obradi podataka, 44 obaveštenja rukovaocima po čl. 50. Zakona u vezi sa najavljenom obradom podataka, 19 odgovora podnosiocima prijave povodom kojih je pokrenut inspekcijski nadzor, podneta je 1 krivična prijava. Obradeno je 394 evidencije zbirke podataka o ličnosti; 3 predmeta iz oblasti unapređenja zaštite i preventive; postupljeno je po 13 zahteva za promenama u Centralnom registru; i doneto je 1 rešenje kojim se dozvoljava iznošenje podataka. U Centralnom registru je registrovano 49 rukovalaca i 368 zbirke podataka. (Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, 2018)

Iz prikazanih podataka jasno se vidi koji stepen aktivnosti postoji kada je reč o zaštiti ličnih podataka, što predstavlja dobar pomak u odnosu na neke ranije periode.

5. KAZNE NE ODREDBE PO OSNOVU ZAKONA O ZAŠTITI PODATAKA O LIČNOSTI

Kaznene odredbe predviđene u glavi X Zakona o zaštiti podataka o ličnosti, tj. u članu 57. Naravno, radi se o prekršajnoj odgovornosti, a zakonodavac je predvideo novčanu kaznu kao vid sankcije.

Predviđa se da će se rukovalac, obrađivač ili korisnik koji ima svojstvo pravnog lica kazniti novčanom kaznom za prekršaj u rasponu od 50.000 do 1.000.000 dinara ako: 1) obrađuje podatke bez pristanka (član 12); 2) obrađuje

podatke suprotno uslovima koji su predviđeni za obradu od strane organa vlasti (član 13); 3) prikuplja podatke od drugog lica suprotno od predviđeno Zakonom (član 14); 4) pre prikupljanja podataka ne upozna lice na koje se podaci odnose, odnosno drugo lice o uslovima koji su predviđeni prilikom obaveštavanja o obradi (član 15); 5) obrađuje naročito osetljive podatke suprotno predviđanju u Zakonu (članovi 16-18); 6) ne učini dostupnim sve podatke u stanju u kakvom se nalaze suprotno (član 27); 7) ne izda kopiju podatka u obliku u kojem se informacija nalazi suprotno (član 28); 8) ne obriše podatke iz zbirke podataka (član 36); 9) ne izvrši rešenje Poverenika po žalbi (član 41); 10) postupi suprotno obavezi čuvanja tajne (član 46); 11) postupi suprotno obavezi preduzimanja organizacionih i tehničkih mera (član 47); 12) ne obrazuje evidenciju, odnosno ne ažurira evidenciju (član 48); 13) ne obavesti Poverenika o nameri uspostavljanja zbirke podataka u propisanom roku (član 49); 14) ne dostavi Povereniku evidenciju, odnosno promene u zbirci podataka u propisanom roku (član 51); 15) iznosi podatke iz Republike Srbije suprotno načinu kako je to predviđeno Zakonom (član 53); 16) ne omogućiti ovlašćenom licu nesmetano vršenje nadzora i ne stavi mu na uvid i raspolaganje potrebnu dokumentaciju (član 55); 17) ne postupi po nalogima Poverenika (član 56).

Za predviđene prekršaje, kazniće se preduzetnik novčanom kaznom od 20.000 do 500.000 dinara, a fizičko lice, odnosno odgovorno lice u pravnom licu, državnom organu, odnosno organu teritorijalne autonomije i jedinice lokalne samouprave kazniće se novčanom kaznom od 5.000 do 50.000 dinara.

Na osnovu prikazanih raspona novčanih kazni, može se smatrati da upravo zbog značajnog raspona, sud može izricanjem novčane kazne postigne adekvatnu individualizaciju kazne. Da li je potrebno pooštriti kaznenu politiku, s obzirom da prilikom ovog istraživanja nismo bili u mogućnosti da dođemo do podataka o povratu, niti smo imali uvida u visine izrečenih kazni, morali bi da ukratimo mišljenje na tu temu.

6. ZAKLJUČCI

Pojedini statistički pokazatelji i analize ukazuju da građani Srbije su do skoro, veoma „lako i često”

davali svoje lične podatke, a posebno matični broj. Na osnovu istih pokazatelja može se videti da svest o mogućim zloupotrebama je bila na niskom nivou, a isto tako na niskom nivou je bilo interesovanje građana o zaštiti ličnih podataka. Podsećanja radi, tokom 2014. godine, desetak meseci, oko 5 miliona matičnih brojeva je bilo javno dostupno na sajtu Agencije za privatizaciju. (Milivojević, 2017)

Računarska tehnologija, posebno tokom poslednje decenije, ima ubrzan razvoj, a paralelno sa njom razvija se obučenost onih koji imaju za cilj da ovu tehnologiju koriste za razne oblike zloupotreba što se često manifestuje kroz nezakonito pristupanje nekom važnom javnom ili privatnom računarskom sistemu, ili kućnim računarima.

Problematika koja je razmatrana u ovom istraživanju prvenstveno se odnosi na nedozvoljenu obradu podataka na osnovu zakona o zaštiti ličnosti i na pitanje prekršajne odgovornosti koja proizilazi iz kršenja pomenutog zakona, a sve kako bi se postigla generalna i specijalna prevencija, ali i da se obezbedi zaštita prava na privatnost.

Zakonom o zaštiti podataka o ličnosti predviđena je prekršajna odgovornost za kršenje odredbi ovog zakona, a sve sa ciljem kako ne bi došlo do nesavesnog ili samovoljnog ponašanja lica ili organa koji te podatke prikuplja u skladu sa zakonom. Na ovaj način ujedno se vrši i prevencija zloupotrebe tih podataka, koji su prikupljeni, kao što je već rečeno, na zakonom predviđen način.

Kaznena politika je isključivo se odnosi na prekršajnu odgovornost, za koju su predviđene novčane kazne. Mišljenja smo da bi bilo dobro da se u nekoj narednoj izmeni i dopuni zakona predvidi i mera zaštite tj. zabrana odgovornom licu da vrši određene poslove kako bi se postigla još veća zaštita.

Ideja i cilj razmatranja ove problematike koja i kada nije u centralnom fokusu ipak predstavlja veoma značajno pitanje, je da pored ukazivanja i razmatranja pitanja od značaja, a koja se odnose na obradu podataka o ličnosti, jeste i da se na indirektan način podigne stepen svesti o pomenutoj problematici i preventivnim merama zaštite, što nesporno predstavlja poseban cilj.

CITIRANA DELA

- Baković Tamburkovski, B, Nedić, B. i Mišljenović, U. (2014). Priručnik za sudije upravnog suda za primenu zakona o zaštiti podataka o ličnosti, Ministarstvo pravde Republike Srbije, Beograd
- Bingulac, N. (2016). Prekršajna odgovornost usled kršenja zakona o zaštiti podataka o ličnosti, Regionalno naučno stručno savetovanje ZITEH-16, održano 3. juna 2016. godine, Beograd. Zbornik radova: „Zloupotreba informacionih tehnologija i zaštita“. Izdavač: *Udruženje sudskih veštaka za informacione tehnologije*, str.125-133.
- Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) OJ L 108, 24.4.2002.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281, 23.11.1995.
- Manolescu, D. (2010). Data protection as a fundamental right, *Effectius – effective justice solutions*, Published as part of the Effectius Newsletter, Issue 5.
- Milivojević, A. (2017). *Privatnost građana godinama na izvolite*, Preuzeto 13.09.2018. sa: <https://www.cins.rs/srpski/news/article/privatnost-gradjana-godinama-na-izvolite>
- Mišljenović, U., Nedić, B. i Toskić, A. (2013). Zaštita privatnosti u Srbiji, *Partneri za demokratske promene Srbija*, Beograd.

- Musar Pirc, N. (2009). Vodič kroz zakon o zaštiti podataka o ličnosti, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, Beograd
- Musar Pirc, N., i Mišić Kraigher, T. (2018). Zaštita podataka i nadležnosti institucija Evropske Unije, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, Beograd
- Povelja o osnovnim pravima Evropske unije, 7. decembar 2000.g., Službeni list Evropskih zajednica, 18. decembar 2000, 2000/C364/01
- Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti (2018). *Zbirni mesečni statistički podaci*, Preuzeto 13.09.2018. sa: <https://www.poverenik.rs/sr-yu/o-nama/mesecni-statisticki-izvestaji.html>
- Zakon o zaštiti podataka o ličnosti Savezne Republike Jugoslavije, Službeni list SRJ, broj 24/98
- Zakon o zaštiti podataka o ličnosti, Službeni glasnik RS, br. 97/2008, 104/2009 - dr. zakon, 68/2012 - odluka US i 107/2012

Datum prve prijave: 10.09.2018.
Datum prijema korigovanog članka: 20.11.2018.
Datum prihvatanja članka: 27.03.2019.

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

Style – **APA Sixth Edition**:

Bingulac, N. (2019, 04 15). Nedozvoljenost obrade podataka o ličnosti i prekršajna odgovornost po osnovu Zakona o zaštiti ličnosti. (Z. Čekerevac, Ed.) *FBIM Transactions*, 7(1), 10-19. doi:10.12709/fbim.07.07.01.02

Style – **Chicago Sixteenth Edition**:

Bingulac, Nenad. 2019. "Nedozvoljenost obrade podataka o ličnosti i prekršajna odgovornost po osnovu Zakona o zaštiti ličnosti." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 10-19. doi:10.12709/fbim.07.07.01.02.

Style – **GOST Name Sort**:

Bingulac Nenad Nedozvoljenost obrade podataka o ličnosti i prekršajna odgovornost po osnovu Zakona o zaštiti ličnosti [Journal] // *FBIM Transactions* / ed. Čekerevac Zoran. - Beograd : MESTE, 04 15, 2019. - 1 : Vol. 7. - pp. 10-19.

Style – **Harvard Anglia**:

Bingulac, N., 2019. Nedozvoljenost obrade podataka o ličnosti i prekršajna odgovornost po osnovu Zakona o zaštiti ličnosti. *FBIM Transactions*, 15 04, 7(1), pp. 10-19.

Style – **ISO 690 Numerical Reference**:

Nedozvoljenost obrade podataka o ličnosti i prekršajna odgovornost po osnovu Zakona o zaštiti ličnosti. **Bingulac, Nenad**. [ed.] Zoran Čekerevac. 1, Beograd : MESTE, 04 15, 2019, *FBIM Transactions*, Vol. 7, pp. 10-19



SOCIJALNI INŽENJERING I LIČNI PODACI

SOCIAL ENGINEERING AND PERSONAL DATA

Srđan Blagojević

Visoka poslovna škola strukovnih studija „Čačak“, Beograd, Srbija

©MESTE

JEL Category: C88, L86

Apstrakt

U današnjem informacionom okruženju sve je više pretnji i opasnosti za bezbednost računarskih korisnika. Jedna od ovih pretnji koja je veoma rasprostranjena i bez izgleda da se u budućnosti umanji, je svakako krađa ličnih podataka. Da bi se do njih došlo, zlonamernici su spremni na obimnu pripremu, istraživanja pojedinaca i kompanija, čekajući pravi trenutak da napadnu i ostvare svoje ciljeve, pa je potrebno uočiti i neke od najkarakterističnijih prevara koje koriste socijalni inženjering, kao i njihovu genezu na Internetu i društvenim mrežama. Korišćenje društvenih mreža je kritično u odnosu na bezbednost i privatnost korisnika. Velika količina informacija objavljenih i često javno podeljenih na profilu korisnika, sve više privlači pažnju napadača. Umesto da napadač inicira kontakt sa žrtvom, metode obrnutog socijalnog inženjeringa se primenjuju da žrtva bude namamljena da prva kontaktira napadača što za posledicu ima ostvaren visok stepen poverenja između žrtve i napadača. Integracija socijalnog inženjeringa u ove napade predstavlja nove, složenije pretnje i pokušaje da se od korisnika Interneta uzmu lični podaci koji su za napadača moneta kojom se trguje ili koja se lako zamenjuje za novac. Da bi se ovi napadi na vreme prepoznali, pomaže nam uočavanje njihovih karakteristika, a da bi smo u potpunosti sagledali problem, neophodno je znati i pravu vrednost ličnih podataka i šta oni predstavljaju u svetu crnog Internet tržišta.

Ključne reči: socijalni inženjering, lični podaci, prevare, bezbednost, zaštita.

Abstract

In today's information environment, there are more threats and dangers to the security of computer users. One of these threats that is very widespread and without the chance to zoom out in the future, is certainly stealing personal data. To occur, the malicious men are ready for extensive preparation, research of individuals and companies, waiting for the right moment to invade and achieve their goals, so it is necessary to spot some of the most distinctive fraud used by social engineering and their genesis on the Internet and social networks. Usage of social networks is critical of the security and privacy of users. A large amount of information published and often publicly shared on users' profile, is increasingly drawing the attention of the attackers. Instead of the attacker initiating contact with the victim, the method of reverse social engineering is applied for the victim to be lured to the first contact with the attacker, which results in a high level of trust between the victim and the attacker. Integration of social engineering in these attacks is a new, more complex threat that attempts to take

Adresa autora:

Srđan Blagojević

srdjan@hotmail.ca



personal data from internet users that is easy to trade with or to cash in. In order to identify these attacks in time, it helps to see their characteristics, and in order to see the problem fully, it is necessary to know the true value of personal information and what they represent in the world of black Internet markets.

Keywords: social engineering, personal data, fraud, security, protection.

1 UVOD

Problem upravljanja bezbednošću ima više aspekata što ga čini veoma kompleksnim. Što je obimniji i kompleksniji softver koji koristi, povećava se i njegova ranjivost. Ovu činjenicu koriste hakeri, zlonamerni kompjuterski stručnjaci, te nalaze ove osetljive tačke i koriste ih u cilju lične promocije, ostvarivanja koristi ili iz puke obesti. Posledice ovih napada, nezavisno od motiva, uvek predstavljaju veliki trošak za pojedince i kompanije. Razni podaci i druge informacije, mogu biti od koristi onima kojima je cilj trka za zaradom. Stoga je poznavanje pretnji i opasnosti koje sa sobom nosi informaciona tehnologija od presudne važnosti za poslovanje i zaštitu kompanija i pojedinca.

Jedna od ovih pretnji koja je veoma rasprostranjena i bez izgleda da se u budućnosti umanji, je svakako krađa ličnih podataka. Da bi se do njih došlo, zlonamernici su spremni na obimnu pripremu, istraživanja pojedinaca i kompanija, čekajući pravi trenutak da napadnu i ostvare svoje ciljeve.

U tu svrhu, razvijaju se i koriste nove metode socijalnog inženjeringa i obrnutog socijalnog inženjeringa na Internetu uz često korišćenje društvenih mreža kao načina za izvođenje napada.

2 SOCIJALNI INŽENJERING

Socijalni inženjering nije nova nauka, ali sa pojavom društvenih mreža, dobija na snazi i značaju zato što su informacije o potencijalnim žrtvama lakše dostupne pa se prikupljaju brže i lakše nego ranije. Takođe, propulzivne metode i taktike, daju socijalnom inženjeringu na značaju u informatičkom okruženju, odnosno na Internetu, jer više nije neophodno sresti nekoga licem u lice, već se napadi mogu izvršiti masovno i bez ličnog kontakta.

Ovaj termin danas se koristi da opiše razne načine koje pojedinci koriste da prevare, obmanu i izmanipulišu svoje žrtve da bi od njih izvukli poverljive informacije i novac.

Kriminalci koriste poverenje ljudi da saznaju brojeve njihovih računa, kreditnih kartica, lozinke i druge lične podatke. Ove kriminalne aktivnosti se obavljaju „online“ odnosno, elektronskom poštom, preko društvenih mreža, sajtova, telefonom ili ličnim kontaktom.

Socijalni inženjering se može podeliti u dve osnovne grupe:

1. Masovni
2. Ciljani

Masovni socijalni inženjering koristi osnovne tehnike i okrenut je prema široj populaciji, kao što je na primer masovno slanje pecačkih poruka ili reklama, dok je ciljani usmeren ka vrlo specifičnim individuama i kompanijama za koje se misli da su veći „ulov“, pa je složeniji i zahteva veći nivo poznavanja funkcionisanja, potreba i okolnosti svojih meta.

Načini na koji se izvodi kriminalna aktivnost su različiti ali metodi kojima se služe kriminalci generalno prate istu matricu koja se sastoji od četiri osnovna koraka:

- Prikupljanje informacija
- Upoznavanje i razvoj poverenja
- Otkrivanje slabosti / ranjivih mesta
- Izvršenje dela.

Tipovi napada koji koriste socijalni inženjering mogu se podeliti na sledeće:

1. Poruke – Forma socijalnog inženjeringa koja koristi poruke, bilo da su poslate elektronskom poštom, SMS-om ili preko neke od multimedijalnih mreža za komunikaciju, je takva da se napadači, kroz dopisivanje, fokusiraju na stvaranje ubedljivih izmišljenih scenarija u cilju ostvarivanja materijalne koristi ili do dolaska do poverljivih informacija.
2. Pecanje sa mamcem je slično kao i obično pecanje ali sa dodatkom linka u poruci koji obećava besplatne sadržaje i/ili stvari. Može se izvršavati kroz poruke ili kroz reklame. Mamci mogu biti postavljeni i kao usluge, što predstavlja drugi oblik ovakvog pecanja.

3. Praćenje u repu je oblik napada kada se napadač približi nekome u cilju da iskoristi drugoga ko ima odobrenje za ulaz u obezbeđeno područje ili zgradu.
4. Diverzija podrazumeva pogrešno usmeravanje kurira ili transportne kompanije u cilju preusmeravanja pošiljke na drugu lokaciju. Takođe se može izvršiti i kroz preusmeravanje plaćanja na drugi račun, što se, u ovom slučaju, ostvaruje kroz pristup nalogu elektronske pošte žrtve.
5. Kidnapovanje je vrsta zlonamernog softvera koji ograničava pristup zaraženom računarskom sistemu na neki način i zahteva da korisnik plati otkup operatorima malvera, zlonamernog programa, da bi uklonio ograničenje.
6. Ronjenje u kontejneru ili, kopanje po đubretu, je tip socijalnog inženjeringa kojim se prikupljaju informacije iz odbačenih materijala kao što su: stara računarska oprema (npr. hard diskovi, disk jedinice, DVD-ovi, CD-ovi) i dokumenti pojedinaca ili preduzeća koji nisu bili bezbedno uklonjeni.
7. Pecanje, koje se može podeliti na:
 - a. pecanje koja cilja na pojedinačne ili izabrane grupe
 - b. pecanje harpunom gde je meta krupna riba
 - c. IGS (IVR) pecanje koje koristi IGS sistem¹
 - d. kompromitovana poslovna elektronska pošta – mutacija od „pecanja harpunom“ ili „kitolovca“, gde se žrtva skenira, pretražuje, a nadzor finansira. Napadač je u ovom napadu prikriven i čeka pravi momenat da izvrši „diverziju“.

U cilju prepoznavanja ovakvih napada na mreži, možemo prepoznati njihove karakteristike koje su prikazane u sledećoj tabeli.

Tabela karakteristika socijalnog inženjeringa (Jain, i drugi, 2016)

Karakteristike napada	Traženje informacija	Potencijalne posledice
Izgled • uglavnom dobre ili loše vesti • osećaj hitnosti • osetljiva i poverljiva stvar • pretvaranje da je neko drugi (slično ime) Zahtevani odgovor • da se dostave specifične informacije • da se apdejtuju lični podaci ili podaci o računu • da se klikne na link u elektronskoj poruci • da se otvori prilog uz mejl Indikatori sumnjivosti • Generisani pozdravi • sumnjiv kontekst • loš pravopis • neuobičajeni ili čudan pošiljalac • netačna informacija • neispravni URL-ovi u poruci	• informacije o računu • korisničkom imenu • Lozinci ili PIN-u • broju kreditne kartice • matičnom broju • broju računa • IBAN-u • adresi elektronske pošte • Broju telefona • drugim ličnim podacima	• Finansijski gubitak • krađa identiteta • krađa ličnih ili poverljivih podataka ili kritične informacije • krađa intelektualne svojine • ugroženi računar, podmetnuti virus ili zlonamerni program • podaci, softver ili hardver izmenjeni ili uništeni • naneta šteta ugledu pojedinca ili kompanije • politička šteta • odbijanje servisa

¹ IGS sistem je Interaktivni Govorni Sistem koji kroz govornu komunikaciju sa lažnim predstavnicima korisničke službe prikuplja podatke od klijenata

Primeri:

Među poznatim prevarama koje koriste metode socijalnog inženjeringa u sferi informacione tehnologije su najčešće:

„Telefonska prevara“

U ovoj situaciji, zlonamernik pronalazi broj telefona, najčešće starije osobe, predstavlja se kao član porodice ili poznanik, koji je u velikom problemu i novac mu je hitno potreban. Razlozi mogu biti predstavljeni kao problemi na putovanju, krađa novca, zelenaški dug, bolest ili neki drugi finansijski problem.

Ovu prevaru, koja zahteva znanje osnovnih podataka o osobi koja se poziva, zbog čega se nalazi u primerima socijalnog inženjeringa, treba razlikovati od sličnih prevarnih šema koje koriste SMS poruke sa sličnim sadržajem ali bez znanja kome su poslate i ne obraćaju se meti po imenu.

„Prevara elektronskom poštom ili porukama“

Ova šema počinje sa kreiranjem scenarija da se ciljana žrtva uključi u neku razmenu poruka odnosno pisanu komunikaciju. Napadač se pretvara da je menadžer banke, poreski službenik, komunalni ili policijski inspektor tražeći lične podatke kao što su brojevi računa ili lozinke. Za ovakvu kriminalnu radnju neophodno je poznavanje osnovnih ličnih podataka i okolnosti žrtve, da bi prevara uspeła.

„Menadžerska prevara“

Prevarant prikuplja javno dostupne informacije o poslovnom sistemu koji namerava da napadne. Pronalazi detalje o Generalnom Direktoratu ili funkcioneru na čelu sistema, kao i o osobama koje imaju ovlašćenja za prenos sredstava sa računa organizacije. Tada koristi dobijene podatke da kreira hitnu potrebu za uplatom na određeni bankovni račun.

„Hakovanje naloga elektronske pošte“

Ukoliko zlonamernik uspe da se domogne pristupa nalogu elektronske pošte žrtve, ili kontakata u mobilnom telefonu, može sa njih poslati poruke svima u listi kontakata, tvrdeći da je u nevolji, u inostranstvu, bez telefona i da mu je hitno potreban novac.

„Lutrijska prevara“

Ovu prevaru karakteriše informacija da je potencijalna žrtva dobila na lutriji, ili da je ušla u samo finale takmičenja sa ogromnim šansama za dobitak, koju moguće prati ček sa upisanim iznosom i ispisanim podacima žrtve u prilogu poruke, a samo je potrebno uplatiti troškove obrade isplate dobitka na račun. Ovde se često koriste imena poznatih kompanija kao organizatora nagradne igre da bi se ostavio utisak.

Da bi se ostvarile sve ove prevare, a i druge slične njima, u kontekstu socijalnog inženjeringa, koriste se i druge metode poput: praćenja, preusmeravanja isporuke, razmene osetljivih podataka „usled nesporazuma“, naizgled slučajnim ostavljanjem zaraženog (USB) diska, zahtevom za forenzičkom analizom inficiranih diskova, itd.

2.1 Socijalni inženjering na društvenim mrežama

Prevare na društvenim mrežama imaju svoje specifičnosti zbog načina na koji funkcionišu i kako se implementiraju. Jedna od ključnih karakteristika društvenih mreža je podrška koja se obezbeđuje za traženje novih prijatelja. Na primer, tipična tehnika sastoji se od automatskog identifikovanja zajedničkih prijatelja u slikama, a zatim promovisanju novih prijateljstva sa porukama kao što su "imate 4 uzajamna prijatelja sa „Petrom Petrovićem“. Da li biste želeli da dodate „Petra Petrovića“ za novog prijatelja? Takođe, informacije o aktivnostima korisnika se često prikupljaju, analiziraju i usmeravaju ka programima za izračunavanje verovatnoće da se dva korisnika poznaju. Ako se otkrije potencijalni poznanik, lokacija sa društvene mreže, kada se korisnik prijavi na sistem, može da prikaže novu preporuku o prijateljstvu.

Jasno je da je korišćenje društvenih mreža kritično u odnosu na bezbednost i privatnost svojih korisnika. U stvari, velika količina informacija objavljenih i često javno deljena, na profilu korisnika sve više privlači pažnju napadača. Napadi na društvenim mrežama su obično varijante tradicionalnih bezbednosnih pretnji (kao što su malver, crvi, bezvredna pošta i pecanje). Međutim, ovi napadi se izvršavaju u drugačijem kontekstu, dodavanjem društvenih

mreža kao novog medijuma za prikupljanje žrtava. Pored toga, napadači mogu da iskoriste odnose poverenja između "prijatelja" na društvenim mrežama da bi izvršili više uspešnih napada korišćenjem ličnih informacija koje su na stranicama žrtava.

2.2 Obrnuti socijalni inženjering

U obrnutom socijalnom inženjeringu, napadač ne inicira kontakt sa žrtvom. Umesto toga, žrtva je namamljena da kontaktira napadača. Kao rezultat toga, ostvaruje se visok stepen poverenja između žrtve i napadača zato što žrtva ostaje u uverenju da je prva želela da uspostavi kontakt. Jednom kada je obrnuti napad uspešan (kada je napadač uspostavio vezu sa žrtvom), on može da pokrene širok spektar napada, kao što su ubeđivanje da kliknu na zlonamerne linkove, ucenjivanje, krađu identiteta i pećanje.

Postoje tri vrste napada korišćenjem obrnutog socijalnog inženjeringa na društvenim mrežama (Irani, Balduzzi, Balzarotti, Kirda, & Pu, 2011):

- Na osnovu preporuke društvene mreže
- Predlog prijatelja za novog prijatelja
- Demografski društveni inženjering

Na samom početku ovakvog napada koriste se preporuke koje društvena mreža napravi za promociju, za svrhu prevare, napravljenog lažnog profila. Napadač želi da svoj cilj zainteresuje preporukom i da ona poželi da kontaktira profil koji je pod napadačevom kontrolom. U praksi, ovo podrazumeva da se aktivira radoznalost običnim pregledom profilne stranice. Notifikacija da je neko lajkovao žrtvinu sliku može biti dovoljna da je privuče da pregleda lažni profil.

Sugestije prijatelja za novog prijatelja mogu biti zloupotrebene zato što se mogu vršiti sa takođe lažnih profila koje je korisnik već ranije prihvatio. Radi uverljivijeg napada, u cilju sticanja poverenja, lažni profil ostvaruje određeni broj zajedničkih prijateljstva. Često je potrebno da samo jednu osobu iz određenog kruga obmane da prihvati prijateljstvo sa lažnim profilom, da bi ostali iz istog kruga, tu osobu prihvatili po automatizmu, često misleći da samo ne mogu trenutno da je se sete i misleći da, kad su oni prethodni, koje stvarno poznaje, prihvatili zahtev, zašto to ne bih uradio i ja. Takođe, razlozi za prihvatanje nepoznatih osoba za prijatelje može biti i želja da

se ima što veći broj prijateljstva da bi se time podigla „svoja važnost“.

U scenariju demografskog napada, napadač pokušava da dođe do svoje žrtve tako što falsifikuje lažne demografske ili lične informacije sa ciljem da privuče pažnju korisnika sa sličnim potrebama (npr. slični muzički ukusi, sličan interesi itd.). Nasuprot zdravoj pameti, istraživanja su pokazala da je dovoljno samo imati profil sa atraktivnom fotografijom da bi se regrutovao veliki broj potencijalnih žrtava. U suštini, napadač mora da obezbedi žrtvama izgovor i podsticaj za uspostavljanje kontakta.

Još jedan primer obrnutog socijalnog inženjeringa je slanje broja telefona ili adrese elektronske pošte za prijavu ili rešavanje određenog problema pre nego što se problem pojavi. Na primer, Internet servis provajder ili banka mogu da obaveste svoje klijente da, ukoliko se pojavi „takav i takav“ problem, treba da kontaktiraju sledeću adresu ili broj telefona. Kada se za nekoliko dana takav problem pojavi, stigne neki račun ili opomena, žrtva se seti informacije koju je nedavno pročitala i odluči se da kontaktira lažni kontakt. Kako je obmanuta da misli da je prva pokrenula kontakt, biće manje sumnjičava i spremna da podeli kritične informacije. (Irani, Balduzzi, Balzarotti, Kirda, & Pu, 2011)

Stotine miliona korisnika registrovano je na društvenim mrežama i redovno ih koriste da bi ostali u kontaktu sa prijateljima, komunicirali, obavljali onlajn trgovinu i delili multimedijalne sadržaje sa drugim korisnicima. Da bi bile u mogućnosti da naprave predloge i promovišu prijateljstva, društvene mreže često prikupljaju lokacije o registrovanim korisnicima. Na primer, činjenica da korisnik traži adresu nečije elektronske pošte, može da podrazumeva da korisnik zna osobu koja je vlasnik tog naloga. Na žalost, takve pretpostavke mogu da budu zloupotrebene od strane napadača da svoju žrtvu zaintrigira lažnom porukom.

Iako je socijalni inženjering dobro proučen, njegova obrnuta verzija, na društvenim mrežama, još nije dobila dovoljno pažnje. Opasnosti koje sa sobom nosi su ogromne.

Komunikacija kroz Internet postaje svakim danom drugačija pa se metode komunikacije potencijalnih učesnika u trgovini ukradenim

podacima, korišćene do samo pre nekoliko godina zamenjuju novim, težim za otkrivanje i praćenje. Sve ovo čini da se poveća zainteresovanost za krađom podataka kompanija i pojedinaca, te se aspekti informacione bezbednosti moraju stalno ojačavati kako bi postali i ostali u skladu sa potrebama i izazovima trenutka.

3 LIČNI PODACI

Kada govorimo o ličnim podacima, govorimo, u stvari, o pojedincu koji se tim podacima može identifikovati. U današnjem svetu se prikupljaju ogromne količine ličnih podataka. Neke organizacije ih koriste za svoje potrebe a neke ih prenose trećim licima iz najrazličitijih razloga. Ovaj trend eksponencijalno raste zajedno sa razvojem složenih informacionih tehnologija za obradu i analizu velikih baza podataka.

Sa ovakvim trendom, raste i zabrinutost pojedinaca o tome ko i kako koristi njihove lične podatke. Stoga je neophodno implementirati politiku informacione bezbednosti koja će sadržati i načine zaštite ličnih podataka, odnosno njihovo prikupljanje, korišćenje i objavljivanje i cilju da se ostvari i održi poverenje pojedinaca u organizacije koje su u posedu ovih podataka.

Povrede bezbednosti ličnih podataka mogu izazvati ozbiljnu štetu i patnju žrtvama zloupotrebe, pa im mogu, čak, dovesti i život u pitanje. Primeri štete nastale gubitkom ili zloupotrebom ličnih podataka ponekad povezanih sa krađom identiteta uključuju:

- Lažne transakcije kreditnim karticama;
- Lažne zahteve za poreskim kreditima tj. povraćajima poreza;
- Lažne priznanice za prijem robe, pozajmice ili dugovanja;
- Lažne testamente;
- Lažnu dokumentaciju o usvajanju;
- Hipotekarne prevare.
- Rizik za svedoke od fizičkih povreda ili zastrašivanja;
- Rizik počinilaca od vaninstitucionalne osvete oštećenih; i
- Rizik saznavanja adresa uslužnog osoblja, policije i zatvorskih službenika, žena žrtava nasilja u porodici, lekara.

Razlozi zašto su lični podaci dragoceni za kiber—kriminalce leže u činjenici da oni zapravo

predstavljaju monetu sive ekonomije kojom se trguje. Vlasnici baza ličnih podataka ili oni koji te baze pribave na dozvoljene ili nedozvoljene načine, mogu ih prodati različitim kupcima, odnosno: kradljivcima identiteta, organizovanim bandama, spamerima i operaterima botnet mreža. Botnet mreža predstavlja mrežu, malverom zaraženih računara, kojom upravlja njen tvorac a koji koriste ove baze podataka da prošire svoje mreže i time pribave još više novca.

Spameri, na primer, mogu dobiti novu listu adresa elektronske pošte, na koju mogu poslati ponude za Cijalis i Vijagru. Zaradu imaju po svakom kliku na link koji su promovisali, ili po broju odgovora, ili po broju pristupa reklamiranim sajtovima. Kradljivci identiteta mogu koristiti adrese za sve oblike pecanja.

Kiber-kriminalci trguju ovim informacijama međusobno da bi kompletirali sliku pojedinca. Ideja je, da svi zajedno, prikupe više informacija o ljudima te da tako da mogu da naprave veću štetu odnosno ostvare veću dobit. Cilj im je da iz više izvora sakupe: ime, broj kreditne kartice, PIN, e-mail adresu i telefonski broj. Otkrivanje pojedinačnih podataka u različitim situacijama i na različitim mestima, možda se ne učini opasno, ali kada pojedinac ili kompanija predstavljaju ciljanu metu radi se o potpuno drugačijoj slici. (Levinson, 2012)

4 MATIČNI BROJ GRAĐANA

Krađa identiteta u Srbiji nije definisana kao krivično delo, iako je broj onih kojima su ukradena dokumenta ili na neki drugi način zloupotrebjeni lični podaci, sve veći. Ljudi uglavnom nisu svesni gde sve „seju“ matični i broj lične karte, i broj bankarske kartice, i ne znaju skoro ništa o opasnostima koje ih zbog toga vrebaju. A život u samo nekoliko minuta može da im se pretvori u pakao.

Kancelarija poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti ukazuje da su kancelariji, do sada, građani prijavili pet krađa identiteta. U MUP tvrde da ovakve podatke nemaju jer Krivični zakonik ne poznaje to krivično delo, a na slične situacije primenjuju se odredbe koje se odnose na falsifikovanje isprava i prevare. 2014. godine je, prema podacima Republičkog zavoda za statistiku, podneto je 1.256 prijava za falsifikovanje isprave, 364 za posebne slučajeve

falsifikovanja isprave i nešto više od 2.600 za prevaru, ali se ne zna koliko od toga za zloupotrebu tuđih podataka. Za falsifikovanje i zloupotrebu platnih kartica policija je podnela 262 prijave. (Crnjanski Spasojević, 2014)

Veoma je opasno davanje jedinstvenog matičnog broja.²

Na osnovu njega bilo ko može da uđe u bazu podataka građanina u poreskoj upravi ili u birački spisak, APR i zloupotrebi ih.

Mnogi prikupljaju podatke i bez zakonskih ovlašćenja (recimo, sportski klubovi). Ali nekada i zakon dozvoljava bespotrebno uzimanje podataka. Centralno pitanje je kako se te baze štite. Više istraživanja pokazalo je da mnogi rukovaoci podacima, kako ih zakon zove, imaju veoma slabu ili čak nemaju nikakvu zaštitu.

Da bi ukrali identitete ljudi, ili počinili prevaru sa kreditnim karticama, kiber kriminalcima treba lozinka, broj kreditne kartice ili broj socijalnog osiguranja na zapadu a kod nas matični broj. Za to se između reklama ubacuju pecačke poruke ili zlonamerni programi koji mogu da instaliraju i „key-logging“ programe.

Ako se dokopaju samo 4 zadnje cifre broja kreditne kartice, mogu to da iskoriste za promenu lozinke na nekim prodajnim sajtovima, zato što neki od njih koriste te cifre kao PIN kod korisnika. Jednom kada promene lozinku mogu promeniti i druge podatke i naručivati robu mimo znanja vlasnika kartice. Takođe, nakon svojih napada, mogu da prodaju ovu informaciju i nekom drugom, ko može da izvrši još neku drugu vrstu napada na ovog korisnika. (Levinson, 2012)

Neke baze podataka imaju zaštitu, ali je pitanje da li je ona dovoljna i srazmera vrednosti zaštićenih podataka. Naročito su opasni upadi u velike elektronske baze kakve imaju banke, sistemi koji se bave trgovinom preko interneta, zdravstvene

službe ili PIO fond. Više od 300.000 institucija rukuje ličnim podacima građana, a procene su da su one napravile milion baza podataka. Najviše evidencija ima MUP, Vojska, bezbednosne službe, Carina, poreznici, pravosuđe, banke, firme, socijalne ustanove, opštine, izborne komisije...

Svi koji rukuju ličnim podacima građana trebalo bi da prijave svoje baze podataka u Centralni registar, kako bi poverenik mogao da kontroliše ko i kako obrađuje nečiji jedinstven matični broj, ime i prezime, adresu... Međutim, u centralni registar je upisano tek 317 rukovaoca ličnim podacima, i oko 1.600 evidencija o zbirkama koje vode. To nije ni 0,5 odsto onoga što se očekuje. (Crnjanski Spasojević, 2014)

Svrha registra je ne samo da se evidentira svaka zbirka, već i da se omogućí svakome da sazna ko obrađuje podatke o ličnosti, u koje svrhe i kome su podaci dostupni.

Inače, krađa identiteta je već godinama, prema Američkoj federalnoj komisiji za trgovinu, prva na listi „naj-prevara“.

5 VREDNOST LIČNIH PODATAKA

Vrednost ličnih podataka pojedinačno nije velika. Kreće se od delića centa do jednog dolara u zavisnosti od svežine prikupljenih podataka i njihovog kvaliteta. Čak i brojevi kreditnih kartica koštaju manje od jednog dolara iz razloga velike ponude.

Ovo možda ne izgleda kao nešto sa čime bi se pojedinac mogao da se obogatiti, ali kada se pomnoži sa milionima podataka, cifre postaju ogromne. Na primeru provale poznate pod imenom „Zappos“, u kojoj je su ukradeni podaci o 24 miliona korisnika, može se izračunati da, ako se proda samo 5 miliona zapisa po 5 centi, dolazi se do cifre od 250,000 dolara za samo jedan

² Jedinstveni matični broj građana (JMBG) je identifikaciji broj dat svim novorođenim građanima SFRJ (Socijalističke Federativne Republike Jugoslavije) od 1976. godine. Svi građani rođeni pre 1976. godine su dobili broj u zavisnosti od regija u kojim su tada živeli. Broj je još uvek u upotrebi u novonastalim državama.

Broj je napravljen od 13 cifara u formi „DD MM GGG RR BBB K“ (bez razmaka), gde su:

DD – dan rođenja

MM – mesec rođenja

GGG – poslednje tri cifre godine rođenja

RR – regija rođenja (za građane rođene pre 1976. godine regija gde su trenutno živeli)

BBB – jedinstveni broj, 000-499 – muški, 500-999 – ženski

K - kontrolna cifra

hakerski napad. Operateri mreže botova mogu da zarade enormne sume novca. Ako se mreža sastoji od recimo 100,000 bot računara, može da se iznajmi za 1000 dolara po satu.

Pravljenje botnet mreže je izuzetno isplativ posao. Kada neko ukrade 24 miliona imejl adresa, kao što se to dogodilo u slučaju „Zappos“-a, i pošalje malver na njih, ako uspe da zarazi 20 procenata onih koji prime i otvore njegov e-mejl, čime postaju deo njegove botnet mreže, uspeće da izgradi mrežu kapaciteta 5 miliona računara koju onda može da izda za 5000 dolara po satu uz vrlo malo truda.

Prvi nivo informacija koji je potreban hakerima da bi počeli svoj posao su adrese elektronske pošte. Sa njima, počinje spamovanje, odnosno zatrpavanje sandučića elektronske pošte raznim komercijalnim porukama.

6 ZAKLJUČAK

Nemaju svi napadi samo finansijske posledice. Mnogi izazivaju posledice druge vrste, kao što su na primer, osramoćenje i neprijatnosti.

CITIRANA DELA

Crnjanski Spasojević, V. (2014, 07 27). Matične brojeve ostavljamo "na izvol'te". *Večernje novosti online*. Preuzeto sa

<http://www.novosti.rs/%D0%B2%D0%B5%D1%81%D1%82%D0%B8/%D0%BD%D0%B0%D1%81%D0%BB%D0%BE%D0%B2%D0%BD%D0%B0/%D0%B4%D1%80%D1%83%D1%88%D1%82%D0%B2%D0%BE.395.html:502763-%D0%9C%D0%B0%D1%82%D0%B8%D1%87%D0%BD%D0%B5-%D0%B1%D1%80%D0%BE%D1%98%D0%B5%D0%B2%D0%B5-%D0%BE%D>

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., & Pu, C. (2011, 05 16). *Reverse Social Engineering Attacks in Online Social Networks*. Preuzeto sa SysSec: <http://www.syssec-project.eu/m/page-media/3/irani-dimva11.pdf>

Jain, A., Tailang, H., Goswami, H., Dutta, S., Mahipal, S. S., & Kumar, R. (2016). Social Engineering: Hacking a Human Being through Technology. *Journal of Computer Engineering (IOSR-JCE)*, 94-100. doi:10.9790/0661-18050594100

Levinson, M. (2012, 01 26). *Are You at Risk? What Cybercriminals Do With Your Personal Data*. Preuzeto sa CIO from IDG: <https://www.cio.com/article/2400064/security0/are-you-at-risk--what-cybercriminals-do-with-your-personal-data.html>

Datum prve prijave:	02.09.2018.
Datum prijema korigovanog članka:	11.03.2018.
Datum prihvatanja članka:	27.03.2019.

Napredak u tehnologiji omogućio je organizacijama da obrađuju sve više ličnih podataka i da lakše razmenjuju informacije. To ima očigledne prednosti ukoliko prikupljaju i dele lične podatke u skladu sa principima zaštite podataka, ali takođe podjednako sadrže i očigledne bezbednosne rizike. Što je veći broj popunjenih baza podataka, i što se više informacija u njima razmenjuje, to je veći je rizik da će informacije biti izgubljene, oštećene ili pogrešno iskorišćene.

Veliki broj poznatih slučajeva gubitaka ličnih podataka je privukao pažnju prema problemu bezbednosti informacija. Međutim, ovi incidenti su takođe jasno dali do znanja da je bezbednost informacija zadatak društva, ali i da postoji i problem tehničke neusaglašenosti. Ako lični podaci nisu propisno čuvani, to može ozbiljno da ošteti reputaciju i prosperitet organizacije i može da ugrozi bezbednost pojedinaca.

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

Style – **APA** Sixth Edition:

Blagojević, S. (2019, 04 15). Socijalni inženjering i lični podaci. (Z. Čekerevac, Ed.) *FBIM Transactions*, 7(1), 20-28. doi:10.12709/fbim.07.07.01.03

Style – **Chicago** Sixteenth Edition:

Blagojević, Srđan. 2019. "Socijalni inženjering i lični podaci." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 20-28. doi:10.12709/fbim.07.07.01.03.

Style – **GOST** Name Sort:

Blagojević Srđan Socijalni inženjering i lični podaci [Journal] // *FBIM Transactions* / ed. Čekerevac Zoran. - Beograd : MESTE, 04 15, 2019. - 1 : Vol. 7. - pp. 20-28.

Style – **Harvard** Anglia:

Blagojević, S., 2019. Socijalni inženjering i lični podaci. *FBIM Transactions*, 15 04, 7(1), pp. 20-28.

Style – **ISO 690** Numerical Reference:

Socijalni inženjering i lični podaci. **Blagojević, Srđan**. [ed.] Zoran Čekerevac. 1, Beograd : MESTE, 04 15, 2019, *FBIM Transactions*, Vol. 7, pp. 20-28



SECURITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES

BEZBEDNOST INFORMACIONIH I KOMUNIKACIONIH TEHNOLOGIJA

Kamil Boc

University of Zilina, Faculty of Security Engineering, Zilina, Slovakia

Zdenek Dvořák

University of Zilina, Faculty of Security Engineering, Zilina, Slovakia

Zoran Čekerevac

“UNION – Nikola Tesla” University, Faculty of Business and Law, Belgrade, Serbia

©MESTE

JEL Category: **C88, L86**

Abstract

With the development of computerization, information and communication technologies (ICT) are rapidly penetrating in all areas of human life. The state of information security and security of information systems is at a relatively low level. Threats and risks related to ICT by relevance and severity of possible consequences are most often directed at the state level, somewhat less towards banks, insurance companies, marketing and other companies that have larger amounts of personal data of users. However, small businesses and individuals are also very often exposed to the attacks. The authors analyze the legal environment in the IT sector of the Slovak Republic. After introductory considerations, the paper analyzes the legal regulations of the European Union and, in particular, of the Slovak Republic. The accent was placed on the security standards of the information systems of Slovakia. After that, the technical norms of relevance to the security of information and communication technologies are discussed. The authors dealt with long-term issues of security and the spread of good practice in the protection of property, information and communication systems. The aim of this article is to present the standard security and information systems of the European Union. Based on the research carried out, the authors point out that the goal of the academic environment should be to continuously find solutions to the new and emerging challenges that arise every day. One of the most difficult tasks is the transfer of this new knowledge into the legal framework and technical standards.

Keywords: security, safety, information and communication technologies, standards, norms, Slovakia

Address of the author:

Kamil Boc

[✉ kamil.boc@fbi.uniza.sk](mailto:kamil.boc@fbi.uniza.sk)

Apstrakt

Sa razvojem kompjuterizacije, informacione i komunikacione tehnologije (IKT) naglo prodiru u



sve oblasti ljudskog života. Stanje sigurnosti informacija i sigurnosti informacionih sistema je na relativno niskom nivou. Pretnje i rizici u vezi sa IKT po značaju i težini mogućih posledica najčešće su usmereni ka državnom nivou, nešto manje ka bankama, osiguravajućim kompanijama, marketinškim i drugim kompanijama koje poseduju veće količine ličnih podataka korisnika. Međutim, napadima su izložena i mala preduzeća i vrlo često i pojedinci. Autori u radu analiziraju pravno okruženje Slovačke Republike. Posle uvodnih razmatranja, u radu se analizira zakonska regulativa Evropske Unije i, posebno, Republike Slovačke. Akcenat je stavljen na bezbednosne standarde informacionih sistema Republike Slovačke. U nastavku su prikazane tehničke norme od značaja za bezbednost informacionih i komunikacionih tehnologija. Autori su se u radu bavili dugoročnim pitanjima bezbednosti i širenja dobre prakse u zaštiti imovine, informacionih i komunikacionih sistema. Cilj ovog članka je predstavljanje standardnih sigurnosnih i informacionih sistema Evropske unije. Na osnovu izvršenih istraživanja, autori ukazuju na to da cilj akademskog okruženja treba da bude neprekidno pronalaženje rešenja novih i novih izazova koji se svakodnevno javljaju. Jedan od veoma teških zadataka je prenošenje ovog novog znanja u zakonski okvir i tehničke standarde.

Ključne reči: bezbednost, sigurnost, informacione i komunikacione tehnologije, standardi, norme, Slovačka.

1 INTRODUCTION

The current development of the company is closely related to the development and modernization of ICT. In recent history, ICT has gradually begun to be used in science and research, military, aerospace, automotive, medicine and, in recent years, the arts and almost all areas of human life. (Cekerevac, et al, 2016) The aim of the researchers at the cooperating universities in Serbia and Slovakia was to gradually focus attention on the number of areas and problems of using ICT in life. Over the past 10 years, authors have been creating a series of articles focused on selected informatization issues (Cekerevac et al, 2016).

The main goal of our research is to shift knowledge into areas related to the use of ICT in human life. We keep learning the results of our research in the teaching of our subjects and present them at international conferences. Part of the research activity is cooperation on the creation of a legal framework in the national environment. The legal environment is generally divided into strategies, e.g. Informatization Strategy, Information Security Strategy, Public Administration Information Strategy (Slovak strategy documents, 2018), laws - e.g. the Act on the Protection of Classified Information, the Personal Data Protection Act (Legal frame of Slovakia, 2018) ordinances and technical standards (ISO27000, 2018).

2 LEGAL REGULATION OF INFORMATION SECURITY IN LAW OF EUROPEAN UNION AND SLOVAK REPUBLIC

EU, realizing the importance and significance of ICT system assets, inter alia, in its Directive no. 2008/114/ES recommended the ICT systems to become an individual sector of critical infrastructure and to subject to corresponding protection. SR in the act no. 45/2011 Coll. on the protection of critical infrastructure accepted this recommendation and listed ICT as an individual sector of critical infrastructure in SR under Ministry of Finances of SR. (EU directive 2008/114, 2018) and (Act no. 45/2011, 2018).

Security of ICT systems in SR is regulated in addition to Directive 2008/114/ES elaborated in Act no. 45/2011 Coll. on critical infrastructure, as well as by other legal and internal regulations, technical norms and international contracts it is bound to.

Other most important legal acts contain:

- a. Directive of European Parliament and Council no. 2002/58/ES from 12th July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
- b. Directive no. 95/46/ES of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with

regard to the processing of personal data and on the free movement of such data.

- c. Act no. 215/2004 Coll. on the protection of classified information and related notices of NBU SR (notice of NBU no. 90/2002 Coll. on the security of technical devices, notice of NBU no. 91/2002 Coll. which establishes details of cryptographic protection of information).
- d. Act no. 428/2002 Coll. on the protection of personal information.
- e. Act no. 300/2005 Coll. criminal law.
- f. Act no. 275/2006 Coll. on information systems of public administration and on amendments of certain acts.
- g. Act no. 513/1991 Coll. commercial law.
- h. Act no. 483/2001 Coll. on banks.
- i. Act no. 324/2011 Coll. on post services and on the amendment of certain acts,
- j. National strategy for information security in the Slovak Republic (UV no. 570/2008).
- k. Decree of the Ministry of Finances of the Slovak Republic no. 312 from 9th June 2010 on standards for information systems of public administration (Legal frame of Slovakia, 2018).
- l. Technical norms – regulating management and security of ICT systems (ISO/IEC 27000:2009, ISO/IEC 27001:2006, ISO/IEC 27002:2009, ISO/IEC 27005:2011, ISO/IEC 27006:2007, ISO/IEC 27008:2011, ISO/IEC 27011:2008, ISO/IEC 27799:2008, developed standards).

Ad a) Directive 2002/58/ES concerning the *processing of personal data and the protection of privacy in the electronic communications sector* harmonizes the regulations of member states required for providing of equal level of protection of basic freedoms and rights, especially right for privacy, with regard to processing of personal information in field of electronic communication and for providing of free movement of these data and electronic communication devices and services.

Ad b) Directive 95/46/ES of the European Parliament and of the Council on the *protection of individuals with regard to the processing of personal data and on the free movement of such data* obliges the member

states to protect the basic rights and freedoms of persons, mainly their right for privacy regarding the processing of personal data. It binds the member states do not limit or obstruct the free flow of data between member states for reasons connected to their protection.

Ad c) Act no. 215/2004 Coll. *on the protection of classified information* defines terms and identifies classified information into four levels of confidentiality, determines organizations and units responsible for their protection, responsibilities, sanctions, which may be used in case of violation of law, determines the obligation to create security project, sets the security standards, etc. (Legal frame of Slovakia, 2018).

Ad d) Act no. 428/2002 Coll. *on the protection of personal data in information systems* has as its goal protection of basic rights and freedoms of persons during processing of their personal information. It establishes the term personal data. Under personal data, all data related to identified or identifiable person, with the person being identifiable directly or indirectly mainly based on identification number (birth registration number) or based on one or more characteristics or marks, which form its physical, physiological, mental, economic, cultural or social identity. It simultaneously determines rights and obligations of persons related to providing of personal data into information system and rights, obligations and responsibility of entities and persons, which partake on processing of personal data, sets rights and obligations of operators of information system, intermediaries and persons affected by providing of personal data from information system, regulates the position and scope of operation of the state supervision authority for protection of personal data in information systems and sanctions for violation of this law. It establishes the obligation to create a security project of the information system (Legal frame of Slovakia, 2018).

Ad e) Act no. 300/2005 Coll. *criminal law* defines subject matters of illegal actions related to the operation of the information system and its

assets. Illegal actions based on their subject matters may be divided into four groups:

1. crimes violating *protection of intellectual property*, competitive environment, trademarks and against fair competition,
2. crimes violating the *general protection of personality*,
3. *computer criminality* and computer piracy,
4. other crimes of *more general* nature, which may be related to a given field (endangering of state secret, economic secret, fraud, violation of the secrecy of messages, etc.) (Legal frame of Slovakia, 2018).

Ad f) Act no. 275/2006 Coll. *on information systems of public administration* and on amendment of certain acts as amended determines rights and obligations of persons liable in field of creation, operation, utilization and development of information systems of public administration, basic conditions for ensuring of integrability and security of information systems of public administration, administration and operation of central portal and process for issuing of electronic transcript of data from information systems of public administration and output from information systems of public administration. It introduces terminology, defining for example *information system*, *meta information system*, *cross-sectoral information system*. It introduces the term *liable persons* and their responsibilities, among which belongs the obligation to protect the information system of public administration from abuse. It introduces *standards*, which are a tool for providing integrability and security of information systems of public administration (Legal frame of Slovakia, 2018).

Ad g) Act no. 513/1991 Coll. *The commercial law* defines *trade secret* (Legal frame of Slovakia, 2018).

Ad h) Act no. 483/2001 Coll. *on banks*, defines *bank secret* (Legal frame of Slovakia, 2018).

Ad i) Act no. 324/2011 Coll. *on postal services* and on the amendment of certain acts defines

postal secret and protection of information and personal data (Legal frame of Slovakia, 2018).

Ad j) National strategy for information security in SR. Its goal is to create a basic framework of information security of SR. The strategy contains the background, competence-based distribution of competencies, a proposal for direction, priorities, and steps for reaching of a set goal. Part of this document is also a basic description of individual tasks with the goal to provide security for the whole digital space of SR, except for the classified information sphere. This contains mainly the measures against information leak and their unauthorized use, integrity breach of data, violation of citizen rights for protection of personal information, protection from damage and abuse of information and communication systems, damage to reputation of state and private institutions, as well as measures for enforcement of relevant law norms of SR and European Union.

Ad k) Decree of the Ministry of Finances of the Slovak Republic no. 312 from 9th June 2010 *on standards for information systems of public administration*. The decree determines standards for information systems of public administration, security standards.

3 SECURITY STANDARDS OF INFORMATION SYSTEMS IN SLOVAK REPUBLIC

Elements of an information system (hereinafter "IS") itself have significant importance for society as a whole. (Prigoda, et al, 2015) National executives are aware that failure of IS would have unforeseeable consequences and would complicate the administration of public issues. It is a similar situation with private entities that use ICT for their entrepreneur activities. For example, the banking sector would, in case of failure of information systems, now only bankrupt, but would also significantly endanger the operation of the national economy. That is why it is necessary to create the standards for protection within public administration. For the purposes of this work, generally, binding legal acts that regulate IS security in conditions of public administration shall be analyzed further on.

In conditions of SR, the security standards for public administration IS are based on the Decree of the Ministry of Finances of the Slovak Republic no. 312, and they regulate (Slovak strategy documents, 2018) (Legal frame of Slovakia, 2018):

3.1 Management architecture

- a) Information security management – the standard is:
- creation, approval, realization, and compliance with the security policy of liable person,
 - selection of person or persons responsible for information security of all information systems of the liable person of public administration in compliance with security policy,
 - ensuring of coordination of activities of organizational units of the liable person while addressing the information security,
 - determination of specific responsibility for individual assets of the liable person,
 - determination of security positions in information systems of public administration, determination of security requirements of individual positions, determination of incompatible positions; security positions consist mainly of the system administrator, operator, auditor, and programmer.
- b) Personnel security – a standard for the personnel security is:
- ensuring all employees are instructed about security policy, their duties, and rights resulting from it, about responsibilities before they gain access to the information system of public administration, and that these are listed in his work contract,
 - ensuring the responsibility of employees to be informed about security incidents,
 - creation of a process for disciplinary action related to persons which violate the security policy of the liable person or any of the related regulations,
 - creation of a process for ending of employment of own employee and ending

of cooperation with an external employee or third party.

- c) Risk management for the field of information security – the standard is:
- implementation of a system for management and monitoring of risks related to information systems of public administration,
 - utilization of system for management and monitoring of risks for all processes of information security management,
 - identification, analysis, and evaluation of risks connected to the use of assets and information systems outside of spaces of liable person and the introduction of adequate procedures and measures for reduction of these risks,
 - analysis of processes important for activities of the liable person from the viewpoint of their dependency on information systems, and determination of processes that cannot continue in case of outage or limitation of the functionality of information systems of public administration; these processes are called *critical processes*,
 - analysis of risks resulting from threats to information systems of public administration, on which the critical processes depend; these information systems are *critical information systems* of the public administration,
 - creation of plans for restoring of non-functional, damaged or destroyed critical information systems of public administration.
- d) Information security management control mechanism – a standard is:
- compliance of security policy of liable person and provision and execution of internal control or audit of information security, whose periodicity is determined by the security policy of liable person,
 - provision of archivization, protection, and evaluation of audit reports.

3.2 Minimal technical provisions

- a) Protection against malicious software – a standard is:

- protection in the scope of control of incoming electronic mail for the presence of malicious code and unallowed types of attachments, detection of the presence of malicious code, check of files received or sent from the internet for the presence of harmful software, detection of the presence of malicious code on all websites of liable person,
 - introduction of protection from unsolicited e-mail (spam),
 - use of only legal and allowed software,
 - setting rules for downloading of files through external networks,
 - support for ensuring of authenticity and integrity of files through the use of cryptographic devices, especially the electronic signature,
 - support for the encryption of electronic documents (ISO 27000, 2018).
- b) Network security – a standard is:
- ensuring of protection of the external and internal environment through tools of network security (firewall),
 - keeping records on all connection points of the network, including connections to external networks,
 - ensuring that the internal act of access management is created for each connection between these networks (ISO 27000, 2018).
- c) Physical security and environment security – the standard is:
- locating the public administration information system in such space, that the information system or at least its vital components are protected from negative natural influences and environmental influences, possible accidents of the technical infrastructure and physical access of the unauthorized persons (protected area),
 - separating the protected area from other spaces by physical devices, especially by walls and barriers,
 - ensuring that in the surroundings of the protected area are no facilities such as sewage, waterworks or materials, mainly flammable, which could represent a threat to public administration information system located in the protected area,
- creation and implementation of rules for work in the protected area,
 - providing protection from power supply outage and ensuring that such outage shall not occur,
 - ensuring that the existing backup capacities of the information system are located in the secondary protected area, sufficiently remote from the protected area,
 - ensuring that the operation, use, and management of information system is in accordance with specific regulations, internal regulations and its contractual obligations,
 - creation, introduction and control of commitment to rules for maintaining, storing and evidence of technical components of the information system, use of information system devices for other purposes than originally intended, use of devices of information system outside of determined spaces, deletion, decommissioning and disposal of information system devices and all types of relevant backups, transport of technical components of information system outside spaces of liable person, handling of electronic documents, system documentation, memory media, input and output data of information system in such way, that their unauthorized publishing, removal, damage or modification is prevented,
 - determination of parameters that define the maximum time period for an outage of information system and creation and the introduction of measures, which are focused on solving of the restoration of operation in case of information system outage (ISO 27000, 2018).
- d) Software updates – standard for software updates are:
- providing of update of versions of protective software, including protecting all other components and connected devices,

- performing of update at least in compliance with security policy (ISO 27000, 2018).
- e) Monitoring and management of security incidents – the standard is:
 - creation of internal act containing the procedure for reporting of security incidents and revealed vulnerable points of information systems, the procedure for solving of individual types of security incidents and method of their evaluation, a method of evidence of security incidents and used solutions,
 - ensuring that all users of an information system are informed on an appropriate way about procedures, and to ensure these rules are observed,
 - introduction of registration of all outages of information system and methods of their solving,
 - use of intrusion detection system,
 - creation and operation of contact point for reporting of security incidents and revealed vulnerable points of information systems (ISO 27000, 2018).
- f) Periodical evaluation of vulnerability
 - a standard is a periodical evaluation of vulnerable points and threats to information system identified in accordance with the security policy of the liable person with a periodicity of at least once per year (ISO 27000, 2018).

4 SECURITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN TECHNICAL NORMS

Information security is in addition to generally binding legislation regulated also by technical norms. The scope of these norms is within all EU states and a demand exists to implement these into the protection of all IS. The affected norms regulate procedures and measures which should ensure achieving of security standards of IS within EU.

Among the most important of technical norms in this field belongs (ISO 27000, 2018):

- a. ISO/IEC 27001 – *Information technologies – Security techniques – Systems of Information Security Management - Requirements*. It is

the main norm for a system of information security management. This international norm covers all types of organizations (e.g. commercial companies, government agencies, non-profit organizations). It is a complex system of information security management from realization, maintaining and enhancing the system of information security management in every organization without regard to its size. It addresses also the character of contractual relations for information security in business connection, as well as contractual relations in maintenance and service for the processing of sensitive information.

- b. ISO/IEC 27002/C1 – *Information technology. Security techniques. Code of practice for information security management*. This international norm introduces guidelines and general principles for initiation, implementation, maintaining and enhancing information security management within the organization. It provides a general manual of recognized goals of information security management. It contains procedures for control of goals in following spheres of information security management.

5 CONCLUSION

The article presented a vision of security of information and communication technologies. The authors address the issue in the long term and aim to spread good practice in the protection of assets, information and information systems.

In recent years, we have seen the data backup and archiving as a basic problem with ICT. Experience from major incidents and natural events often resulted in a complete loss of data and information.

Modern ICTs, such as cloud computing, create options for their proper backup and archiving. On the other hand, the likelihood of their misuse, damage and loss increases.

The big challenge today is data mining from all electronic sources. The gradual penetration of the Internet of Things and the Internet of Everything brings a whole host of challenges and challenges.

Our goal is to educate students who choose their security and information and information systems

for lifetime work. This area of human work is very promising and well paid.

The goal of the academic environment is to permanently explore new and new challenges that

need to be addressed. The difficult task is to transfer this new knowledge into the legal framework and technical standards.

WORKS CITED

- Act no. 45/2011 Col. of critical infrastructure (2018, September 2018) <http://www.zakonypreludi.sk/zz/2011-45> in Slovak,
- Cekerevac Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2016) Big vs small data in micro and small companies. *Communications: scientific letters of the University of Žilina*, 18(3), p. 34-40. ISSN 1335-4205.
- Dvorak, Z., Leitner, B., & Mocova, L. (2016) *The need for education in the field of security management and critical infrastructure protection*. Menadžment 2016: međunarodna naučna konferencija : zbornik rezimea : Beograd, Srbija, ICIM plus, ISBN 978-86-6375-053-1. p. 185-187.
- European Union directive no. 2008/114 ES (2018, September 2018) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN>
- ISO 27000. (2018, September 2018) <https://www.iso.org/isoiec-27001-information-security.html>
- Legal frame of Slovakia (2018, September 2018) <http://www.informatizacia.sk/legislativa-sr/684s>
- Prigoda, L., Cekerevac, Z., Dvorak, Z. & Cekerevac, P. (2015, Apr 19) *One look at modern information security*. *Sustainable Development of Mountain Territories*, 4(22) (2014), p. 99-103. ISSN 199B-4502.
- Slovak strategy documents (2018, September 2018) <http://www.informatizacia.sk/strategicke-dokumenty-is/600s>

This publication was created thanks to supporting under the R & D project for the project:

Centrum excelentnosti pre systémy a služby inteligentnej dopravy II., ITMS 26220120050 co-funded by the European Regional Development Fund.



"We support research activities in Slovakia / The project is co-financed from EU sources"

Received for publication: 08.09.2018
Revision received: 20.11.2018
Accepted for publication: 27.03.2019

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

Style – **APA Sixth Edition:**

Boc, K., Dvorak, Z., & Čekerevac, Z. (2019, 04 15). Security of information and communication technologies. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 29-37. doi:10.12709/fbim.07.07.01.04

Style – **Chicago Sixteenth Edition:**

Boc, Kamil, Zdenek Dvorak, i Zoran Čekerevac. 2019. „Security of information and communication technologies.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 29-37. doi:10.12709/fbim.07.07.01.04.

Style – **GOST Name Sort:**

Boc Kamil, Dvorak Zdenek i Čekerevac Zoran Security of information and communication technologies [Časopis] // *FBIM Transactions* / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. – pp. 29-37.

Style – **Harvard Anglia:**

Boc, K., Dvorak, Z. & Čekerevac, Z., 2019. Security of information and communication technologies. *FBIM Transactions*, 15 04, 7(1), pp. 29-37.

Style – **ISO 690 Numerical Reference:**

Security of information and communication technologies. **Boc, Kamil, Dvorak, Zdenek i Čekerevac, Zoran.** [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, *FBIM Transactions*, T. 7, pp. 29-37.



POREKLO ISLAMSKJE DRŽAVE

ORIGINS AND HISTORY OF ISLAMIC STATE

Boris Bursać

Gradska opština Čukarica, Beograd, Srbija

©MESTE

JEL Category: **Z12**

Apstrakt

Terorizam kakav danas poznajemo nikako nije nova tvorevina već se on krije u društvenoj zajednici u obliku taktike, strategije, doktrine, metode i sredstva oko kojih samo treba da se postigne konsenzus da bi izašao na svetlost dana. Dok terorizam neki vide kao zločin drugi ga opisuju kao svetu dužnost, i dokle god postoje ove dve zavađene strane terorizma će biti. Teroristi su danas obučeniji i opremljeniji samim tim i neuhvatljiviji kao nikad do sad, to je dovelo da se ovaj fenomen brzo proširi i zahvati celu planetu. Apsolutno ovoj rasprostranjenosti doprinosi i neadekvatna i pre svega nejedinstvena terminološka određenost terorizma kao pojma. Iako se svetska javnost slaže oko toga da je terorizam svetsko zlo a terorističke organizacije okarakterisane su kao zločinačke, globalni centri moći koriste ovu konfuziju a terorizam koriste radi postizanja sopstvenih interesa. Tako da se sedište terorističkih aktivnosti u skladu sa tim interesima danas stacioniralo na Bliskom istoku a u mnoštvu terorističkih organizacija jedna se istakla kao vodeća i na svom razvojnem putu prerasla je u nešto što danas nazivamo Islamska država.

Ključne reči: terorizam, Ansar al Islam, salafizam, vehabizam, Islamska država

Abstract

Terrorism as we know today is not a new creation it is hiding in the community in form of tactics, strategies, doctrines, methods and means around which only a consensus is needed to reach the light of the day. While some see terrorism as a crime, others describe it as a sacred duty, and as long these two sides exist terrorism will flourish. Terrorists today are better trained and better equipped therefore elusive as never before, this fact has led that this phenomenon rapidly expanding and reaching the whole planet. Inadequate and above all the non-unified terminological definition of terrorism as a concept contributes to this prevalence. Although the world community agree that terrorism is a global evil and terrorist organizations are characterized as criminal, the global power centers utilize this confusion and use terrorism to achieve their own interests. The headquarters of terrorist activities in accordance with those interests have now been stationed in the Middle East and in a multitude of terrorist organizations, one has emerged as a leading one known as Islamic state.

Adresa autora:

Boris Bursać

boris.bursac89@gmail.com

Keywords: Terrorism, Ansar al Islam, Salafism, Wahhabism, Islamic State



1 UVOD

Današnje, kako ih novinari često nazivaju „violentne grupe“ najčešće se vezuju za islam pogotovu posle napada na Svetski trgovinski centar u Njujorku 11.09.2001 godine. Često se laički povezuju islam i islamistički fundiran terorizam gde jedni zastupaju tvrdnju da ove violentne grupe, terorističke organizacije, radikalne grupacije - nazovimo ih kako hoćemo inspiraciju za svoje akte nalaze u islamu kao religiji, dok sa druge strane imamo grupaciju koja forsira termin „islamistički terorizam“ koji svoje uporište ima u islamu ali kao svojevrstan oblik političkog delovanja. Hteli mi ili ne terorizam se danas bez bilo kakve sumnje najčešće vezuje za religiju. Pa i nedavni krvavi teroristički napad u Parizu nije bio dovoljan sam po sebi, već su pojedini teoretičari zavere iskoristili ovaj okrutni događaj da bi plasirali teoriju koja tvrdi da iza ovog napada stoji takozvani „Novi svetski poredak“ koji teži produbljivanju mržnje i izazivanju ratova između hrišćana i muslimana, pa se kao logičan sled događaja, otkopava po ko zna koji put Hantingtonova „Teorija sukoba civilizacija“. Suština je u tome da ni jedna religija prema svojim jedinim autentičnim, a tu pre svega mislim na pisane izvore ne propagira nasilje već kao aksiom ima za cilj promovisanje mira i blagostanja. Dakle, da podvučem religija je kroz istoriju bila upravo ta koja je obuzdavala zaraćene strane i suzbijala agresiju ali kao jedan multidimenzionalan fenomen ona može posredno ili neposredno biti uzrok i povod raznih oblika nasilja pa i terorizma. Jednostavno pojedini interpretatori religije iako možda veruju u reč Božiju nalaze načina da istu oskrnave, pre svega pogrešnim tumačenjem odnosno falsifikovanjem svetih spisa ili bolje rečeno njihovim zloupotrebljavanjem. Stoga nijednu religiju ne smemo kriviti već te pojedince i njihove zločinačke akte koji tu religiju svojataju izmenjuju i stvaraju pogrešnu sliku o njoj odnosno etiketiraju je kao terorističku. Da bi saznali šta je u suštini izvor gore napomenutih sukoba mora se oformiti jasan stav oko terorizma na globalnom nivou. Pisao sam u svojim prethodnim radovima da terorizam nije jasno definisan i da to predstavlja izuzetno velik problem. Posle terorističkih događaja u Parizu verovalo se da će doći do nekog jasnijeg stava svetske političke scene ali

po svemu sudeći konsenzus još nije postignut, problem se javlja prvenstveno kada pojedinac, kojeg jedan deo društva naziva teroristom, postaje simbol borca za slobodu drugom delu tog društva i samim tim taj problem ostavlja otvorenim i uvek aktuelnim. Dakle sa pravom možemo zaključiti da terorizam očigledno nije samo prosta reč već oružje. Očito su definicije politički motivisane tako je bilo, jeste i biće iz prostog razloga što se ljudi kao predatori njima služe kako bi određene pojedince i grupe obeležili i njima naudili. Dakle ne postoji univerzalna definicija terorizma i sumnjam da će ikad i postojati ali konsenzus se mora postići bar oko glavnih odrednica odnosno aspekata terorizma kao što su: politički ili ideološki motivi, nasilje, strah, napad na neborce, pretnja, zastrašivanje, način borbe, strategija, taktika itd. Kao što sam napomenuo jedna od najtužnijih činjenica je to da se jedna religija čija god ona bila naziva terorističkom i kao takva doživljava ogromnu društvenu degradaciju, konkretno kada govorimo o islamu - dolazimo do situacije da ti manipulatori i falsifikatori svojim delima dovode do toga da religija kojoj pripadaju biva percipirana kao fundamentalistička iako ogromna većina muslimanskog stanovništva uopšte ne pripada niti učestvuje u fundamentalističkim pokretima. E baš zato moramo ući u srž problema jer kao što znamo danas verski sukobi vrlo retko nastupaju samostalno već imaju svoju političku, ekonomsku ili neku drugu pozadinu. Za neke ti teroristički akti predstavljaju vid komunikacija nekih terorističkih organizacija, za neke vid zastrašivanja a u svojoj biti nije ništa drugo do običnog zločina koji izaziva još veću represiju. Upravo će terorističke organizacije na čelu sa ISIL odnosno Islamskom državom biti predmet daljeg istraživanja ovog rada.

2 KRATAK OSVRT NA ISTORIJU

Islamska država koja danas „drma“ svetom nikako nije nova teroristička organizacija već je to grupacija koja je više puta u svojoj istoriji menjala ime i prilagođavala se datom trenutku. Prema podacima koja su poznata javnosti, ova organizacija je osnovana od strane Jordanca Abu Musaba al-Zarkavija (Abu Musab al-Zarqawi) koji je još kao mladić počeo da radikalizuje svoje ideje i stavove. Osamdesetih godina upravo te ideje su ga navele ka Avganistanu kako bi se

priključio borbi protiv Sovjetske okupacije, ali kao što znamo taj sukob se brzo završio i al-Zarkavi se upućuje na pakistansku granicu gde otpočinje svoju karijeru na dobro razvijenom crnom tržištu. Tu usvaja salafističku ideologiju, o kojoj ću kasnije pisati i to pod mentorstvom palestinskog šeika Abu Muhameda al-Makdisija (Sheikh Abu Muhammad al-Maqdisi) inače salafi-džihadiste. Zajedno u Jordanu osnivaju svoju prvu militantnu organizaciju pod nazivom Bajat al-Imam (Bayat al – Imam) (Kirdar, AQAM Futures Project Case Studies: Al Qaeda in Iraq, 2011), naravno organizaciju baziranu na salafističkoj ideologiji inače preteći daleko poznatije al-Zarkavijeve terorističke organizacije Tavhid val Džihad (Jama'at al-Tawhid wal-Jihad), skraćeno JTJ. Njihove intrige nisu dugo zaživele i brzo bivaju uhapšeni od strane vlasti zbog kritika upućenih na račun vladajuće dinastije Hašamita (Hashemite). Naravno kao i svaki učenik pa i Al - Zarkavi težio je da zaseni svog mentora svojim sposobnostima švercujući svoje još radikalnije stavove iz zatvora koji će biti objavljeni na salafističkim sajtovima. Nakon puštanja iz zatvora, kako je njihov plan dostigao najnižu lestvicu, vraća se u Avganistan gde vodi islamistički militantni trening kamp kod Herata. Apsolutno moramo napomenuti da ovi događaji nisu promakli tadašnjem lideru Al - Kaide (Al – Qaeda), Osami bin Ladenu koji je nakon izlaska Al - Zarkavija iz zatvora stupio sa njim u kontakt. Iako postoji dosta razlika između njih, pre svega zbog različitih taktika i ciljeva, do koalicije je nekako došlo. Prema postojećim podacima (Felter & Fishman, 2007) i događajima iz naše bliske prošlosti vidi se sledeće da Al Zarkavi cilja svoje „bliske neprijatelje“ kao što su vlade Izraela, Jordana dok Al Kaida na čelu sa bin Ladenom bira „daleke neprijatelje“ kao što su SAD. Još jedna stavka koja ih je razdvajala jeste to što Al Zarkavi potencira i napade na neistomišljenike unutar islama, konkretno govorimo o šiitima. Ipak pored svih ovih razlika Al Zarkavi je kasnije primljen u Al Kaidu. Stvari počinju da se zahuktavaju. Naime, oktobra 2004. godine Al Zarkavi učvršćuje veze sa Al Kaidom i kao logičan sled događaja zaklinje se na vernost bin Ladenu. Ovaj akt mu u mnogome pomaže, ne samo što je postao lider organizacije džihada u Mesopotamiji, odnosno lider Al Kaide u Iraku (Tanzim Qaidat al-Jihad fi Bilad al-Rafidayn Zarqawi) već je sada na raspolaganju imao jednu jasno organizovanu terorističku organizaciju koja

deluje na globalnom nivou sa mnogo više ljudstva i resursa za vođenje sve opšteg džihada što mu je i bila namera. On je možda formalno podržao bin Ladena i njegove ciljeve ali u suštini ostao je pri svojim stavovima da treba napadati neprijatelja koji je blizu, što konkretno znači ići u okrutnu gerilsku borbu protiv američkih i koalicioni snaga i protiv šiitske populacije u Iraku. Ideja je bila sledeća, da se iskoriste suniti koji su bili uz Sadama Huseina a uz to manjina u Iraku a pre svega iskoristiti njihov strah od dolaska šiita na vlast. Tako da su suniti na početku davali podršku Al Zarkaviju. Pošto je, kao što sam napomenuo Al Zarkavi još u mladim danima bio izuzetno radikaln, ta njegova tamna strana stvarala mu je velike probleme. Forsirao je borbu starih „assasina“, odnosno borbu zasnovanu na samoubilačkim napadima što je docnije dovelo do gubljenja podrške u narodu Iraka pa tako i samih sunita. Ne mogu sa sigurnošću da tvrdim da je on oživeo tu vrstu borbe ali su samoubilački napadi postali izuzetno učestali u njegovo vreme i vreme bin Ladena. Nije sam metod borbe smetao sunitima već spremnost da kolateralna šteta ili cilj bude narod Iraka i neki sunitski lideri koji se smatraju izdajnicima. Osuda nije samo stizala od naroda Iraka već i od čelnika Al Kaide: Ajmana al Zavahirija (Ayman al-Zawahiri) koji je urgirao da se odnosi sa iračkim liderima poboljšaju i bin Ladena lično (Brown, 2007). Mnogi su bili protiv njegove strategije ubijanja velikog broja šiita i rušenja njihovih religijskih objekata ali je Al Zarkavi naravno ignorisao naloge centrale organizacije čak je i preuzeo odgovornost za bombaške napade u Jordanu gde je život izgubilo najviše osoba islamske veroispovesti. To mu nije bilo dovoljno već je u februaru 2006 godine organizovao napad (Worth, 2006) na al Askari džamiju poznatiju kao „Zlatna Džamija“ koja se nalazi u iračkom gradu Samari. Taj napad je produbio krizu u odnosima šiita i sunita i proizveli niz sukoba u kojima je napadnuto veliki broj sunitskih džamija a koji su završeni nekoliko dana kasnije uvođenjem policijskog časa. Dakle na osnovu svega gore navedenog Al Zarkavi je morao da potraži neku sigurniju podršku, kako bi njegovi planovi eksplicitno bili sprovedeni u delo. Podršku je naravno ubrzo našao u kurdsjoj islamističkoj grupi poznatoj kao Ansar al-Islam ili partizani islama, koji su takođe kao ideologiju koristili selafizam.

3 ANSAR AL ISLAM

Ansar al – Islam, poznata još kao Ansar al-Suna ili Džemat Ansar al-Islam je organizacija koja je bila mahom sastavljena od militantnih kurda koji su bili pripadnici selafističkog pravca¹ islama sa sedištem u iračkom delu Kurdistanu. Na početku su u organizaciju primani samo Kurdi ali zbog potreba organizacije članstvo je prihvatilo i pristalice iz Jemena, Iraka i Sudijske Arabije. Zvanično ova organizacija nastala je 2001. godine fuzijom više organizacija prethodno članova Islamskog pokreta Kurdistanu, od kojih su najpoznatije (Rubin, 2001):

- Al Tavhid
- Kurdski Hamas
- Al Tavhid – Islamski front
- Druga soranska jedinica
- Reformska grupa Mule Krekara
- Džund al Islam

Na čelo novoosnovane organizacije postavlja se Kurd stroge islamske ideologije Mula Krekar čije puno ime glasi Nažmudin Faradž Ahmed (Najmuddin Faraj Ahmad). Moram da naglasim da je Ansar al Islam morao imati izuzetno dobru saradnju sa Al Kaidom iz jednostavnog razloga što su neke organizacije koje su činile Ansar al Islam bile obučavane od strane Al Kaide, možda nisu sve direktno bile povezane ali se na primer za Džund al Islam sa sigurnošću to zna. Ovo napominjem iz prostog razloga što je kasnije osporavana saradnja između Ansar al Islama i Al Kaide, što se kosi sa zdravom logikom jer je većina tih da kažemo prvih članova novoosnovane organizacije učestvovalo u ratu u Avganistanu tik uz „rame bin Ladena“, znači bili su svojevrtni ratni veterani. Prilog tome govori i činjenica da je preko 100 članova Ansar al Islama bilo obučeno i učestvovalo u nekim ratnim dejstvima na strani Al Kaide (O'Toole, 2003). Možemo zaključiti iz gore navedenog teksta da ova organizacija nastala od nekoliko manjih militantnih grupacija ima jedan jasan cilj a to je: da nameće svoje striktno viđenje islama, kažnjava one koji ne poštuju te dekrete, naoružava i obučava borce, formira dobro

organizovane grupe koje će se za te svoje ideale boriti. Dakle ostalo je samo izabrati metu, a meta se ubrzo i našla to je „Patriotski savez Kurdistanu“ koji sa „Kurdsom demokratskom strankom“ čini Regionalnu kurdsku vladu. Patriotski savez Kurdistanu bio je nacionalistički nastrojen ali i sekularan što nikako nije odgovaralo Ansar al Islamu koji je zastupao totalno drastičniji stav koji podrazumeva sledeće:

- Uspostavljanje islamskog kalifata na prostoru Kurdistanu
- Striktno uvođenje šerijatskog prava
- Uvođenje zakona koji obavezuje muškarce da nose bradu
- Zabrana osobama ženskog pola na edukaciju i traženju posla
- Zabrana emitovanja televizijskih i muzičkih programa
- Uvođenje oštrijih kazni tipa : amputacija, kamenovanje, šibanje za zločine kao što su krađa, konzumiranje alkohola i preljube

Ansar al Islam je odgovoran za otprilike 14 napada od kojih se 5 dogodilo u provinciji Kirkuk, oko 5 napada na putevima između Kirkuka i Tikrita, dve operacije su izvršene u samom Tikritu a ostala dva napada vezana su za grad Mosul, odnosno prostor između Mosula i Bagdada. Dakle vidimo da je ova teroristička organizacija delovala uglavnom na severoistoku Iraka, mete su skoro sve bile ili iračka vojska ili policija, odnosno njeni oficiri ili policajci, zauzimanje oružja i vojnih vozila, otimanje municije i jednom je u opciji bio napad na naftna polja.

Najpoznatija operacija je pokušaj ubistva premijera Regionalne vlade Kurdistanu Berhama Saleha (Barham Ahmed Salih) u aprilu 2002. godine, inače pripadnika Patriotskog saveza Kurdistanu i uspešno izvršeni atentat na generala Ševketa Hadži Mušira (Shawkat Haji Mushir) i još pet članova Patriotskog saveza Kurdistanu u februaru 2003. godine. Upravo ova organizacija se jednostavno nametnula Al Zarkaviju i njegovoj organizaciji kao pogodan partner ali se isprečila invazija na Irak. Ubrzo potom Regionalna vlada Kurdistanu koristi ovaj pogodan trenutak da krene

¹ Iako većina Kurda pripada Šafi učenju sunitskog islama, u organizaciji su dominirali Kurdi selafističkog opredeljenja

u opštu ofanzivu protiv Ansar al Islama. Optužba je glasila da je (Schanzer, 2004):

- Ansar al Islam u direktnoj vezi sa Al Kaidom
- Da su članovi prošli vojnu obuku u Avganistanu
- Da je 57 avganinstanskih boraca ušlo u Irački Kurdistan preko Irana

Većina članova je ili ubijeno ili zarobljeno a deo je prebegao u susedni Iran. Mula Krekar zbog toga što je osuđen na smrtnu kaznu napušta Irak i beži u Norvešku u kojoj se nalazi i danas. Ansar al Islam je možda pretrpeo poraz ali nije totalno uništen. Na mesto lidera ubrzo dolazi još radikalniji Abu Abdulah al Šafi (Abu Abdullah al-Shafi) (Gregory, 2008), takođe poznat javnosti kao Warba Holiri al Kurdi (Warba Holiri al-Kurdi) i preuzima komandnu odgovornost u organizaciji. Ovaj put organizacija nastavlja sa radom iz Irana i to pod pristalicama šafističke škole islama gde ubrzo menja ime u Ansar al Suna da bi se kasnije 2007. godine vratili na stari naziv Ansar al Islam. I ovom periodu mete su ostale iste, stim što su pojačani napadi na koalicione snage u Iraku. Najkrvaviji napad svakako je onaj iz februara 2004. godine kada se desilo više simultanih samoubilačkih napada na kancelarije Patriotskog saveza Kurdistanu u Erbilu, a rezultat je bio preko 100 poginulih i preko 130 ranjenih. Ova teroristička organizacija je do februara 2007. godine izvršila preko 1600 terorističkih napada (Schanzer, 2004) i ni u jednom trenutku nije krila da je sarađivala sa Al Kaidom. U maju 2007. godine postojao je pokušaj da se Ansar al Islam integriše u jednu pan - islamsku organizaciju sa oštrijim stavom prema koalicionim snagama u Iraku. Uz pomoć nekoliko viđenijih grupacija formiraće se anti koaliciona organizacija pod nazivom „Reformacija i džihad front“ i biće svojevrstan pandan Al Kaidi. To se na kraju i desilo ali se Ansar al Islam ubrzo vratio svojim korenima odnosno Al Kaidi, gde su zajedničkim snagama napadali koalicione snage i one Iračane koji su bili deo vlade koja je formirana od strane SAD. I nakon povlačenja američkih trupa ova teroristička organizacija ostala je aktivna napadajući iračke bezbednosne snage. Otpočinjanjem novih sukoba u Siriji, Ansar al Islam okreće se toj ratnoj zoni. Odnosi između Ansar al Islama i novonastale Islamske države menjale su se iz časa u čas, prelazila su iz stanja saradnje do totalnih neprijateljstava, razlog tome

je što Islamska država teži da potčini Ansar al Islam pod svoje rukovodstvo. Kratak period je Ansar al Islam odolevao Islamskoj državi ali se ipak desilo ono što je bilo neminovno. Već sredinom 2014. godine skoro kompletni irački deo Ansar al Islama prelazi u Islamsku državu a sirijski deo ostaje nezavisan (Al-Tamimi, 2015). Abu Abdulah al Šafi biva uhapšen 2010. godine i stacioniran u Bagdadskom centralnom zatvoru. Na njegovo mesto 2011. godine dolazi šejk Abu Hašim (Sheikh Abu Hashim Muhammad bin Abdul Rahman al Ibrahim) koji se na njemu nalazi i danas. Ostao sam dužan da dovršim priču o Al Zarkaviju, koji je kao što sam već naglasio našao partnera u gore pomenutoj terorističkoj organizaciji ali ne zadugo koliko je možda on želeo. Nakon rušenja režima Sadama Huseina, nova meta se nameće a to su pre svega snage predvođene Sjedinjenim Američkim Državama. Al Zarkavi sa svojom dobro „podmazanom mašinom“ u 17 meseci izvodi na desetine organizovanih terorističkih napada od kojih su najpoznatiji oni u šiitskim gradovima Karbali i Nadžafu (Najaf) u kom su korišćene auto bombe gde je život izgubilo 60 ljudi. Zatim na pijaci Musajiba (Musayyib) (Howard, 2005) grada nadomak Bagdada, u trodnevnim samoubilačkim napadima život izgubilo oko 150 ljudi a ranjeno je oko 260. Onda za vreme parlamentarnih izbora u januaru 2005. godine. Taj dan se desilo više od 100 oružanih napada širom Iraka. U tom krvavom danu život je izgubilo najmanje 44 osobe uključujući 9 bombaša samoubica.

Svi ovi gore napomenuti događaji samo su podstakli iračke vlasti i koalicione snage na sve žešću borbu protiv terorizma i samog Al Zarkavija kao jednog od najozloglašnijih terorističkih lidera. U jednom momentu pristao je da zajedno sa ostalim selafističkim pokretima povрати poverenje naroda i oformi pokret gde će svi zajedno delovati pod nazivom Medžlis Šura al Mudžahidin (Majlis Shura al-Mujahidin), ali ovaj projekat je propao i ostao zapamćen kao samo jedna medijska ideja koja je imala za cilj da približi Al Kaidu iračkom narodu. Već sredinom 2006. godine Al Kaida u Iraku gubi svoja utvrđenja u provinciji Anbar. Finalni udarac zadat je juna 2006. godine ubistvom Al Zarkavija (Burns & Filkins, 2006) i njegovog duhovnog savetnika šejka Abd al Rahmana (Sheik Abd-Al-Rahman), ciljanim bombardovanjem skloništa u kom su se

nalazili 50 kilometara od Bagdada u gradu Bakubah (Baqubah) - od strane američkih vazduhoplovnih jedinica. Navodno njegovu lokaciju je odala sama Al Kaida, odnosno njegov saborac iz same organizacije koji je kao razlog naveo njegov ekstremni stav prema pripadnicima islama, prevashodno se misli na šiite. Nakon Al Zarkavijeve smrti na čelo ove organizacije postavlja se Abu Ajub al Masri (Abu Ayyub al-Masri), egipatski bombaš koji je takođe obučavan u Avganistanu. Smatralo se da će smrt Al Zarkavija trajno oštetiti organizaciju ali Al Masri uspeva da je održi. On je pre svega upeo da izdejstvuje spajanje sa još nekim iračkim organizacijama i time stvorio vreme da se organizacija brzo reformiše. Formira Islamsku državu Iraka a na čelo postavlja Hamida Muhameda (Hamid Dawud Mohamed Khalil al Zawi), poznatijeg kao Abu Omar al Bagdadi, kasnije se postavlja pitanje da li je Al Bagdadi uopšte vodio organizaciju i bio njen pravi lider (Felter & Fishman, 2007) ili je bio marioneta odnosno deo ideje Al Masrija da se pridobije irački narod. E sad stalno potenciram ovu temu pridobijanja iračkog naroda i nikako da je objasnim. Dakle Al Kaida u Iraku kao što sam već pominjao i za vreme Al Zarkavija i za vreme Al Masrija gubila je poverenje u narodu Iraka, ne samo zbog terorističkih napada u kome je često nedužna žrtva bio isti taj narod već i zbog velikog broja stranih ratnika koji nikakve veze nemaju sa Irakom i iračkim narodom. Prema nekim podacima koje je izdala sama Al Kaida u Iraku, oko 200 stranih boraca (Felter & Fishman, 2007) je učestvovalo u oružanim sukobima na prostoru Iraka. Al Masri i Al Bagdadi su manje ili više uspešno delovali na ovom prostoru sve do aprila 2010. godine kada su u zajedničkoj američko - iračkoj akciji ubijeni. Kasnije se u 2011. godini koalicione snage povlače iz Iraka, ali ostaju tesno povezane sa plemenskim odnosno lokalnim snagama bezbednosti. Al Kaida u Iraku još jednom doživljava snažan potres ali uspeva da se zadrži i to pod novim liderom još jednim Al Bagdadijem poznatijim kao Abu Bakar al Bagdadi (Abu Bakr al-Baghdadi).

4 SELAFIZAM, DŽIHADIZAM I VEHABIZAM

U javnom životu se sve češće susrećemo sa terminima poput selafizma, džihadizma, i

vehabizma te se nameće potreba za njihovim objašnjenjem. Pripadnici selafizma su u suštini najekstremniji fundamentalisti koji teže oživljavanju jednog izvornog to jest autentičnog islama. On se konkretno odnosi na „al-salaf al-saleh“ odnosno prve tri generacije islama sledbenika samog proroka poznatijih kao „pobožni prethodnici“. U savremenoj upotrebi selafizam se definiše kao ultra ekstremni oblik sunitskog islama, koji teži da preoblikuje društvo u skladu sa islamskim zakonima baziranim na šerijatskom pravu. Svoju inspiraciju u suštini ovaj pravac crpi od poznatog salafiste iz Damaska ibn Tajmija (Taqieddin ibn Taimiya) i Muhmeda al Vahaba (Muhammad ibn ‘Abd al-Wahhab) ali je ovaj pravac dodatno razvijen od strane Saudijske Arabije odnosno njenih iskazanih teologa. U suštini pojam „selafi“ znači onaj ko ima posebna znanja ili sposobnosti koja su iznad većine muslimanskog stanovništva, da dosledno prati selafistička ubeđenja. Kao što sam napomenuo pravac crpi inspiraciju od Ibn Tajmija i Al Vahaba ali je dodatno razvijen od strane Muhameda Abduha (Muhammad Abduh), Džamal al Afganija (Jamal al-Din al-Afghani) i Rašida Rida (Rashid Rida). Sa obzirom da je Al Afgani bio politički aktivista a Abduh nastavnik koji se zalagao za socijalne i obrazovne reforme možemo reći da je ovaj pravac postavljen na širokim temeljima.

Ono što je stav svih ovih teologa a zvanično ga je oformio Al Tajmije jeste da je islam monoteistička religija koja zahteva priznanje i da bilo koji organ bio on verski, socijalni ili politički može biti legitiman samo ako je duboko ukorenjen u islamu. Postoje neke opšta pravila ili karakteristike koje su svojstvena svim selafistima a to su:

- Da su oni jedini koji mogu da šire taj izvorni odnosno autentični islam
- Kategorički odbacuju bilo kakvu mogućnost simboličke ili metaforičke interpretacije ili tumačenja božanskih imena ili atributa
- Ekskluzivno pravo Boga je da bude slavljen i obožavan
- Osuđuju i protive se svim inovacijama unutar religije
- Poštuju i pribegvaju samo Al Tajmijevim pravnim i teološkim pravilima

Neke salafitičke grupe su izuzetno pacifistički nastrojene, ali su ih glasovi izuzetno radikalnih

manjina nadvladali i oformili stav gde je džihad najvažnija obligacija članova selafističkog pokreta. Na osnovu uticaja tih grupa selafizam ima jedan jasan stav da:

- Sve sekularne lidere treba ukloniti sa muslimanskih zemalja
- Treba održavati trajni konflikt protiv svih nemuslimanskih vlada koje intervenišu na muslimanskoj teritoriji

Ova dva stava su dovela do toga da se razvije to radikalno krilo islama i da dan danas bude izuzetno aktivno pre svega na teritoriji Bliskog istoka ali i šire. Sve selafističke frakcije možemo podeliti u 7 grupa:

- Matica saudijskog selafizma: ovu grupu čine sveštenici iz Saudijske Arabije koji su navodno protiv ekstremnih džihad grupa i izuzetno su verni svojim vladarima.
- Jordanski lanac selafizma: na čelu ove grupe je Muhamed Al Albani (Muhammad Nasir-ud-Dīn al-Albani). Zvanično ova grupa je najtiša i izbegava sve veze sa ekstremnim selafistima. Teže da budu najstroži u primeni svih koncepata bid'ah² u islamu.
- Sahwa grupa: predstavnici ove grupe su Salman al Oda (Salman al-Oadah) i Safar al Havali (Safar al-Hawali). Ova grupa se smatra jednom od najpametnijih u selafističkom pokretu i jedna je od najprisutnijih na društvenim mrežama. Zahvaljujući tome ona ima masovnu podršku mladih i obrazovanih muslimana. Njihova borba za muslimane iskazana je u aktivnoj borbi protiv socijalnih problema.
- Madkali grupa: ovo je grupa sa najviše podela, ona se koncentriše najviše na pitanje jesu li pojedinci na ispravnom salafi putu ili ne.
- Egipatski selafizam: ovaj pravac je bio u velikom haosu zbog Arapskog proleća, ali je najbližiji Al Albanijevom pravcu. Najznačajniji ogranak je Nur partija.
- Takfiri salafisti: ova grupa obično se bavi sa takfir pitanjima odnosno pitanjima ko je i da li je nevernik. Naglašava negativan uticaj Zapadnog intervencionizma i licemeran stav

nekih muslimanskih vlasti. Ova grupacija se smatra jednom od najoštrijih.

- Radikalni salafi-džihadisti: ova grupa ima najradikalnije teološke ali i političke stavove. Njoj pripadaju velike terorističke organizacije kao Al Kaida i Islamska država. U svojim teološkim stavovima osuđuju sve ostale salafi grupe zbog manjka borbenosti i smatraju da sve grupe moraju da implementiraju njihovu verziju džihada.

Za mnoge terorističke organizacije se vezuje termin džihadizma pa bi trebalo nešto više napisati o njemu. Džihad sa danas najčešće prevodi kao „sveti rat“ ali u svom originalnom značenju predstavlja „napor ka Božijem putu“. Prvobitno se termin upotrebljavao kao vid duhovne unutrašnje borbe kako bi se vernik umilostivio Bogu a kasnije se termin preobrazio u nešto sasvim drugo. Koncept džihada se tako jednostavno nametnuo kao izgovor za razna delovanja mislim pre svega na muslimanska osvajanja u prošlosti a danas je tu ulogu preuzeo upravo islamistički terorizam.

Tako da sa apsolutnim pravom možemo reći da je iskorišćavanje džihada za agresiju protiv nevernika odnosno nedužnih ljudi samo zloupotreba pravog, suštinskog značenja termina. Kada govorimo o vehabizmu, ovaj pojam se čest poistovećuje sa selafizmom i zato moramo napraviti distinkciju odnosno povući crtu između ova dva pomalo slična ali ipak različita pojma. Naime vehabizam kao jedan konzervativni pravac osnovao je Muhamed ibn Al Vahab (Muhammad ibn Abd al-Wahhab) u 18 veku. Vahabov reformski pokret se bazira na njegovoj ideji i stavu da je islam nakon trećeg veka muslimanske ere (950 godina) lažan i kao takvog treba ga iskoreniti. Muslimani da bi bili pravi odnosno istinski vernici moraju se isključivo pridržavati originalnih verovanja koja su utvrđena direktno od Muhameda. Ovaj njegov ekstremni stav nastao je iz straha od regresije ka islamskog politeizmu. Tu se pre svega misli na razna hodočašća ka specijalnim džamijama, posete nekim njima važnim pećinama, poklonstvo nekim kamenjima, razna žrtvovanja u nečiju čast itd. To su sve prakse koje su bile ukorenjene u narodu i nekako su se tradicionalno vezale i za ovu religiju,

²Inovacija

ali u vehabizmu su izričito zabranjene. A današnja sekularna ponašanja nekih muslimanskih vernika su pod svojevrsnom anatemom vehabijskih sledbenika. I upravo ovi razlozi protiv sekularizma i modernizma dovode do ekstremizma i kasnije nasilja. Ovaj pravac se dakle zasniva na apsolutnom monoteizmu a sve ostalo se smatra jeretičkim inovacijama (bid'ah). Takođe se protive svim reformističkim grupama u islamu koje su nastale u 18. i 19. veku, smatrajući ih pro-zapadnim odnosno ustrojenim po Zapadnim standardima a posebno se misli na rodne odnose, porodično pravo, participativnu demokratiju i ličnu autonomiju. Al Vahab je potencirao da njegovi sledbenici tumače svete knjige kako on nalaže a ako primete ili saznaju da neko ne interpretira na taj način, tu osobu javno obeleže kao nevernika. Njega mogu ubiti a njegovu imovinu mogu podeliti među vehabijama. Na taj način je uspeo vrlo brzo da prikupi veliki broj sledbenika koji su pored verske podrške dobijali i materijalnu i samim tim imali su razloga da se priključe ovoj radikalnoj grupaciji. Vremenom ovaj pravac se raširio i van granica Saudijske Arabije, čak se smatra da je uticao i na raspad Otomanskog carstva 1920. godine. Pod maskom reformi ovaj pravac je uzeo maha u poslednje tri decenije naravno uz veliku podršku bogatih pojedinaca. Vehabizam je pretrpeo velike podele a rezultat je evidentan i odsososi se na totalnu radikalizaciju ovog pravca. Vehabizam je uz pomoć bin Ladena proširio svoj uticaj na Bliski istok, istini za volju ne u tolikoj meri kao u Saudijskoj Arabiji ali postoje grupe koje ga izričito podržavaju. Svakako možemo reći da je to manjinski pravac u muslimanskom svetu ali je ipak uticajan za razliku od drugih ekstremističkih pokreta. Danas sledbenici vehabizma imaju jedan izuzetno radikalan odnosno konfrontirajući stav prema onima koji osporavaju njihovu ideologiju. Iako se islam uvek predstavljao kao religija mira i tolerancije: njihov prorok Muhamed sklapao je sporazume sa nemuslimanima, njihova sveta knjiga kaže da nema prisile u veri i da su svi ljudi slobodni da uživaju bilo koju religiju, ipak ovakvi pokreti samo stvaraju pogrešnu sliku. Ta slika govori da je osnovni islamski princip ukinut a sve zahvaljujući ovim modernim ideološkim ekstremistima. Vehabijski sledbenici selektivno primenjuju stavove islamske svete knjige forsirajući tako svoj pravac kao jedini istinski a osnovna ideja je da se nametnu njihova

verovanja svima bilo to muslimani ili pripadnici drugih religija. Ovako selektivno tumačenje islamske svete knjige ne samo da daje versku i ideološku potporu već im daje za pravo da formiraju razne militantne pokrete koji na osnovu tih stavova uzimaju oružje u ruke i uperuju ga protiv neistomišljenika. Dakle iako su ovi pokreti ideološke prirode oni vrlo lako pribegavaju nasilju odnosno oružanoj borbi, šta više, ovi ekstremistički pokreti odbacuju bilo kakvu vrstu primirja ili kompromisa insistirajući tako na svom radikalnom putu i nameri da se dostavi jasna poruka javnosti. Šta možemo zaključiti iz svega ovoga? Vehabije u svakom trenutku mogu objaviti rat bilo kome – odnosno onome za koga oni smatraju da je nevernik. Tako je dolazilo do situacija da su cele vlade nekih zemalja proglašene neverničkim i njima je objavljivao rat, klasičan primer su: Egipat, Pakistan, Alžir, Jordan, Sirija. Oni imaju jednu jasnu taktiku:

- Infiltrirati se u džamiju, islamske centre, dobrotvorne organizacije
- Vršiti indoktrinaciju svojim idejama, stavovima i ciljevima
- Nametnuti stav o slabom društvu što će kasnije služiti kao izgovor za određene nasilne akte
- Pokrenuti džihad protiv tog društva i na osnovu njega pravdati svoja nelegalna finansiranja

Danas su na osnovu ovih ciljeva mete vrlo jasno definisane i mnoge radikalne islamističke grupe ili pojedinci objavljuju rat ovim metama gde je na čelu kolone kao meta SAD sa svojim koalicionim partnerima. I zato se islam najčešće povezuje sa terorizmom i ekstremizmom jer su ga jednostavno te grupacije zloupotrebile i predstavile kao religiju koja propagira upotrebu terora, bombaških napada i jednostavno došlo je do stava koji nije tačan a to je da islam kao religija daje potporu jednom opštem stanju rata.

5 ISLAMSKA DRŽAVA

Sa apsolutnim pravom možemo reći da se danas jedan teror širi svetom a to je teror Islamske države. Ova nekada mala militantna teroristička grupa danas kontroliše prostor na kojoj živi oko 8.000.000 stanovnika i u svom sastavu ima nekoliko teritorija različitih država. Ova organizacija brzo je postala sinonim za zverstvo i

brutalnost - odsecanja glava, kamenovanja, masakre, etnička čišćenja. Ova divljaštva velika većina civilizovanih ljudi smatra nenormalnim a pripadnici Islamske države ih smatraju jednim racionalnim izborom. Oni su nemilosrdne fanatične ubice sa jasnim zadatkom a to je uspostavljanje halifata na temeljima šerijatskog prava (što im je donekle i uspelo) a ako im se bilo ko nađe na putu biće zverski ubijen. Kao što sam već napomenuo, Islamska država kakvu danas poznajemo nije nova tvorevina već je to organizacija koja postoji duže a u suštini samo je menjala nazive i delom rukovodstvo. Ona korene vuče još od 2004. godine odnosno priklanjanja Al Zarkavija Bin Ladenu i Al Kaidi gde dolazi do osnivanja Al Kaide u Iraku inače „majke“ odnosno preteče današnje Islamske države. Nakon ubistva Al Zarkavija 2006. godine na čelo ove organizacije dolazi egipatski bombaš Abu Ajub Al Masri (Abu Ayub al-Masri), koji je po svemu sudeći uspeo da očuva ovu organizaciju koja je doživela veliki poraz a uz to je izgubila svog lidera i osnivača Al Zarkavija. Mnogi Iračani kritikovali su Al Kaidu u Iraku zbog prisustva stranih boraca, tako da je Al Masri došao na ideju da integriše nekoliko manjih iračkih grupacija u svoju organizaciju i time je jasno brendira kao iračku. To mu polazi za rukom i on ubrzo menja ime organizacije u „Islamska država Iraka“ a na čelo postavlja svoju marionetu Abu Omara al Bagdadija. Za vreme prvog Al Bagdadija koalicione i lokalne snage ubile su oko 2400 članova Islamske države Iraka i zarobile oko 8800 (Kirdar, 2011). Do 2009. godine SAD su finansirale 100.000 lokalnih sunita za borbu protiv Islamske države Iraka (Kirdar, 2011), a već 2010. godine Islamska država Iraka gubi komunikaciju sa centralom Al Kaide a većina rukovodstva biva ili pobijeno ili zarobljeno (Hashim, 2014). Tako da i Al Masri i Al Bagdadi ginu u američko-iračkoj raciji o kojoj sam već pisao. Još jednom ova organizacija doživljava snažan poraz i leaderska pozicija ostaje upražnjena ali ne zadugo jer na čelo dolazi još jedan Al Bagdadi ali inteligentniji i sposobniji od prethodnog. Drugi Al Bagdadi poznatiji kao Abu Bakar al Bagdadi (Abu Bakr al-Baghdadi), uspeva da pregrupiše snage u vrlo kratkom roku i već 2012 krene u akciju pod nazivom „Breaking walls“ (rušenje zidova) u cilju oslobađanja svojih članova iz zatvora (Hashim, 2014). U tom periodu otvara se novi front na prostoru Sirije i Al Bagdadi premešta svoju sferu

interesovanja. Shodno tome on u aprilu 2013. godine objavljuje da teži udruživanju snaga sa nekim organizacijama i osnivanju nove krovne organizacije pod nazivom Islamska država Iraka i Levanta. To spajanje je odbila Al Nusra i Al Kaida što je posle stvorilo sukobe između ovih organizacija, ali to nije sprečilo neke borce iz ovih organizacija koji su se prepoznali u ovoj Al Bagdadijevoj ideji da se priključe novonastaloj organizaciji. Do kraja 2013. godine ova organizacija uz pomoć bivših Huseinovih pristalica u Iraku zauzima i preuzima kontrolu nad gradom Faludžom (Fallujah) a u Siriji grad Raku (Al-Raqqa). Nakon toga dolazi do izjave Islamske države Iraka i Levanta da je na teritoriji koju ona kontroliše nastala nova nacija, bez državnih granica i pod vođstvom halifa, poglavara svih muslimana. I desilo se da u toku jednog dana dojučerašnji građani Iraka i Sirije, hteli oni to ili ne postaju građani najmonstruoznije samoproglašene države poznate pod nazivom Islamska država Iraka i Levanta, na čijem je čelu Abu Bakar al Bagdadi kao njen halifa odnosno najveći verski autoritet u državi.

Iz svog uporišta u Raki, Islamska država Iraka i Levanta vodi ofanzivu i širi se na dva fronta i u Iraku i u Siriji. Do 2014 zauzimaju drugi najveći irački grad Mosul i napreduju ka Bagdadu usput vršeći najsvirepije zločine i uništavajući veliki broj etničkih i verskih manjina. Do kraja ove godine oni konsoliduju svoju vlast nad desetinama gradova i zvanično proglašavaju halifat u junu iste godine ali pod nazivom Islamska država. Nakon toga ovaj novonastali halifat preuzima funkcije na teritoriji koja se nalazi pod njihovom vlašću kao što su ubiranje poreza, rad policije, zdravstva i školstva, naravno u skladu sa svojim ekstremnim tumačenjima islama. Kako bi obezbedili stabilnost i podršku u ovim oblastima primenjuju ekstremno nasilje prema svojim neistomišljenicima koje se ogleda u javnim pogubljenjima, amputacijama i tome slično. Zahvaljujući intervenciji SAD i njenoj podršci šiitskoj vladi u Iraku, sprečen je dalji prodor Islamske države kojoj je malo falilo da zauzme Bagdad. Islamska država tada se žestoko okreće dešavanjima u Siriji i kreće u ofanzivu u severnom delu tačnije na granici Sirije i Turske. Sa obzirom da je to teritorija koju kontrolišu Kurdi, Islamska država ulazi u otvorene sukobe sa njima. Zahvaljujući vazdušnim napadima i finansijskoj podršci od strane

međunarodne koalicije pod vođstvom SAD poznate pod nazivom „Combined Joint Task Force - Operation Inherent Resolve (CJTF–OIR)“, Kurdi odolevaju napadima Islamske države i uspevaju da ostvare blagu prednost početkom 2015. godine. Pored toga što osvaja i kontroliše teritorije Islamska država uništava sve kulturne i verske objekte koji nisu u skladu sa njenom ideologijom bili oni jevrejski, hrišćanski ili muslimanski. Tako je svetsku javnost zaokupio snimak razaranja drevnih gradova Nimruda i Hatre koji su pod zaštitom UNESCO - ovi postupci su okarakterisani kao ratni zločini. Islamska država se tu ne zaustavlja već širi svoja delovanja van Sirije i Iraka i to u Libiji, Egiptu, Etiopiji, Tunisu i kasnije u Evropi tačnije u Francuskoj. Sve ove aktivnosti kao što sam napomenuo iziskuju novac i to je u suštini najveći izazov Islamske države da održi stalni izvor prihoda. Za sada im uspeva a pre svega zahvaljujući „petro-dolaru“ odnosno prodaji nafte, zatim prodaji antikviteta, ubiranju poreza i iznudama. Kako se Islamska država širila tako su joj prihodi rasli, prema navodima Rand korporacije ukupan prihod Islamske države sa početnih 1.000.000\$ mesečno krajem 2008. godine raste na nivo između 1.000.000\$ i 3.000.000\$ dnevno u 2014. godini (Johnston, 2014). U ovom izveštaju se navodi da pored finansiranja terorističkih aktivnosti novac odlazi u policiju, školstvo i zdravstvo. Ono što je interesantno jeste da Islamska država prema navodima ove korporacije plaća oko 400 \$ svoje borbe na mesečnom nivou, što je više nego što primaju neki službenici iračke vlade - i to možemo navesti kao još jedan razlog stalnog porasta broja boraca u redovima Islamske države. Procvat Islamske države polako se dovodi u pitanje pre svega zahvaljujući ulasku nove svetske sile u sirijske sukobe Rusije. Naime ruska intervencija, odnosno svojevršno Asadovo spasavanje od strane Rusije mnoge je bacila na razmišljanje, pre svega Zapadne centre moći. Mi Siriju moramo posmatrati kao saveznika Rusije jer se Asad upravo ovoj svetskoj sili obratio za pomoć, zato pro-zapadni analitičari ovu rusku kampanju obeležavaju kao povratak Moskve na Bliski istok. Kada bolje sagledamo celu situaciju mi možemo tvrditi da se Rusija nije uplitala mnogo u dešavanja na Bliskom istoku još od Sadatove izdaje i njegovom okretanju SAD, ali isto tako ona je ostala u tesnim vezama sa svojim saveznicima

iz Hladnog rata. I vidimo da na prvi oficijelni saveznički zahtev Rusija odgovara adekvatno. Otuda moramo odbaciti tvrdnju da se Rusija vraća na Bliski istok - ona se ne vraća, već je bila oduvek tu i kao pritajeni tigar čekala svoj trenutak.

6 ZAKLJUČAK

Na osnovu gore navedenog teksta, možemo zaključiti da terorizam iz veka u vek postaje prepreka na putu razvoja savremenog sveta kao globalnog društva. Zahvaljujući svojoj prilagodljivosti, terorizam se stalno menja po formi, sadržini, tipovima i oblicima organizovanja, načinima delovanja, tehničkoj opremljenosti i slično. Bilo da se služe ubistvima, otmicama, bombaškim napadima, oni teže jednom a to je ispunjenje svojih političkih odnosno ideoloških ciljeva. Svojim pojavnim oblikom terorizam nam oduzima ono što nam je najdraže, a to je sloboda, on stvara strah i nepoverenje među ljudima i samim tim remeti normalno društveno funkcionisanje.

Zato je danas upravo terorizam ta internacionalna pretnja oko koje svi treba da se ujedini i da joj se suprotstavimo. Dakle nekoliko puta sam napomenuo da je terorizam fenomen koji stalno prisutan u društvu a jedina razlika između „starog“ i „današnjeg“ terorizma jeste da je ovaj drugi globalniji, smrtonosniji i napredniji, a sve zahvaljujući tehnologiji i medijima. Neprijatelj je sada spreman i na otvorenu borbu jer je zahvaljujući „petro-dolaru“ 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 postaje značajan geopolitički faktor na Bliskom istoku i šire. Da bi se ova tvorevina nazivala državom mora da ima teritoriju i zato će uraditi sve kako bi zadržala svoje postojeće obrise države, što nam govori samo jedno da će sukobi potrajati. Za utehu nam je činjenica da nijedna država u svetu nije priznala ovu samoproklamovanu državu i da većina muslimana i druge islamističke terorističke organizacije imaju negativan stav prema Islamskoj državi. Kad sve uzmemo u obzir možemo formulisati zaključak koji kaže da dosadašnji model borbe ne samo da nam nije skinuo ovaj „jaram čovečanstva“, već je potpomogao da se ovaj fenomen proširi i u pravom smislu reči doživi svoj procvat.

CITIRANA DELA

- Al-Tamimi, A. J. (2015, 06 03). *Jamaat Ansar al-Islam: Fighting in North Aleppo Countryside: Tanslation and Analysis*.
- Brown, V. (2007). *Cracks in the Foundation: Leadership Schisms in Al-Qa'ida from 1989-2006*. West Point: Combating Terrorism Center.
- Burns, J. F., & Filkins, D. (2006, 06 13). Middle East - A Jihadist Web Site Says Zarqawi's Group in Iraq Has a New Leader in Place. *The New York Times*. Retrieved from <https://www.nytimes.com/2006/06/13/world/middleeast/13iraq.html>
- Felter, J., & Fishman, B. (2007). *Al-Qaeda foreign fighters in Iraq: A First Look at the Sinjar Records*. West Point: Combating Terrorism Center, Department of Social Sciences, US Military Academy.
- Gregory, K. (2008). *Ansar al-Islam (Iraq, Islamists/Kurdish Separatists), Ansar al-Sunnah*. New York: The Council on Foreign Relations.
- Hashim, A. (2014). *The Islamic State: From Al-Qaeda Affiliate to Caliphate*. Washington DC: Middle East Policy.
- Howard, M. (2005). *Three days of suicide bombs leave 150 dead*. London: The Guardian.
- Johnston, P. B. (2014). *Countering ISIL's Financing*. Santa Monica, California: Rand Office of External Affairs.
- Kirdar, M. (2011). *Al-Qaeda in Iraq*. Washington, D.C: AQAM Futures Project.
- Kirdar, M. (2011). *AQAM Futures Project Case Studies: Al Qaeda in Iraq*. Washington DC: CSIS.
- O'Toole, P. (2003). *Mullah denies Iraq al-Qaeda link*. London: BBC News.
- Rubin, M. (2001). *The Islamist Threat from Iraqi Kurdistan*. Washington D.C: Middle East Intelligence Bulletin.
- Schanzer, J. (2004). *Ansar al-Islam: Back in Iraq*. Philadelphia: Middle East Quarterly.
- Worth, R. F. (2006, 02 23). Blast at Shiite Shrine Sets Off Sectarian Fury in Iraq. *The New York Times*. Retrieved from <https://www.nytimes.com/2006/02/23/world/middleeast/blast-at-shiite-shrine-sets-off-sectarian-fury-in-iraq.html>

Datum prve prijave: 23.05.2018.
Datum prijema korigovanog članka: 20.11.2018.
Datum prihvatanja članka: 27.03.2019.

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

Style – **APA Sixth Edition:**

Bursać, B. (2019, 04 15). Poreklo Islamske države. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 38-49. doi:10.12709/fbim.07.07.01.05

Style – **Chicago Sixteenth Edition:**

Bursać, Boris. 2019. „Poreklo Islamske države.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 38-49. doi:10.12709/fbim.07.07.01.05.

Style – GOST Name Sort:

Bursać Boris Poreklo Islamske države [Časopis] // FBIM Transactions / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 38-49.

Style – Harvard Anglia:

Bursać, B., 2019. Poreklo Islamske države. *FBIM Transactions*, 15 04, 7(1), pp. 38-49.

Style – ISO 690 Numerical Reference:

Poreklo Islamske države. **Bursać, Boris.** [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, FBIM Transactions, T. 7, str. 38-49



SAVREMENA RAČUNARSKA FORENZIKA I FORENZIČKI ALATI

MODERN COMPUTER FORENZICS AND FORENZIC TOOLS

Zoran Čekerevac

Poslovni i pravni fakultet, „Union – Nikola Tesla“ Univerzitet, Beograd,
Srbija

Zdenek Dvorak

University of Žilina, Faculty of Security Engineering, Žilina, Slovakia

Lyudmila Prigoda

Maykop State Technological University, Maykop, Russian Federation

©MESTE

JEL Category: **C88, L86**

Apstrakt

Sve veća upotreba računara i na njima zasnovanih uređaja i opreme omogućila je znatna poboljšanja u funkcionisanju preduzeća i ustanova, ali i pojedinačnih korisnika. Istovremeno su se pojavili i rizici zbog njihove nepravilne upotrebe ili zloupotrebe. Do gubitka ili krađe podataka može doći na najrazličitije načine, od greške u radu korisnika, do pojedinačnih ili masovnih napada zlonamernih napadača. Neke od problema je moguće rešiti upotrebom alata samog operativnog sistema ili korišćenog softvera, a za pojedine situacije, kada je (ne)delo već izvršeno, potrebno je koristiti specijalne, namenske forenzičke alate. U slučaju potrebe za sudskim veštačenjem, zadatak forenzičara postaje još kompleksniji, jer uz otkrivanje uzroka, forenzičar mora da pruži i valjane dokaze da je delo učinjeno i (ako je moguće) ko ga je učinio, ali i da sam artefakt ostavi u nepromenjenom stanju da bi mogla da se izvrše i druga forenzička istraživanja bilo u vezi sa drugim razlozima bilo da ih izvrši druga institucija (ili drugi forenzičar). Zbog toga, a i zbog drugih razloga, neophodno je korišćenje specijalizovanih forenzičkih alata. U ovom radu se posle uvodnog dela u kome se razmatraju forenzika i antiforenzika, kratka istorija i savremena zakonska regulativa, kao i izazovi u vezi sa forenzikom i alatima, detaljnije razmatraju računarski forenzički alati. Akcenat je stavljen na besplatne forenzičke alate. U zaključcima rada su sumirani stavovi o forenzici i forenzičkim alatima i ukazano na pravce budućeg razvoja, posebno u vezi sa masovnijom primenom Interneta stvari.

Adresa autora zaduženog za korespondenciju:

Zoran Čekerevac

[✉ zoran@cekerevac.eu](mailto:zoran@cekerevac.eu)

Ključne reči: forenzika, antiforenzika, IT alati, računari, Internet stvari, bezbednost, zaštita.



Abstract

Increased use of computers and devices and equipment based on them has made significant improvements in the functioning of companies and institutions, but also individual users. At the same time, risks have arisen due to their improper use or misuse. The loss or theft of data can occur in a variety of ways, from a user's error to an individual or mass attacks of malicious attackers. Some of the problems can be solved using the operating system's or application software's tools, but for specific situations, when the misdoing has already been done, it is necessary to use special, dedicated forensic tools. In case of need for judicial expertise, the task of forensic experts becomes even more complex, as with the detection of causes, the IT forensic expert must provide valid evidence that the act was done and (if possible) who made it, but also left the artifact in an unchanged state that other forensic research could be carried out either in connection with other reasons, or by another institution (or another forensic expert). Therefore, and for other reasons, it is necessary to use specialized forensic tools. In this paper, after the introductory part, which examines forensics and anti-forensics, short history and contemporary legislation, as well as the challenges associated with forensics and tools, the computer forensic tools are discussed in greater detail. The accent is placed on free forensic tools. The conclusions of the paper summarize views on forensics and forensic tools and point out the directions for future development, especially in connection with the massive use of the Internet of Things.

Keywords: Forensics, anti-forensics, IT tools, computers, IoT, security, protection.

1 UVOD

Neverovatno brz razvoj računara i softvera i masovnost njihove upotrebe poslednjih par decenija i perspektive daljeg ubrzanog razvoja, pre svega kroz „Internet stvari“ (IoT), donele su mnoge blagodeti čovečanstvu i otvorile nove mogućnosti daljeg napretka, ali su sa sobom donele i mnogobrojne izazove koji su nepovratno promenili svet i način rada i razmišljanja. Sa jedne strane, svaki pojedinac ima (praktično) neograničene mogućnosti za komunikaciju, za sticanje novih saznanja, prikupljanja podataka o svemu i svačemu, za daljinsko upravljanje ličnim uređajima, pa i velikim postrojenjima, zabavu i još mnogo šta. I dok mu to kao korisniku sasvim

odgovara, u jednom trenutku se i on može pojaviti kao objekat interesovanja, što mu u najmanju ruku može biti neprijatno. Tada poželi da sve ono što je ranije sa ponosom ili lakomisleno objavljivao, nekako obriše, skloni ili sakrije. Sa druge strane, sa povećanjem broja uređaja koje koristi, raste i mogućnost da se neki od njih ošteti ili da postane nefunkcionalan iz najrazličitijih razloga. Sa pristupom Internetu i korišćenjem Internet resursa raste i opasnost od zlonamernih napada na korisničke podatke, pa čak i napada na funkcionisanje celih, fizičkih, postrojenja. Kada se sve ovo ima u vidu, lako je zaključiti da su potrebe korisnika veoma raznovrsne i da ih je, najverovatnije, teško u potpunosti zadovoljiti.

Tabela 1. Neki od nedavnih slučajeva gubitka podataka

Datum	15.07.2017.	01.05.2017.	06.03.2017.	13.06.2017.
Žrtva	Equifax	Motor Vehicles Department in Kerala	River City Media	Deep Root Analytics
Broj zapisa	147.700.000	200.0000.000	1.340.000.000	198.000.000
Šta je ukradeno	Krađa identiteta	Krađa podataka o registraciji vozila	Krađa e-mail adresa	Krađa identiteta
Ko je izvršilac	Maliciozni spoljašnji napadač	Maliciozni spoljašnji napadač	Greška administratora	Greška administratora
Vrsta vlasnika podataka	Kreditni biro	Država	Marketing organizacija	Republikanski Nacionalni Komitet
Država	SAD	Indija	SAD	SAD
Ocena rizika	10	9,9	9,8	9,6

Izvor: (Breach Level Index, 2018)

Gubici podataka su svakodnevni, a Breach Level Index pokazuje više od 9.728.017.988 podataka koji su izgubljeni ili ukradeni od 2013. do 17.08.2018. To govori da se 55 zapisa gubi svake sekunde. Samo 4% izgubljenih zapisa su zapisi kod kojih je korišćena enkripcija. (Breach Level Index, 2018)

Neka od najvećih gubljenja podataka su slučajevi: JP Morgan Chase, Bank of America, HSBC, TD Bank, Target, Tumbler, Home Depot, MySpace, eBay, Adobe System Inc, iMesh, a neki od nedavnih slučajeva su prikazani u tabeli 1.

Juniper Research (Smith, 2015) sugerise da će do 2019. godine IT kriminal kompanije koštati preko 2 biliona dolara. Zbog toga će se povećati i zahtevi za računarskom forenzičkom ekspertizom.

Aktivnosti u oblasti zaštite podataka su obično podeljene u dve osnovne grupe, preventivne mere i forenzičke mere. Preventivnim merama se nastoji da se negativni uticaji preduprede. Za ove svrhe se koriste različite mere zaštite, od zaštitnog zida (fajervola) i antivirusnih programa, do redovnih bekapa. Kada je šteta već učinjena, na red dolazi forenzika, koja po definiciji predstavlja proces otkrivanja i tumačenja elektronskih podataka sa ciljem da "sačuva bilo koji dokaz u svom najoriginalnijem obliku dok vrši strukturiranu istragu sakupljanjem, identifikacijom i validacijom digitalnih informacija u svrhu rekonstrukcije prošlih događaja" (Techopedia, 2016). Forenzika i forenzički alati se mogu koristiti i preventivno, u cilju provere zaštite sistema, ali ta primena, kao ni preventivne mere u zaštiti računarskih sistema, ovde neće biti razmatrani.

1.1 Forenzika i antiforenzika

Donedavno se moglo govoriti sa velikom tačnošću da je forenzika nauka koja se bavi pronalaženjem razloga zašto nešto više nije kako treba. I ta bi se definicija tada mogla preneti i na računarsku forenziku. Danas to više tako verodostojna definicija, jer se pored računara u oblasti digitalne forenzike pojavljuju i mnogi drugi učesnici kao višestruki operativni sistemi, mreže, uređaji za umrežavanje, serveri za različite namene, baze podataka, softverske aplikacije... Naravno, ne treba gubiti iz vida nadirući IoT. Predmet ovog rada je računarska forenzika u užem smislu i prvenstveno će biti razmatrani računari i podaci koji se u njima nalaze.

U mnogim slučajevima korisnici računara imaju interes da unište sve ili neke zapise tako da se ne mogu oporaviti i pročitati. Mada je to najčešći slučaj kod nedozvoljenih aktivnosti, to može da bude i legalna i legitimna potreba korisnika u slučajevima kada otuđuje opremu koja još ima upotrebnu vrednost ili je menja novom. Zato se može reći da uz forenziku, vrlo često, paralelno ide i antiforenzika koja po definiciji ima suprotne ciljeve. Kada se govori o antiforenzici, obično se razmišlja o tome da ona služi da počisti tragove napada, zlonamerne upotrebe i tragove upada, da na neki način spreči rad forenzičkih alata ili da ga uspori do neisplativosti. Međutim, antiforenzika može i da posluži kao metod odbrane od krađe podataka. Posebna vrsta upotrebe antiforenzike je provera sposobnosti i pravilnosti rada računarskih forenzičkih alata i podsticanje njihovih kreatora na dalji rad i usavršavanje alata.

Ako se zanemare ekstremni slučajevi IT kriminala, koji uzgred i retko stižu u sudove, većina slučajeva iz sudske prakse se svodi na potvrđivanje ili pobijanje sumnje da je neki korisnik zloupotrebio pravo pristupa i preuzeo i/ili preneo podatke koje nije smeo, da je komunicirao sa nekim ili da je izvršio neku transakciju, napravio neku fotografiju ili dokument u određenom trenutku ili vremenu i slično. Vrlo često se u praksi IT veštaka javljaju slučajevi da su akteri samouki ili delimično obučeni, pa je rad veštaka time olakšan. Međutim, zbog raznovrsnosti korišćenih uređaja i po vrsti i po karakteristikama i po proizvođačima, rad IT veštaka postaje svakim danom sve kompleksniji. U slučajevima kada se radi o vrhunskim IT ekspertima, teško je naći odgovarajućeg IT veštaka, pa čak i veoma razvijeni timovi moraju tražiti pomoć specijalizovanih veštaka negde u svetu.

1.2 Kratka istorija i zakonska regulativa

IT forenzika je po svojoj suštini jedna od grana dobro poznate forenzičke nauke koja teži da prikupi sve moguće dokaze vezane za neki događaj, samo što se ovde radi o digitalnom svetu, o prikupljanju nula i jedinica, koje predstavljaju meta-podatke, datoteke dnevnika, IP adrese i slično. Računari i njihova intenzivna primena su novijeg datuma, pa je i IT forenzika mlada nauka. U početku, u prvoj polovini sedamdesetih godina

bilo je malo računara, pristup računarima je bio ograničen na vrlo mali broj ljudi, načini prenosa podataka su bili ekstremno neudobni i, objektivno, veća pažnja je bila posvećena njihovoj fizičkoj bezbednosti nego sadržajima koje su posedovali ili mogli da poseduju. Zbog toga se privatnošću i računarskom bezbednošću bavio samo mali broj ljudi. Šta više, ni zakon nije prepoznavao delo računarskog kriminala. Pojavom personalnih računara i razvojem računarskih mreža situacija se naglo menja, pa je moguće reći da je prekretnicu predstavljao Zakon o računarskom kriminalu Floride iz 1978. godine (Norman, 1978). Ovim zakonom su prepoznati prvi računarski zločini u SAD i uključeni su u zakonodavstvo protiv dela neovlašćenog brisanja ili modifikacije računarskih podataka. Uskoro su usledili drugi zakoni kao Američki Federalni zakon o računarskim prevarama i zlostavljanju (Cole, 2012) i britanski Zakon o računarskim zloupotrebama (Computer Misuse Act, 1990). Posle toga su usledile dugotrajne, deceniju duge, diskusije uglavnom oko prepoznavanja kompjuterskih zločina kao ozbiljnih pretnji ličnoj, organizacionoj i nacionalnoj bezbednosti. 2004. godine Naučna radna grupa za digitalne dokaze (SWGDE), objavila je "Najbolje prakse za računarsku forenziku" (SWGDE, 2004). Ovo izdanje je doživelo bitnu reviziju 2013. godine i minimalne korekcije 2014. godine.

2005. godine publikovan je standard ISO 17025 „Opšti zahtevi za kompetentnost laboratorija za ispitivanje i laboratorija za etaloniranje“ (ISO/IEC 17025, 2005) koji je kasnije revidiran 2017. godine. U Republici Srbiji su obe verzije standarda prevedene i objavljene kao SRPS ISO/IEC 17025:2006 i 2017, uz korekciju Ispr.1:2018. Ovi standardi i uputstva pomogli su publikovanje najboljih praksi računarskih forenzičara, specijalista, i pokrenuli mnoge forenzičke kompanije da kreiraju nova softverska rešenja koja su mogla da idu u korak sa novim zahtevima. U Republici Srbiji je IT kriminal dobio svoju zakonsku regulativu u obliku Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala (NSRS, 2005). Republika Srbija je potpisala i Konvenciju o sajber kriminalu i Dodatni protokol uz Konvenciju u Helsinkiju 2005. godine.

1.3 Izazovi za forenzičare i forenzičke alate

Tipični forenzički proces ima nekoliko različitih faza (n.d., 2018): zaplenu, forenzičku akviziciju, analizu i izradu izveštaja zasnovanog na prikupljenim podacima. U slučaju javnog sektora, rad IT forenzičara se najčešće svodi na podržavanje ili odbacivanje hipoteze pred krivičnim ili građanskim sudovima, ali mnogo raznovrsnije je angažovanje IT forenzičara u privatnom sektoru i u istraživanju upada u sisteme. Tu su zadaci toliko raznovrsni da se forenzičari vrlo često fokusiraju na samo jednu ili nekoliko podgrupa digitalne forenzike kako bi mogli da ostvare odgovarajući nivo znanja. Iako zadaci forenzičara mogu da budu vrlo slični, ili, čak, isti, forenzika se najčešće grubo deli prema vrsti posmatranih uređaja, pri čemu se izdvajaju računarska forenzika, forenzika mobilnih uređaja, forenzika u mreži, forenzička analiza podataka i forenzika baza podataka. Forenzika mobilnih uređaja doživljava najintenzivniji rast pre svega zbog enormnog rasta broja korišćenih mobilnih uređaja.

IT forenzičari se u praksi susreću sa različitim slučajevima. Jedan od slučajeva je slučaj skrivanja podataka. Napadači pokušavaju da naprave tajni ulaz (tzv. zadnja vrata, „back door“), ali da bi ostao tajni, potrebno je sakriti podatke o njegovom postojanju, bilo šifrovanjem, steganografijom ili kombinacijom više tehnika. Najbazičniji načini skrivanja podataka, koji ne zahtevaju posebne IT veštine, su premeštanje datoteka, korišćenje skrivenog medijuma, preimenovanje datoteka i ekstenzija, deljenje datoteka na manje segmente i njihovo smeštanje na različite lokacije. Nešto kompleksniji metod je šifrovanje datoteka, meta-podataka o datotekama, pa i čitavih diskova. Steganografija koristi princip da je najlakše sakriti papir među papirima. Naime, glavni uslov je da se zapis ne razlikuje po svom spoljašnjem izgledu od okruženja. Praktično, maskira se i postavlja među regularne, korisne, zapise. Jedan od načina je čista eliminacija izvora podataka o napadu. Na mesto napada se dovede zlonamerni kod, raspakuje se, iskoristi, a potom zapakuje i ukloni sa mesta napada. Na sličan način se mogu koristiti virtualne mašine, anonimni identiteti, preusmeravanje sistemskih poziva, itd.

Druga grupa slučajeva sa kojima se sreću IT forenzičari su slučajevi brisanja podataka. Kod

potpunih amatera vlada uverenje da je dovoljno samo obrisati određenu datoteku. Oni malo obučeniji znaju da im to ne daje nikakvu zaštitu, pa pribegavaju povratnom ili (za sada) nepovratnom brisanju svih podataka i/ili fizičkom uništavanju medijuma kako bi se obrisali svi tragovi. Najjednostavniji način brisanja podataka je ponovno pisanje drugih podataka preko postojećih podataka. Ovaj način ne garantuje da prethodni zapis neće biti u potpunosti ili delimično nečitljiv. Za sigurnije brisanja podataka postoje aplikacije koje ceo disk popunjavaju nulama ili jedinicama, ili, čak, omogućavaju višestruko pisanje i brisanje, tako je da praktično nemoguće povratiti početne podatke. Manje destruktivni programi ciljaju samo na sektore koje treba ukloniti. Tako se samo kod sektora na kojima postoje forenzički tragovi vrši ponovni upis podataka. Ovaj postupak je znatno kompleksniji, zahteva nadzor i ne briše sve meta-podatke. U slučaju magnetnih diskova, moguće je uraditi potpunu demagnetizaciju diska što omogućava potpuno brisanje diska, ali pri tome disk mora biti fizički dostupan, a može postati i potpuno neupotrebljiv. A, ako se želi potpuno uništavanje diska postoje mnoge druge, jeftinije, fizičke i hemijske metode.

Treću grupu slučajeva čini zametanje tragova, zamagljivanje situacije. Tu su na raspolaganju brojne mogućnosti, od brisanja tragova, do postavljanja raznih brojnih tragova koji ne vode nikuda, do postavljanja beznačajnih izmena na datotekama čije će uzaludno izučavanje oduzeti mnogo vremena. Promene zaglavlja datoteka, uz promenu vremenskog žiga i brisanje dnevnika zapisa, u suštini predstavlja vrlo efikasan metod koji pravi skoro nepremostive probleme IT veštaku pri izradi valjanog izveštaja o veštačenju. U tu svrhu mogu se koristiti i neki besplatni open-source programi.

Četvrta grupa slučajeva sa kojima se susreću IT forenzičari su slučajevi direktnih napada na alate i tehnike koje forenzičari koriste. Ovo su retki slučajevi i zahtevaju posebnu pripremu i posebna znanja napadača kako o računaru koji napada, tako i o onima koji ga štite, kao i alatima koje koriste. Svaki forenzičar ima svoj omiljeni alat, a svaki alat ima svoje slabosti. Ovo su ipak situacije sa kojima se sudski veštaci retko susreću i ovde neće biti detaljnije razmatrani.

2 RAČUNARSKI FORENZIČKI ALATI I OPREMA

Zadatak sudskog veštačenja je da sudu pruži relevantne informacije o učinjenom ili neučinjenom delu, a alati su najbolji prijatelji IT veštaka. Omogućavaju im da iz šume podataka izvuku ono što im je važno. Pored toga, da bi se dobili verodostojni podaci, veštak mora da ispoштуje određenu proceduru.

U slučaju veštačenja sadržaja hard diska (HD), prvo što IT veštak radi je uklanjanje hard diska iz računara i njegovo povezivanje na uređaj za onemogućavanje novih upisa na HD. Na taj način je sprečeno svako brisanje podataka ili naknadno upisivanje podataka na HD, a omogućeno čitanje i kopiranje zapisa sa HD. Za kopiranje sadržaja diska sa tačnošću do nivoa bita mogu se koristiti razni alati i platforme kao što su Digital Forensics Framework, Open Computer Forensics Architecture, CAINE (Computer Aided Investigative Environment), X-Ways Forensics, SANS Investigative Forensics Toolkit (SIFT), EnCase, itd., mada mnogo profesionalnih forenzičara više voli da umesto neke sveobuhvatne platforme koristi grupu forenzičkih alata po svom sopstvenom izboru. Na taj način iz bogate ponude softverskih rešenja biraju samo ono što im je potrebno za ekspertize za koje su se specijalizovali.

Karakteristike i mogućnosti profesionalnih forenzičkih alata se razlikuju prvenstveno zbog razlika u njihovim osnovnim namenama, ali se očekuje da veliki softverski paketi podržavaju heširanje svih datoteka i celog diska, vremenske i datumske žigove, akviziciju i filtriranje podataka, te učitavanje bekapa iOS-a i analizu njegovih podataka. Za razliku od državnih institucija, privredne organizacije obično nisu zainteresovane za iščitavanje RAM memorije, kao i za mogućnost prethodnog pregleda zapisa. Razlog je vrlo jednostavan, jer kompanije obično ne raspolažu ni odgovarajućim stručnim kadrom koji bi mogao da realizuje te aktivnosti.

Da bi se omogućila efikasnija i uspešnija ispitivanja i istrage, programeri su kreirali mnogo različitih računarskih forenzičkih alata, koji bi se u zavisnosti od toga čemu su namenjeni, mogli podeliti na (Shankdhar, 2018):

- alati za snimanje diska i podataka,
- alati za pregled i oporavak fajlova,
- alatke za analizu datoteka,

- alati za analizu registara,
- Internet analitički alati,
- alati za analizu e-pošte,
- alati za analizu mobilnih uređaja,
- OS analitički alati,
- mrežni forenzički alati i
- forenzički alati za baze podataka

U ovu podelu se svakako mogu dodati i:

- alati za ekstrakciju meta-podataka iz dokumenata,
- anti-forenzički alati i
- alati za sigurno brisanje podataka.

Podela alata bi se mogla izvršiti i sa drugih tački gledišta, u zavisnosti od toga da li su proaktivni ili namenjeni za upotrebu posle samog događaja, kojim su operativnim sistemima i uređajima namenjeni, kao i mnogo detaljnije, na osnovu delova uređaja za koje su specijalizovani, no to ovde neće biti učinjeno. Jedna od bitnih, nezaobilaznih, podela je podela na besplatne i na one koji se plaćaju. S obzirom na dostupnost forenzičkih alata ovde ćemo pažnju posvetiti besplatnim alatima.

Kvalitet forenzičkih alata je postao vrlo visok tako da se uz njihovu primenu do sticanja osrednjih forenzičkih veština može stići relativno brzo. Interesovanje za vrhunske eksperte u računarskoj forenzici postaje sve ređe kako zbog kvaliteta forenzičkih alata, tako i zbog boljeg obrazovanja bilo da je ono realizovano kroz specijalne treninge ili kroz univerzitetsko obrazovanje. Toliko je velika konkurencija za obuku i sertifikaciju u organizacijama za obuku na komercijalnom nivou da su neke neprofitne organizacije kao što je napustile tržište. Nedavno je Internet Systems

Consortium (ISC)² objavio da je napustio sertifikat CCFP (*Certified Cyber Forensics Professional*), jedini takav sertifikat u svetu koji je zahtevao ili značajno iskustvo (šest godina) ili univerzitetsku diplomu. (Stephenson, 2017)

Pre analize nekih od forenzičkih alata, neizostavno je konstatovati da je uvek dobro imati na raspolaganju više alata, pa makar oni radili skoro iste stvari. To je dobro i za forenzičare, ali i za proizvođače forenzičkih alata.

Prateći razvoj forenzičkih alata može se zapaziti da se od nekadašnjih pojedinačnih specijalizovanih alata došlo do sveobuhvatnih platformi koje obuhvataju mnoštvo različitih alata koji su međusobno povezani i koji omogućavaju glatko prelaženje sa jednog na drugi, iz jedne oblasti u drugu. Međutim, današnje takve platforme su ipak retke, a zbog mnoštva novih proizvoda i alata nije nemoguće da će u jednom trenutku postati same sebi prepreka daljem razvoju. Pored toga, može se zapaziti i da neki ne-forenzički alati kao npr. SIEM-i (*Security Information and Event Management*) počinju da dobijaju forenzičke zadatke. I to nam može pomoći da razumemo realnost digitalne forenzike.

U tabeli 2 je prikazano deset popularnih forenzičkih alata po slučajnom rasporedu. Treba imati u vidu da njihov položaj u tabeli ne odražava njihov značaj u forenzičkoj praksi. Pored toga, treba naglasiti i da ne postoje egzaktni kriterijumi kojima se može doći do „najboljeg forenzičkog alata“. U tabeli su pored kratkog opisa prikazane i osnovne karakteristike i URL adrese sa kojih je moguće preuzeti softver.

Tabela 2 Deset besplatnih forenzičkih alata

R.Br.	Naziv alata	Opis	Osnovne karakteristike	URL
1	SIFT - SANS Investigative Forensic Toolkit	SIFT ima mogućnost ispitivanja diskova, tj. podataka, na nivou bajtova direktno sa hard diska ili bilo kojeg drugog uređaja za skladištenje, više fajl sistema i formata dokaza. U osnovi je baziran na Ubuntuu i predstavlja Live CD uključujući i alate za koji su potrebni za detaljnu forenzičku istragu. Najbolja stvar oko SIFT alata je to što je slobodan i "Open Source".	- Ubuntu LTS 14.04 Base. - 64-bit base system. - Bolje korišćenje memorije. - Automatsko ažuriranje DFIR paketa i prilagođavanja. - Najnovije forenzičke alati i tehnike. - VMware Appliance spreman za forenziku. - Kompatibilnost između Linux-a i Windows-a. - Opcija za samostalno instaliranje putem (.iso) ili korišćenje preko VMware Player/Workstation. - Onlajn dokumentacija na ReadTheDocs - Podrška za Expanded Filesystem.	https://digital-forensics.sans.org/community/downloads

R.Br.	Naziv alata	Opis	Osnovne karakteristike	URL
2	Nmap	Nmap ("Network Mapper") je besplatan i open source (licencirani) alat za otkrivanje mreže i reviziju bezbednosti. Mnogi sistem i mrežni administratori takođe smatraju ga korisnim za inventarisanje mreže, upravljanje vremenskim planovima za nadogradnju usluge i nadzor nad vremenom rada hosta ili usluge. Nmap koristi sirove IP pakete kako bi utvrdio koji su hostovi dostupni na mreži, koje usluge (naziv aplikacije i verzija) hostovi nude, koje operativne sisteme (i verzije OS-a) pokreću, koje vrste paketnih filtera i zaštitnih zidova su u upotrebi i desetine drugih karakteristika. Dizajniran je za brzo skeniranje velikih mreža, ali radi dobro i sa pojedinačnim hostovima. Nmap radi na svim većim računarskim operativnim sistemima, a službeni binarni paketi su dostupni za Linux, Windows i Mac OS X. Pored klasične Nmap izvršne komandne linije, Nmap paket uključuje napredni pregledač GUI i pregled rezultata (Zenmap), fleksibilnu alatku za prenos, preusmeravanje i debugovanje podataka (Ncat), uslužni program za upoređivanje rezultata skeniranja (Ndiff) i alatku za generisanje paketa i analizu odgovora (Nping). Nmap je proglašen za "Sigurnosni proizvod godine" od strane Linux žurnala, Info World-a, LinuxQuestions.Org i Codetalker Digest.	- Fleksibilan: Podržava desetine naprednih tehnika za mapiranje mreža. - Moćan: Nmap se koristi za skeniranje ogromnih mreža sa bukvalno stotinama hiljada mašina. - Prenosiv: Podržani su većini operativnih sistema, uključujući Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UKS, NetBSD, Sun OS, Amiga itd. - Lak za upotrebu: Dostupne su i tradicionalne komandne linije i grafičke verzije (GUI). - Besplatan: Nmap je dostupan za besplatno preuzimanje, a dolazi i sa punim izvornim kodom koji možete modifikovati i distribuirati pod uslovima licence. - Dobro dokumentovan. - Podržan: Nmap nema garanciju, ali, dobro ga podržava zajednica programera i korisnika. - Nagrađivan: Nmap je osvojio brojne nagrade. - Popularan: Uključen je u mnoge operativne sisteme (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, itd.).	https://www.magnetforensics.com/free-tool-encrypted-disk-detector/
3	Volatility Framework	Volatility Framework je platforma objavljena od strane Black Hat-a. Neposredno se odnosi na Advance Memory Analysis & Forensics. Advance Memory Analysis & Forensics u osnovi analiziraju RAM memoriju žrtvinog računara. Ova memorija je nestabilna i njen se sadržaj može promeniti samim startovanjem računara. Analiza ovih podataka se može izvršiti upotrebom Volatility Framework-a. Ovaj okvir je omogućio praćenje procesa rada i stanja bilo kog sistema korišćenjem podataka pronađenih u RAM-u. On takođe omogućava jedinstvenu platformu za forenzička istraživanja u u cilju povećanja efikasnosti. Njega koriste policijski organi, odbrambene snage, ali i komercijalni istražitelji širom sveta	- Jedinstveni, kohezioni okvir - To je Open Source GPLv2 - Napisan je u Pitonu (Python) - Pokreće Windows, Linux ili Mac - Proširiv i podržava API skripte - Odlični kompleti funkcija zasnovani na reversnom inženjerstvu i specijalizovanim istraživanjima - Sveobuhvatna pokrivenost formata datoteka - Brzi i efikasni algoritmi - Ozbiljna i moćna zajednica - Forenzički/IR/malver fokusiran	https://www.darknet.org.uk/2016/09/volatility-framework-advanced-memory-forensics-forensics/
4	Sleuth Kit (+Autopsy)	The Sleuth Kit (+Autopsy) podržava interfejs baziran na komandnoj liniji. Korisnici/klijenti izdaju komande programskom programu uzastopnim redovima teksta, na isti način kao komande u programskom jeziku. Sleuth Kit omogućava korisnicima da ispituju imidže žrtvinih diskova i da oporavljaju oštećene datoteke. Obično se koristi u Autopsy zajedno sa mnogim drugim "Open Source" ili komercijalnim	- Multi-User rad: zajednički rad više forenzičara u složenijim slučajevima. - Analiza vremenske linije: Prikazuje sistemske događaje u grafičkom interfejsu kako bi se identifikovala aktivnost. - Pretraživanje ključnih reči: ekstrakcija teksta i indeksirani pretraživači omogućavaju pronalaženje datoteka u kojima se pominju specificirani izrazi.	https://www.sleuthkit.org/

R.Br.	Naziv alata	Opis	Osnovne karakteristike	URL
		alatima. Autopsy® zajedno sa Sleuthkit-om je program baziran na GUI-u. Omogućava korisniku da ispituje hard diskove i pametne telefone sa boljom efikasnošću od drugih alata.	- Veb artefakti: Ekstrakcija veb aktivnost iz uobičajenih pretraživača kako bi se identifikovala korisnikova aktivnost. - Analiza registra: koristi RegRipper za identifikaciju nedavno posećenih dokumenata i USB uređaja. - LNK fajl analiza: Identifikuje prečice i dokumenta kojima je pristupljeno. - Analiza elektronske pošte: analizira poruke MBOX formata, kao što je Thunderbird. - EXIF: Ekstrakcija geolokacija i informacije o kameri iz JPEG datoteka. - Sortiranje datoteka po tipovima: Grupisanje datoteka po tipovima za pronalaženje svih slika ili dokumenata. - Media plejbek: omogućava pregled video zapisa i slika u aplikaciji bez spoljnih pregledača. - Thumbnail pregledač: Prikazuje sličice slika za brzi pregled slika.	
5	Caine (Computer Aided Investigative Environment)	CAINE (Computer Aided INvestigative Environment Live USB/CD/DVD) je izgrađen na Linuks okruženju. To je u stvari Live CD sa nizom forenzičkih alata. S obzirom da je najnovija verzija CAINE izgrađena na Ubuntu Linux LTS, MATE i LightDM, svako ko je upoznat sa njima ne mora da ulaže dopunske napore da bi mogao da koristi CAINE.	- CAINE Interface – korisnički interfejs koji okuplja neke dobro poznate forenzičke alate, od kojih su mnogi otvorenog koda. - Ažurirano i optimizirano okruženje za vođenje forenzičke analize. - Poluautomatski generator izveštaja.	https://www.caine-live.net/
6	Xplico	Xplico je Open Source mrežni forenzički alat koji može rekonstruisati sadržaj bilo kojih akvizicija izvršenih od strane sniffera za pakete, kao što su Wireshark, ettercap itd. Ovaj alat može izvući i rekonstruisati sadržaj sa bilo kog mesta. Xplico je podrazumevano instaliran u nekim od digitalnih forenzika i testiranja penetracije operativnih sistema Kali Linux, BackTrack i drugim.	- Podržani protokoli: HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IPv4, IPv6. - Port Independent Protocol Identification (PIPI) za svaki protokol aplikacije. - Multithreading - tehnika pomoću kojeg jedan set koda može koristiti nekoliko procesora u različitim fazama izvršenja. - Izlazni podaci i informacije u SQLite bazi podataka ili MySQL bazi podataka i/ili datotekama. - Svakom podatku koji je Xplico ponovo sklopio asocirana je XML datoteka koja jednoznačno identifikuje tokove i pcap koji sadrži ponovno sastavljene podatke. - Nema ograničenja veličine podataka za unos ili broja ulaznih datoteka (jedina granica je veličina HD). - Modularnost. Svaka Xplico komponenta je modularna.	https://www.xplico.org/
7	X-Ways Forensics	X-Ways Forensics je napredno radno okruženje koje forenzičari masovno koriste. Jedan od problema sa kojim se suočava stručnjak pri korišćenju nekog forenzičkog alata jeste nedostatak resursa, spor rad, nemogućnost da se dođe do svih lokacija sa podacima. Toga kod X-Ways nema. Ovaj forenzički alat je jednostavan i potpuno prenosiv i može se	- Kloniranje diska i izrada imidž datoteka. - Mogućnost čitanja strukture particioniranja i strukture fajl sistema u sirovim (.dd) imidž datotekama, ISO, VHD i VMDK imidžima. - Potpuni pristup diskovima, RAID-u i imidžima veličine veće od 2TB.	http://www.x-ways.net/forensics/

R.Br.	Naziv alata	Opis	Osnovne karakteristike	URL
		nositi na USB memorijskom elementu. Ne zahteva nikakvu dodatnu instalaciju na Windows sistemima.	- Automatska identifikacija izgubljenih/izbrisanih particija. - Pregled i izmena binarnih struktura podataka pomoću šablona. - Rekurzivan pregled svih postojećih i izbrisanih datoteka u svim poddirektorijima.	
8	Bulk Extractor	Bulk_extractor skenira sliku diska, datoteku ili direktorijum datoteka i izvlači korisne informacije ne obračavajući pažnju na strukturu datotečnog sistema. Na taj način dobija u brzini rada i u mogućnosti da paralelno obrađuje različite delove diska. U praksi, program deli disk na stranice i obrađuje jednu stranicu na svakom dostupnom jezgri. To znači da mašine sa više jezgara obrađuju disk približno toliko puta brže koliko imaju jezgara u poređenju sa mašinama sa jednim jezgrom (Garfinkel, 2013). Bulk_extractor je takođe temeljan. Testiranje je pokazalo da postoji značajna količina komprimiranih podataka u nedodeljenim područjima datotečnog sistema koju propusti većina danas korišćenih forenzičkih alata, ali ne i bulk_extractor. Još jedna od prednosti je što se može koristiti za obradu praktično svakog digitalnog medijuma. Za pregled rezultata poseduje automatizovane alate.	Bulk_extractor - je alat za forenziku podataka na disku. Skenira medije i izdvaja prepoznatljive sadržaje. - deli disk na 16M "stranice" (blokove) i obrađuje svaku stranicu nezavisno. - ispituje svaki bajt da vidi da li je to početak "kodiranog" regiona. - ima tri faze rada: ekstrakcija; stvaranje histograma; naknadna obrada. - pokreće se iz komandne linije i kreira direktorijum "funkcionalnih datoteka" i rezultata. - GUI radi na Windows, Mac i Linux operativnim sistemima.	http://www.softpedia.com/get/Compression-tools/Bulk-Extractor.shtml
9	Mandiant Redline	RedLine je popularan alat za analizu memorije i datoteka, a prikuplja informacije o procesima koji se odvijaju na hostu i upravljačkim programima iz memorije, i druge podatke kao što su meta podaci, podaci iz registara, zadaci, usluge, informacije o mreži i Internet istorija kako bi se kreirali odgovarajući izveštaji. Redline®, FireEie-ova besplatna sigurnosna alatka, pomoću analize memorije i datoteka, pruža korisnicima istraživačke mogućnosti pri traženju znakova zlonamerne aktivnosti i izradi profila procene pretnji.	- Temeljno vrši reviziju i prikuplja sve programe i upravljačke programe iz memorije, meta podatke datotečnog sistema, podatke iz registra, evidencije događaja, informacije o mreži, usluge, zadatke i veb istoriju. Analizira i prikazuje uvezene podatke o reviziji, uključujući i mogućnost filtriranja rezultata oko datog vremenskog okvira. - Ubrzava analizu memorije dokaznim alatima za analizu malvera zasnovano na relativnom prioritetu. - Izvodi IOC (Indicators of Compromise) analize. - Snaždeven setom IOC-ova, Redline Portable Agent se automatski konfiguriše da prikupi podatke potrebne za izvođenje i prikaz rezultata IOC analize.	https://www.mandiant.com/resources/download/redline
10	Linux 'DD'	DD dolazi podrazumevano uz većinu danas dostupnih Linux distribucija (npr. Ubuntu, Fedora). Ovaj alat može se koristiti za različite forenzičke zadatke kao što su forenzičko brisanje diskova i stvaranje sirovog imidža diska. DD je veoma moćan alat koji može imati razorne efekte ako se ne koristi sa pažnjom. Modifikovana „dd“ verzija 'dc3dd' uključuje i funkcije koje su dodate posebno za zadatke digitalne forenzičke nabavke.	DC3DD predstavlja dodatak GNU dd programa. Ova verzija ima nekoliko funkcija namenjenih forenzičkoj akviziciji podataka. Najznačajniji dopunski sadržaji uključuju: Prikupljanje digitalnih dokaza "hashing on-the-fly", deljenje izlaznih datoteka, šablone za pisanje izveštaja, merač napredovanja i verifikaciju datoteka.	https://sourceforge.net/projects/dc3dd/

3 ZAKLJUČAK

Računarska ili digitalna forenzika, iako mlada grana, zahvaljujući ubrzanom razvoju informacionih tehnologija i softvera i hardvera poslednjih godina dobija veliki zamah u svom razvoju. Posebno veliki pomak se očekuje sa masovnom primenom Interneta stvari (IoT). Svaki korisnik računara se nebrojeno puta našao u situaciji da preuzima ulogu IT forenzičara, bilo da traži zagubljeni dokument ili fotografiju na hard disku ili u svoj arhivi, bilo da traži razlog neregularnog rada svog računara. Navedene situacije koje se mogu rešiti upotrebom alata korišćenog operativnog sistema, iako brojne, samo su mali deo ukupnih potreba. Na nivou sudskih IT veštaka zadaci su kompleksniji i odgovorniji. Sudski IT veštaci imaju zadatak da otkrivaju i opisuju informacije sadržane na digitalnom artefaktu ili njihovom stanju ili postojanju pri čemu digitalni artefakti uključuju mobilne telefone, računarske mreže, računarske sisteme, hard diskove, DVD- i CD-ove i druge uređaje za skladištenje podataka, kao i elektronska dokumenta i datoteke poput e-pošte, JPEG ili PNG slika, PDF dokumenata, itd. Za takve aktivnosti su neophodni i odgovarajuća stručnost i odgovarajući alati. Logično je očekivati da komercijalni programi pružaju veće forenzičke mogućnosti, da su pouzdaniji i da pružaju garanciju kvaliteta. S druge strane, takvi programi su relativno glomazni, skupi i neisplativi većini korisnika, razvija ih ograničen broj eksperata, a iako korisnik očekuje garanciju, dobija garanciju za kupljeni softver, ali ne i garanciju za rezultate rada kupljenog softvera. Za rešavanje većine forenzičkih zadataka vrlo uspešno se nametnula

mogućnost korišćenja besplatnih forenzičkih alata. Besplatni forenzički alati su svakim danom sve brojniji i bogatije opremljeni, sposobni da urade najširi spektar zadataka, čak se i ugrađuju kao podrazumevane komponente pojedinih operativnih sistema, a koristi ih i usavršava brojna korisnička zajednica. Za svaku od aktivnosti može se naći jedan ili više odgovarajućih alata čijom se upotrebom ili paralelnom upotrebom može uspešno doći do rezultata.

Iako su mu na raspolaganju brojni alati, IT veštak ima veoma težak zadatak u svom radu. Većina digitalnih dokaza se nalazi tamo gde im je teško prići. U prvom redu se tu misli na privremene datoteke i privremene memorije, kao i na obrisane datoteke bilo da su one poruke elektronske pošte, dokumenta u najrazličitijim formatima ili obrisane particije diska. Sami počinoci zlonamernih aktivnosti pokušavaju da zametnu tragove. Da zadatak forenzičara bude teži dopunski „se trude“ sam operativni sistem i njegovi alati. Da bi olakšao rad korisniku operativni sistem se širi po memoriji, masovno generiše nove i pamti stare podatke prepisujući nove preko starih zapisa uništavajući dokaze. Zato se sa dobrom dozom sigurnosti može reći da se najkvalitetniji dokazi nalaze u oblastima koje su nedostupne standardnim alatima operativnog sistema.

Na osnovu trendova u razvoju računara i opreme može se reći da će do rasta potrebe za forenzičarima i forenzičkim alatima doći rastom upotrebe Interneta stvari. Pored nesumnjivih blagodeti primene ove tehnologije, pojaviće se i niz novih slabih tačaka koje treba štititi od napada ili istraživati posledice napada i pronalaziti izvršioca.

CITIRANA DELA

Breach Level Index. (2018, avgust 17). *Data Breach Statistics*. Preuzeto sa Breach level index: <https://breachlevelindex.com/>

Cole, B. (2012, juni). *Computer Fraud and Abuse Act (CFAA)*. Preuzeto sa TechTarget: <https://searchcompliance.techtarget.com/definition/The-Computer-Fraud-and-Abuse-Act-CFAA>

Computer Misuse Act. (1990). Preuzeto sa [legislation.gov.uk: https://www.legislation.gov.uk/ukpga/1990/18/contents](https://www.legislation.gov.uk/ukpga/1990/18/contents)

Garfinkel, S. L. (2013). Digital media triage with bulk data analysis and bulk_extractor. *Computers & Security*(32), 56-72.

ISO/IEC 17025. (2005). *General requirements for the competence of testing and calibration laboratories*. ISO.

- n.d. (2018, mart). *Forensic Software: Everything You Need to Know About Computer Forensics*. Preuzeto sa Disk Drill: <https://www.cleverfiles.com/howto/computer-forensic.html>
- Norman, J. (1978, maj 30). *Probably the First U. S. Legislation against Computer Crimes (1978)*. Preuzeto sa HistoryofInformation: <http://www.historyofinformation.com/expanded.php?id=3888>
- NSRS. (2005). Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala. *Sl. glasnik RS*(61).
- Shankdhar, P. (2018, mart 26). *22 Popular Computer Forensics Tools [Updated For 2018]*. Preuzeto sa Infosec Institute: <https://resources.infosecinstitute.com/computer-forensics-tools/>
- Smith, S. (2015, maj 12). *Cybercrime will Cost Businesses Over \$2 Trillion by 2019*. Preuzeto sa Juniper research: <https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion>
- Stephenson, P. (2017, oktobar 02). *It's forensic tools time again*. Preuzeto sa SC Magazine: <https://www.scmagazine.com/its-forensic-tools-time-again/article/696487/>
- SWGDE. (2004). *SWGDE Best Practices for Computer Forensics*. Washington DC: SWGDE.
- Techopedia. (2016, Sep 14). *Digital Forensics*. Preuzeto sa techopedia: <https://www.techopedia.com/definition/27805/digital-forensics>

Datum prve prijave: 27.08.2018.
Datum prijema korigovanog članka: 20.11.2018.
Datum prihvatanja članka: 27.03.2019.

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

Style – **APA Sixth Edition**:

Čekerevac, Z., Dvorak, Z., & Prigoda, L. (2019, 04 15). Savremena računarska forenzika i forenzički alati. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 50-60. doi:10.12709/fbim.07.07.01.06

Style – **Chicago Sixteenth Edition**:

Čekerevac, Zoran, Zdenek Dvorak, i Lyudmila Prigoda. 2019. „Savremena računarska forenzika i forenzički alati.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 50-60. doi:10.12709/fbim.07.07.01.06.

Style – **GOST Name Sort**:

Čekerevac Zoran, Dvorak Zdenek i Prigoda Lyudmila Savremena računarska forenzika i forenzički alati [Časopis] // *FBIM Transactions* / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 50-60.

Style – **Harvard Anglia**:

Čekerevac, Z., Dvorak, Z. & Prigoda, L., 2019. Savremena računarska forenzika i forenzički alati. *FBIM Transactions*, 15 04, 7(1), pp. 50-60.

Style – **ISO 690 Numerical Reference**:

Savremena računarska forenzika i forenzički alati. **Čekerevac, Zoran, Dvorak, Zdenek i Prigoda, Lyudmila**. [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, *FBIM Transactions*, T. 7, str. 50-60.



TEHNIČKA SPECIJALIZACIJA LJUDSKIH RESURSA U SEKTORU MSPP U SRBIJI KAO USLOV RAZVOJA

TECHNICAL SPECIALISM OF HUMAN RESOURCES AS CONDITION FOR DEVELOPMENT OF SMES IN SERBIA

Aleksandar Gračanac

Privredna komora Srbije, Beograd, Srbija

Vladimir Stojanović

Poslovni i pravni fakultet, Univerzitet "Union – Nikola Tesla", Beograd, Srbija

Nada Živanović

Poslovni i Pravni Fakultet, Univerzitet "Union – Nikola Tesla", Beograd, Srbija

©MESTE

JEL kategorija: **O12, O15**

Apstrakt

Raspoloživi ljudski resursi su jedan od potencijalnih uslova za razvoj MSPP sektora i preduzetništva u Srbiji. Uprkos tome, prisutna je nepovoljna struktura ljudskih resursa, u kojoj tehničke specijalizacije za viši tehnološki nivo, ne dominiraju što uslovljava širenje tehnološkog jaza. Karakteristično je da poslednjih godina u Srbiji postoji i nesklad ponude i tražnje na tržištu menadžera, i to bez obzira kojoj kategoriji firme pripadaju i koje delatnosti obavljaju. Postoji nesklad ponude i tražnje za određenim profilima zanimanja u funkcionisanju neophodnom za MSPP sektor. Ipak, preimućstvo malih firmi je u njihovoj inovativnosti i fleksibilnosti a isto tako, ono što je prednost može postati i nedostatak. Njihova resursna snaga je mala, jer ne mogu pokriti sve funkcije sa dovoljno specijalizovanog tzv. „kadra“ i pribegavaju zapošljavanju trenutno ponuđenim ljudskim resursima sa opštim znanjima zbog racionalizacije. Usvajanjem Strategije za MSPP sektor i preduzetništvo 2015. godine, stvoreni su osnovni uslovi za razvoj preduzetništva i viši nivo ljudskih resursa. Sveobuhvatnim aktivnostima u realizaciji Strategije, prvenstveno u delu izvora finansiranja i alternativnih izvora finansiranja, inovacijama proizvodnji i tehnološkoj opremljenosti, inovativnijim zakonskim rešenjima u narednim godinama, tehnička specijalizacija ljudskih resursa će značajno doprineti rastu konkurentnosti i profitabilnosti. U radu se objašnjava značaj Menadžment ljudskih resursa koji zauzima jednu od najvažnijih tema i pozicija u kreiranju razvoja, funkcionisanja i uspešnosti MSPP sektora u Evropskoj Uniji i kod nas. Zato, Prvo i najznačajnije

Adresa autora zaduženog za korespondenciju:

Aleksandar Gračanac

 aleksandar.gracanac@pks.rs



pitanje različitosti u strukturi zaposlenih, kao i različitosti u menadžmentu, definiše u osnovi i posebno kategorizuje uspešnost mikro, malih srednjih firmi i preduzetnika. U takvom definisanom konceptu, koji implicira nivo konkurentnosti, u fokus angažovanja menadžmenta se postavlja strategija kontinuiranog kreiranja nivoa visoko stručnih menadžera i zaposlenih. Ovaj evropski trend je posledica, primene 10 principa Akta o malom biznisu iz juna 2008. godine, u cilju postizanja prestižne konkurentnosti. Strateški dokument koji je Evropska Unija usvojila i postavila u prioritete ekonomske politike, omogućio je stabilan rast preduzetništva i usavršavanje inovativnih rešenja, koja su proizvela i nova visoko tehnička zanimanja i novu generaciju menadžera.

Ključne reči: Tehnička specijalizacija ljudskih resursa, MSPP sektor, menadžer, strategija, menadžment, preduzetništvo.

Abstract

Technical progress and adequate staff profiling are two essential conditions for the development of forces of production, in one company and one country alike. The competitive advantage of SME-s grouped in to the sectors with Low-tech, Medium-low tech, Medium-high tech, High-tech on aspects. These aspects are two technical specialization and flexibility. Technical Specialism of companies is the most important condition to the development and success of SME-s, because in this fashion small companies focus their resources (which are usually extremely limited) to what they do best. Small and medium enterprises SME-s, usually have no problems with quality control, as they deal in only one business activity, but this activity they need to give their full contribution so as to meet the set standards. The key point, considered are: management of human resources and staff qualifications and training level of workforce, productivity and innovation, collaboration with universities and research institutions, use of consulting services and adopted standards of quality. By adopting the Strategy for the SME-s sector and entrepreneurship in 2015, basic conditions have been created, but not enough for the development of entrepreneurship and a higher level of human resources. Comprehensive activities in the realization of the Strategy, primarily in the part of the sources of financing and alternative sources of financing, more innovative legal solutions in the coming years, technical specialization of human resources will contribute to the growth of competitiveness and profitability. The paper explains the importance of Human Resource Management, which takes up one of the most important topics and positions in creating the development, functioning and success of the SME-s sector in the European Union and in our country. Therefore, the first and most important issue of diversity in the structure of employees, as well as differences in management, defines basically and specifically categorizes the success of micro, small medium-sized companies and entrepreneurs. In such a defined concept, which implies competitiveness levels, the focus of management engagement is the strategy of continuously creating the level of highly professional managers and employees. This European trend is due to the implementation of 10 principles of the Small Business Act of June 2008, with the aim of achieving prestigious competitiveness. The strategic document adopted by the European Union and set in the priorities of economic policy has enabled stable growth of entrepreneurship and the development of innovative solutions, which have produced new high technical professions and a new generation of managers.

Keywords: Technical Specialism Human Resources, Strategy of SME-s, management of human resources, managers, strategy, management, entrepreneurs.

1 UVOD

Menadžment ljudskih resursa u MSPP sektoru u Srbiji, se poslednjih godina suočavao sa atipičnim procesima u odnosu na predstavnike ovog sektora u EU, i pored korelacije u broju i zastupljenosti MSPP firmi u privredi, pa i prema zaposlenosti. Naime, zastupljenost MSPP sektora u Srbiji se izjednačila sa EU (99,9%), dok je prema broju zaposlenih nešto manja i iznosi 60%, a u EU 81%.

U nestandardne procese koji su prisutni, ubraja se nedostatak tehničkih, finansijskih, kvalifikovanih performansi koje bi nivo konkurentnosti dovele na nivoa EU, koji je sada ispod proseka. To ima za posledicu nedovoljno kvalitetnih ljudskih resursa prema potrebama globalne konkurencije i tržišta. (Burns, 2001, str. 48)

Uzroci su sadržani u sledećem:

- dugogodišnja neadekvatna ekonomska politika i aktivnostima na institucionalnom nivou za poboljšanje ambijenta poslovanja,
- u razvoju preduzetništva i pored usvajanja četiri značajne strategije za razvoj mikro, malih srednjih firmi i preduzetnika i preduzetništva od 2000 godine (Tabela 1).

Tabela 1. Učešće u privredi (u %)

	Preduzetnici	Mikro	Mala	Srednja	Preduzetnički sektor
Br. preduzeća	71,5	24,7	3	0,7	99,9
Br. zaposlenih	19,4	12,1	16	18,2	65,7
Promet	11,0	14,5	19,2	20,3	65,1
BDV	13,1	8,7	15,6	18,9	56,2
Izvoz	1,0	8,4	11,2	20,2	40,8
Uvoz	0,7	11,9	19,6	24,2	56,3

Izvor: Autor na osnovu podataka Ministarstvo privrede Republike Srbije

2 PREDUZETNIŠTVO I MIKRO, MALA I SREDNJA PREDUZEĆA

Preduzetnički potencijal mikro, malih srednjih firmi i preduzetništva u Srbiji postoji i razvija se u poslednje četiri godine, posebno usvojenom sveobuhvatnom Strategijom razvoja MSPP sektora i preduzetništva 2015.godine, za period (2015-2020).

Osnovni nedostaci za viši nivo internacionalne konkurentnosti, ogledaju se u:

1. nedovoljnoj tehničkoj specijalizaciji ljudskih resursa,
2. strukturi zaposlenih i među menadžerima u ovom sektoru, sa jedne strane i nedovoljno finansijske i institucionalne podrške za usavršavanje kadrova i ulaganja u ljudske resurse na nivou MSPP firmi u EU, sa druge strane (Farvaque, Voss, Lefebvre, & Schuetze, 2009).

Trendovi u strukturi MSPP sektora se uglavnom kreću u segmentu uslužno prerađivačkih kapaciteta, u svim granama industrijskih

delatnosti, i u korelaciji su sa stepenom tehnološke opremljenosti. Poslednjih godina se posebno izdvaja (IT) sektor sa povećanim stepenom konkurentnosti i izraženom potrebom za visoko tehnološki kvalifikovanim kadrovima. Preimućstvo malih kompanija je u njihovoj fleksibilnosti (Šević, Pendić, Ivanek, Marković, & Kovačević, 2002).

Istovremeno, u praksi, ono što je prednost može postati i nedostatak. Sposobnost brže adaptacije na tržište, podstaknute manjim brojem zaposlenih koji mogu imati bolju interakciju i neposredniji odnos sa vlasnikom i poslovnim partnerima, doprinosi lakšoj identifikaciji sa vizijom, ciljevima i misijom firme. U isto vreme, i hipersenzibilnost ih čini i ranjivim kada su u pitanju troškovi i racionalizacije poslovanja (EC, 2016).

3 ZAPOSLENOST U FIRMAMA U SRBIJI

Resursna snaga malih firmi je na nižem nivou, i to ih često dovodi u vazalni položaj u odnosu na velike kompanije (Tabela 2).

Tabela 2 – Tehnološki jaz sektora MSPP (u %)

	Preduzeća		Zaposlenost		BDV	
	MSPP	Velika	MSPP	Velika	MSPP	Velika
Low-tech	62,5	50,7	59,6	39,9	48,4	38,7
Medium – low tech	28,4	22,0	25,0	27,7	30,9	34,7
Medium – high tech	6,6	25,4	12,1	29,4	15,7	22,6
High tech	2,6	2,0	3,3	3,0	5,0	4,0

Izvor: Autor na osnovu podataka Ministarstvo privrede Republike Srbije

Istovremeno, karakteristično je da razvoj MSPP specijalizacije u ljudskim resursima i firmi u IT sektoru nije pratio i tehničke menadžmentu. Formirao se nesklad ponude i

tražnje na tržištu menadžera i izvršioca, kao posledica svih ne konkurentnih performansi u MSPP sektoru, što se reflektovalo u izraženom tehnološkom jazu prema tehnološkoj kategorizaciji firmi. Isto tako, i bez obzira kojoj kategorizaciji firme pripadaju i svejedno kojim delatnostima se bave, izražena je potreba za ljudskim resursima u različitim profilima zanimanja (Tabela 3), (Tabela 4).

Tabela 3 – Startapi u Srbiji (trendovi)

Ukupno (privredna društva + preduzetnici)			
Godina	Novo-osnovani	Ugašeni	Neto efekat
2010.	44.765	46.553	1,0
2011.	40.706	48.869	0,8
2012.	38.848	40.208	1,0
2013.	39.666	39.077	1,0
2014.	37.311	29.669	1,3
2015.	41.614	35.116	1,2
2016.	42.044	24.728	1,7
2017.	43.121	23.631	1,6

*Izvor: Autor na osnovu podataka Ministarstvo privrede
 Republike Srbije*

Tabela 4. Prikaz stanja stope osnivanja, gašenja i opstanka od 2010. do 2017.

Godina	Stopa osnivanja	Stopa gašenja	Stopa opstanka
2010.	13,5	14,0	61,8
2011.	12,5	15,0	63,8
2012.	12,0	12,4	59,1
2013.	12,3	12,1	64,0
2014.	11,3	9,0	67,5
2015.	12,6	10,6	69,3
2016.	12,5	7,3	70,9
2017.	12,0	7,8	71,0

*Izvor: Autor na osnovu podataka Ministarstvo privrede
 Republike Srbije*

Analiza trenutnog ambijenta ljudskih resursa, prema statističkim podacima Zavoda za statistiku pokazuje da je, obrazovna struktura ukupno zaposlenih u privredi Srbije, sledeća (Gračanac, 2012):

- srednja stručna sprema je zastupljena sa 43%,

- najviši nivo obrazovanja je prisutan kod 14,2% zaposlenih,
- procenat zaposlenih sa nižom stručnom spremom iznosi 15,6%.

U saradnji sa institucionalnim predstavnicima MSPP sektora u institucijama (PKS, APR, Ministarstvo privrede) u periodu od 1. januara 2018. do 1. marta 2018. godine, realizovana je jednostavna anketa, e-mail poštom, za 500 MSPP firmi iz svih delatnosti. Za potrebe ovog rada postavljeno je pitanje:

Kategorizujte obrazovnu strukturu zaposlenih u vašoj firmi

Od ukupno 500 anketiranih odgovorilo je 127 ispitanika.

Na osnovu primljenih odgovora i njihovom analizom došlo se do sledećih podataka:

- zastupljenost zaposlenih u MSPP sektoru sa nižom stručnom spremom iznosi 19,2%
- zastupljenost zaposlenih u MSPP sektoru sa srednjom stručnom spremom iznosi 59%
- zastupljenost zaposlenih u MSPP sektoru sa visokom stručnom spremom iznosi 8,2%
- stepen obrazovanja trenutnih menadžera u MSPP sektoru sa visokim obrazovanjem iznosi 33,7%.

4 ZAKLJUČAK

Prema podacima realnog stanja zaposlenosti u firmama tehnička specijalizacija ljudskih resursa u MSPP sektoru u Srbiji, neizostavno se mora kreirati na nivou strateških ciljeva i odluka u mikro, malim srednjim firmama i među preduzetnicima u narednom periodu.

Evropska iskustva u MSPP sektoru, u podizanju nivoa konkurentnosti su za uslov imala razvoj visokog tehnološkog nivoa ljudskih resursa, i to; inovacijama u tehnološkim rešenjima opreme, primenom najnovijih tehnologija, sa pratećim visoko sofisticirano kvalifikovanim ljudskim resursima, da bi se dostigao nivo konkurentnosti koje diktira globalizovana konkurencija i tržište.

U tom smislu, uslov za razvoj preduzetništva i MSPP sektora u Srbiji, se može jedino pratiti u odnosu na stepen napredovanja zaposlenih i menadžera, kao efikasno rešenje dugoročnog privrednog rasta, a ne kao deo problema.

Istovremeno i menadžment struktura u MSPP firmama moraće da se usavršava novim menadžment veštinama, na bazi novih tehnologija, što će dodatno povećati efektivnost i operativne kapacitete.

Na taj način može se očekivati smanjivanje tehnološkog jaza između kompanija u nekom srednjoročnom vremenskom periodu.

Smanjivanjem tehnološkog jaza u preduzetništvu, značilo bi postepeno povećavanje konkurentnosti, profitabilnosti, obima investicija i povećanje broja zaposlenih.

Prema rezultatima istraživanja prikazanih u sprovedenoj anketi to jasno potvrđuju dobijeni rezultati gde je

neminovno, da se poveća procenat srednje stručne sprema i njihova zastupljenost u firmama, kao i da se poveća najviši nivo obrazovanja zaposlenih.

Ono što čini osnovnu kariku uspešnog poslovanja mikro, malih i srednjih preduzeća u zemlji je, povećanje zastupljenosti kvalifikovanih i kvalitetnih menadžera u svim oblastima privrednog razvoja u svetu i kod nas.

CITIRANA DELA

Burns, P. (2001). *Entrepreneurship and Small Business*. New York: Palgrave.

EC. (2016, april 01). *Enterprise and Industry - SBA Fact sheet Serbia (2013)*. Preuzeto sa European Commission:

<http://ec.europa.eu/DocsRoom/documents/16149/attachments/37/translations/en/renditions/pdf>

Farvaque, N., Voss, E., Lefebvre, M., & Schuetze, K. (2009). *Guide for Training in SMEs*. Lile/Hamburg: ORSEU.

Gračanac, A. (2012). Akt o malom biznisu (Small Business Act) EU Faktor uspešnog menadžmenta malih i srednjih preduzeća u Srbiji. *International scientific conference Management 2012* (str. 219-223). Belgrade. Serbia: ICIM+. Preuzeto sa http://www.meste.org/konf/Arhiva/Man_2012/pdf/RADOVI/Gracanac.pdf

Šević, L., Pendić, Z., Ivanek, R., Marković, Z., & Kovačević, L. (2002). Market requires human resources management. *Kvalitet*, 12(1-2), 26-28.

Datum prve prijave: 16.03.2018.

Datum prijema korigovanog članka: 03.08.2018.

Datum prihvatanja članka: 27.03.2019.

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

Style – **APA Sixth Edition:**

Gračanac, A., Stojanović, V., & Živanović, N. (2019, 04 15). Tehnička specijalizacija ljudskih resursa u sektoru MSPP u Srbiji kao uslov razvoja. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 61-66. doi:10.12709/fbim.07.07.01.07

Style – **Chicago Sixteenth Edition:**

Gračanac, Aleksandar, Vladimir Stojanović, i Nada Živanović. 2019. „Tehnička specijalizacija ljudskih resursa u sektoru MSPP u Srbiji kao uslov razvoja.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 61-66. doi:10.12709/fbim.07.07.01.07.

Style – **GOST** Name Sort:

Gračanac Aleksandar, Stojanović Vladimir i Živanović Nada Tehnička specijalizacija ljudskih resursa u sektoru MSPP u Srbiji kao uslov razvoja [Časopis] // *FBIM Transactions* / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 61-66.

Style – **Harvard** Anglia:

Gračanac, A., Stojanović, V. & Živanović, N., 2019. Tehnička specijalizacija ljudskih resursa u sektoru MSPP u Srbiji kao uslov razvoja. *FBIM Transactions*, 15 04, 7(1), pp. 61-66.

Style – **ISO 690** Numerical Reference:

Tehnička specijalizacija ljudskih resursa u sektoru MSPP u Srbiji kao uslov razvoja. **Gračanac, Aleksandar, Stojanović, Vladimir i Živanović, Nada.** [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, *FBIM Transactions*, T. 7, str. 61-66



OBAVEZA PODUZIMANJA TEHNIČKIH MJERA ZAŠTITE PODATAKA TEMELJEM EU UREDBE O ZAŠTITI PODATAKA

OBLIGATION TO IMPLEMENT TECHNICAL MEASURES FOR DATA PROTECTION BASED ON EU GDPR

Haris Hamidović

MKF/MKD EKI Sarajevo, Sarajevo, Bosna i Hercegovina

©MESTE

JEL kategorija rada: **K22, M15**

Apstrakt

25. maja 2018. godine u svim zemljama Evropske unije stupila je na snagu Uredba o zaštiti pojedinaca u vezi s obradom ličnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opšta uredba o zaštiti podataka - Uredba). Zaštita prava i sloboda pojedinaca s obzirom na obradu ličnih podataka zahtijeva da se poduzmu odgovarajuće tehničke i organizacijske mjere radi osiguravanja poštovanja uslova ove Uredbe. Za kršenje odredbi koje se odnose na sigurnost obrade predviđene su upravne novčane kazne u iznosu do 10 000 000 EUR, ili u slučaju poduzetnika do 2 % ukupnog godišnjeg prometa na svjetskom nivou za prethodnu finansijsku godinu. U ovom radu predstavljamo obaveze provođenja odgovarajućih tehničkih i organizacijskih mjera zaštite ličnih podataka i mogućnost korištenja međunarodnih standarda za dokazivanje sukladnosti.

Ključne reči: informacijska sigurnost, privatnost, GDPR, ISMS, PIMS, ISO/IEC 27001, ISO/IEC CD 27552

Abstract

On 25 May 2018 in all countries of the European Union came into force The General Data Protection Regulation – GDPR. The protection of the rights and freedoms of individuals with regard to the processing of personal data requires that appropriate technical and organizational measures be taken to ensure compliance with the requirements of this Regulation. For breaches of the provisions relating to the security of processing, administrative fines of up to EUR 10 000 000 are envisaged, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. In this paper, we present the obligations of carrying out the appropriate technical and organizational measures for the protection of personal data and the demonstration of conformity with the use of international standards.

Keywords: information security, privacy, GDPR, ISMS, PIMS, ISO/IEC 27001, ISO/IEC CD 27552

Adresa autora:

Haris Hamidović

haris.hamidovic@eki.ba



1. UVOD

Sukladno tekstu preambule Opšte uredbe o zaštiti podataka svaka obrada ličnih podataka trebala bi biti zakonita i poštena. Za pojedince bi trebalo biti transparentno kako se lični podaci koji se odnose na njih prikupljaju, upotrebljavaju, daju na uvid ili na drugi način obrađuju, kao i do koje se mjere ti lični podaci obrađuju ili će se obrađivati. Načelom transparentnosti traži se da svaka informacija i komunikacija u vezi s obradom tih ličnih podataka bude lahko dostupna i razumljiva te da se upotrebljava jasan i jednostavan jezik. To se načelo posebno odnosi na informacije ispitaniku o identitetu voditelja obrade i svrhama obrade te daljnje informacije radi osiguravanja poštenosti i transparentnosti obrade s obzirom na pojedince o kojima je riječ i njihovo pravo da dobiju potvrdu i na obavještenje o ličnim podacima koji se obrađuju, a koji se odnose na njih. Pojedinci bi trebali biti upoznati s rizicima, pravilima, zaštitnim mjerama i pravima u vezi s obradom ličnih podataka i načinom ostvarenja svojih prava u vezi s obradom. Posebno, određena svrha u koju se lični podaci obrađuju trebala bi biti izrijeком navedena i opravdana te određena u vrijeme prikupljanja ličnih podataka. Lični podaci trebali bi biti primjereni, bitni i ograničeni na ono što je nužno za svrhe u koje se podaci obrađuju. Zbog toga je posebno potrebno osigurati da je razdoblje u kojem se lični podaci pohranjuju ograničeno na strogi minimum. Lični podaci trebali bi se obrađivati samo ako se svrha obrade opravdano ne bi mogla postići drugim sredstvima. Radi osiguravanja da se lični podaci ne drže duže nego što je nužno, voditelj obrade trebao bi odrediti rok za brisanje ili periodično preispitivanje. Trebalo bi poduzeti svaki razumno opravdani korak radi osiguravanja da se netačni lični podaci isprave ili izbrišu. I na kraju, a što je i tema ovog rada, lične podatke bi trebalo obrađivati uz odgovarajuće poštovanje sigurnosti i povjerljivosti ličnih podataka, što obuhvaća i sprečavanje neovlaštenog pristupa ličnim podacima i opremi kojom se koristi pri obradi podataka ili njihove neovlaštene upotrebe. (Uredba, 2016)

2. TEHNOLOŠKI RAZVOJ I IZAZOVI U ZAŠTITI LIČNIH PODATAKA

Zbog brzog tehnološkog razvoja i globalizacije pojavili su se novi izazovi u zaštiti ličnih podataka, navodi se u preambuli Opšte uredbe o zaštiti podataka. Opseg prikupljanja i razmjene ličnih podataka značajno se povećava. Tehnologijom se privatnim društvima i tijelima javne vlasti omogućuje upotreba ličnih podataka u dosada nedosegnutom opsegu radi ostvarenja njihovih djelatnosti. Pojedinci svoje lične informacije sve više čine dostupnima javno i globalno. Tehnologija je preobrazila i privredu i društveni život te bi trebala dalje olakšavati slobodan protok ličnih podataka u Evropskoj uniji i prijenos trećim zemljama i međunarodnim organizacijama, osiguravajući pri tome visok nivo zaštite ličnih podataka. (Uredba, 2016)

Pojedinci mogu biti pridruženi mrežnim identifikatorima koje pružaju njihovi uređaji, aplikacije, alati i protokoli, kao što su adrese internetskog protokola, identifikatori kolačića ili drugim identifikatorima poput oznaka za radiofrekvencijsku identifikaciju. Tako mogu ostati tragovi koji se, posebno u kombinaciji s jedinstvenim identifikatorima i drugim informacijama koje primaju poslužitelji, mogu upotrijebiti za izradu profila pojedinaca i njihovu identifikaciju, a što je i prepoznato odredbom člana 4. Opšte uredbe o zaštiti podataka koja proširuje definiciju „ličnih podataka” na sve podatke koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi - izravno ili neizravno, posebno uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više elemenata svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca. (Uredba, 2016)

Temeljem člana 6. Opšte uredbe o zaštiti podataka obrada ličnih podataka je zakonita i ukoliko je ispitanik dao privolu za obradu svojih ličnih podataka u jednu ili više posebnih svrha. Privola bi se trebala davati jasnom potvrdnom radnjom kojom se izražava dobrovoljan, poseban, informiran i nedvosmislen pristanak ispitanika na obradu ličnih podataka koji se odnose na njega, poput pisane izjave, uključujući elektroničku, ili usmene izjave, navodi se u preambuli Opšte uredbe o zaštiti podataka To bi moglo obuhvaćati

označivanje polja kvačicom pri posjetu internetskim stranicama, biranje tehničkih postavki usluga informacijskog društva ili drugu izjavu ili ponašanje koje jasno pokazuje u tom kontekstu da ispitanik prihvata predloženu obradu svojih ličnih podataka. Šutnja, unaprijed kvačicom označeno polje ili manjak aktivnosti stoga se ne bi smjeli smatrati privolom. Bitno je napomenuti da ukoliko se obrada temelji na privoli ispitanika, voditelj obrade trebao bi moći dokazati da je ispitanik dao privolu za postupak obrade. (Uredba, 2016)

Obrada ličnih podataka je zakonita i ukoliko je nužna i proporcionalna za potrebe osiguravanja sigurnosti mreže i informacija, odnosno sposobnosti mreže ili informacijskog sistema da se odupre, na danom stepenu povjerljivosti, slučajnim događajima ili nezakonitim ili zlonamjernim radnjama koje ugrožavaju dostupnost, autentičnost, integritet i povjerljivost pohranjenih ili prenesenih ličnih podataka te sigurnost povezanih usluga koje nude ili koje su dostupne putem tih mreža i sistema, koju provode tijela javne vlasti, jedinice za hitne računarske intervencije (CERT-ovi), jedinice za računarske sigurnosne incidente (CSIRT-ovi), pružatelji elektroničkih komunikacijskih mreža i usluga te davatelji sigurnosnih tehnologija i usluga. To bi, na primjer, moglo uključivati sprečavanje neovlaštenog pristupa elektroničkim komunikacijskim mrežama i širenja zlonamjernih kodova te zaustavljanje napada „uskraćivanjem usluge” te sprečavanje štete na računarskim i elektroničkim komunikacijskim sustavima, navodi se u preambuli Opšte uredbe o zaštiti podataka. (Uredba, 2016)

Nadalje, kako bi se osiguralo da pojedincima nije uskraćena zaštita na koju imaju pravo temeljem Opšte uredbe o zaštiti podataka, na obradu ličnih podataka ispitanika koji se nalaze u Evropskoj uniji, a koju obavlja voditelj obrade ili izvršitelj obrade bez poslovnog nastana u Evropskoj uniji, trebala bi se primjenjivati ova Uredba i ako su aktivnosti obrade povezane s ponudom robe ili usluga takvim ispitanicima, bez obzira na to ima li ta ponuda veze s plaćanjem. Kako bi se utvrdilo nudi li takav voditelj obrade ili izvršitelj obrade robu ili usluge ispitanicima koji se nalaze u Evropskoj uniji, trebalo bi utvrditi je li očito da voditelj obrade ili izvršitelj obrade namjerava ponuditi usluge ispitanicima koji se nalaze u

jednoj ili više država članica Evropske unije. Iako su sama dostupnost internetskih stranica voditelja obrade, izvršitelja obrade ili posrednika u Evropskoj uniji ili adrese elektroničke pošte i drugih kontaktnih podataka ili korištenje jezikom koji je općenito u upotrebi u trećoj zemlji u kojoj voditelj obrade ima poslovni nastan nedovoljni za utvrđivanje takve namjere, elementi kao što je korištenje jezikom ili valutom koji su općenito u upotrebi u jednoj ili više država članica s mogućnošću naručivanja robe i usluga na tom drugom jeziku, ili spominjanje kupaca ili korisnika koji se nalaze u Evropskoj uniji, mogu jasno pokazati da voditelj obrade namjerava nuditi robu ili usluge ispitanicima u Evropskoj uniji. (Uredba, 2016)

Temeljem člana 35. Opšte uredbe o zaštiti podataka 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. U slučajevima gdje nije jasno da li je procjena učinka na zaštitu podataka potrebna, EU WP29 radna grupa preporučuje da se ipak provede, zato što je ona koristan alat koji pomaže voditeljima obrade da budu u skladu sa zahtjevima Opšte uredbe o zaštiti podataka. Zahtjevi Opšte uredbe o zaštiti podataka ne diktiraju neki određeni metodološki ili standardni pristup kako bi se izvodila procjena učinka na zaštitu podataka, no koriste smjernice se mogu naći u međunarodnim standardima kao što je ISO/IEC 29134 ili ISO 22307. (Hamidović, 2010) (Babić, 2018)

3. TEHNIČKE I ORGANIZACIJSKE MJERE ZAŠTITE

Zaštita prava i sloboda pojedinaca s obzirom na obradu ličnih podataka zahtijeva da se poduzmu odgovarajuće tehničke i organizacijske mjere radi osiguravanja poštovanja uslova Opšte uredbe o zaštiti podataka. Radi dokazivanja sukladnosti sa Uredbom voditelj obrade trebao bi uvesti interne politike i provesti mjere koje osobito ispunjavaju načela tehničke zaštite podataka i integrirane zaštite podataka. (Hamidović, 2013) (Uredba, 2016) Takve mjere mogle bi se, među ostalim, sastojati od smanjenja količine obrade ličnih podataka, pseudonimizacije ličnih podataka što je

prije moguće, transparentnosti u vezi s funkcijama i obradom ličnih podataka, omogućavanja ispitaniku da prati obradu podataka, omogućavanja voditelju obrade da stvara i poboljšava sigurnosne značajke. Prilikom razvijanja, osmišljavanja, odabira i upotrebe aplikacija, usluga i proizvoda koji se temelje na obradi ličnih podataka ili obrađuju lične podatke kako bi ispunili svoju zadaću, proizvođače proizvoda, usluga i aplikacija trebalo bi poticati da uzmu u obzir pravo na zaštitu podataka prilikom razvijanja i osmišljavanja takvih proizvoda, usluga i aplikacija i da uzimajući u obzir najnovija dostignuća osiguraju da voditelji obrade i izvršitelji obrade mogu ispuniti svoje obveze u pogledu zaštite podataka. Načela tehničke i integrirane zaštite podataka trebalo bi također uzeti u obzir u kontekstu javnih natječajja. (Uredba, 2016)

Temeljem člana 83. Opšte uredbe o zaštiti podataka za kršenja odredaba u vezi zaštite ličnih podataka mogu se izreći upravne novčane kazne u iznosu do 10 000 000 EUR, ili u slučaju poduzetnika do 2 % ukupnog godišnjeg prometa na svjetskom nivou za prethodnu finansijsku godinu, ovisno o tome što je veće. Pri odlučivanju o izricanju upravne novčane kazne i odlučivanju o iznosu te upravne novčane kazne u svakom pojedinom slučaju dužna pozornost, između ostalog, posvećuje se (Uredba, 2016):

(d) stupnju odgovornosti voditelja obrade ili izvršitelja obrade uzimajući u obzir tehničke i organizacijske mjere koje su primijenili u skladu s članovima 25. i 32.

Predmetni članovi Opšte uredbe o zaštiti podataka glase:

Član 25. Tehnička i integrirana zaštita podataka

1. Uzimajući u obzir najnovija dostignuća, trošak provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih nivoa 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, poput pseudonimizacije, za omogućavanje učinkovite primjene načela zaštite podataka, kao što je smanjenje količine podataka, te uključivanje zaštitnih mjera u obradu kako bi se ispunili zahtjevi iz ove Uredbe i zaštitila prava ispitanika.

2. Voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kojima se osigurava da integriranim načinom budu obrađeni samo lični podaci koji su nužni za svaku posebnu svrhu obrade. Ta se obveza primjenjuje na količinu prikupljenih ličnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost. Tačnije, takvim se mjerama osigurava da lični podaci nisu automatski, bez intervencije pojedinca, dostupni neograničenom broju pojedinca.

3. Odobren mehanizam certificiranja sukladno članu 42. može se iskoristiti kao element za dokazivanje sukladnosti sa zahtjevima iz stavaka 1. i 2. ovog člana.

Član 32. Sigurnost obrade

1. Uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih nivoa vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajući nivo sigurnosti s obzirom na rizik, uključujući prema potrebi:

- (a) pseudonimizaciju i enkripciju ličnih podataka;
- (b) sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sistema usluga obrade;
- (c) sposobnost pravodobne ponovne uspostave dostupnosti ličnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta;
- (d) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

2. Prilikom procjene odgovarajućeg nivoa sigurnosti u obzir se posebno uzimaju rizici koje predstavlja obrada, posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ličnih podataka ili neovlaštenog pristupa ličnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.

3. Poštovanje odobrenog kodeksa ponašanja iz člana 40. ili odobrenog mehanizma certificiranja iz člana 42. može se iskoristiti kao element za

dokazivanje sukladnosti sa zahtjevima iz stavka 1. ovog člana.

4. Voditelj obrade i izvršitelj obrade poduzimaju mjere kako bi osigurali da svaki pojedinac koji djeluje pod odgovornošću voditelja obrade ili izvršitelja obrade, a koji ima pristup ličnim podacima, ne obrađuje te podatke ako to nije prema uputama voditelja obrade, osim ako je to obavezan učiniti prema pravu Unije ili pravu države članice.

Osim toga, kako bi se osiguralo poštovanje zahtjeva iz Opšte uredbe o zaštiti podataka u vezi s obradom koju provodi izvršitelj obrade u ime voditelja obrade, pri povjeravanju aktivnosti obrade izvršitelju obrade, voditelj obrade trebao bi angažirati samo izvršitelje obrade koji u zadovoljavajućoj mjeri jamče, osobito u pogledu stručnog znanja, pouzdanosti i resursa, provedbu tehničkih i organizacijskih mjera koje udovoljavaju zahtjevima iz Uredbe, među ostalim u pogledu sigurnosti obrade. (Uredba, 2016)

4. DOKAZIVOST USKLAĐENOSTI SA ZAHTJEVIMA UREDBE

Opštom uredbom o zaštiti podataka države članice, nadzorna tijela, Odbor i Komisija se potiču na uspostavu mehanizama certificiranja zaštite podataka te pečata i oznaka za zaštitu podataka u svrhu dokazivanja da su postupci obrade koje provode voditelj obrade i izvršitelj obrade u skladu s ovom Uredbom.

Određeni mehanizmi certificiranja postoje već izvjesno vrijeme na EU tržištu. Jedan od njih je i EuroPriSe certifikat namijenjen proizvođačima i prodavačima IT proizvoda i IT servisa. Proizvodi koji se mogu certifikovati su hardverski (kao npr. firewall) i softverski (kao npr. baza podataka). IT servisi su servisi kao naprimjer online bankarstvo, email servisi i slično. Predmet certifikovanja može biti proizvod u cjelini, dio proizvoda te više proizvoda zajedno, a isto se odnosi i na IT servise. EuroPriSe je certifikat koji izdaje nezavisna treća strana i koji potvrđuje da su IT proizvodi i IT bazirani servisi u skladu sa evropskim regulativama o privatnosti i sigurnosti podataka. Projekat je pokrenut u junu 2007. godine sa fondom od 1,3 miliona eura, a finansiran je od strane Evropske komisije. U martu 2009. EuroPriSe je preuzet od strane ULD (Unabhängiges Landeszentrum für Datenschutz -

Nezavisni Centar za zaštitu podataka), Ured povjerenika za zaštitu podataka i slobodu informacija Schleswig-Holstein, Njemačka.

U EuroPriSe navode da se prilikom procesa tehničke evaluacije potrebna dubina tehničke kontrole može znatno smanjiti ukoliko podnositelj zahtjeva za EuroPriSe certifikat posjeduje široko priznat certifikat kao što je ISO / IEC 27001, koji je aktuelan i relevantan za predmetni cilj procjene. Osim toga, navodi se da će budući međunarodni standard ISO / IEC 27552 ("PIMS standard") bit će još korisniji u ovom pogledu nego što je ISO / IEC 27001 danas. (Meissner, 2017) Korisne smjenice u vezi kontrola sigurnosti takođe se mogu naći i u ISO/IEC 27018 i ISO/IEC 29151.

Korištenje međunarodnih standarda kao okvira za implementaciju i procjenu zahtjeva informacijske sigurnosti već je korištena praksa od strane EU regulatora u sektoru telekomunikacija. (Hamidović, 2012) Dokument „Tehničke smjernice za minimalne sigurnosne mjere“ predstavlja smjernice za nacionalna regulatorna tijela u vezi provedbe članka 13a EU Direktive 2009/140/EC, a posebno u vezi sigurnosnih mjera koje pružatelji javnih komunikacijskih usluga moraju poduzeti kako bi se osigurala sigurnost i integritet njihovih mreža. Ovaj dokument navodi minimalne sigurnosne mjere koje nacionalna regulatorna tijela trebaju uzeti u obzir prilikom ocjenjivanja usklađenosti pružatelja javnih komunikacijskih usluga sa stavkama 1. i 2. članka 13a EU Direktive 2009/140/EC. Minimalne sigurnosne mjere izvedene su iz skupa međunarodnih i nacionalnih standarda koji se obično koriste u telekomunikacijskim organizacijama, kao što su:

- ISO/IEC 27001 i ISO/IEC 27002 za sistem upravljanja informacijskom sigurnošću,
- ISO/IEC 27005 za upravljanje rizikom informacijske sigurnosti,

BS 25999-1 i BS 25999-2 za upravljanje kontinuitetom poslovanja i dr

Sukladno tekstu preambule Opšte uredbe o zaštiti podataka osoba sa stručnim znanjem prakse zaštite podataka trebala bi pomagati voditelju obrade ili izvršitelju obrade pri praćenju unutarnje usklađenosti s ovom Uredbom. (Uredba, 2016) Osim korištenja međunarodnih standarda kao okvira za implementaciju sistema

informacijske sigurnosti u vezi zaštite ličnih podataka, francuska nacionalna Agencija za zaštitu privatnosti i podataka korisnika – CNIL preporučuje da se i prilikom procjene stručnosti pojedinaca koji se bave pitanjima tehničke zaštite ličnih podataka koriste poznate i priznate certifikacijske sheme kao što su CISSP - Certified Information Systems Security Professional, CISM - Certified Information Security Manager, ISO 27001 Auditor i dr. (CNIL, 2018)

5. ZAKLJUČCI

Rizik za prava i obaveze pojedinaca, različitih vjerojatnosti i ozbiljnosti, može proizaći iz obrade ličnih podataka koja bi mogla prouzročiti fizičku, materijalnu ili nematerijalnu štetu, posebno ako ta obrada može dovesti do diskriminacije, krađe identiteta ili prijevare, finansijskog gubitka, štete za ugled, gubitka povjerljivosti ličnih podataka zaštićenih poslovnom tajnom, neovlaštenog obrnutog postupka pseudonimizacije, ili bilo koje druge znatne ekonomske ili društvene štete.

Opšta uredbe o zaštiti podataka adresira, između ostalog, rješavanje pitanja rascjepkanosti provedbe zaštite podataka u Evropskoj uniji, pravne nesigurnosti i rasprostranjenog javnog mišljenja da osobito kod internetskih aktivnosti

postoje znatni rizici povezani sa zaštitom pojedinaca.

Zaštita prava i sloboda pojedinaca s obzirom na obradu ličnih podataka zahtijeva da se poduzmu odgovarajuće tehničke i organizacijske mjere zaštite ličnih podataka. Uredbom se od organizacija zahtijeva dokaziva usklađenost, a što se može realizovati i kroz akreditirane mehanizme certifikacije.

Budući da je Sporazumom o stabilizaciji i pridruživanju Bosna i Hercegovina preuzela obavezu usklađivanja svog zakonodavstva vezano za zaštitu ličnih podataka s pravom Zajednice i drugim evropskim i međunarodnim zakonodavstvom o privatnosti, privredni subjekti u Bosni i Hercegovini, ali i drugim državama kandidatkinjama za pristup EU, bi trebali izvršiti procjenu implementiranih tehničkih i organizacijskih mjera zaštite ličnih podataka i njihove usklađenosti sa zahtjevima iz Opšte uredbe o zaštiti podataka. Kao okvir za implementaciju i procjenu tehničke usklađenosti mogu se koristiti priznati međunarodni standardi iz oblasti informacijske sigurnosti kao što su ISO/IEC 27001, a posebno standard u razvoju ISO/IEC 27552.

CITIRANI RADOVI

- Babić. T. (2018). Procjena rizika i procjena učinka na zaštitu podataka Preuzeto sa: <http://www.gdpr-simpozij.com/assets/00---procjena-rizika-i-procjena-ucinka-na-zastitu-podataka.pdf>
Pristupljeno 24.08.2018
- CNIL. (2018). Privacy Impact Assessment (PIA) 3 : knowledge bases. 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. (2012). EU smjernice iz oblasti informacijske sigurnosti u sektoru telekomunikacija. Telekomunikacije. God.11, br. 37, 2012, Bosanskohercegovačko udruženje za telekomunikacije Sarajevo
- Hamidović, H. (2013). Opći model upravljanja zakonskim zahtjevima informacijske sigurnosti. Zbornik radova sa Treće internacionalne naučne konferencije "Ekonomija integracija" ICEI 2013 „Znanjem od recesije ka prosperitetu“, održane od 6. – 7. decembar 2013. god. Tuzla, Bosna i Hercegovina, Univerzitet u Tuzli
- Meissner S. (2017). Experiences from data protection certification and the use of standards or the lack thereof Preuzeto sa: <https://www.enisa.europa.eu/events/enisa-cscg-2017/enisa-cscg-2017-agenda>
Pristupljeno 23.08.2018

- Standard. (2013). ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems – Requirements. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)
- Standard. (2014). ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)
- Standard. (2017). ISO/IEC 29151:2017 Information technology -- Security techniques -- Code of practice for personally identifiable information protection. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)
- 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 CD 27552 Information technology -- Security techniques -- Enhancement to ISO/IEC 27001 for privacy management -- Requirements. 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

Datum prve prijave: 24.08.2018.
Datum prijema korigovanog članka: 11.03.2019.
Datum prihvatanja članka: 27.03.2019.

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

Style – **APA Sixth Edition:**

Hamidović, H. (2019, 04 15). Obaveza poduzimanja tehničkih mjera zaštite podataka temeljem EU uredbe o zaštiti podataka. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 67-73.
doi:10.12709/fbim.07.07.01.08

Style – **Chicago Sixteenth Edition:**

Hamidović, Haris. 2019. „Obaveza poduzimanja tehničkih mjera zaštite podataka temeljem EU uredbe o zaštiti podataka.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 67-73.
doi:10.12709/fbim.07.07.01.08..

Style – **GOST Name Sort:**

Hamidović Haris Obaveza poduzimanja tehničkih mjera zaštite podataka temeljem EU uredbe o zaštiti podataka [Časopis] // *FBIM Transactions* / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 67-73.

Style – **Harvard Anglia:**

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

Style – **ISO 690 Numerical Reference:**

Obaveza poduzimanja tehničkih mjera zaštite podataka temeljem EU uredbe o zaštiti podataka.

Hamidović, Haris. [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, *FBIM Transactions*, T. 7, str. 67-73.



IDENTIFIKACIJA SCENARIJA OTKAZA I KONCEPIRANJE MATEMATIČKIH ALATKI U NUMERIČKOM PROCENJIVANJU RIZIKA

IDENTIFICATION OF FAILURE SCENARIO AND THE CONCEPTION OF MATHEMATICAL TOOLS IN NUMERIC RISK ASSESSMENT

Goran Jovanov

Kriminalističko policijska akademija-Beograd, Beograd, Srbija

Nemanja Jovanov

Poslovni i pravni fakultet "Union – Nikola Tesla" univerziteta u Beogradu,
Beograd, Srbija

Radovan Radovanović

Kriminalističko policijska akademija-Beograd, Beograd, Srbija

©MESTE

JEL Kategorija rada: **D81, G32**

Apstrakt

U procesnoj industriji menadžment rizika je tradicionalno fokusiran na razmatranje verovatnoće specifičnih događaja ili havarijskih situacija. U energetske postrojenjima koja predstavljaju najznačajnije polje primene, od 70-tih godina prošlog veka u SAD je uveden strukturirani pristup za identifikaciju scenarija otkaza. Procena rizika predstavlja proces odlučivanja u odnosu na to da li se postojeći rizici nalaze u opsegu prihvatljivog rizika i da li su postojeći postupci za kontrolu rizika adekvatni. Glavni razlog zbog čega je potrebno napraviti procenu rizika je mogućnost za upravljanje rizikom, njegovo smanjenje ili eliminaciju. Procena rizika treba da bude što je moguće objektivnija i da ista zavisi od naučnih kriterijuma. Po dobijanju informacije u vezi sa rizikom, možemo početi sa primenom efektivnih metoda za njegovo smanjenje, čime ćemo ostvariti povećanje efikasnosti u smanjenju rizika. Metodološki tok procedure procene rizika predstavlja osnovu za pravilno procenjivanje

Adresa autora:

Goran Jovanov

[✉ goran.jovanov@kpa.edu.rs](mailto:goran.jovanov@kpa.edu.rs)

odnosno snimanje situacije poslovnog sistema. Rezultat stanja sistema u primeni određenih modela za procenu rizika, zavisi isključivo od pravilno donošanih rezultata u metodološkom toku



procene rizika. Na osnovu daljih rezultata vrši se rangiranje numeričko procenjivanje rizika, odnosno Rizik (R) se rangira od prihvatljivog (zanemarljivo malog rizika) ranga R1 do ekstremno visokog rizika ranga R5, koji ne dozvoljava da aktivnost niti počne niti se nastavi, dok se nivo rizika ne smanji. Takođe se daje tabelarni prikaz opisa kriterijuma za procenu verovatnoće, kao i kriterijumi za učestalost otkaza i rangiranje rizika. Vrednovanje procene rizika se postiže prikazom modela matrice. Postoje matrice sa različitim brojem nivoa, ali najjednostavniji model matrice rizika je 3x3 sa tri nivoa rizika. Na osnovu matrice za ocenu rizika definiše se rang rizika za klasifikaciju i karakterizaciju procene rizika.

Ključne reči: Verovatnoća, rangiranje, procenjivanje, kriterijum učestalosti, kriterijum otkaza

Abstract

In the process industry, risk management is traditionally focused on considering the probability of specific events or accidents. In energy plants which represent the most important field of application, in 1970's of the last century, in the USA the structural approach for identification of failure scenario was introduced. Risk assesment represent the decision process related to whether the existing risks are within the range of acceptable risk and whether the existing procedures for risk control are adequate. The main reason why it is necessary to make risk assesment is the possibility for risk management, its decrease or elimination. Risk assesment should be as objective as possible, and to depend on scientific criteria. After having received the information on risk, it can be started with the application of effective methods for its decrease, by which the increased efficiency in risk assesment will be accomplished. Methodological course of risk assesment procedure represents the ground for proper estimation, i.e. for monitoring the situation of business system. The result of system's condition at the application of certain models for risk assesment, depends exclusively on properly made results within the methodological course of risk assesment. Based on further results, the ranking of numerical risk assesment is made, i.e. the risk (R) is ranked from acceptable (insignificantly low risk) of the rank R1 through extremely high risk of the rank R5, which does not allow for activity to either to start or to continue until the risk level is reduced. Also, the table containing the description of criteria for probability estimate is provided, as well as of criteria for the frequency of failure and risk ranking. The evaluation of risk assesment is accomplished by showing the matrix model. There are matrices with different number of levels, but the simplest model of risk matrix is 3x3 with 3 risk levels. Based on the matrix of risk estimate the range of risks for classification and characterization of risk estimate is defined.

Keywords: Possibility, ranking, estimate, frequency criteria, failure criteria

1 UVOD

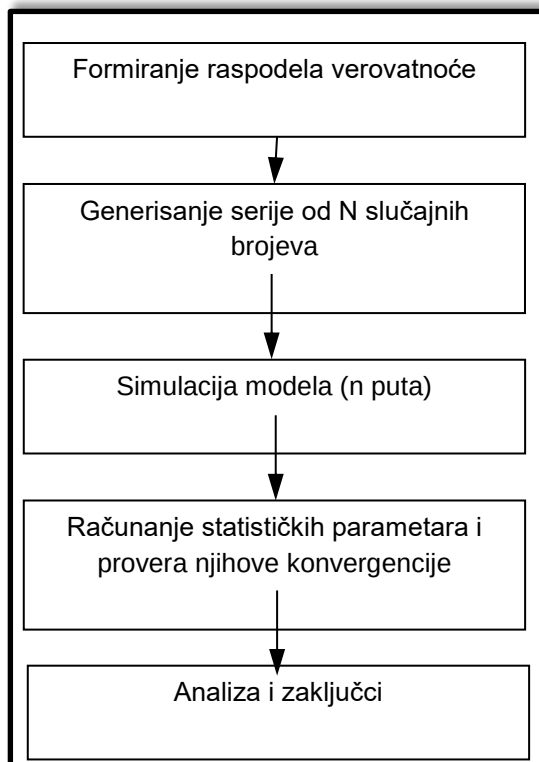
Ekonomске štete koje se javljaju u proizvodno poslovnim sistemima tokom njihovog životnog veka, motivisale su naučnike širom sveta da se posvete razvoju metoda i tehnika za minimizaciju štetnih, aksidentnih i havarijskih situacija. Poslovanje savremenih proizvodno poslovnih sistema se odvija, danas, 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, a što svakako zahteva novo znanje i veštine kod zaposlenih. Rizik je oduvek privlačio pažnju

velikog broja istraživača i naučnika, ali uglavnom sa različitih aspekata, tako da ni do danas nemamo jedinstvenu definiciju rizika. Nije problem samo u razlici pristupa već i u pojavnosti prirodi rizika, što je postalo fenomen, pa rizik nije ni moguće jednoznačno pojasniti. Pojam rizika je vrlo relativiziran, ali svim rizicima je zajedničko to da moraju biti budući i neizvesni događaji. Prisustvo rizika ne može se neutralisati, pa pojedinci i poslovni sistemi traže puteve njegovog rešavanja. Rizici fundamentalne prirode rešavaju se putem kolektivnih napora društva. Iako društvo može pomoći da se olakša teret rizika u mnogim oblastima, postoje neki rizici za koje su odgovorni pojedinci.

2 MERENJA I OCENA RIZIKA

Prirodno je da ljudi nastoje da izbegnu rizik, ili da ga svedu na najmanju moguću meru. Zbog toga se oni najčešće prilikom izbora između rizika i moguće koristi, odlučuju za njihovu optimalnu kombinaciju (alternativu), pri čemu se podrazumeva mogućnost merenja ili ocene rizika. Odluke se i danas donose sa određenom dozom rizika i to ponekad direktno na bazi iskustva, a ponekad koristeći istorijske podatke koji su se generacijski prenosili i to tako da se vremenom doza učešća rizika u tim odlukama i nepovoljan ishod smanjuje sa sticanjem iskustva. Smatra se da je osnovni zadatak menadžmenta posebno prevođenje neizvesnosti u rizik. Da bi se taj zadatak ispunio, potrebno je pravilno oceniti rizik, čime se, pored ostalog, bavi teorija verovatnoće. Vršni događaj se obično izražava u zavisnosti od minimalne sekvence otkaza. Ove sekvence se sastoje iz niza događaja, od kojih je svaki definisan pomoću parametara. Pretpostavimo da je osnovni događaj sa verovatnoćom pojave - p . Ova vrednost nije poznata egzaktno već je estimirana na osnovu podataka ili ekspertnog znanja. Neizvesnost p je kvantifikovana raspodelom verovatnoće: srednja vrednost je najbolja estimacija za p , disperzija raspodele je mera neodređenosti za p , tj. veća li manja neodređenost reflektuje respektivno veću ili manju neodređenost vrednosti verovatnoće p . Za sve osnovne događaje, slučajni uzorci verovatnoća se uzimaju na bazi neodređenosti raspodela. Ove vrednosti verovatnoća se tada koriste za proračun verovatnoće vršnog događaja. Ukoliko se ovi uzorci i vršni događaj proračunavaju više puta, raspodela neodređenosti vršnog događaja se može odrediti empirijski. Srednja vrednost raspodele indukuje verovatnoću vršnog događaja, a disperzija kvantifikuje neodređenost verovatnoće. Za opisivanje analize pomoću višestrukog ponavljanja slučajnog uzorkovanja koristi se Monte Carlo metoda (slika 1). Korišćenjem generatora slučajnih brojeva, realizuje se višestruko kvantifikovanje vršnog događaja. Za analizu neodređenosti potrebno je poznavanje raspodela verovatnoća (lognormalna, eksponencijalna, normalna, beta itd.) Kvantifikacija neodređenosti na nivou tehničkog sistema mora biti deo procesa finalnog donošenja

odluka. Poznavanje neodređenosti (neizvesnosti) u celokupnom riziku je veoma važno radi mogućnosti odlučivanja na osnovu više informacija (Adamović & Milošević, 2008).



Slika 1 Procedura Monte Carlo metode

Onog trenutka kada se na bilo koji način želi utvrditi mera opasnosti od štetnog događaja u nekom sistemu, moraju se utvrditi granice tog sistema, a takođe se mora ograničiti i vreme u kome se mera opasnosti utvrđuje. Ako se konstatuje da je meru neke opasnosti najbolje utvrđivati preko verovatnoće nastanka štetnog događaja i veličine njegovih posledica, onda se pojam rizik može shvatiti kao kompleksna veličina koja obuhvata verovatnoću nastanka štetnog događaja i očekivanu veličinu posledice tog događaja u nekom zaokruženom sistemu i tokom nekog vremenskog intervala ili određenog procesa, što se može predstaviti slikom 2. Iskazano matematičkim jezikom rečeno možemo napisati na sledeći način:

$$R(T) = P(T) \times L(T)$$

gde su:

T - neželjeni rizicni ili štetni događaj,

R(T) - rizik od događaja T,

$P(T)$ - verovatnoća da će se događaj T i odigrati,
 $L(T)$ - veličina štete koju bi izazvao događaj T .

Ova matematička relacija rizika često izaziva sa teoretskog i matematičkog aspekta određena podozrenja i nerazumevanja. Glavni nesporazum leži u činjenici da se rizik izražava kao proizvod dve komponente: jedne koja je realna (posledice) i druge koja je imaginarna, odnosno koju je čovek definisao i nazvao verovatnoća (Adamović et.al., 2008, p.45).

Iako očigledno ne postoji jedinstvena definicija rizika, može se zaključiti da u svim definicijama postoje zajednički elementi, a to su neizvesnost i šteta. Neophodno je stalno istraživati mogućnosti za redukcije rizika. Rizik, koji se definiše kao proizvod verovatnoće i posledice, uvek se posmatra za pretpostavljene scenarije u konkretnim situacijama i okolnostima nastanka opasnosti i očekivanog štetnog događaja. Kada postoji rizik, ishodi se ne mogu predvideti sa sigurnošću. Stoga rizik izaziva neizvesnost. Međutim, za razliku od neizvesnosti koja je subjektivni koncept i koja se ne može direktno meriti, rizik je objektivni koncept, što znači da se on može meriti, samim tim identifikovati scenario otkaza na osnovu teorije pouzdanosti i same tehnologije održavanja nekog tehničkog sistema.

Ukoliko poznajemo sve navedene termine možemo izgraditi koncept matematičkih alati kroz numerički sistem procenjivanja rizika.

2.1 Analiza rizika

Analiza rizika je postupak kojem je cilj ustanoviti "ranjivosti" sistema, uočiti potencijalne rizike, te na odgovarajući način kvantifikovati moguće posledice da bi se mogao odabrati najdelotvorniji način zaštite, odnosno proceniti opravdanost uvođenja dodatnih "protivmera". Analizom rizika moraju se utvrditi sledeće činjenice:

- kritični resursi i njihova vrednost (relativna ili novčana),
- pregled mogućih opasnosti i verovatnoće njihove pojave,
- potencijalni gubici koje prouzrokuje ostvarenje opasnosti,
- preporučene protivmere (nadzor) i zaštita.

Na temelju dobijenih rezultata potrebno je odlučiti kakve protiv-mere treba preduzeti.

Postoje tri mogućnosti delovanja koje nisu međusobno isključive:

1. smanjenje rizika,
2. prenos rizika, i
3. prihvatanje rizika.

Tabela 1. Tipične verovatnoće rizika

Verovatnoća pojave		Kriterijum
Kvalitativne	Kvantitativne	
Vrlo retko	< 0.1	Procenjena verovatnoća pojave ne prelazi 10%, odnosno verovatnoća ponavljanja prevazilazi period od 10.000 godina
Retko	>0.1 ali <0.4	Procenjena verovatnoća pojave ne prelazi 40%, ali je veća od 10%, odnosno verovatnoća ponavljanja prevazilazi period od 1.000 godina
Verovatno	>0.4 ali <0.8	Procenjena verovatnoća pojave prelazi 40%, ali nije veća od 80%, odnosno verovatnoća ponavljanja se kreće u periodu od 10 do 1.000 godina
Vrlo verovatno	> 0.8	Procenjena verovatnoća pojave prelazi 80%, odnosno verovatnoća ponavljanja je manja od 10 godina

Jedini važan parametar pri odabiru načina delovanja je isplativost za organizaciju. Smanjenje rizika predstavlja proces u kojem se na temelju sprovedene analize rizika nastoje sprovesti odgovarajuće protivmere i uveste sigurnosni nadzor da bi se zaštitili resursi

organizacije. U tom postupku nastoji se smanjiti verovatnoća opasnosti i/ili njen uticaj na proces. Ukoliko se pokaže isplativijim, rizik je moguće preneti na treću stranu (npr. osiguravajuće društvo).

Isto tako moguće je da implementacija protivmera ili prenos rizika nisu isplativi. U tom slučaju preduzeće može odlučiti da prihvati rizik, odnosno troškove koji iz toga proizilaze. Jedini pristup koji u upravljanju rizikom nije prihvatljiv je ignorisanje ili zanemarivanje rizika. Treba znati da je upravljanje rizikom kontinualan proces, te da se odnos vrednosti resursa, ranjivosti i opasnosti sa vremenom menja. Postoje dva osnovna pristupa analizi rizika (tabela 1), a to su:

1. kvalitativna analiza, i
2. kvantitativna analiza.

2.1.1 Kvalitativni pristup analize rizika (matrica rizika)

Kvalitativna analiza rizika predstavlja subjektivniji pristup pri kojem se resursi, rizici i protivmere posmatraju relativno s obzirom na sistem. Za sprovođenje kvalitativne analize nije nužno egzaktno poznavanje materijalne vrednosti pojedinih resursa, već je za njihovo vrednovanje bitno poznavati važnost za pojedine poslovne procese. Rezultat kvalitativne analize iskazuje samo relativan odnos vrednosti šteta nastalih delovanjem neke opasnosti i uvođenja protivmera. Pritom trebamo imati na umu da je ta procena subjektivne prirode te je stoga podložna greškama. Kvalitativni kriterijumi koriste reči kao što su verovatno, moguće, često i retko, kako bi

se opisala verovatnoća pojave i reči kao što su neznatno, katastrofalno, itd., kako bi se opisale posledice događaja (Adamović et.al., 2007, p.158).

Kvalitativni pristup kao metoda započinje dodeljivanjem kvalitativnih vrednosti verovatnoćama događaja i posledica koje se kasnije koriste pri determinisanju kvalitativnog faktora rizika. Ključne karakteristike ovog metoda su da:

- omogućava nezavisno određivanje verovatnoća i posledica rizika,
- obezbeđuje kvalitativno definisanje rizika i njegove težine.

Metodologija se odvija u sledeća tri koraka:

1. Adresiranje svake rizične situacije na osnovu pojedinačnih formi za određivanje rizika.
2. Determinisanje kvalitativne verovatnoće pojave (P) za svaki rizik na podesan način i na osnovu realnog kriterijuma. Na slici 2. prikazani su tipični kriterijumi za ustanovljavanje kvalitativnih vrednosti verovatnoća.
3. Determinisanje kvalitativnih vrednosti posledica pojave (C) za svaki rizik na podesan način i na osnovu realnog kriterijuma. Na slici 2. prikazani su tipični kriterijumi za ustanovljavanje kvalitativnih vrednosti posledica.

Posledice pojave		Kriterijum				
Kvalitativne	Kvantitativne					
Beznačajne	< 0.1	Minimalne ili nebitne posledice				
Neznatne	od 0.1 do 0.4	Neznatno utiču na proces koji se analizira				
Znatne	od 0.4 do 0.8	U velikoj meri doprinose povećanju troškova				
Kritične	od 0.8 do 0.9	Ozbiljno ugrožavaju proces, osoblje				
Katastrofalne	> 0.9	Katastrofalne posledice po organizaciju, okolinu, ljude				
Vrlo verovatno	Nizak	Srednji	Visok	Visok	Visok	Verovatnoća pojave
Verovatno	Nizak	Srednji	Visok	Visok	Visok	
Retko	Nizak	Nizak	Srednji	Srednji	Visok	
Vrlo retko	Nizak	Nizak	Nizak	Nizak	Visok	
		Beznačajne	Neznatne	Znatne	Kritične	Katastrofalne

Slika.2 Tipične posledice rizika sa Matricom rizika

Određivanje nivoa rizika na bazi preseka kvalitativnih vrednosti za verovatnoće i posledice (P i C) rizičnih situacija u matrici rizika 5x4 prikazan je na slici 2. U zavisnosti od aktivnosti i sposobnosti da se izdiferencira nivo rizika, mogu se konstruisati matrice različitih nivoa "osetljivosti". Na primeru na slici 2. izvršena je kategorizacija na tri nivoa rizika (nizak, srednji, visok).

2.1.2 Kvantitativni pristup analize rizika

Ovaj metod se zasniva na dodeljivanju kvantitativnih vrednosti verovatnoćama pojave i posledicama događaja, koje se koriste za determinisanje kvantitativnog faktora rizika. Kvantitativni kriterijumi koriste numeričke vrednosti kako bi opisali verovatnoću i posledice događaja. Ključne karakteristike metoda ogledaju se u sledećem:

- omogućava kvalitativno definisanje rizika, ali na osnovu kvantitativnih podataka o nivou rizika,
- pruža finiju izdiferenciranost unutar nivoa rizika.

Metod je koristan za definisanje prioriteta aktivnosti, posebno u slučaju kada postoji veliki broj identifikovanih rizičnih situacija. Metodologija se zasniva na jednačini za faktor rizika:

$$RF = (P \times C)$$

gde su:

- RF - faktor rizika,
- P - verovatnoća pojave,
- C - posledice pojave.

Metodologija se odvija u sledećim koracima:

1. Adresiranje svake rizične situacije na osnovu pojedinačnih formi za određivanje rizika.
2. Determinisanje kvantitativne verovatnoće pojave (P) za svaki rizik na podesan način i na osnovu realnog kriterijuma. Verovatnoća se izražava kao decimalni broj od 0 do 1, pri čemu 0 označava nemoguć događaj, a 1 događaj koji će se realizovati sa verovatnoćom od 100%.
3. Determinisanje kvantitativnih vrednosti posledica pojave (C) za svaki rizik na podesan način i na osnovu realnog kriterijuma.
4. Korišćenjem formule $RF = P \times C$, determiniše se faktor rizika za svaki identifikovani rizik.

5. Na osnovu dobijenih vrednosti određuje se nivo rizika za svaki identifikovani rizik.

Da bi se uradila kvantitativna analiza rizika, mora biti ustanovljen model sistema. Model predstavlja pojednostavljenu reprezentaciju realnog sistema i sadrži opise relacija između posmatranih kvantiteta.

Postoje nekoliko različitih metoda za modelovanje sistema, a u cilju proračuna njegove pouzdanosti. Dva od tih metoda su:

1. funkcionalno, i
2. hardversko modelovanje.

Funkcionalni model sistema je model koji prvo opisuje, a zatim logički povezuje funkcije neophodne za operacioni rad sistema.

Hardversko modelovanje koristi opremu koja je potrebna za rad sistema kako bi prikazao logičke veze između individualnih komponenti i opisuje funkcije neophodne za funkcionisanje sistema. Često se ova dva metoda modelovanja kombinuju. U kvantitativnoj analizi rizika interesuje nas verovatnoća pojave neželjenog događaja. U tu svrhu razvijeni su razni modeli, npr. stablo otkaza sa verovatnoćama osnovnih događaja kao parametrima. Ove verovatnoće su subjektivne i izražavaju neizvesnost kvantiteta. Razvojem i korišćenjem probabilističkih modela moguće je udruživanje neizvesnosti sa svakom slučajnom promenljivom u modelu (Drobnjak et.al., 2014;53).

2.2 Proces analize rizika

Primarni cilj bilo koje analize rizika je da se identifikuju opasnosti, kako bi bili u mogućnosti da redukujemo ili eliminišemo verovatnoću pojave neželjenog događaja i njegove konsekvence po čoveka, njegovu okolinu ili ekonomiju. Do ovoga dolazi kada je inicijalni događaj praćen greškom sistema.

Do sada identifikovani događaji koji su uzročnici osnovnih tipova otkaza:

- događaji koji su posledica ljudskog faktora, tj. greške u dizajnu i odžavanju,
- događaji koji su posledica hardvera, (npr. curenje ventila) i
- događaji koji su posledica uticaja okoline (zemljotresi, poplave).

Internacionalni standard IEC 60300-3-9:1995 definiše analizu rizika kao "Sistemske korišćenje raspoloživih informacija radi identifikacije opasnosti i procenjivanje rizika pojedinca, populacije, imovine ili okoline" (Starčević et.al., 2010, p. 48). Analiza rizika može biti izvedena kvantitativno pri čemu epizodni događaji sa potencijalno vezanim posledicama su identifikovani i rangirani shodno šemi vrednovanja u zavisnosti od kriterijuma (imovinska šteta, ljudska povreda, proizvodni zastoj). Rangiranje rizika omogućava menadžerima da odrede prioritete preventivnih aktivnosti i resurse za rizični scenario. Ove metode se obično nazivaju indeksne metode, point scheme metode, itd., a razmatraju i frekvenciju i posledice.

Analiza rizika može biti podeljena u različite nivoe detalja, kao npr. u nuklearnoj industriji, gde se analiza rizika izvodi na tri nivoa:

- Nivo 1 - analiza sistema, analiza verovatnoće pojave kritičnih stanja;
- Nivo 2 - analiza sistema i analiza posledica pojave različitih kritičnih stanja sa odgovarajućim verovatnoćama; ili
- Nivo 3 - dalja analiza za moguće (negativne) efekte na ljude, uključujući procenu opasnosti za ljudski život i slučajevi u kojima može do toga da dođe.

Krajnji proizvod analize rizika tada zavisi od nivoa detalja koji se koriste i treba da bude određen već pri definisanju predmeta analize, odnosno pre izvođenja analize (George, 2005, p. 33).

3 MODEL KONCEPIRANJA MATEMATIČKIH ALATA U NUMERIČKOM PROCENJIVANJU RIZIKA

Procena rizika se izvodi za svaku aksidentnu situaciju, determinisanjem odgovarajućeg rizika za dati scenario, tehnički sistem ili tehnički proces, kao funkciju težine moguće štete i verovatnoće njene pojave. Metode koje se koriste u proceni rizika su često kvantitativne, mada stepen zahtevanog ulaska u detalje za pripremu procene zavisi od specifične aplikacije.

U ovom koraku treba uraditi sledeće analize:

- analizu frekventnosti,

- analizu posledica, i
- kalkulaciju rizika.

Analiza frekventnosti se koristi za procenu verovatnoće svakog identifikovanog neželjenog događaja. Postoje tri opšta pristupa koja se upotrebljavaju za određivanje frekventnosti događaja:

1. korišćenje relevantnih istorijskih podataka,
2. izvođenje pomoću analitičkih ili simulacionih tehnika,
3. korišćenje ekspertne procene.

Sve ove tehnike mogu se koristiti individualno ili zajednički. Kada se koriste istorijski podaci, tada podaci moraju biti relevantni, odnosno moraju da odgovaraju tipu sistema ili aktivnostima koje se razmatraju.

Određivanje ukupnog rizika na osnovu skupa scenarija, omogućava polaznu osnovu za identifikaciju i rangiranje udela rizika. Na slici 3. prikazana je pomenuta metodologija.



Slika 3. Metodologija identifikacije i rangiranja udela rizika

Metod Markova se koristi u izvođenju analize raspoloživosti inženjerskih sistema. Osnovne postavke ove metode su:

- verovatnoća prelaza sistema iz jednog stanja u drugo u konačnom vremenskom intervalu Δt , data je sa $\alpha \Delta t$, pri čemu je α koeficijent prelaza iz jednog stanja sistema u drugo,
- verovatnoća pojave više od jednog prelaza iz jednog stanja sistema u drugo u konačnom vremenskom intervalu Δt je neznatna, tj. $(\alpha \Delta t) \rightarrow 0$,
- svi događaji su nezavisni jedan od drugog.

U određenom trenutku vremena sistem se nalazi u jednom od konačnog broja stanja.

Primer:

Pretpostavimo da sistem može da iz normalnog radnog stanja pređe u stanje otkaza na bezbedan i nebezbedan način. Na slici 4. su predstavljena stanja sistema.

Uz pomoć modela Markova mogu se napisati jednačine stanja prikazanog sistema:

$$P_0(t + \Delta t) = P_0(t)(1 - \lambda_{nb}\Delta t)(1 - \lambda_b\Delta t)$$

$$P_1(t + \Delta t) = P_0(t)\lambda_{nb}\Delta t + P_1(t)$$

$$P_2(t + \Delta t) = P_0(t)\lambda_b\Delta t + P_2(t)$$

gde su:

$P_i(t + \Delta t)$, $i = 0, 1, 2$ - verovatnoće i -tog stanja sistema u trenutku $(t + \Delta t)$,

$P_i(t)$, $i = 0, 1, 2$ - verovatnoće i -tog stanja sistema u trenutku t ,

$\lambda_{nb}\Delta t$ - verovatnoća bezbednog otkaza sistema u konačnom vremenskom intervalu t ,

$\lambda_b\Delta t$ - verovatnoća nebezbednog otkaza sistema u konačnom vremenskom intervalu t .

Rangiranje scenarija rizika na osnovu njihovih frekvencija pojavljivanja omogućava nam ograničen uvid u celokupnu raspodelu rizika, s obzirom na važnost udela individualnih događaja u ukupnom riziku. Rangiranje scenarija pruža nam uvid u važnost grupe greške/otkaza, ali ne i greške/otkaza pojedinih komponenti jednog poslovnog sistema. Neželjeni događaj (npr. greška/otkaz komponente X) koji se desio u strukturi scenarija male verovatnoće pojave, može biti zanemaren u definisanju dominantnog scenarija rizika. Ukoliko je udeo scenarija male verovatnoće pojave u ukupnom riziku uporediv sa manje dominantnim scenarijem rizika, tada rangiranje scenarija neće obuhvatiti važnost rizika komponente X.

Iz tog razloga na raspolaganju nam stoji nekoliko kvantitativnih merenja značaja individualnih događaja. Suština ovih merenja je da

se definišu promene u kvantitativnoj matrici rizika prouzrokovane promenom u verovatnoći pojave događaja u modelu rizika. Na osnovu izračunatih mera značaja, događaji jednog modela rizika se rangiraju na osnovu njihovih relativnih vrednosti mera značaja. Informacije koje se generišu na osnovu ovog procesa se često koriste u donošenju odluka na osnovu rizika i služe kao polazna tačka aktivnostima i naporima na redukovanju rizika, kao što su to redizajn hardverskih komponenti, dodatna redudancija, i sl. U realizaciji „Singapurskog” modela (3x3), rizik se predstavlja kao proizvod verovatnoće nastanka neželjenog događaja (V) i posledica težine neželjenog događaja (T), tj.:

$$R = V \cdot T$$

Vrednovanje procene rizika se postiže prikazom modela matrice. Postoje matrice sa različitim brojem nivoa, ali najjednostavniji model matrice rizika je 3x3 sa tri nivoa rizika. U tabeli 2. su predstavljeni nivoi verovatnoće i dat je njihov opis, u tabeli 3. date su posledice težine neželjenog događaja i njihov opis, a u tabeli 4 je prikazana matrica za određivanje nivoa rizika. Na osnovu matrice za ocenu rizika definiše se rang rizika za klasifikaciju i karakterizaciju procene rizika kao što je to prikazano u tabeli 5.

Tabela 2. Nivoi verovatnoće i njihov opis

Verovatnoća nastanka neželjenog događaja (V)		Opis
Mala verovatnoća	1	neželjeni događaj verovatno se neće dogoditi
Srednja verovatnoća	2	moгуće je nastajanje neželjenog događaja (poznato je da se događa)
Velika verovatnoća	3	neželjeni događaj se događa često ili se ponavlja

Tabela 3. Posledice težine neželjenog događaja sa opisom događaja

Posledica težine neželjenog događaja (T)		Opis
Male posledice	1	Na primer, ako je povreda na radu, zahteva se samo mera prve pomoći (manje posekotine, iritacija kože, itd.).
Srednje posledice	2	Na primer ako je povreda na radu, zahteva se medicinska pomoć, oboljenje izaziva privremenu nesposobnost ili invalidnost (opekotine, uganuća, prelomi malih kostiju, naglupost, i dr.).
Velike posledice	3	Na primer ako je povreda na radu, imamo smrtni ishod, teške povrede, profesionalne bolesti praćene teškim posledicama (amputacije, prelomi velikih kostiju, rak, teška trovanja, bolesti opasne po život, i dr.).

Tabela 4. Kriterijumi za klasifikaciju i karakterizaciju procene rizika

Posledica težine neželjenog događaja (T)		Verovatnoća nastanka neželjenog događaja (V)		
		Mala	Srednja	Velika
		1	2	3
Velika	3	Mali rizik 3	Veliki rizik 6	Vrlo veliki rizik 9
Srednja	2	Vrlo mali rizik 2	Umeren rizik 4	Veliki rizik 6
Mala	1	Zanemarljivo mali rizik 1	Vrlo mali rizik 2	Mali rizik 3

Tabela 5 Matrični model procene rizika kod "singapurske" metode

Procena ranga rizika	Klasifikacija nivoa rizika	Karakterizacija rizika
R1	Zanemarljivo mali rizik	Prihvatljiv rizik
R2	Vrlo mali rizik	
R3	Mali rizik	Povećani rizik
R4	Umeren rizik	
R6	Veliki rizik	Neprihvatljiv rizik
R9	Vrlo veliki rizik	

4 ZAKLJUČCI

Razvoj automatike doveo je do sve kompleksnijih bezbednosnih funkcija na tehničkim sistemima, što je uslovalo i daleko složenije postupke održavanja istih. Uticaj funkcije održavanja na bezbednost rada tehničkog sistema postao je presudan. Radnici službe održavanja su zaduženi za preventivno otklanjanje nebezbednih uslova rada u proizvodnom pogonu. Pravilno upravljanje funkcijom održavanja dobija ključnu ulogu u kontroli i identifikaciji opasnosti po pitanju rada tehničkog sistema.

Upravljanje funkcijom održavanja na bazi rizika, nalazi veoma bitnu oblast primene "rezonovanja" sa stanovišta rizika, upravo u stvaranju bezbednog radnog okruženja, tj. u slučaju održavanja – osiguranju bezbednog izvođenja aktivnosti održavanja. Identifikacija i analiza rizika i donošenje racionalnih odluka na bazi procesa procene rizika (RAP) (RAP – Risk Assessment Process) je najbolje preventivno sredstvo u rukama održavaoca za uspešno i sigurno izvođenje aktivnosti održavanja. Poznavanje rizika omogućava privrednom sistemu da maksimizuje efikasnost bezbedonosnog programa i minimizuje broj pojava stanja "u otkazu" kod tehničkih sistema.

Model koncipiranja matematičkih alata u numeričkom procenjivanju rizika nam daje široku lepezu primene modela za određivanje pravilne tehnologije održavanja tehničke dijagnostike.

Takođe nas upućuje na primenu tehničke dijagnostike stanja i primene modela održavanja tehničkih sistema na bazi rizika.

Rezultat stanja sistema u primeni određenih modela za procenu rizika, zavisi isključivo od pravilno donošenih rezultata u metodološkom toku procene rizika. Na osnovu daljih rezultata izvršeno je rangiranje numeričko procenjivanje rizika, odnosno, rizik (R) se rangira od prihvatljivog (zanemarljivo malog rizika) ranga R1 do ekstremno visokog rizika ranga R5, koji ne

dozvoljava da aktivnost niti počne niti se nastavi, dok se nivo rizika ne smanji. Takođe su dati tabelarni prikazi opisa kriterijuma za procenu verovatnoće, kao i kriterijumi za učestalost otkaza i rangiranje rizika. Vrednovanje procene rizika se postiglo prikazom modela matrice. Postoje matrice sa različitim brojem nivoa, ali u ovom radu je primenjen model matrice rizika je 3x3 sa tri nivoa rizika. Na osnovu matrice za ocenu rizika definisan je rang rizika za klasifikaciju i karakterizaciju procene rizika.

CITIRANA DELA

- Adamović, Ž., Jovanov, G., & Meza, S. (2008). *Upravljanje rizikom*. Univerzitet u Novom Sadu. Tehnički fakultet „Mihajlo Pupin“, Zrenjanin.
- Adamović, Ž., Voskresenski, V., & Tul, R. (2007). *Održavanje na bazi rizika*. TEHDIS, Beograd
- Adamović, Ž., Milošević, Ž., i dr. (2008). *Modeli održavanja na bazi rizika*. Društvo za energetske efikasnost Bosne i Hercegovine, Banja Luka.
- Drobnjak, R., Drobnjak, P., & Vasović, V. (2014). *Procena rizika jednog radnog mesta polukvantitativnom metodom – Guardmaster*. Zbornik radova Prve regionalne međunarodne konferencije: Primijenjena zaštita i njeni trendovi, Međunarodni institut za upravljanje znanjem Novi Sad, ISBN 978-86-80048-00-0, Zlatibor, 17-19. septembar
- George, E. Rejda. (2005). *Principles of Risk Management and Insurance*. Ninth Edition. Addison 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: 20.09.2018.
Datum prijema korigovanog članka: 11.03.2019.
Datum prihvatanja članka: 27.03.2019.

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

Style – APA Sixth Edition:

Jovanov, G., Jovanov, N., & Radovanović, R. (2019, 04 15). Identifikacija scenarija otkaza i koncipiranje matematičkih alatki u numeričkom procenjivanju rizika. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 74-84. doi:10.12709/fbim.07.07.01.09

Style – Chicago Sixteenth Edition:

Jovanov, Goran, Nemanja Jovanov, i Radovan Radovanović. 2019. „Identifikacija scenarija otkaza i koncipiranje matematičkih alatki u numeričkom procenjivanju rizika.“ Urednik Zoran Čekerevac. *FBIM Transactions (MESTE)* 7 (1): 74-84. doi:10.12709/fbim.07.07.01.09.

Style – GOST Name Sort:

Jovanov Goran, Jovanov Nemanja i Radovanović Radovan Identifikacija scenarija otkaza i koncipiranje matematičkih alati u numeričkom procenjivanju rizika [Časopis] // *FBIM Transactions* / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 74-84.

Style – Harvard Anglia:

Jovanov, G., Jovanov, N. & Radovanović, R., 2019. Identifikacija scenarija otkaza i koncipiranje matematičkih alati u numeričkom procenjivanju rizika. *FBIM Transactions*, 15 04, 7(1), pp. 74-84.

Style – ISO 690 Numerical Reference:

Identifikacija scenarija otkaza i koncipiranje matematičkih alati u numeričkom procenjivanju rizika.
Jovanov, Goran, Jovanov, Nemanja i Radovanović, Radovan. [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, *FBIM Transactions*, T. 7, str. 74-84.



KRIPTOVALUTE, BLOKČEJN I BITKOIN

CRYPTOCURRENCY, BLOCKCHAIN, AND BITCOIN

Mario Lukinović

Pravni fakultet Univerziteta Union, Beograd, Srbija

©MESTE

JEL kategorija: **E41, E51**

Apstrakt

Kriptovalute (engl. "cryptocurrency") su digitalne (virtualne) valute, koje iako su sredstvo razmene, još uvek nisu strogo regulisane zakonom u većini država, a u pojedinim su čak i zabranjene. Veliki broj ljudi, uključujući i IT stručnjake i programere ne znaju mnogo o ovoj temi, a šira javnost izjednačava pojmove blokčejna i bitkoina. Tržište kriptovaluta danas iznosi gotovo 770 milijardi dolara. Od pojave prvih digitalnih valuta do danas, nastalo je preko 1.300 aktivnih kriptovaluta koje se razlikuju prema svojim svojstvima i upotrebi. Pre bitkoina bilo je mnoštvo neuspelih pokušaja stvaranja digitalnih valuta (digikeš, heškeš, Fejsbuk kredit i dr.). Utopistička ideja da matematika i fizika mogu rešiti društvene probleme započela je svoj život kroz pojavu bitkoina. Genijalna ideja po kojoj funkcioniše bitkoin zasnovana je na tehnologiji blokčejna, čiji kapacitet doseže daleko iznad kripto valuta. Iako se još uvek vode polemike ko stoji iza pseudonima Satoši Nakamoto, njegova zaostavština ima potencijal da promeni svet. Uspeh bitkoina leži u prednostima koje ima u odnosu na druge slične valute, ali njegov značaj prevazilazi i pogodnosti koje je doneo. Banke nisu potrebne za čuvanje podataka o novcu, evidenciju o imovini i svakoj transakciji bitkoina čuvaju računari svih korisnika mreže u zajedničkoj bazi podataka blokčejnu. Sve transakcije su mnogo brže od bankarskih, bez taksi, uz drastično lakše plaćanje preko državnih granica. Bitkoin svojim korisnicima pruža bezbednosti bez identifikacije, iako blokčejn beleži transakciju, ne beleži ko stoji iza nje. U radu su predstavljeni osnovni principi na kojima su zasnovani bitkoin i druge kriptovalute, pojašnjen odnos između blokčejna i bitkoina.

Keywords: kriptovalute, digitalni novac, kriptografija, blokčejn, bitkoin.

Abstract

Cryptocurrencies are digital (virtual) currencies, which, although they are a means of payment, are not yet strictly regulated by law in most states, and in some, they are even prohibited. Many people, including IT professionals and programmers, do not know much about this topic, and the general public equates the terms blockade and bitcoin. The crypto-market today amounts to nearly \$ 770 billion. Since the emergence of the first digital currencies to date, over 1,300 active crypto sites have appeared, which differ in their properties and uses. Before the bitcoin, there were a lot of unsuccessful attempts to create digital currencies (DigiCash, Hashcash, Facebook credit, etc.). Utopian idea that mathematics and physics can solve social problems began its life through the appearance of bitcoin. The genial idea on which is a bitcoin functioned is based on blockchain technology, whose potential reaches far

Adresa autora:

Mario Lukinović

mlukinovicmario@gmail.com



beyond the cryptocurrencies. Although there is still a controversy over the pseudonyms of Satoshi Nakamoto, his legacy has the potential to change the world. The success of bitcoin is in the advantages it has in relation to other similar currencies, but its importance goes beyond the benefits it has made. The banks do not need to store the data on money, property records and every bit of transaction stored by computers of all network users in a common database - blockchain. All transactions are much faster than banking, no tax, with drastically easier payment across state borders. Bitcoin provides to users security without identification, although blockchain registers a transaction, does not record who is behind it. The paper presents the basic principles on which bitcoin and other cryptocurrencies are based, the relationship between blockchain and bitcoin is explained.

Keywords: cryptocurrencies, digital money cryptography, blockchain, bitcoin.

1 UVOD

Ideal o novcu koji se ne oslanja na centralne institucije (koje mogu propasti, ali i koje vrše nadzor nad korisnicima), postojao je decenijama. U digitalnom svetu prvi ga je uobličio pisac naučne fantastike Nil Stivenson 1999. godine u svojoj noveli Kriptonomikon. On je opisao podzemni svet koji funkcioniše zahvaljujući digitalnom zlatu zasnovanom na kriptografiji, pri čijoj upotrebi korisnici ne moraju odavati ko su i šta su (Popper, 2016).

Kriptovalute (engl. *cryptocurrency*) su digitalne (virtualne) valute, koje iako su sredstvo razmene, još uvek nisu strogo regulisane zakonom u većini država, a u pojedinim su čak i zabranjene (Jovanović, 2014).

Da bi se razumeo nastanak i funkcionisanje kriptovaluta, neophodno je sagledati ih iz različitih uglova na kojima su one bazirane: matematici, sociologiji, ekonomiji, pravu i politici. To je verovatno i glavni razlog zbog koga veliki broj ljudi (uključujući i IT stručnjake i programere) ne znaju mnogo o ovoj temi. Takođe, šira javnost izjednačava pojmove blokčejna i bitcoina.

Sve kriptovalute su bazirane na jedinstvenom nizu brojeva za svaku jedinicu valute, koje korisnici mogu jedni drugima slati preko mreže. U prošlosti su se ti nizovi mogli lako kopirati i trošiti više puta, zbog čega nisu imali vrednost. Kriptograf Dejvid Čaum je taj problem rešio stvaranjem jedinstvene centralizovane knjige, u kojoj su se čuvale beleške o transakcijama svakog korisnika, čime ni jedna jedinica valute više nije mogla da se nalazi na dva mesta istovremeno (Bertlet, 2016).

Kriptovalute svoj nastanak duguju težnjama levo orijentisanih utopističkih posvećenika IT tehnologija koji su sanjali o univerzalnom novcu koji bi svako mogao da poseduje i troši, čija je

vrednost onolika koliko su korisnici voljni da plate (na principu ponude i potražnje), ali pre svega na liniji fronta za onlajn anonimnost i slobodu, bez cenzure i nadzora. Pojavi bitcoina prethodio je Sajberpankerski manifest Done Haravej (Haraway, 1985) koji počinje rečima: „U elektronsko doba, privatnost je neophodan uslov za postojanje otvorenog društva“.

Kriptovalute su univerzalni novac koji se može koristiti bilo gde u svetu, one su lako prenosive i teško se krivotvore.

Neki podaci pokazuju da tržište kriptovaluta danas iznosi gotovo 770 milijardi dolara. Od pojave prvih digitalnih valuta do danas, nastalo je preko 1.300 aktivnih kriptovaluta koje se razlikuju prema svojim svojstvima i upotrebi.

Prema odredbama Zakona o Narodnoj banci Srbije celokupni unutrašnji promet u Republici Srbiji izražava se u dinarima, osim ako nekim zakonom nije drukčije određeno. „Zakonom o platnom prometu propisano je da se poslovi platnog prometa obavljaju u dinarima, a Zakonom o deviznom poslovanju da se plaćanje, naplaćivanje i prenos između rezidenata i između rezidenata i nerezidenata u Republici Srbiji vrši u dinarima, a izuzetno se može vršiti i u devizama u slučajevima koji su propisani ovim zakonom“ (NBS, 2014).

Tržište kriptovaluta u Srbiji postoji, sve je veći broj rudara. Iako trgovanje kriptovalutama nije nelegalno, Narodna Banka Srbije - NBS je u više saopštenja navela da one ne predstavljaju zakonsko sredstvo plaćanja u Republici Srbiji. Takođe, zbog toga što ih ne izdaje centralna banka, NBS za korišćenje virtuelnih valuta, ulaganje u njih, kao ni za njihovu vrednost. Narodna banka Srbije je više puta upozoravala javnost da virtuelne valute ne predstavljaju

zakonsko sredstvo plaćanja u Republici Srbiji (NBS, Politika – u vezi s bitcoinom, 2017).

Ukoliko kriptovalute promatramo kao novac onda njihove transakcije mogu biti upitne shodno Zakonu o sprečavanju pranja novca i finansiranja terorizma, gde je propisana obaveza preduzimanja radnji i mera za sprečavanje pranja novca, kao što su identifikacija stranaka koje trguju preko tih platformi, uzimanjem kopije ličnog dokumenta. Kako poslovanje platformi na kojima se vrše transakcije kriptovalutama nije zakonom regulisano u Republici Srbiji, a uglavnom ni u uporednom pravu, a čl. 552. Zakona o obligacionim odnosima Republike Srbije („Sl. list SFRJ“, br. 29/78, 39/85, 45/89 - odluka USJ i 57/89, „Sl. list SRJ“, br. 31/93 i „Sl. list SCG“, br. 1/2003 - Ustavna povelja) predviđa razmenu robe kao jedan od načina trgovine, otvara se put ka legalnoj trgovini kriptovalutama (Bubanja, 2017).

Praksa je pokazala da su se korisnici kriptovaluta kada su imali problem sa njima, obraćali vlastima i njihovim regulatornim telima, zbog čijeg su zaobilazjenja i smišljeni. Nažalost, korisnici ne uživaju pravnu zaštitu čak i kada je reč o trgovini putem registrovanih privrednih subjekta.

2 BITCOIN

Prva decentralizovana kriptovaluta koja se pojavila je bitcoin (eng. „Bitcoin“). Termin bitcoin označava istoimenu organizaciju, softver i protokol, kao i jedinicu mere ove kriptovalute (skraćeno BTC) (Bertlet, 2016). Koncept na kome se zasniva bitcoin prvi put je predstavljen 2008. godine u članku "Bitcoin: A Peer-to-Peer Electronic Cash System", a u januaru 2009. godine bitcoin je pušten u promet. Njegov tvorac nije poznat do danas i krije se iza pseudonima Satoši Nakamoto. Novu vrstu digitalne kriptovalute formirao je tako što je stvorio distribuirani sistem verifikacije. Bitcoin nastaje u procesu koji se naziva „rudarenje“ (engl. mining). Njegova jedinstvenost je u tome što je decentralizovana valuta, iza koje ne stoji nijedna država, niti banka. Bitcoin je digitalna valuta, koja nastaje i čuva se elektronski.

Kriptovalute u cilju maksimizacije bezbednosti, upotrebljavaju metod - dokaz o radu (engl. *proof-of-work*), metod baziran na informacijama koje je teško stvoriti, ali koje ostalim učesnicima u rudarenju obezbeđuju laku proveru i verifikaciju transakcija. Kriptovalute se čuvaju na bitcoin

adresama za koje ključ predstavlja jedinstven niz slova i brojeva. Svaka transakcija bitcoinom se beleži u blokovima koji se zovu blokčejn. Transakcije se hronološki ređaju u blokove, u svakom se nalazi digitalni potpis prethodnog bloka, time se uređuje redosled i garantuje da novi blok može da se pridruži lancu samo ako počne na mestu na mestu završetka prethodnog. Jedan od osnovnih činilaca bezbednosti bitcoina je da se kopija svake izvedene transakcije beleži na svakom nalogu na kome je instaliran bitcoin softver. Blokčejnove neprekidno verifikuju računari svih korisnika softvera, tako sistem zna u bilo kom trenutku, koliko bitcoina svaki korisnik u svom novčaniku poseduje. Novčanik je program koji služi za slanje, primanje i skladištenje kriptovaluta. Digitalni novčanik sadrži prikaz količine kriptovalute koju korisnik poseduje, zapise o svim njegovim transakcijama, korisnički tajni ključ i njegove adrese (Bertlet, 2016). Novčanik je moguće instalirati na računar, mobilni telefon i tablet.

Falsifikovanje bitcoina nije moguće, jer iako vlasništvo može da se menja ono se ne može nikada duplirati (Bertlet, 2016). On je pseudo-anoniman, bitcoin mreža čuva sve podatke o svakoj transakciji koja se dogodila unutar mreže. Svako ko ima bitcoin softver i adresu na bitcoin mreži, može videti koliko novca ima na mreži, ali ne i kome oni pripadaju. Za razliku od otvaranja računa u bankama, otvaranje bitcoin računa (adrese) je brzo, bez troškova i „papirologije“. Jedna od glavnih prednosti bitcoin mreže je brzina transakcija.

Svako ko snagu svog računara posveti verifikaciji transakcija u blokčejnu može biti „rudar“. To je proces dodavanja transakcija u registar svih bitcoin transakcija. Rudarenje čini rešavanje matematičkog algoritma za čije se uspešno rešavanje dobija određena količina bitcoina.

Iako bitcoin ima reputaciju nestabilnosti, velikih fluktuacija i nezakonitog poslovanja, čemu mnogi pridodaju i urušavanje tradicionalnog koncepta nacionalnih država, ipak većina se slaže u tome da je njegova pojava najvažnija nova ideja od stvaranja Interneta (Vigna & Casey, 2016).

Razloga za uspeh bitcoina ima više. Finansijska kriza povoljno je uticala na njegov razvoj, poverenje u postojeći finansijski ali i politički

sistem je bilo poljuljano i brojni korisnici su u njemu prepoznali drugačije rešenje.

Anonimnost koju pruža prilikom transakcija jedan je od ključnih razloga njegovog uspeha. Prilikom digitalnog plaćanja bitkoinom u većini slučajeva nije potrebno davanje ličnih podataka. Ovakva vrsta anonimnosti, nažalost pogodovala je i usponu tamne strane upotrebe i popularnosti bitkoina u kriminalnim krugovima.

Računi u bitkoinu nisu opterećeni visokim bankarskim dažbinama.

Takođe, nije beznačajan ni potencijal plaćanja izdataka koji su manji od trenutnih ograničenja u konvencionalnim transakcijama na internetu (npr. naplata čitanja jednog novinskog članka ili preskoči reklamu, koji koštaju manje od 20 ili 30 centi kolika je najmanja transakcija) (Popper, 2016).

Kao što su svi učesnici na internetu povezani protokolima (TCP/IP, FTP, SMTP, HTTP i dr.) zahvaljujući kojima mogu međusobno da komuniciraju, bitkoin je stvorio svoje softverske protokole koji uređuju funkcionalna pravila upravljanja sistemom.

Bitkoin je omogućio novi način stvaranja, čuvanja i transfera novca.

Od svog nastanka bitkoin se unapređivao, podržan od internet zajednice, posebno od posvećenika slobodi interneta i anonimnosti, mnogi od problema koji su uočeni su rešavani zajedničkim naporom internet zajednice.

3 BLOKČEJN

Blokčejn (engl. blockchain) nije samo bitkoin, on je tehnologija za koju mnogi predviđaju da će promeniti svet (OECD, 2018).

Ukoliko bismo pojednostavljeno opisivali blokčejn mogli bismo da kažemo da je to nova vrsta baze podataka, iako bi to bilo pojednostavljeno objašnjenje slično kao kada bi smo imejl (email) opisali kao novi način za slanje pisama.

Iako blokčejn jeste nova vrsta baze podataka, to ne objašnjava u dovoljnoj meri genijalnost načina na koji funkcioniše.

Kada bilo gde i bilo kada položimo novac, oslanjamo se na zapis u bazi podataka treće strane, banke, firme i sl. Poverenje u banke

zasnovano je na zakonu koji reguliše rad banke, poverenju u državu da će u slučaju propasti banke država nadoknaditi klijentima njihov ulog.

Kada plaćamo on line usluge ili vršimo neku drugu transakciju kreditnim karticama, poklanjamo poverenje kompanijama koje posreduju u našem plaćanju (Mastercard, VISA i dr.) koje za to uzimaju određenu materijalnu nadoknadu. Čak i prilikom tradicionalnih oblika plaćanja gotovinom u papirnom novcu, mi dajemo papir na kome je ispisana vrednost za koju prodavac veruje da će mu biti isplaćena (ili garantovana) od strane vlade koja ju je štampala. Digitalno plaćanje zbog prisustva trećih strana (banke, kreditne kompanije i dr.) uvek je bilo moguće pratiti. I kod plaćanja gotovinom klijenti veruju bankama i kreditnim kompanijama koje rukovode platnim karticama, da imaju pouzdane baze podataka. I vlade država veruju da banke i kreditne kompanije vode baze podataka koje su tačne i pouzdane.

Baze podataka sadrže mnoštvo ličnih podataka, od npr. medicinske dokumentacije u domu zdravlja koja sadrži važne informacije o nama i našem zdravstvenom stanju, kada smo i od koje bolesti bolovali, koje lekove smo koristili i sl. I druge baze podataka sadrže mnoštvo naših ličnih podataka koje su važne ne samo za nas, već i za državu, grad, privredu, druge građane itd.

Osim što omogućava anonimne i sigurne transakcije, blokčejn ima i potencijal da sačuva sve vredne informacije, od podataka o rođenim i umrlim, preko osiguranja, do katastarske nepokretnosti, pa čak i glasova (Tapscott, 2018).

Sagledavši mogućnosti koji blokčejn nudi u transformaciji industrija i tržišta, povećanju transparentnosti i poverenja između građana, kao i olakšanom pristupu tržištu (uz bolju efikasnost transakcija), ali i rizicima koje sa sobom nosi, Organizacija za ekonomsku saradnju i razvoj - OECD organizovala je od 4. do 5. septembra 2018. godine Forum politike OECD-a za blokčejn. To je bila ujedno i prva glavna međunarodna konferencija na kojoj se razmatrao uticaj blokčejna na aktivnosti vlada i javnih prioriteta. Forum se bavio prednostima i rizicima blokčejna za ekonomiju i društvo, pokušajem određivanja adekvatnog regulatornog pristupa, kao i javnih politika prema blokčejnu.

Učesnici Foruma su diskutovali o mogućnostima globalnog ekonomskog uticaja blokčejna,

njegovim implikacijama na privatnost i sajber bezbednost, upotrebi blokčejn tehnologija za povećanje inkluzivnosti, njegovoj upotrebi u promovisanju zelenog rasta i održivosti, kao i jačanju kapaciteta javne uprava i primene u praksi (OECD, 2018).

4 ZAKLJUČAK

Pre bitcoina bilo je mnoštvo neuspelih pokušaja stvaranja digitalnih valuta (digikeš, heškeš, Fejsbuk kredit i dr.). Uspeh bitcoina leži u prednostima koje ima u odnosu na druge slične valute, ali njegov značaj prevazilazi i pogodnosti koje je doneo.

Svaki korisnik bitcoina ima potpunu kontrolu nad novcem na svom računu (adresi), jedino osoba sa privatnim ključem može pristupiti bitcoinima na toj adresi. Banke nisu potrebne za čuvanje podataka o novcu, evidenciju o imovini i svakoj transakciji bitcoina čuvaju računari svih korisnika mreže u zajedničkoj bazi podataka blokčejnu. Sve transakcije su mnogo brže od bankarskih, bez taksi, uz drastično lakše plaćanje preko državnih granica.

Bitcoin svojim korisnicima pruža bezbednosti bez identifikacije, iako blokčejn beleži transakciju, ne beleži ko stoji iza nje. Zahvaljujući peer-to-peer komunikaciji i kriptografiji, povezivanje bitcoin transakcija sa osobom u stvarnom životu je veoma teško. To je u ujedno možda i njegova najveća mana, jer su oporezivanje i nadzor nad korisnicima krajnje teški.

Garancija vrednosti bitcoina osmišljena je po uzoru na plamenite metale kojih ima ograničeno u prirodi. Zbog toga je Satoši u kodu bitcoina odredio da ih ima maksimalno 21 milion, te da ukoliko bitcoin protokol ostane isti, poslednji bitcoin će biti izrudaren 2140. godine. Do sada je izrudareno oko 17 miliona bitcoina, što znači da je ostalo 4 miliona, ili oko 19%.

Do sada je bitcoin uspeo da prevlada sve krize koje su ga zahvatile (u više slučajeva nestajali su iznosi koji su dostizali i 400 miliona dolara). Kakva god sudbina bitcoina bila u budućnosti, njegova uloga se neće moći zanemariti, prvenstveno zbog toga što je zahvaljujući njemu izneden blokčejn. Bez obzira na skepticima u vezi sa kriptovalutama, teško se mogu osporiti mogućnosti koje blokčejn pruža, pre svega u zaštiti baza podataka.

CITIRANA DELA

- Bertlet, D. (2016). *Darknet: u digitalnom podzemlju*. Beograd: Laguna.
- Bubanja, B. (2017). *Sve što bi trebalo da znate o trgovini kriptovalutama*. PC Press.
- Haraway, D. J. (1985). *A Cyborg Manifesto*. Manifestly Haraway, University of Minnesota Press. Preuzeto sa users.uoa.gr/~cdokou/HarawayCyborgManifesto.pdf
- Jovanović, U. (2014). *Kriptovalute*. Beograd: Matematički fakultet. Preuzeto sa <http://poincare.matf.bg.ac.rs/~vladaf/Courses/Matf%20MNSR/Prezentacije%20Individualne/>
- NBS. (2014, 10 2). *Narodna banka Srbije upozorava da bitcoin ne predstavlja zakonsko sredstvo plaćanja u Srbiji*. Preuzeto sa Narodna banka Srbije, Kabinet guvernera: <http://www.nbs.rs/internet/latinica/scripts/showContent.html?id=7605>
- NBS. (2017, 11 3). *Politika – u vezi s bitcoinom*. Preuzeto sa Narodna banka Srbije, Kabinet guvernera: <https://www.nbs.rs/internet/latinica/scripts/showContent.html?id=12079&konverzija=yes>
- OECD. (2018). *Distributed Ledgers: Opportunities and Challenges*. OECD Blockchain Policy Forum. OECD Conference Centre, Paris: OECD.
- Popper, N. (2016). *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*. Harper Paperbacks.
- Tapscott, D. (2018). *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World*. Portfolio.
- Vigna, P., & Casey, M. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order*. Picador.

Datum prve prijave: 14.09.2018.
Datum prijema korigovanog članka: 16.03.2019.
Datum prihvatanja članka: 27.03.2019.

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

Style – **APA** Sixth Edition:

Lukinović, M. (2019, 04 15). Kriptovalute, blokčejn i Bitcoin. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 85-90. doi:10.12709/fbim.07.07.01.10

Style – **Chicago** Sixteenth Edition:

Lukinović, Mario. 2019. „Kriptovalute, blokčejn i Bitcoin.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 85-90. doi:10.12709/fbim.07.07.01.10.

Style – **GOST** Name Sort:

Lukinović Mario Kriptovalute, blokčejn i Bitcoin [Časopis] // *FBIM Transactions* / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 85-90.

Style – **Harvard** Anglia:

Lukinović, M., 2019. Kriptovalute, blokčejn i Bitcoin. *FBIM Transactions*, 15 04, 7(1), pp. 85-90.

Style – **ISO 690** Numerical Reference:

Kriptovalute, blokčejn i Bitcoin. **Lukinović, Mario**. [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, *FBIM Transactions*, T. 7, str. 85-90.



INFORMACIJSKA SIGURNOST U BOSNI I HERCEGOVINI

INFORMATION SECURITY IN BOSNIA AND HERZEGOVINA

Branka Mijić

Fakultet za kriminalistiku, kriminologiju i sigurnosne studije, Sarajevo,
Bosna i Hercegovina

©MESTE

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

Apstrakt

U današnje vrijeme informacijsku sigurnost najčešće povezujemo s raznim internetskim prijetnjama poput hakerskih napada, virusa ili raznih drugih aplikacija koje imaju funkciju da naprave štetu našem računalu, informacijskom sustavu, a samim tim i informacijama. Međutim, informacijsku sigurnost treba promatrati u širem kontekstu. Moguće nekontrolirano „curenje“ važnih i vrijednih informacija izvan sustava predstavlja veliku prijetnju organizaciji, kompaniji. Možemo reći da informacije koje često mogu biti vrlo važne ili okarakterizirane kao tajne i povjerljive, nisu uvijek u elektronskom obliku, one mogu biti i u pisanim dokumentima, slikama, tablicama, grafikonima i sl. U današnje vrijeme, velika većina spomenutih informacija je u digitalnom obliku, te se tema ovog rada, odnosi na sigurnost informacija, rizicima, procjeni i upravljanju rizicima i zakonskim regulativama a sve u svrzi zaštite, odnosno, sigurnosti informacije i informacionog sustava, a za sve to je potrebna primjena standarda iz serije ISO27001.

Ključne riječi: *informacijska sigurnost, procjena rizika, upravljanje rizikom, zakonske regulative i ISO 27001.*

Abstract

At present, information security is most commonly associated with various Internet threats such as hacking attacks, viruses, or various other applications that have the potential to harm our computer, information system, and even information. However, information security should be seen in a wider context. Possible uncontrolled "leak" of important and valuable information outside the system poses a major threat to the organization, the company. We can say that information that can often be very important or characterized as secret and confidential, not always in electronic form, can be in written documents, pictures, tables, charts, etc. Nowadays, most of the information mentioned is in digital form,

the subject of this paper relates to the security of information, risks, risk assessment and risk management and legal regulations, all for the

Adresa autora:

Branka Mijić

[✉ brankica_mijic@net.hr](mailto:brankica_mijic@net.hr)



purpose of protection, respectively, information security and information system, and for all this it is necessary to apply ISO27001 standards.

Keywords: information security, risk assessment, risk management, legal regulations and ISO 27001.

1 UVOD

U vrijeme snažnog utjecaja globalizacije teško je pronaći područje poslovanja koje nije pod utjecajem informacijskih tehnologija. Sukladno tome, informacijski sustavi postali su nezaobilazni u današnjem visoko integriranom društvu. Visoka razina primijenjenosti, te visoka razina integriranosti informacijskih sustava nameće sve češća pitanja sa aspekta sigurnosti informacija. Informacijski sustav i informacije su postali stalna meta kao unutar organizacije, tako i izvana. Razloga tome je jako mnogo, jedan od tih razloga je to da je cilj napada uništenje ili promjena izvornih podataka ili krađa istih. Od 2000. godine informacijska sigurnost se počela znatnije razvijati, radi zaštite istih. Svjetske organizacije su sve više svjesne činjenice da su informacijski podaci postali nesigurni, te su se počele baviti ovom problematikom.

Najčešći vidovi napada na računarske mreže, Internet, tipa su: prisluškivanje, lažno predstavljanje, napad tipa ukidanje servisa, ponavljanje poslanih poruka, pogađanje lozinke, kriptanaliza, napadi tipa Trojanskog konja i virusi. Mogući načini odbrane od navedenih napada su sljedeći: šifriranje, primjena tehnologije digitalnog potpisa, procedura jake autentifikacije, korištenje jakih ključeva i česta izmjena ključeva, zaštita adresa servera, korištenje digitalnih certifikata kao jednoznačnih identificiranih parametara subjekata u komunikaciji, korištenje Smart kartica za generiranje digitalnog potpisa, više-nivovska virusna zaštita. (Sinkovski & Lučić, 2006)

Zbog toga mnoge tvrtke u svijetu posvećuju veliku pažnju zaštiti svojih informacija i informacijskoj sigurnosti primjenjujući ISO/IEC standard kao ključni element u upravljanju informacijskom sigurnošću. Informacijska sigurnost uključuje kako zaštitu informacijskog sustava, tako i samih informacija, bez obzira u kakvom obliku bile. Koncept informacijske zaštite je izuzetno širok, od tehničke mjere zaštite obuhvata i fizičku zaštitu, programske, logičke i administrativne mjere

zaštite. Sve te mjere su propisane normama iz serije standarda ISO/IEC 27000.

Informacijska sigurnost je jako važna javnim i privatnim organizacijama. Povezanost javnih i privatnih računalnih mreža i dijeljenje informacija otežava kontrolu pristupa informacijama. Upravljanje informacijskom sigurnošću zahtijeva sudjelovanje svih zaposlenika organizacije, a često je potrebna pomoć konzultanta izvan organizacije.

2 INFORMACIJSKA SIGURNOST

2.1 Pojam sigurnosti

Pleskonjić i dr. (Pleskonjić, Maček, Đorđević, & Carić, 2007) sigurnost definiraju kao proces održavanja prihvatljive razine, dok Hadjina (2013) i Krapac (1992) sigurnost opisuju kao proces smanjenja rizika ili vjerojatnosti nastajanja štete.

Sigurnost je osjećaj pojedinca da je zaštićen (*engl. safe, protected, secure, franc. sauf, njem. sicher, gesch tzt, gefahrlos*) od fizičke, društvene, duhovne, novčane, političke, ekonomske, osjećajne, profesionalne, psihološke, odgojne ili bilo koje druge prijetnje, ugroze, opasnosti, štete, povrede ili bilo kakvog događaja koji se može tumačiti kao neželjen. Isto tako, navodi da je sigurnost kontrola neizvjesnosti pri čemu se prepoznata opasnost svodi u granice prihvatljivog rizika. (Cingula, 2016)

Kada se govori o sigurnosti i zaštiti informacijskih sustava i mreža, nekoliko principa danas vrijede kao osnovni postulati:

1. Sigurnost je proces. Sigurnost nije gotov proizvod, usluga ili procedura, već skup koji ih sadržava, i još mnogo elemenata i mjera koje se stalno provode.
2. Ne postoji apsolutna sigurnost.
3. Uz različite metode tehničke zaštite, treba imati u vidu i ljudski faktor, sa svim slabostima.

2.2 Informacijska sigurnost

Informacijska sigurnost je disciplina kojoj je osnovni cilj osigurati zaštitu informacija i informacijskih sustava od neovlaštenog pristupa, korištenja, primjene ili uništavanja. (Antoliš, i

drugi, 2010) Informacija je jako važan resurs i kao takav je potrebno zaštititi, a to je iznimno zahtijevan posao s obzirom da su informacije izložene velikom broju prijetnji.

Cilj informacijske sigurnosti je zaštita informacija od velikog broja prijetnji u svrhu smanjenja poslovnih rizika, osiguranja poslovnog kontinuiteta, te povećanja broja poslovnih prilika i povrat od investicija. Važno je naglasiti da se informacijska sigurnost postiže primjenom raznih kontrola kao što je sigurnosna politika, razni procesi i procedure.

Danas se sve češće upotrebljava termin osiguranje informacija, kao zamjenski za pojam informacijska sigurnost, a sve zbog širokog značenja sigurnosti.

Osiguranje informacija predstavlja međudjelovanje tehnologije koja osigurava uvjete sigurnosti, procesa koji osnažuju djelovanje tehnologije i ljudi koji omogućavaju rad tehnologije u operativnoj uporabi. (Klaić, 2010)

Sustav informacijske sigurnosti se sastoji od uravnoteženog skupa sigurnosnih mjera, fizičke sigurnosti, sigurnosti podataka, sigurnosti informacijskih sustava, koordiniranog uvođenja formalnih procedura, kao što su procjene rizika, certificiranje uređaja i akreditacije tehničkih sustava za primjenu u određenim segmentima poslovnih procesa u institucijama. Uravnoteženost i koordiniranje mjera i postupaka treba da se postiže organizacijom i upravljanjem sustavom informacijske sigurnosti.

Informacijska sigurnost uključuje:

1. oporavak informacijskih sustava
2. detekciju i odvratanje napada
3. primjenu zakonski propisa koji se odnose na privatnost, računalni kriminal, računalnu forenziku i slično.

2.3 Sustav informacijskom upravljanja sigurnošću (ISMS)

Sustav upravljanja informacijskom sigurnošću (ISMS, engl. *Information Security Management System*) dio je sveukupnog sustava upravljanja, utemeljen na pristupu upravljanju rizicima, u cilju uspostavljanja, provođenja, praćenja, revidiranja, održavanja i unapređenja informacijske sigurnosti. (ISO/IEC, HRN ISO/IEC 27001:2005, 2005)

Da bi organizacija dobila certifikat koji potvrđuje upravljanje informacijskom sigurnošću organizacije moraju ispuniti skup zahtjeva koje definira standard ISO 27001. Osnovni koraci u implementaciji standarda ISO 27001 su početak projekta, definiranje ISMS-a, procjena rizika, upravljanje rizikom, obuka, priprema za reviziju, revizija i kontinuirano unapređenje.

Uspostava ISMS-a je važan zbog zaštite informacijske imovine što omogućuje organizaciji da postigne veću garanciju sigurnosti u zaštiti informacija i imovine od informacijskih rizika na kontinuiranoj osnovi, održava strukturiran sveobuhvatan radni okvir, identifikaciju i procjeni rizika informacijske sigurnosti, odabir i primjenu odgovarajući sigurnosni mjera (kontrola), te mjerenje i poboljšanje njihove učinkovitosti kao i da kontinuirano poboljšava kontroliranu okolinu, te da djelotvorno postiže zakonsku i regulatornu usklađenost.

Da bi se postavio temelj informacijske sigurnosti i odredio njezin okvir, te omogućilo razumijevanje sigurnosnih zahtjeva organizacije i potrebu za uspostavom ciljeva na području informacijske sigurnosti, upotrebljavaju se ISO standardi.

2.4 Definiranje sigurnosnih zahtjeva

Najvažnije za organizaciju je da identificiraju svoje sigurnosne zahtjeve, a to su: procjena rizika, izbor odgovarajućih kontrola i zakonske regulative (Hamidović, 2010):

- Procjena organizacijskih sigurnosnih rizika. Kroz procjenu rizika identificiraju se prijetnje imovini, ranjivosti, te procjena vjerojatnosti incidentne pojave i njenog potencijalnog utjecaja
- Kako bi rizik sveli na prihvatljiv nivo nakon identificiranja sigurnosnih zahtjeva i izrade procjene rizika, potrebno je izabrati i implementirati adekvatne kontrole. Izbor kontrola ovisi o instituciji, odnosno prihvatljivosti rizika i načinu upravljanja rizikom, ali i o državnim i međunarodnim zakonskim pravima i obvezama.
- Zakonom regulirane kontrole presudne za instituciju odnose se na zaštitu tajnosti osobnih podataka i informacija, čuvanje institucijskih izvješća i poštivanje prava intelektualnog vlasništva.

Proces upravljanja rizikom informacijske sigurnosti može se primijeniti na organizaciju kao cjelinu, ili na dio organizacije, bilo koji informacijski sistem.

2.5 Procjena rizika

ISO 27005:2018 (ISO, 2018) definira rizik informacijske sigurnosti kao potencijal da će prijetnja iskoristiti ranjivosti imovine i time uzrokovati štetu za organizaciju.

Rizik informatičko/internetske tehnologije je opasnost da njezina primjena dovede do neželjenih posljedica (šteta) u organizacijskom sustavu i/ili njegovoj okolini. Do zlouporabe uglavnom dolazi zbog dva razloga, i to radi ostvarivanja neopravdanih ili protupravnih koristi od strane pojedinaca ili organiziranih skupina ili radi nanošenja materijalne ili nematerijalne štete pojedincu, skupini ili zajednici. Najugroženiji su informacijski sustavi iz koji se može pristupiti Internetu, jer je i sam Internet izuzetno ugrožen. (Klasić & Klarić, 2009, str. 160)

Rizici kojima su tvrtke izložene u svom poslovanju i za koje minimalno moraju biti propisani postupci mjerenja, procjene i upravljanja uključuju i rizik koji proizlazi iz neadekvatnog upravljanja informacijskim i pridruženim tehnologijama. Upravljanje rizikom informacijskog sustava obuhvaća postupke procjene rizika te poduzimanja radnji za smanjenje rizika na prihvatljivu razinu i održavanje prihvatljive razine rizika. Tvrtke danas moraju obavljati mjerenje, procjenu i upravljanje svim rizicima kojima su u svom poslovanju izložene.

Rizik se uglavnom smanjuje na jedan od tri moguća načina (Uremović, 2009):

- Smanjivanje, provođenjem sigurnosnih kontrola – ovim se načinom primjenjuju sigurnosne kontrole koje smanjuju vjerojatnost ostvarivanja prijetnje ili smanjuju njezin utjecaj,
- Izbjegavanje rizika – bilo koja akcija kod koje se mijenjaju poslovne aktivnosti ili način vođenja poslovanja kako bi se spriječila pojava rizika, primjerice nekorištenjem e-trgovine ili Interneta za određene poslovne aktivnosti, izbjegava se čitav niz prijetnji koje vrebaju uslijed ovakvog načina poslovanja,
- Prenošenje rizika – ovim se načinom uglavnom pokrivaju rizici kod kojih bi primjena

sigurnosnih kontrola bila neekonomična, pa se pribjegava prenošenju rizika na drugu organizaciju, primjerice ugovaranjem polica osiguranja i sl.

3 UPRAVLJANJE INFORMACIJSKOM SIGURNOŠĆU

3.1 Upravljanje i procjena rizika

Upravljanje rizicima općenito, znači baviti se pojmom vjerojatnosti. Svaki događaj koji se dogodi i koji za posljedicu ima određeni učinak nosi određenu vjerojatnost, te su vjerojatnosti podaci koji se najčešće izračunavaju naknadno i koji služe za retroaktivnu analizu u procesima upravljanja rizicima.

Upravljanje rizicima može se općenito definirati kao identifikacija, procjena i prioritizacija rizika, nakon kojih slijedi koordinirana i ekonomična uporaba sredstava kako bi se smanjila, nadzirala i bolje kontrolirala vjerojatnost i/ili utjecaj neželjenih događaja.

Upravljanje rizicima možemo istaći u dvije faze i to:

- procjena rizika,
- obrada rizika

Procjena rizika u oblasti sigurnosti informacija, podrazumijeva prepoznavanje uzroka koji bi mogli dovesti do neželjenih ishoda, tj. proučavanje vjerojatnoće pojavljivanja i težine posljedica koje oni izazivaju. U okviru tog procesa potrebno je uzeti u obzir sve raspoložive informacije, kao i sve ostale potrebne resurse. Konkretnije, procjena rizika u oblasti sigurnosti informacija podrazumijeva procjenu vjerojatnoće pojavljivanja i težine posljedica neželjenih događaja koji narušavaju sigurnost informacija, tj. njihovu povjerljivost, cjelovitost i raspoloživost.

Prilikom procjene rizika dodjeljuju se vrijednosti vjerojatnosti i posljedici rizika. Ove vrijednosti mogu biti kvantitativne ili kvalitativne. Tako možemo reći da se procjena rizika temelji se na procjeni posljedica i vjerojatnosti.

Nakon procjene slijedi korak koji je izbor i provođenje mjera zaštite kako bi se rizici umanjili, odnosno njihove posljedice izbjegle ili barem ublažile.

Nakon provođenja koraka koji obuhvaćaju praćenje, mjerenje i izvještavanje o riziku može se

govoriti o upravljanju rizikom u oblasti sigurnosti informacija koje je potrebno utemeljiti na detaljno razrađenim planovima.

Poslije procjene rizika, slijedi obrada rizika. Obrada rizika uključuje određivanje prioriteta, procjenu, odabir i provođenje sigurnosnih kontrola za smanjivanje rizika. Prilikom pravljenja plana za obradu rizika, prvo se pristupa opisu kako se procijenjeni rizici trebaju tretirati, da bi zadovoljili kriterije prihvatljivosti. Da bi plan bio prihvaćen potrebno je da rukovodstvo organizacije pregleda i odobri predložene planove obrade rizika i rezultirajuće zaostale rizike, te da se dokumentiraju uvjeti povezani s takvim odobrenjem.

Kriteriji prihvatljivosti rizika mogu biti složeniji od pukog utvrđivanja da li se ili ne preostali rizik nalazi iznad ili ispod praga prihvatljivosti. Prihvaćanjem rizika potrebno je osigurati da su preostali rizici izričito prihvaćeni od rukovodstva organizacije.

3.2 Analiza rizika

Analiza rizika je postupak kojem je cilj da se ustanove ranjivosti sustava, uoče potencijalne prijetnje (rizici), te da na odgovarajući način kvantificirati moguće posljedice kako bi se mogao odabrati najprimjereniji način zaštite, odnosno procijeniti opravdanost uvođenja dodanih protumjera. Analiza rizika se sastoji od identifikacije rizika, opisa rizika i procjenjivanju rizika. Rezultati analize rizika se mogu koristiti za dobivanje profila rizika koji daje ocjenu značajnosti za svaki rizik i osiguranje instrumentarija za definiranje prioriteta u reguliranju rizika.

Postoje dva temeljna pristupa analizi rizika: kvantitativna i kvalitativna analiza. Kvantitativna analiza podrazumijeva iskazivanje rizika u očekivanim novčanim troškovima na godišnjoj razini, dok rezultat kvalitativne analize iskazuje samo relativan odnos vrijednosti šteta nastalih djelovanjem neke prijetnje i uvođenja protumjera.

Nakon završetka procesa analize rizika, potrebno je usporediti procijenjeni rizik sa kriterijima rizika koje je organizacija ustanovila.

3.3 Standardi informacijske sigurnosti

Da bi se postavio temelj informacijske sigurnosti, odredili njeni okviri, te omogućilo razumijevanje

sigurnosnih zahtjeva organizacija, kompanija, te potreba za uspostavljanjem ciljeva na području informacijske sigurnosti, upotrebljavaju se standardi (ISO).

Slijed standarda ISO27000 (Rječnik termina koji se koriste unutar ISO 2700 serije standarda) sadrži set smjernica i specifikacija za pomoć organizacijama u razvoju sustava upravljanja informacijskom sigurnošću.

Standardi su od velike važnosti za sigurnost informacijskog sustava su:

- ISO 27001 (ISO/IEC, HRN ISO/IEC 27001:2005, 2005), zamjena za BS7799-2 – predstavlja sustav za upravljanje informacijskom sigurnošću, temeljni standard ISO 27000 serije standarda, a definira zahtjeve za uspostavu, implementaciju, rad, nadzor, reviziju, održavanje i poboljšanje dokumentiranog sustava upravljanja informacijskim sustavom;
- ISO 27002 (2013) – Zbirka pravila, odnosno postupaka za upravljanje informacijskom sigurnošću.

Da bi se uspostavio kvalitetan sustav za upravljanje sigurnošću informacijama, potrebno je uvesti u upotrebu oba standarda. Oba ova standarda glavni su međunarodni standardi informacijske sigurnosti koje je objavila Internacionalna organizacija za standardizaciju (ISO). Ovi standardi su važni zahvaljujući činjenici da ih je moguće primjenjivati skoro u svim organizacijama jer osiguravaju fleksibilnost, definiraju upravljački okvir, a pri tom ne ulaze u konkretnu tehničku implementaciju.

Pored ova dva standarda postoje i upotrebljavaju se još i standardi i to:

- ISO 27003 – Vodič za implementaciju ISMS (ISO/IEC 27003, 2017);
- ISO 27004 – Mjerenje i metrika efikasnosti informacijske sigurnosti (ISO/IEC 27004, 2016);
- ISO 27005 – Upravljanje rizicima informacijske sigurnosti (ISO/IEC 27005:2018, 2018);
- ISO 27006 – Zahtjevi za postupkom analize i certificiranja standarda (ISO/IEC 27006, 2015);

Najnovija inačica ovog standarda je objavljena 2013. godine, te je sadašnji puni naziv ISO/IEC 27001:2013. Najvažnije izmjene u verziji 2013. se odnose na strukturu glavnog dijela standarda, zainteresirane strane, ciljeve, praćenje i mjerenje. Međutim, sve te izmjene nisu zapravo mnogo promijenile standard u cjelini – njegova temeljna filozofija se i dalje bazira na procjeni i obradi rizika, a zadržane su iste faze uspostave, primjene, pregledavanja i poboljšavanja. Ova nova verzija standarda je lakša za čitanje i razumijevanje, te je mnogo jednostavnija za integriranje s drugim standardima upravljanja kao što su ISO 9001, ISO 22301, itd. (ISO/IEC, ISO/IEC 27000 family - Information security management systems, 2018)

3.4 Zakonska regulativa - Sigurnost informacijskog sustava u BiH

Bosna i Hercegovina je zemlja koja je ne tako davno izašla iz ratnog perioda, a i složenog je državnog ustroja sa dva entiteta (Entitet Federacije BiH i Entitet Republike Srpske) i Brčko Distrikt. Ekonomski i socijalni uvjeti u Bosni i Hercegovini su loši, što je i rezultat sporijeg razvoja informacijskih sustava kako u organizacijama tako i u državnim tijelima, tj. danas su na dosta nižoj razini nego u ostalim razvijenim zemljama u okruženju.

Zakonske regulative po pitanju informacijske sigurnosti u Bosni i Hercegovini doneseni su samo par okvirnih zakona koji pokrivaju ovu oblast, sam zakon, kao „Zakon o informacijskoj sigurnosti“ ne postoji, mada je za njega urađen nacrt, a bilo je i nekoliko prijedloga ali do dan danas nije usvojen.

Dok se čeka usvajanje ovog zakona, po pitanju informacijske sigurnosti u Bosni i Hercegovini, postoje zakoni koji su izuzetno značajni po ovom pitanju, a to su:

- Zakon o zaštiti tajnih podataka (Službeni glasnik BiH br. 54/05. i prečišćeni 12/09.);
- Zakon o zaštiti osobnih/ličnih podataka (Službeni glasnik BiH br.32/01, 49/06, 76/11. i prečišćeni 89/11.);
- Zakon o centralnoj evidenciji i razmjeni podataka (Službeni glasnik br.32/01, 16/02, 32/07. i 44/07 (prečišćeni));
- Zakon o komunikacijama (Službeni glasnik BiH br. 31/03, 75/06, 32/10 i 98/12. ;
- Odluka - Politika upravljanja informacijskom sigurnošću u institucijama Bosne i

Hercegovine, za razdoblje 2017 - 2022. godine (Službeni glasnik BiH br.38/17.),

U Parlamentu BiH je u proceduri Zakon o Agenciji za razvoj informacijskog društva (ZARID) od listopada 2008.godine, ali do danas nije donesen. Za razliku od ovoga, formirana je Agencija za zaštitu osobnih podataka, prema preporukama Europske unije (EU) koja jednim dijelom radi i na zaštiti informacijskih sustava institucija BiH, ali samo u segmentu administracije i upravljanja /radio-relejnog mrežom putem koje su povezane sve institucije BiH).

U Entitetu Republike Srpske formirana je Agencija za informacijsko društvo koji se bavi stanjem informacijskog sustava (AIDRS- koje je počelo sa radom 01.07.2015.godine, Službeni glasnik RS br.70/11.) što nažalost, ista nije usvojena i na državnoj razini.

Za razliku od Bosne i Hercegovine kao države koja nema CERT (*Computer Emergency Response Team*) koja bi se bavila koordinacijom i suradnjom u rješavanju sigurnosnih incidenata između zemalja, radili na edukaciji korisnika Interneta i državne mreže na prevenciji sigurnosnih incidenata, Entitet Republike Srpske ima oformljeno „Odjeljenje za informacijsku bezbjednost“ (OIB) koji vrši funkciju CERT-a Republike Srpske. OIB – CERT Republike Srpske je za sada jedini organ ove vrste u Entitetu Republike Srpske i Bosne i Hercegovine. (CERT RS, 2019)

4 ZAKLJUČAK

Suvremena poslovna praksa pokazuje da se, danas, sigurnost informacija ne tiče samo sektora informacijskog sistema već se tiče cjelokupnog poslovanja jer se sve odluke i rješavanja problema na nivou organizacije se moraju temeljiti na informacijama. Primjene novih tehnologija, organizacije sve teže mogu da prežive na tržištu koje se sve više globalizira. Svjedoci smo da su, informacije i informacioni resursi (hardverski i softverski) danas mnogo više izloženi brojnim prijetnjama po sigurnost, te se koncept zaštite, odnosno sigurnosti informacija nameće kao jedan od prioriteta poslovanja.

Unutar organizacijskih informacijskih sistema sve više se prikupljaju, obrađuju, pohranjuju i razmjenjuju podaci i informacije od vitalnog

interesa za organizaciju, a nerijetko i od društvenog interesa, njihov neometan rad postaje preduvjetom, ne samo njihovog funkcioniranja već sve više i cijelog društva, koje se na njih sve više oslanja. Budući da je to moguće postići samo ako postoji zadovoljavajući stepen njihove sigurnosti, načelo sigurnosti je jedan od temelja njihovog rada.

Organizacije bi prilikom zaštite svojih informacija i svoga informacijskog sustava trebale prvo da obave analizu rizika informacijske sigurnosti, zatim da dokumentiraju rezultate analize, zatim da implementiraju odgovarajuće sigurnosne mjere. Procjenom rizika određuje se vrijednost informacijske imovine, identificiraju primjenjive prijetnje i ranjivosti, identificiraju postojeće sigurnosne kontrole i njihov utjecaj na identificirane rizike, određuju potencijalne posljedice i konačno određuje prioritet identificiranih rizika.

Rizici su dinamični. Prijetnje, ranjivosti, vjerojatnosti ili posljedice mogu se promijeniti naglo bez nagovještaja o promjeni.

Upravljanje informacijskom sigurnošću i kontinuitetom poslovanja, te upravljanje rizicima informacijske sigurnosti zakonska je, moralna i poslovna obaveza svake organizacije i društva, te

se stoga treba stalno pratiti, pregledati i poboljšavati, te bi trebalo postati obvezna i razumna aktivnost svake organizacije. Uspostava normi i standarda zahtijeva razumijevanje i iskustvo u uspostavi odredbi iste. Standard ISO 27001 se može promatrati kao model tj. dobra praksa u obliku smjernica i preporuka za osiguranje djelotvornog sistema sigurnosti informacija. Primjenom standarda se stvara sistem koji je fokusiran na poboljšavanja i smanjenje incidenata, a što je najvažnije je eliminiranje uzročnika grešaka i incidenata u samom sistemu.

Iz navedenog je vidljivo da je informacijska sigurnost u Bosni i Hercegovini još uvijek na niskoj razini, a za to je najveći krivac nedostatak zakonskih regulativa koje država iz samo njoj poznatih razloga do sada nije usvojila, te zanemarivanje informacijske tehnologije (IT) od strane države. Ne postoji Agencija na državnom nivou koja bi se bavila ovom problematikom, kao što ne postoji ni okvirni zakon. Pozitivno je jedino to što je sve veći broj organizacija i institucija koji su svjesni vrijednosti informacija, te je sve veće interesiranje organizacija za ovu oblast i porast broja certifikata izdanih po ovim standardima, a i zbog zahtjeva EU, te Agende za Jugoistočnu Europu.

CITIRANA DELA

Antoliš, K., Ždrnja, B., Pakšić, I., Vugrek, A., Pavliček, J., Marijenović, I., . . . Jušić, S. (2010). *Sigurnost informacijskih sustava*. Zagreb: Algebra d.o.o.

CERT RS. (2019). *CERT RS Odjeljenje za informacionu bezbjednost*. Preuzeto sa <https://oib.aidrs.org/>

Cingula, M. (2016). KORPORATIVNA SIGURNOST - Pojam sigurnosti i temeljni srodni pojmovi. U B. Vukelić, *Sigurnost informacijskih sustava* (str. 6). Rijeka: Veleučilište u Rijeci.

Hajdina, N. (2013). *Osnove informacijske sigurnosti*. Zagreb: FER - Zavod za primijenjeno računarstvo.

Hamidović, H. (2010). Upravljanje rizikom informacijske sigurnosti. *Telekomunikacije*, 33-37.

ISO. (2018). *ISO 27005:2018 Information technology -- Security techniques -- Information security risk management*. Preuzeto sa ISO: <https://www.iso.org/standard/75281.html>

ISO/IEC. (2005, 10 27). *HRN ISO/IEC 27001:2005*. Preuzeto sa Hrvatski zavod za norme: <https://www.iso.org/news/2005/10/Ref976.html>

ISO/IEC. (2018). *ISO/IEC 27000 family - Information security management systems*. Preuzeto sa ISO: <https://www.iso.org/isoiec-27001-information-security.html>

ISO/IEC 27002. (2013, 10). *Information technology -- Security techniques -- Code of practice for information security controls*. Preuzeto sa ISO: <https://www.iso.org/standard/54533.html?browse=tc>

- ISO/IEC 27003. (2017, 03). *Information security management systems — Guidance*. Preuzeto sa ISO: <http://www.iso27001security.com/html/27003.html>
- ISO/IEC 27004. (2016, 12). *Information security management — Monitoring, measurement, analysis and evaluation*. Preuzeto sa ISO: <https://www.iso.org/standard/64120.html?browse=tc>
- ISO/IEC 27005:2018. (2018, 07). *Information technology -- Security techniques -- Information security risk management*. Preuzeto sa ISO: <https://www.iso.org/standard/75281.html?browse=tc>
- ISO/IEC 27006. (2015, 10). *Requirements for bodies providing audit and certification of information security management systems*. Preuzeto sa ISO: <https://www.iso.org/standard/62313.html?browse=tc>
- Klaić, A. (2010, 02 08). *Pregled stanja i trendova u suvremenoj politici informacijske sigurnosti i metodologijama upravljanja informacijskom sigurnošću*. Preuzeto sa FER - Fakultet elektrotehnike i računarstva: https://www.fer.hr/_download/repository
- Klasić, K., & Klarić, K. (2009). *Informacijski sustavi*. Zagreb: Intus informatika.
- Krapac, D. (1992). *Kompjuterski kriminalitet*. Zagreb: Pravni fakultet.
- Pleskonjić, D., Maček, N., Đorđević, B., & Carić, M. (2007). *Sigurnost računarskih sistema i mreža*. Beograd: Mikro knjiga.
- Sinkovski, S., & Lučić, B. (2006). Informaciona bezbednost i kriptografija. *ZITEH 2006* (str. R25 1-16). Beograd: IT Veštak. Preuzeto sa <http://www.itvestak.org.rs/media/biblioteka/zbornik-radova-ZITEH-06.zip>
- Uremović, D. (2009). Kako upravljati IT rizicima. *InfoTrend*(5), 42-47.

Zakoni:

- Zakon o zaštiti tajnih podataka (Službeni glasnik BiH br. 54/05. i prečišćeni 12/09.;
- Zakon o zaštiti osobnih/ličnih podataka (Službeni glasnik BiH br.32/01, 49/06, 76/11. i prečišćeni 89/11.;
- Zakon o centralnoj evidenciji i razmjeni podataka (Službeni glasnik br.32/01, 16/02, 32/07. i 44/07 (prečišćeni));
- Zakon o komunikacijama (Službeni glasnik BiH br. 31/03, 75/06, 32/10 i 98/12. ;
- Službeni glasnik BiH, broj 38/17 Odluka - Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine, za razdoblje 2017 - 2022. godine

Datum prve prijave: 01.09.2018.
Datum prijema korigovanog članka: 24.03.2019.
Datum prihvatanja članka: 27.03.2019.

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

Style – APA Sixth Edition:

Mijić, B. (2019, 04 15). Informacijska sigurnost u Bosni i Hercegovini. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 91-99. doi:10.12709/fbim.07.07.01.11

Style – Chicago Sixteenth Edition:

Mijić, Branka. 2019. „Informacijska sigurnost u Bosni i Hercegovini.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 91-99. doi:10.12709/fbim.07.07.01.11.

Style – GOST Name Sort:

Mijić Branka Informacijska sigurnost u Bosni i Hercegovini [Časopis] // FBIM Transactions / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 91-99.

Style – Harvard Anglia:

Mijić, B., 2019. Informacijska sigurnost u Bosni i Hercegovini. *FBIM Transactions*, 15 04, 7(1), pp. 91-99.

Style – ISO 690 Numerical Reference:

Informacijska sigurnost u Bosni i Hercegovini. **Mijić, Branka.** [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, FBIM Transactions, T. 7, str. 91-99.



PRAVNA REGULATIVA DEČIJE PORNOGRAFIJE NA INTERNETU

LEGAL REGULATION OF CHILDREN'S PORNOGRAPHY ON THE INTERNET

Živanka Miladinović Bogavac

Poslovni i pravni fakultet, Univerzitet Union Nikola Tesla, Beograd, Srbija

©MESTE

JEL kategorija: **K1, L86**

Apstrakt

Dečija pornografija, tj. zloupotreba dece u pornografske svrhe, nesporno je veliki problem društva u eri kada se prava čoveka i deteta stavljaju na prvo mesto. Ona je i ozbiljan kriminološki, sociološki i viktimološki problem, te se njime bave i stručnjaci raznih naučnih sfera, a ne samo pravnici. Iskorišćavanje dečijeg psihičkog i fizičkog integriteta doživljava svoju ekspanziju, nasuprot preventivnim i restriktivnim naporima međunarodne zajednice kao i naporima Republike Srbije da se taj problem na legalan način suzbije. Vode se brojne naučne rasprave širom sveta, kojima se pokušava doći do „idealnog“ rešenja. Moderno doba olakšava ekspanziju dečije pornografije sa razvojem tehnologija. Sa nastankom modernih računara i programa razvila se najpoznatija svetska društvena mreža koja ima širok spektar funkcija i mogućnosti - internet. Ona svakako ima svoje pozitivne strane, na prvom mestu što omogućuje ljudima da se povezuju širom sveta, komuniciraju, upoznaju, razmenjuju informacije i iskustva preko poruka, slika, snimaka... Sve pozitivne strane interneta su podložne i zloupotrebi. Kako je velika količina informacija postala lako dostupna korisnicima širom sveta, ona je počela da predstavlja i pogodnu osnovu za vršenje različitih krivičnih dela. Mogućnost anonimnosti na internetu, slobodan protok sadržaja i dostupnost tom istom sadržaju, stvaraju brojne opasnosti, od kojih je jedna dečija pornografija.

Ključne reči: dečija pornografija, pornografija, visokotehnološki kriminal, internet, zloupotreba dece

Abstract

Child pornography i.e. abuse of children for pornographic purposes, it's a big problem of today's society in an era when human and children's rights are placed first. It is also a serious criminological, sociological and victimological problem, so it is dealt with by not only lawyers, but also experts of various scientific fields. Exploitation of children's psychological and physical integrity is experiencing its expansion, as opposed to preventive and restrictive efforts of the international community, as well as efforts of the Republic of Serbia to suppress this problem in a legal way. Numerous scientific discussions are being held around the world, their purpose being an attempt to reach an "ideal" solution. With the development of technology, modern age facilitates expansion of child pornography. The world's most

Adresa autora:

Živanka Miladinović Bogavac

zivankamiladinovic@gmail.com



famous social network that has a wide range of functions and possibilities – the internet – has developed with emergence of modern computers and programs. It certainly has its positive sides, primarily because it allows people all over the world to connect, communicate, meet, share information and experiences through messages, pictures, recordings... All positive sides of the internet are also susceptible to abuse. As a large amount of information became easily accessible to users around the world, it has also become a good basis for commission of various criminal offenses. The possibility of anonymity on the internet, the free flow of content and access to that very same content create many dangers, one of which is child pornography.

Keywords: *child pornography, pornography, high technology crime, internet, child abuse*

1 POJAM I TEORIJSKO ODREĐENJE DEČIJE PORNOGRAFIJE

Nesporno pojam dečije pornografije treba nedvosmisleno odrediti zbog poštovanja načela zakonitosti odnosno njegovog segmenta koji glasi „nulla poena sine lege stricta“, tj. da se ne mogu stvarati inkriminacije po osnovu sličnosti, odnosno da se analogija ne može primeniti na kreiranje krivičnih dela i kazni za njih. (Škulić, 2010)

U cilju svestranog i potpunog izučavanja samog pojma i značenja dečije pornografije, na samom početku rada poći ćemo od etimologije reči „pornografija“. Na izvornom grčkom jeziku, pojam „pornografija“ vodi poreklo od reči „porne“ koja označava prostitutku, i reči „graphein“ što bi se moglo prevesti kao „pisati“ ili „beležiti“. Prema Šoliću, izvorno značenje ove reči označava opisivanje radnji i ponašanja bludnica. On ističe da se pojam pornografije često neopravdano meša sa pojmom erotike koji nesumnjivo nosi šire atribute od samog predstavljanja seksualnog čina. (Šolić, 1991) Ako ovo značenje stavimo u današnji društveni kontekst, možemo dobiti različite definicije ovog pojma, koje se uvek svode na istu suštinu. Komlen-Nikolić i saradnici (2010) navode da pornografska sadržina na eksplicitan i specifičan način prikazuje seksualne odnose sa isticanjem pojedinih detalja. Takođe, korisna definicija ovog pojma se nalazi i u članu 252. Krivičnog zakona SFRJ o proizvodnji i rasparčavanju pornografskih spisa, koji navodi da pornografija obuhvata spise, slike i druge predmete koji teško vređaju moral. (Zakon, Krivični zakon SFRJ, 1977) Najpreciznija definicija pornografije bi bila ona koju je dao V. Slavković, a to je da se pod njom podrazumeva „seksualno eksplicitni materijal čiji je primarni cilj izazivanje seksualnog uzbuđenja kod gledalaca“. (Slavković, 2014)

Prihvatajući ovu definiciju pornografije, prvi vid dečije pornografije postojao u Kini u knjizi „Predivni diskursi obične devojčice“ u 12. veku. (Uljanov & Ivanović, 2009) Ipak dečija pornografija kakvu danas poznajemo ekspanziju doživljava sa nastankom kamere, a to je sredina 19. veka.

60-ih i 70-ih godina 20. veka dolazi do značajnijeg organizovanog kriminalnog prisustva dečije pornografije. (Stanić, 2007) Veliki broj fotografija i časopisa ovakvog sadržaja (gde su deca predstavljena u eksplicitnom seksualnom kontekstu) je postojao najviše u zemljama poput Švedske, Norveške i Holandije. Prema nekim mišljenjima, razlog zašto su se najviše pornografski magazini i filmovi krijumčarili u Sjedinjene Američke Države i u zemlje Zapadne Evrope, baš iz ovih zemalja, pogotovo skandinavskih, jeste „slabljenje zakonskih normi koje su regulisale razvratna ponašanja u Skandinaviji“. (Wortley & Smallbone, 2012) U prvo vreme fotografije dečije pornografije nisu bile objavljene, one su čuvane kao privatno vlasništvo. Međutim, već sredinom šezdesetih godina određeni nudistički magazini su objavili slike dece u eksplicitnim pozama. Posledica toga je bila pojava prvog magazina koji se bavio dečijom pornografijom pod nazivom „Bambino seks“. Jedan od najpopularnijih takvih magazina, takođe je bio holandski „Lolita“ koji je 1984. godine prekinuo publikovanje. (Rudolph, 2003)

Naime, došlo je do zakonskih promena u mnogim zemljama u kojima je dečija pornografija uvrštena u nelegalno ponašanje. Počele su da se vode razne javne debate o ovom problemu, a svi su se slagali da ovakve fotografije predstavljaju ekstremno oblik devijantnog ponašanja. Zaključak je da bilo koji vid ovakvog ponašanja predstavlja zlostavljanje dece jer samo dete ne može dati pravni pristanak za učešće u radnji. Postoji više manifestacija uvredljivih slika dece koje potpadaju

pod ovu temu. Najčešće se pri stvaranju ovih slika koristi:

- slika deteta koja se neprimereno tretira seksualno (npr. uklonjena odeća);
- pornografska slika odrasle osobe kojoj se dodeljuju karakteristike deteta (npr. smanjenje veličine grudi, uklanjanje stidnih dlaka);
- slika deteta koja se kombinuje sa pornografskom slikom odrasle osobe ili drugog deteta;
- montaža više uvredljivih slika. (Beech, Elliot, Birgden, & Findlater, 2008)

Da bi upotpunili pojam dečije pornografije, treba odrediti koja su to lica koja se smatraju decom u smislu ovog krivičnog dela.

Konvencija o pravima deteta UN daje u 1. delu u članu 1. određenje deteta. Za potrebe konvencije pod detetom se smatra svako ljudsko biće koje nije navršilo osamnaest godina života, ukoliko se, po zakonu koji se primenjuje na dete, punoletstvo ne stiče ranije. Nakon određivanja kategorije u članu 2. Konvencije je naznačeno: da će strane ugovornice Konvencije poštovati i obezbeđivati prava utvrđena konvencijom svakom detetu koje se nalazi pod njihovom jurisdikcijom bez ikakve diskriminacije i bez obzira na rasu, boju kože, pol, jezik, veroispovest, političko i drugo uverenje, nacionalno, etničko ili socijalno poreklo, imovinsko stanje, onesposobljenost, rođenje ili drugi status deteta, njegovog roditelja ili zakonskog staratelja. U tom cilju će strane ugovornice preduzeti sve odgovarajuće mere kako bi se obezbedila zaštita deteta od svih oblika diskriminacije ili kažnjavanja zasnovanog na statusu, aktivnostima, izraženom mišljenju ili uverenju. (UN, Konvencija o pravima deteta, 1989)

Zakon o maloletnim učiniocima krivičnih dela na indirektni način u članu 2. „Isključenje krivičnih sankcija prema deci” za decu smatra lica do četrnaest godina starosti. U istom zakonu u članu broj 3., „Uzrast učinioca” lica od četrnaest do osamnaest godina su klasifikovana na sledeći način: maloletnik, mlađi maloletnik, stariji maloletnik i mlađe punoletno lice.

Maloletnik je lice koje je u vreme izvršenja krivičnog dela navršilo četrnaest, a nije navršilo osamnaest godina.

Mlađi maloletnik je lice koje je u vreme izvršenja krivičnog dela navršilo četrnaest, a nije navršilo šesnaest godina.

Stariji maloletnik je lice koje je u vreme izvršenja krivičnog dela navršilo šesnaest, a nije navršilo osamnaest godina.

Mlađe punoletno lice je lice koje je u vreme izvršenja krivičnog dela navršilo osamnaest, a u vreme suđenja nije navršilo dvadeset jednu godinu i ispunjava ostale uslove iz člana 41. ovog zakona. (Zakon, 2005)

Do 2009. godine smatrala su se decom lica koja spadaju u starosnu kategoriju do 14 godina. 2009. godine donesen je Zakon o izmenama i dopunama Krivičnog zakonika kojim je ova inkriminacija osnovano upotunjena proširenjem starosne kategorije sa 14 na 18 godina. (Zakon, 2009A) To preciznije znači da je pomerena granica za žrtve krivičnog dela prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju. (Zakon, 2014)

Ovde treba napraviti jednu digresiju. S obzirom na pomeranje starosne granice žrtve krivičnog dela u pomenutom članu, postoji jedna kontradiktornost u Krivičnom zakoniku Republike Srbije. Naime, prema članu 180. KZ Republike Srbije, žrtve krivičnog dela Obljuba sa detetom su lica mlađa od 14 godina. Dakle, do pomeranja starosne granice Zakonom o izmenama i dopunama Krivičnog zakonika iz 2009. godine kod ovog dela nije došlo, pa tako sledi zaključak da je dozvoljeno stupati u seksualni odnos sa maloletnicima, ali ne i posedovati pornografske sadržaje.

2 DEČIJA PORNOGRAFIJA NA INTERNETU KAO OBLIK VISOKOTEHNOLOŠKOG KRIMINALA

Dečija pornografija, odnosno zloupotreba dece u pornografske svrhe je naročito zastupljena na internetu jer je tu i najlakše sprovodljiva. Činjenica je da su deca ranjiva kategorija lica, nezrela i time podobna za iskorišćavanje u ove svrhe. Sama psihologija dece omogućuje učiniocima ovog krivičnog dela da se lakše usude na njegovo preduzimanje. Pod time podrazumevamo da su deca često neoprezna, slobodnija u pružanju podataka o sebi, svojim godinama, mestu stanovanja i drugim ličnim podacima i osobinama. Treba ukazati na to da su zloupotrebe dece jednostavnije sa pojavom društvenih mreža, kao što su Instagram, Fejsbuk i Tviter, gde deca željna

dokazivanja i prihvatanja neoprezno ulaze u poznanstvo sa nepoznatim osobama (Miladinovich Bogavats, 2017, str. 130).

Da bi se dečija pornografija podvela pod visokotehnološki kriminalitet, potrebno je odrediti i njegov pojam, odnosno definiciju. Brojne su definicije koje proizilaze iz međunarodnih dokumenata, ali i one koje su izradili poznati kriminolozi.

Definicija visokotehnološkog kriminaliteta data je u dokumentu „Kriminalitet vezan za računarske mreže“ koji je donet na Desetom kongresu Ujedinjenih nacija. U ovom dokumentu visokotehnološki kriminalitet se definiše kao kriminalitet koji se odnosi na bilo koji oblik krivičnog dela koje se može izvršavati računarskim sistemima i mrežama, u računarskim sistemima i mrežama ili protiv računarskih sistema i mreža. Istovremeno, visokotehnološki kriminalitet je određen u užem i širem smislu. U užem, sajber kriminalitet podrazumeva svako ilegalno ponašanje usmereno ka sredstvima elektronskih operacija koje ugrožavaju bezbednost kompjuterskih sistema i podataka koje sadrže. U širem smislu, to je svako ilegalno ponašanje izvršeno ili u vezi sa sredstvima kompjuterskih sistema ili mreža, uključujući krivična dela kao što su nelegalno posedovanje, nuđenje ili distribucija informacija korišćenjem kompjuterskih sistema ili mreža. (UN, 2000)

Jedna od teorijskih određenja visokotehnološkog kriminala jeste da je to kriminalitet izvršen u celini ili delimično u elektronskoj sredini, kao poseban vid inkriminisanih ponašanja u kojima se računarski sistem pojavljuje ili kao sredstvo izvršenja, ili kao objekt krivičnog dela ukoliko se delo na drugi način ili prema drugom objektu uopšte ne bi moglo izvršiti, ili bi ono imalo bitno drugačije karakteristike. (Urošević, Ivanović, & Uljanov, 2012)

Prva definicija visokotehnološkog kriminaliteta u Republici Srbiji propisana Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala.¹ Prema članu 2., visokotehnološki kriminalitet predstavlja vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku. Pod proizvodima se podrazumevaju računarski programi i autorska dela koja se mogu upotrebiti u elektronskom obliku. (Zakon, 2005 i 2009)

Nakon ovih razmatranja, možemo doći do zaključka da dečija pornografija predstavlja jedan od pojavnih oblika visokotehnološkog kriminaliteta, jer se sastoji u zloupotrebi i iskorišćavanju računara i računarskih mreža, najčešće interneta, radi proizvodnje, prodaje, razmene, posedovanja i gledanja pornografskog materijala u kojima su glavni akteri maloletna lica, a sve to u cilju zadovoljenja izopačenih polnih nagona ili ostvarivanja materijalne koristi.

Dakle, pornografski sadržaj koji je vezan za maloletnike se u ovom slučaju možemo zaključiti, vezuje za nematerijalni, neografineni interaktivni prostor kreiran od računarskih mreža. (Miladinović Bogavac & Rutović, 2016)

- S tim u vezi, u okviru odeljka 4., Konvencija o visokotehnološkom kriminalu Saveta Evrope predviđa „krivična dela u odnosu na sadržaj“, koja se odnose pre svega na krivična dela vezana za dečiju pornografiju tj. pornografski materijal koji vizuelno prikazuje:
- maloletnika koji učestvuje u eksplicitno seksualnom činu;
- lice po čijem se izgledu može zaključiti da je maloletnik, koje učestvuje u eksplicitno seksualnom činu;
- realističke slike koje predstavljaju maloletnika koji učestvuje u eksplicitno seksualnom činu;

¹ Zakonodavac u Republici Srbiji u Krivičnom zakoniku u čl. 112, definiše značenje izraza u ovom zakoniku. Tač. 17 – Računarski podatak je svako predstavljanje činjenica, informacija ili koncepta u obliku koji je podesan za njihovu obradu u računarskom sistemu, uključujući i odgovarajući program na osnovu koga računarski sistem obavlja svoju funkciju. Tač. 18 – Računarskom mrežom smatra se skup međusobno

povezanih računara, odnosno računarskih sistema koji komuniciraju razmenjujući podatke. Tač. 19 – Računarskim programom smatra se uređeni skup naredbi koje služe za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara. Tač. 33 – Računar je svaki elektronski uređaj koji na osnovu programa automatski obrađuje i razmenjuje podatke.

Konvencija o visokotehnološkom kriminalu upućuje da države članice usvajanjem ovog krivičnog dela može postaviti nižu starosnu granicu, koja ne sme biti manja od napunjenih šesnaest godina. (Zakon, 2009)

Dalje, Konvencija u članu 9. predviđa koje radnje izvršenja treba sankcionisati u slučaju dečije pornografije na internetu:

- „proizvodnja dečije pornografije u cilju njene distribucije preko kompjuterskih sistema;
- nuđenje ili stavljanje na raspolaganje dečije pornografije preko kompjuterskih sistema;
- distribucija ili prenošenje dečije pornografije preko kompjuterskih sistema;
- dobavljanje dečije pornografije preko kompjuterskih sistema za sebe ili za druga lica;
- posedovanje dečije pornografije u kompjuterskom sistemu ili na medijima za smeštanje kompjuterskih podataka”. (Zakon, 2009)

Ove radnje na Internetu koje potpadaju pod visokotehnološki kriminal mogu uzrokovati posledice koje možemo podeliti na finansijske, nematerijalne i kombinovane. Finansijske posledice nastaju kada učinilac vrši delo radi sticanja protivpravne imovinske koristi, pa tu korist za sebe ili drugog zaista i stekne. Za razliku od finansijskih, nematerijalne posledice se ogledaju u neovlašćenom otkrivanju poverljivih informacija, ili drugom indiskretnom štetnom ponašanju poput sajber uznemiravanja ili sajber proganjanja. (Miladinović Bogavac, 2017) Nematerijalne i kombinovane posledice dečije pornografije na internetu mogu ostaviti traga u daljem razvoju ličnosti deteta, te je neophodno preventivnim i represivnim merama u što većoj meri nastojati da se ova pojava iskoreni.

3 MEĐUNARODNOPRAVNA REGULATIVA DEČIJE PORNOGRAFIJE NA INTERNETU

Pojava interneta, kao što je rečeno, dala je veće mogućnosti za vršenje ovog krivičnog dela i omogućila teže otkrivanje izvršilaca. Zato je danas internet glavni izvor ovakvog nedozvoljenog sadržaja, koji predstavlja društveno-pravni problem u svim zemljama sveta.

U slučajevima kriminaliteta ove vrste postoji potreba sinhronizovanog angažovanja država u borbi protiv kriminala, jer ni jedan vid visokotehnološkog kriminala nikada nije problem samo jedne države. Zato je dečija pornografija pravno regulisana kako međunarodnim aktima, tako i domaćim pozitivnim zakonodavstvom.

Konvencija o pravima deteta predstavlja osnov svih daljih međunarodnih akata koji se bave pravima deteta, pa time i zloupotrebom dece u pornografske svrhe. Ova konvencija je doneta na 44. zasedanju Generalne skupštine Ujedinjenih nacija u Njujorku 20. novembra 1989. godine. SFRJ ju je ratifikovala 1990. godine i time preuzela obavezu da uskladi svoje domaće pozitivno zakonodavstvo sa načelima koje ova konvencija proklamuje. Ovim aktom je definisana zaštita dece od svih oblika seksualnog zlostavljanja i iskorišćavanja.²

SR Jugoslavija ju je usvojila 2000. godine, a zatim i ratifikovala 10. oktobra 2002. godine Fakultativni protokol uz konvenciju o pravima deteta o prodaji dece, dečijoj prostituciji i dečijoj pornografiji koji je Generalna skupština Ujedinjenih nacija usvojila u originalu zvanično na više jezika: arapskom, kineskom, engleskom, francuskom, ruskom i španskom. Ovaj protokol upućuje na mere koje države potpisnice treba da preduzmu kako bi garantovale zaštitu deteta od prodaje dece, dečije prostitucije i dečije pornografije. U članu 2. Protokola, naglašava se da se države potpisnice saglašavaju u ovom protokolu s obzirom na zabrinutost zbog sve veće dostupnosti dečije pornografije na internetu i u drugim tehnologijama u razvoju. Protokol se poziva na Konferenciju o borbi protiv dečije pornografije na internetu, održanoj u Beču 1999. godine, a posebno na njen zaključak kojim poziva na univerzalnu inkriminaciju proizvodnje, distribucije, izvoza, prenosa, uvoza, namernog posedovanja i reklamiranja dečije pornografije. Takođe, ovaj Protokol uzima u obzir i Hašku konvenciju o zaštiti dece i saradnji u vezi sa međunarodnim usvojenjem, Hašku konvenciju o građanskim aspektima međunarodne otmice deteta, Hašku konvenciju o jurisdikciji, primenljivoj pravu, priznavanju, sprovođenju i saradnji u pogledu roditeljske odgovornosti i mera

² Službeni list SFRJ – Međunarodni ugovori, br. 15/90

za zaštitu dece, Konvenciju Međunarodne organizacije rada br. 182 o zabrani i hitnoj akciji za suzbijanje najtežih oblika dečijeg rada kao i Program akcije za sprečavanje prodaje dece, dečije prostitucije i dečije pornografije, Deklaraciju i Agendu za akciju usvojenih na Svetskom kongresu protiv komercijalnog seksualnog iskorišćavanja dece u Stokholmu 1996. godine. (Zakon, Zakon o potvrđivanju Fakultativnog protokola o prodaji dece, dečijoj prostituciji i dečijoj pornografiji, uz Konvenciju o pravima deteta, 2002)

Protokolom je, pre svega, predviđeno da države ugovornice zabrane prodaju dece, dečiju prostituciju i dečiju pornografiju. Pod pojmom dečija pornografija se podrazumeva bilo kakvo predstavljanje, bilo kojim sredstvom, deteta u stvarnim ili simuliranim eksplicitnim seksualnim aktivnostima ili bilo kakvo predstavljanje seksualnih delova tela (primarnih i seksualnih organa deteta), prvenstveno u seksualne svrhe. Predviđa se da svaka država ugovornica obezbedi da određene radnje budu u punoj meri obuhvaćene njenim krivičnim ili kaznenim zakonom, bez obzira da li su takva dela izvršena u zemlji ili transnacionalno, odnosno na individualnoj ili organizovanoj osnovi. U te radnje spadaju: proizvodnja, distribucija, širenje, uvoz, izvoz, nuđenje, prodaja ili posredovanje dečije pornografije. Odredbe se kako na izvršeno krivično delo, odnose i na pokušaj, a tako i na saučesništvo pored glavnog izvršioca. (Zakon, 2002)

Svaka država ugovornica je obavezna da preduzima potrebne mere kako bi se utvrdila njena nadležnost nad delima u slučajevima kada je izvršilac državljanin te države ili lice koje ima prebivalište na njenoj teritoriji, ali i kada je žrtva državljanin te države. O ekstradiciji, u Protokolu se navodi da su krivična dela podložna ekstradiciji po svim ugovorima o ekstradiciji koji postoje između država ugovornica i biće uključena kao dela koja podležu ekstradiciji, u svaki ugovor o ekstradiciji naknadno zaključen između njih, u skladu sa uslovima u tim ugovorima. Države ugovornice će pružiti jedna drugoj najveću meru pomoći u vezi sa istražnim radnjama ili krivičnim postupkom, odnosno postupkom za ekstradiciju u vezi sa krivičnim delima, uključujući i pomoć o prihvatanju

dokaza koji su im na raspolaganju, a neophodni su za postupak. (Zakon, 2002)

Značaj protokola je u tome što su se države ugovornice usaglasile da će usvojiti, jačati i širiti obaveštenost o zakonima, upravnim merama, socijalnoj politici i programima, kako bi sprečile pomenuta dela. Države se obavezuju da će jačati svest javnosti u celini, uključujući i decu, kroz obaveštavanje pomoću svih odgovarajućih sredstava, obrazovanje i obuku o preventivnim merama i štetnim posledicama svih dela koja su Protokolom obuhvaćena. Takođe, države će preduzeti sve izvodljive mere u cilju obezbeđivanja svake odgovarajuće pomoći žrtvama takvih dela, uključujući njihovu punu socijalnu reintegraciju i njihov kompletan fizički i psihološki oporavak. (Zakon, 2002)

U vezu sa pojmom kompjuterskog kriminaliteta, dečija pornografija se prvi put dovodi u Konvenciji o sajber kriminalitetu koju je doneo Savet Evrope novembra 2001. godine. (Zakon, 2009) Pored definisanja dečije pornografije, Konvencija obavezuje države potpisnice da preduzmu sve neophodne zakonodavne ili druge mere kako bi sankcionisale bavljenje seksualnim aktivnostima sa detetom koje nije navršilo pravni uzrast u kome su seksualne aktivnosti dopuštene. (Zakon, 2009)

Savet Evrope je oktobra 2007. godine usvojio Konvenciju o zaštiti dece od seksualne eksploatacije i zlostavljanja. Ovaj međunarodnopravni dokument je važan iz razloga što se njime povećava efikasnost krivičnih postupaka u kojima se deca javljaju kao žrtve seksualne eksploatacije i zlostavljanja. Republika Srbija je ratifikovala ovu Konvenciju donošenjem Zakona o potvrđivanju Konvencije Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja.³ Sa aspekta borbe protiv visokotehnološkog kriminaliteta Konvencija ima značajnu ulogu ka harmonizaciji nacionalnih zakonodavstava, posebno u onim slučajevima gde se računarske mreže i tehnologije koriste s ciljem razmene, distribucije i skladištenja nedozvoljenih sadržaja. Njom se pojam dečije pornografije definiše kao: svaki materijal koji vizuelno prikazuje dete koje se stvarno ili simulirano eksplicitno seksualno ponaša ili svaki

³ Sl. glasnik RS – Međunarodni ugovori, br. 1/2010

prikaz detetovih polnih organa za prvenstveno seksualne svrhe. (CE, 2007)

Slično prethodnoj Konvenciji i ova se osvrće na radnje koje se odnose na zloupotrebu dečije pornografije, uz upotrebu računarskih sistema i tehnologija. Ona uvodi novinu, a to je krivično delo umišljajnog ostvarivanja pristupa sadržajima dečije pornografije putem informatičkih tehnologija, što znači da je kažnjiv i sam pristup svim pornografskim sajtozima sa nedozvoljenim sadržajem.⁴ Međutim Republika Srbija još uvek nije inkriminisala u svom zakonodavstvu ovu radnju.

Pored pravne regulative na međunarodnom planu se poslednjih godina razvijaju projekti koji bi povezali države u otklanjanju ove svetske opasnosti koja pogađa najosetljiviju kategoriju - decu.

U tom cilju, Evropska komisija je 2013. godine uspostavila Centar za bezbedni internet u okviru Programa za bezbedni internet (engl. Safer Internet Programme). Cilj projekta je da se povežu evropske zemlje radi zajedničkog osnaživanja i zaštite dece i mladih na internetu. Kroz edukativne aktivnosti u vidu održavanja radionica i tribina podstiču se roditelji, učenici i nastavnici, kao i ostala zainteresovana lica na bezbedno korišćenje interneta i izbegavanje zamki njegove zloupotrebe. (Klikni Bezbedno, n.d.)

U okviru Centra za bezbedni internet razvijen je i mehanizam za prijavu nedozvoljenih sadržaja na internetu, pod nazivom „Net patrola“. „Net patrola“ je deo mehanizma Međunarodnog udruženja operatera internet mehanizama za prijave nedozvoljenog i štetnog sadržaja na internetu – „INHOPE“. INHOP mreža uključuje linije za hitnu prijavu ilegalnih materijala koji sadrže fizičko zlostavljanje i maltretiranje, seksualno iskorišćavanje i psihološko maltretiranje dece, a kruže internetom. Suština ovog mehanizma je da omogućiti prijavu ilegalnog sadržaja čim bude primećen, te se prijava prosleđuje odgovarajućem telu koje će po prijavi postupiti. (Inhope, 2013)

Svakako treba razvijati mehanizme poput navedenih ili poboljšavati postojeće. Neophodan je zajednički rad što većeg broja zemalja kako bi se razvila strategija za uspešno otklanjanje ove

štetne društvene pojave koja narušava prava deteta, njegov fizički i psihički integritet. Dovoljno jaki internet mehanizmi bi svakako smanjili ako ne i u potpunosti uticali na to da internet ne može više biti sredstvo distribuiranja dečije pornografije. Može se slobodno smatrati da je ovo sveopšti svetski problem, a ne problem samo jedne zemlje, više zemalja ili jednog kontinenta. Da je to svetski problem ukazuju i sami akti međunarodnih organizacija koje su dale osnove za zakonsku regulativu dečije pornografije, a deo tih akata, najbitniji, već je spomenut u prethodnom tekstu.

4 PRAVNA REGULATIVA DEČJE PORNOGRAFIJE NA INTERNETU U REPUBLICI SRBIJI

Potpisivanjem raznih međunarodnih ugovora od strane Republike Srbije u vezi sa ovom materijom, ona je preuzela obavezu da svoje zakonodavstvo usaglasi sa klauzulama tih ugovora. To je učinjeno izmenama i dopunama Krivičnog zakonika izmenama postojećih inkriminacija i uvođenjem novih. Krivična dela koja su predviđena Konvencijom o visokotehnološkom kriminalu u grupi „krivičnih dela u odnosu na sadržaj“, svoju regulativu u okviru Krivičnog zakonika Republike Srbije ostvaruju u glavi osamnaestoj: „Krivična dela protiv polne slobode“ i to kao krivično delo „prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju“. (SE, 2001)

Osnovna izmena zakonskog opisa ovog krivičnog dela se ogleda u tome da žrtva krivičnog dela nije više „dete“, već „maloletno lice“ što je i u skladu sa ratifikovanim međunarodnim ugovorima. Delo ima 4 oblika. Prvi postoji kada se maloletniku proda, prikaže ili javnim izlaganjem, ili na drugi način učine dostupnim tekstovi, slike, audio-vizuelni ili drugi predmeti pornografske sadržine ili mu se prikaže pornografska predstava. Za izvršenje krivičnog dela neophodan je umišljaj, ali je dozvoljen i eventualni umišljaj, jer je dovoljno i pristajanje da se maloletnik upozna sa sadržinom pornografskog predmeta. Kao kazna je predviđena novčana kazna ili kazna zatvora do 6 meseci. (Krivični zakonik, 2009)

Drugi oblik postoji u slučaju iskorišćavanja maloletnika za proizvodnju slika, audio-vizuelnih ili

⁴ Sl. glasnik RS – Međunarodni ugovori, br. 1/2010

drugih predmeta pornografske sadržine ili za pornografsku predstavu. Izvršilac je lice koje napravi fotografski, filmski ili drugi snimak maloletnika radi pornografskog sadržaja ili ga navede na učestvovanje u pornografskoj predstavi. Dakle, za razliku od prvog oblika gde se radi o tome da se maloletniku čini dostupnim pornografija, kod ovog oblika se maloletnik iskorišćava za proizvodnju predmeta ili predstava pornografskog sadržaja. Kazna za drugi oblik je 6 meseci do 5 godina zatvora. (Krivični zakonik, 2009)

Treći oblik je kvalifikovani oblik prvog i drugog oblika i on postoji kada je neko od tih dela izvršeno prema detetu. Za kvalifikovani oblik prvog dela predviđa se kazna zatvora od 6 meseci do 3 godine, dok je za kvalifikovani oblik drugog dela zaprećena kazna zatvora od 1 do 8 godina. (Krivični zakonik, 2009)

Četvrti oblik predstavlja posebni oblik dela koji postoji kada lice pribavlja za sebe ili drugog, poseduje, proda, prikaže, javno izloži ili elektronski i na drugi način učini dostupnim slike, audio-vizuelne i druge predmete pornografske sadržine nastale iskorišćavanjem maloletnog lica. (Krivični zakonik, 2009) Propisana kazna za ovaj oblik je zatvor od 3 meseca do tri godine.

Svi oblici ovog krivičnog dela se mogu izvršiti samo sa umišljajem. Umišljaj mora obuhvatiti i okolnost da se radi o maloletniku, odnosno detetu. (Stojanović & Perić, 2009) Kako navode Stojanović i Perić, pornografiju u smislu ovog krivičnog dela treba shvatiti kao eksplicitno prikazivanje seksualnog akta bilo koje vrste, ili seksualnog organa koje nema edukativne, naučne, umetničke ili slične ciljeve. Pornografsku sadržinu mogu imati tekstovi, slike, audio vizuelni (kompakt diskovi, video trake, audio kasete...) i drugi predmeti. Osim toga može se raditi o pornografskoj predstavi kao što je tzv. peep show i live show. (Stojanović & Perić, 2009)

Srpsko zakonodavstvo iako je u velikoj meri prilagođeno ratifikovanim međunarodnim ugovorima, ipak i dalje ima dosta nedostataka u ovoj oblasti. U prvom redu se nameće razmatranje uporednopravnih rešenja kojima se sankcionišu granične forme krivičnih dela koja se odnose na seksualno zlostavljanje dece i dečiju pornografiju.

Posebna pažnja i stalna težnja ka unapređenju bi trebalo da se posveti krivičnim sankcijama, tretmanu lica koja su osuđena za krivična dela iz ove grupe (psihijatrijsko lečenje) ali i mehanizmima da do krivičnog dela ne dođe.

5 ZAKLJUČNA RAZMATRANJA

Kako smo videli, problem dečije pornografije postoji još od najstarijih vremena, ali se u današnjim uslovima visoke tehnologije ubrzano širi. Svakako je neophodna dobra zakonska regulativa i sistem kažnjavanja, ali i sistemi prevencije koji će smanjiti broj učinilaca ovog krivičnog dela, time što će im kompjuterski sistemi to na vreme onemogućiti. Treba ostati pri stavu kojeg se drži naš Krivični zakonik da se ovo krivično delo odnosi na maloletna lica, odnosno sve navedene kategorije maloletnika koje su propisane Zakonom o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica što je i u skladu sa međunarodnim standardima. Neopravdano je da žrtva dečije pornografije može biti samo dete, odnosno lice do 14. godine života kako je nekada bilo propisano, jer ukoliko svako lice stiče poslovnu sposobnost tek sa 18 godina, što je uslovljeno biološkim karakteristikama, zašto se onda ne bi sankcionisalo i ugrožavanje njegovog integriteta pre navršene 18. godine života? Poslovna sposobnost podrazumeva da lice ima pravo da sklapa pravne poslove, dakle da je tek tada dovoljno zrelo da može davati svoj pristanak za stupanje u različite pravne odnose. Analogno tome, takvo shvatanje se mora primenjivati i kod slučaja dečije pornografije. U Republici Srbiji se poslednjih godina dosta radilo na zakonskoj regulativi ove oblasti i možemo ustanoviti značajne pomake. Međutim sa razvojem tehnologije, izvršioci opet nalaze načine da izvrše krivično delo. Zato akcenat treba da bude, pre svega na preventivi, a to bi bio razvoj mreža poput INHOP mreže i „Net patrole“. Što više ovakvih sistema može da spreči razvoj ove vrste kriminaliteta, što je i cilj, da se više radi na sprečavanju, nego na kažnjavanju, jer kada je delo već počinjeno, detetovo pravo je povređeno kao i njegov integritet, što može ostaviti znatne posledice na njegov dalji život, bez obzira na to koliko kaznu će počinilac odslužiti.

CITIRANA DELA

- Beech, A., Elliot, I., Birgden, A., & Findlater, D. (2008). The Internet and child sexual offending: A criminological review. *Aggression and Violent Behavior*, 13(3), 216-228. doi:10.1016/j.avb.2008.03.007
- CE. (2007, 10 25). *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*. Preuzeto sa Council of Europe: <http://conventions.coe.int>
- Inhope. (2013, 11 14). *INHOPE expands and strengthens presence in the Balkans and South America*. Preuzeto sa INHOPE: http://www.inhope.org/tns/news-and-events/news/13-11-14/INHOPE_expands_and_strengthens_presence_in_the_Balkans_and_South_America.aspx
- Klikni Bezbedno. (n.d.). Preuzeto 08 02, 2018 sa <https://kliknibezbedno.wordpress.com/>
- Komlen-Nikolić, L., Gvozdenović Radulović, S., Milosavljević, A., Jerković, R., Živković, V., Živanović, S., . . . Aleksić, I. (2010). *Suzbijanje visokotehnološkog kriminala*. Beograd: Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije.
- Krivični zakonik. (2009). Krivični zakonik Republike Srbije. *Sl. glasnik RS*(72/2009).
- Miladinovich Bogavats, Z. (2017). Narušeniya prav detey v kiberprostranstve, kiberopasnost' i pravoye regulirovaniye. *Yuridicheskiy vestnik Samarskogo universiteta*, 3(3).
- Miladinović Bogavac, Ž. (2017). Modeli ispoljavanja psihološkog uznemiravanja u sajber prostoru sa osvrtom na najpoznatije medijske slučajeve. *Časopis za istraživanje medija i društva - Medijski dijalozi*, IX(26).
- Miladinović Bogavac, Ž., & Rutović, V. (2016). Međunarodna regulativa zloupotrebe sajber prostora kao globalno povezane informaciono – komunikacione infrastrukture. *Časopis za istraživanje medija i društva - Medijski dijalozi*, IX(25), 67-77.
- Rudolph, T. (2003). Child pornography. U S. Peterson, M. Durfee, & K. Coulter, *Child Abuse and Neglect: Guidelines for Identification, Assessment, and Case Management*. New York: Volcano Press.
- SE. (2001, 11 23). Konvencija o visokotehnološkom kriminalu. Preuzeto sa http://www.podaci.net/_z1/2129877/Z-pkvkri03v0919.html
- Slavković, V. (2014). Krivičnopravno regulisanje pornografije u savremenom zakonodavstvu. *Pravni zapisi*, 5(2).
- Stanić, I. (2007). Dječja pornografija. *Pedagoška stvarnost*(3-4).
- Stojanović, Z., & Perić, O. (2009). *Krivično pravo – posebni deo*. Beograd.
- Škulić, M. (2010). Načelo zakonitosti u krivičnom pravu. *Anali pravnog fakulteta u Beogradu*(1).
- Šolić, P. (1991). Fenomenološki pristup pornografiji. *Crkva u svetu*(1).
- Uljanov, S., & Ivanović, Z. (2009). Seksualna eksploatacija dece sa aspekta uporednopravne analize međunarodne saradnje u kriminalističkim istragama. *Evropsko zakonodavstvo*(29-30).
- UN. (1989). *Konvencija o pravima deteta*. Preuzeto sa UNHCR: <http://www.unhcr.rs/dokumenti/osnovni-dokumenti/konvencije-protokoli.html>
- UN. (2000, 07 19). *Tenth UN Congress on the Prevention of Crime and Treatment of Offenders*. Preuzeto sa United Nations: https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-EN.pdf
- Urošević, V., Ivanović, Z., & Uljanov, S. (2012). *Mač u World wide web-u: Izazovi visokotehnološkog kriminala*. Beograd: Eternal miks.

Wortley, R., & Smallbone, S. (2012). *Internet child pornography: Causes, Investigation and Prevention*. NewYork: ABC-CLIO.

Zakon. (1977). Krivični zakon SFRJ. *Sl. list SFRJ*(44/77).

Zakon. (2002). Zakon o potvrđivanju Fakultativnog protokola o prodaji dece, dečijoj prostituciji i dečijoj pornografiji, uz Konvenciju o pravima deteta. *Sl. list SFRJ – Međunarodni ugovori*(7/2002).

Zakon. (2005 i 2009). Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, član 2. *Sl. glasnik RS*(61/05 i 104/09,).

Zakon. (2005). Zakon o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica. *Sl. glasnik RS*(85/2005).

Zakon. (2009). Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu. *Sl. glasnik RS – Međunarodni ugovori*(19/2009).

Zakon. (2009A). Zakon o izmenama i dopunama Krivičnog zakonika. *Sl. glasnik RS*(72/2009).

Zakon. (2014). Krivični zakonik Republike Srbije. *Sl. glasnik RS*(108/2014).

Datum prve prijave: 01.09.2018.

Datum prijema korigovanog članka: 24.03.2019.

Datum prihvatanja članka: 27.03.2019.

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

Style – APA Sixth Edition:

Miladinović Bogavac, Ž. (2019, 04 15). Pravna regulativa dečije pornografije na internetu. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 100-109. doi:10.12709/fbim.07.07.01.12

Style – Chicago Sixteenth Edition:

Miladinović Bogavac, Živanka. 2019. „Pravna regulativa dečije pornografije na internetu.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 100-109. doi:10.12709/fbim.07.07.01.12.

Style – GOST Name Sort:

Miladinović Bogavac Živanka Pravna regulativa dečije pornografije na internetu [Časopis] // *FBIM Transactions* / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 100-109.

Style – Harvard Anglia:

Miladinović Bogavac, Ž., 2019. Pravna regulativa dečije pornografije na internetu. *FBIM Transactions*, 15 04, 7(1), pp. 100-109.

Style – ISO 690 Numerical Reference:

Pravna regulativa dečije pornografije na internetu. **Miladinović Bogavac, Živanka**. [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, *FBIM Transactions*, T. 7, str. 100-109.



INFORMACIONO-BEZBEDNOSNA KULTURA MLADIH U SRBIJI

INFORMATION-SECURITY CULTURE OF YOUTH IN SERBIA

Zoran Milanović

Kriminalističko-policijska akademija, Beograd, Srbija

©MESTE

JEL Kategorija rada: **L86**

Rezime

Mlađe populacije su najčešći korisnici interneta, a posebno društvenih mreža i kao takve su najugroženija ciljna grupa većine pojava oblika zloupotrebe. Zato je sprovedeno istraživanje korišćenjem upitnika, a sa ciljem utvrđivanja njihovih trenutnih znanja i ponašanja na internetu i njihove informaciono-bezbednosne kulture. Rezultati istraživanja treba da imaju za posledicu podizanje svesti krajnjih korisnika o potrebi zaštite podataka, informacija i znanja. Istraživanje je pokazalo postojanje nedoslednosti između stečenih znanja (svesti) o informaciono-bezbednosnim rizicima i ponašanju (informaciono-bezbednosne kulture) ispitanika. Uzroke ovih nedoslednosti autor vidi u nedostatku praktičnih (primenjivanih) znanja i smatra da mlade treba podsticati da budu aktivniji u sticanju većeg opsega znanja, razumevanja i mogućnosti da se suoče sa problemima.

Ključne reči: mladi, znanje, ponašanje, svest, informaciono-bezbednosna kultura.

Abstract:

Younger populations are the most common Internet users, especially social networks, and as such are the most vulnerable target group for most forms of abuse. Therefore, a survey was conducted using a questionnaire, with the aim of determining their current knowledge and behavior on the Internet and their information and security culture. The research results should have the effect of raising the awareness of the end users about the need to protect data, information and knowledge. The research has shown the existence of inconsistencies between the acquired knowledge (awareness) of the information-security risks and behavior (information-security culture) of the respondents. The author believes that the causes of these inconsistencies lack of practical (applicable) knowledge and thinks that young people should be encouraged to be more active in acquiring a greater scope of knowledge, understanding and ability to cope with problems.

Keywords: youth, knowledge, behavior, awareness, information-security culture.

Adresa autora:

Zoran Milanović

[✉ zoran.milanovic@yahoo.com](mailto:zoran.milanovic@yahoo.com)

1. UVOD

Vreme u kome živimo odlikuje se primenom naprednih informaciono-komunikacionim tehno-

logijama (IKT) u svim sferama života i rada, unapređujući ih kako u kvalitativnom tako i u kvantitativnom smislu. Ova činjenica je, između ostalog, nametnula i novu društvenu vrednost: informaciono-bezbednosnu kulturu i kao takva postala je predmet interesovanja mnogih istraživača. Obzirom da je posmatrana sa različitih aspekata i da su se fokusi istraživača međusobno razlikovali, nastale su i različite definicije informaciono-bezbednosne kulture. Jednu od najopštijih definicija dao je Roer (2015) u knjizi "Izgradnja bezbednosne kulture", ističe: Bezbednosna kultura pomaže i olakšava ljudima da koriste informacione tehnologije na zadovoljavajući način, bez opasnosti i pretnji. Na sličan način su definisali informaciono-bezbednosnu kulturu i Kizist i Ilvonen (2003), Vrum i Solms (2004) i Tomson i ostali (2006). Roer (2015), takođe, navodi da je jedan od ključnih faktora izgradnje informaciono-bezbednosne kulture promena ponašanja pojedinaca podizanjem svesti o informaciono-bezbednosnim rizicima i mogućim posledicama.

S druge strane, najranjiviji deo svakog društva su deca i mladi. Njihova ranjivost u informaciono-bezbednosnom smislu potiče pre svega zbog njihovog neiskustva i naivnosti, te njihovog rizičnog ponašanja kao posledice nedostatka svesti o mogućim posledicama. 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, a rizik za njihov razvoj predstavlja i prekomerna upotreba digitalnih sadržaja“. 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 on-line igrice. 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 nasta-

janju, razvoju i širenju dečije pornografije. Ciljana edukacija, kao i razgovori sa roditeljima igraju najznačajniju ulogu u prevenciji i rešavanju ovog problema. Tako mnoge zemlje u svetu uvode obavezno obrazovanje, a poslednji primer uvođenja edukacije na svim obrazovnim nivoima je Indija. Ona se na ovaj korak odlučila zbog širenja velikog broja lažnih vesti putem interneta, a koji su za posledicu imali više od 25 ubistava (BBC, 2018). Adekvatna bezbednosna kultura svih korisnika, a naročito mladih, imperativ je savremenog društva (Bjelajac, 2014).

U tom smislu nastao je i ovaj rad, kao želja autora da skrene pažnju javnosti na trenutno stanje i nivo informaciono-bezbednosne kulture mladih kao i da ukaže na hitnost preduzimanja sveobuhvatnih mera kako bi se podigla svest i bezbednosni nivo ovog najosetljivijeg i najizloženijeg, a pre svega najvažnijeg dela našeg društva.

U radu su prezentovani rezultati i zaključci anonimnog upitnika kao istraživačkog instrumenta koji je doveo u korelaciju nivo znanja, kao merila svesti o mogućim informaciono-bezbednosnim rizicima i ponašanje kao merila informaciono-bezbednosne kulture.

2. ISTRAŽIVANJE

Cilj istraživanja je utvrđivanje postojećeg znanja i ponašanja korisnika IKT-a, ali i njihova edukacija, kao i posredno i neposredno unapređenje njihove bezbednosne kulture i podizanja svesti o narastajućim bezbednosnim problemima, pretnjama i rizicima, i moguća rešenja za zaštitu.

Prva faza se odnosi na kreiranje anonimnog upitnika, tj. strukturu pitanja i istraživačke oblasti – konstrukte. Pitanja za intervju koji je obavljen „licem u lice“ i elektronski veb upitnik su kreirani na osnovu značajnog teorijskog i praktičnog iskustva autora, kroz njegov dvadesetogodišnji rad na održavanju i zaštiti digitalnih sistema, kao i pregleda velikog broja elektronskih publikacija i veb sajtova iz oblasti informacione bezbednosti.

Po formiranju upitnika koji je imao 35 pitanja, izvršeno je preliminarno testiranje na kontrolnoj grupi od 18 korisnika IKT-a, oba pola od 18 do 27 godina. Cilj probnog testiranja je provera konzistentnosti postavljenih pitanja unutar dve varijable: znanja i ponašanja.

Broj i redosled pitanja je isti kod upitnika za intervju i elektronski.

Konačan izgled upitnika (Tabela 1) je 34 pitanja, od kojih se na 31 pitanje odgovara sa DA ili NE.

2.1. Metod anketiranja i distribucije podataka

Za potrebe elektronskog upitnika dizajnirana je klijentska veb orjentisana aplikacija (www.mzt.in.rs/Anketa.php), kao i MySQL baza u koju se slivaju svi prikupljeni podaci. Ovaj automatizovani način anketiranja u mnogome je olakšao proces popunjavanja i slanja odgovora. Sa jedne strane, korisnici IKT-a koji su se anketirali nisu bili vezani ni za mesto ni za vreme popunjavanja, a sa druge strane, administratoru baze podataka koji je istovremeno sa popunjavanjem upitnika imao i ažuriran tabelarni prikaz rezultata.

Tabela 1 – Upitnik

	PITANJE
1.	Pol:
2.	Koje od ponuđenih digitalnih uređaja koristite:
3.	Da li znate koji je operativni sistem se nalazi na njima?
4.	Da li znate za pristup operativnom sistemu koji nalog koristite (admin ili korisnički)?
5.	Da li znate koji zaštitni softver se nalazi na njima?
6.	Da li bi prepoznali nasilje na internetu (govor mržnje, uznemiravanje...)?
7.	Da li bi prijavili problem nasilja na internetu?
8.	Da li imate nalog na nekoj od društvenih mreža?
9.	Da li ostavljate lične podatke na internetu (ime, datum i mesto rođenja, šta studirate, slike)?
10.	Da li ste upoznati sa problemom krađe identiteta na internetu?
11.	Da li igrate on-line igrice?
12.	Da li skidate filmove, serije i muziku sa interneta?
13.	Da li gledate filmove ili slušate muziku on-line?

14.	Da li ste nekada povredili nečija autorska prava?
15.	Da li menjate lozinke (bar jednom u tri meseca) na svojim internet nalogima?
16.	Da li koristite istu lozinku za dva različita naloga (servisa, računara)?
17.	Da li znate nečiju pristupnu lozinku za: mail nalog ili društvenu mrežu?
18.	Da li neko zna Vašu pristupnu lozinku?
19.	Da li redovno pravite rezervne kopije svojih podataka?
20.	Na čemu pravite kopije podataka (DVD, flash, cloud, drugo)?
21.	Da li Vam se desilo da izgubite ili da Vam je ukraden neki od mobilnih uređaja (telefon, tablet, laptop)?
22.	Da li ste se susreli sa nekim oblikom malicioznog softvera (virus, trojanac...) na računaru ili telefonu?
23.	Da li znate šta je enkripcija?
24.	Da li znate šta je bitcoin?
25.	Da li znate šta je ransomver (Ransomware)?
26.	Da li znate šta je DDoS?
27.	Da li znate šta je fišing?
28.	Da li znate šta je ZeroDay (Zero Day)?
29.	Da li znate čime se bavi digitalna forenzika?
30.	Da li znate čime se bavi digitalna anti-forenzika?
31.	Da li znate neki od standarda koji se bave informacionom bezbednošću?
32.	Da li znate šta je ISO 27000 i NIST 800?
33.	Da li ste učestvovali na predavanjima, seminarima ili kursovima gde se govorilo o informacionoj bezbednosti, zaštiti korisnika na internetu, o društvenim mrežama itd?
34.	Da li na internetu čitate tekstove koji se bave zaštitom korisničkih podataka i informacija?

2.2. Obrazloženje pitanja iz upitnika

U obrazloženju je dato šta sve korisnici IKT-a treba da znaju kako bi bili bezbedni tj. kako bi što

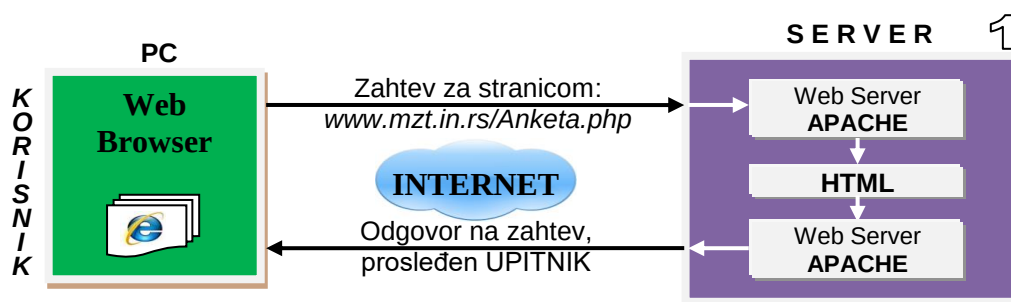
bolje zaštitili svoju privatnost i podatke na internetu.

Tabela 2 – Obrazloženje pitanja iz upitnika

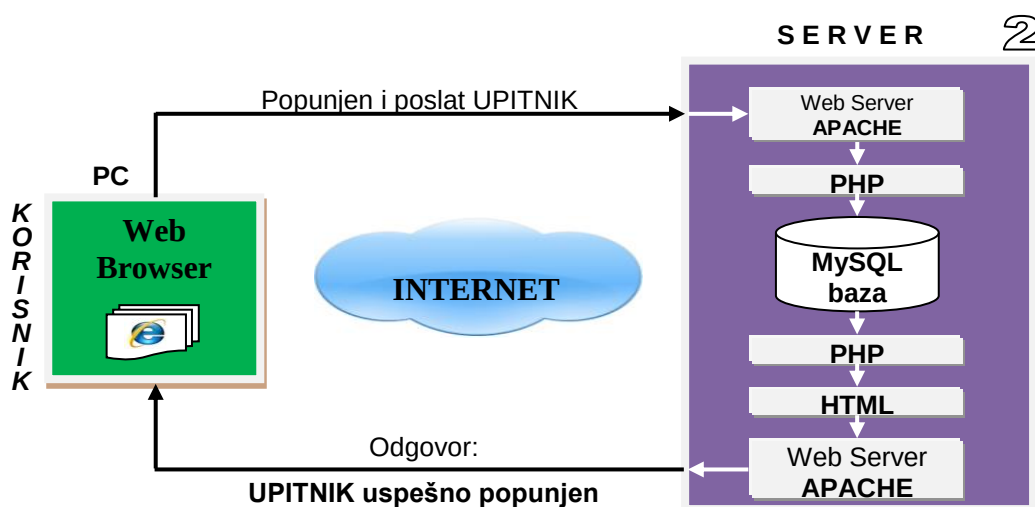
	OBRAZLOŽENJE
1.	Muško, Žensko, Nije važno
2.	Računar, laptop, pametni telefon, tablet.
3.	Korisnici treba da znaju koji OS koriste i da ni jedan od OS (<i>Windows OS</i> , <i>Mac OS</i> , <i>Linux</i> ...) nije apsolutno bezbedan, kao i da novije verzije OS imaju manje bezbednosnih propusta. Novi OS imaju najnoviju i najbolju zaštitu, kao i podršku proizvođača.
4.	Korisnici treba da znaju da li pristupaju sa administratorskim nalogom, koji zlonamernim korisnicima pruža mnogo više privilegija za preuzimanje sistema, nego kada se koristi nalog sa ograničenim funkcijama.
5.	Korisnici treba da znaju da li imaju i da li je ažuriran antivirusni softver ili neki drugi program za zaštitu od malicioznog softvera.
6.	Korisnici treba da prepoznaju nasilje na internetu, ali i da prijave nadležnim organima, jer posledice mogu biti katastrofalne.
7.	Korisnici treba da prijave probleme koje imaju na internetu, jer tako mogu zaštititi i pomoći velikom broju korisnika koji su potencijalne žrtve.
8.	Korisnici treba da znaju da društvene mreže predstavljaju potrebu, ali i opasnost, jer se na njima odvija veliki broj kriminalnih radnji.
9.	Korisnici treba da budu svesni da društvene mreže prikupljaju veliku količinu informacija koje su za nas naizgled nevažne, ali koje spadaju u kategoriju ličnih podataka i koje kriminalni korisnici (Zdnet, 2016), a i velike tehnološke kompanije mogu zloupotrebiti. (Engadget, 2018a)
10.	Korisnici treba da budu upoznati sa svim vidovima nasilja i mogućih metoda iskorišćavanja njihovih ličnih podataka. Krađa identiteta je među pet najobimnijih vrsta internet kriminala (Business reporter, 2016).
11.	Najčešći korisnici su deca i mladi koji predstavljaju najosetljiviju grupu za informacionu bezbednost, jer što su duže u on-line komunikaciji veće su šanse i da budu napadnuti ili zloupotrebjeni.

	OBRAZLOŽENJE
12.	Korisnici treba da budu svesni da skoro svako skidanje i striming datoteka sa interneta povlači za sobom i mogućnost nesvesnog dovlačenja i aktiviranja malicioznog softvera, aki i narušavanje nećijih autorskih prava.
13.	Korisnici treba da budu svesni da gledanjem i slušanjem, tj. njihovim traženjem i izborom mogu ugroziti svoju bezbednost.
14.	Korisnici treba da budu svesni da gledanjem i slušanjem mogu da ugroze nećija autorska prava, što je veoma čest slučaj.
15.	Korisnici treba da razmišljaju o važnosti i potrebi ne samo kvalitetnih (jakih) lozinki, već i o njihovoj redovnoj zameni, kao i da ih ne ponavljaju na više servisa.
16.	Korisnici treba da znaju da je čest slučaj u praksi da zlonamerni korisnici upotrebljavaju otkrivene korisničke lozinke na drugim servisima u potrazi za još nekim nalogom sa koga će slati neželjenu elektronsku poštu, ali i krađu identiteta.
17.	Korisnici treba da znaju značaj jedinstvenih lozinki i da svako zna svoju, a ne i tuđu. Nije dobro deliti pristupne lozinke sa porodicom i prijateljima, jer u svim slučajevima one mogu, svesno ili nesvesno biti zloupotrebjene.
18.	Nije dobra praksa da svako svakome zna lozinku, jer kada dođe do bezbednosnog incidenta nikad se ne zna ko je kriv i gde je nastao problem. Sve ovo otežava rešenje problema.
19.	Pravilno i redovno pravljenje rezervnih kopija je sigurno jedan od najvažnijih elemenata zaštite.
20.	Rezervne kopije treba praviti izvan izvornog digitalnog uređaja, na uređajima ili medijumima koji su fizički odvojeni. Preporuke su, zbog dostupnosti, da to bude negde na mreži, ali da se isključi svaka mogućnost automatskog ažuriranja.
21.	Veliki broj digitalnih uređaja se izgubi ili bude ukraden, a sa njima i važni podaci i informacije. Ovaj segment predstavlja veliki problem za bezbednost.
22.	Danas nema korisnika IT-a koji se nisu susreli sa nekim vidom malicioznog softvera. Jedino se može postaviti pitanje da li su toga svesni i da li su u stanju da prepoznaju oblike savremenog kriminaliteta.

	OBRAZLOŽENJE		OBRAZLOŽENJE
23.	Enkripcija, pored pravljenja rezervnih kopija, predstavlja drugi najvažniji element zaštite. Sva nova IKT rešenja poseduju neki vid enkripcije, da li u procesu komunikacije ili u zaštiti intelektualne svojine.	28.	Ranjivost u sistemu (hardver, softver, mreža, servis...) za koje ni njihovi proizvođači ne znaju da postoje, a koji su čest uzrok napada. (Norton)
24.	Digitalni novac predstavlja sadašnjost i budućnost razmene vrednosnih sredstava. Veliki značaj ima primena savremenih tehnologija gde je skoro nemoguće ispratiti transakciju tj. tok (ko uplaćuje i kome).	29.	Korisnici treba da imaju osnovna saznanja o forenzici i šta uraditi kada se desi bezbednosni incident.
25.	Vrsta malicioznog softvera koja je napravila do sada najveću štetu, kako organizacijama, tako i običnim korisnicima. (Business reporter, 2016)	30.	Korisnici treba da budu svesni da se većina digitalnog kriminala prikriva i da je primena ovih metoda usporila njihovo razjašnjavanje.
26.	DDoS su postali sve veći, kompleksniji ali i učestaliji metod hakerskih napada, koji se koristi za zatrpavanje i obaranje servera, slanjem miliona upita. (Digital attack map)	31.	Korisnici treba da su bar čuli da postoje propisani bezbednosni standardi.
27.	Glavni hakerski napad, gde se od najivnih i lakomislenih korisnika očekuje da ostave svoje poverljive podatke. (Deloitte, 2014)	32.	Osnov za holistički pristup informacionoj bezbednosti od koga treba početi. Sa sadržajima ove familije standarda treba upoznati i edukovati korisnike, jed pored bezbednosne terminologije tu se nalaze i osnovne mere zaštite.
		33.	Ovo je neophodni korak u edukaciji svakog korisnika digitalnih uređaja.
		34.	Korisnici treba da prate preporuke bezbednosnih stručnjaka i da u nekim posebnim situacijama postupaju po njihovim preporukama.



Slika 1 – Blok dijagram povezivanja zahteva korisnika sa odgovorom servera



Slika 2 – Blok dijagram povezivanja poslatog upitnika sa bazom podataka

Blok dijagram (slika 1) pokazuje vezu između principa rada servera i računara korisnika tj. povezivanja zahteva korisnika sa odgovorom servera. Korisnik koji pristupa anketiranju, preko svog Web Browser-a šalje zahtev serveru tako što unosi već naznačenu URL adresu. Server odgovara na zahtev i prosleđuje upitnik.

Korisnik popunjava i šalje upitnik serveru (slika 2) na kome se nalazi **APACHE Web** server koji skladišti primljene podatke u **MySQL** bazu i prosleđuje odgovor klijentu da je anketiranje uspešno obavljeno.

Na kraju, kada administrator baze podataka želi da pregleda i preuzme tabelu sa prikupljenim podacima, takođe, preko Web Browser-a šalje zahtev serveru, tako što unosi određenu URL adresu: <http://mzt.in.rs/preuzmipodatke.php>. Zatim, prostim selektovanjem i kopiranjem tabele, prebacuje podatke u alat za statističku analizu.

2.3. Analiza rezultata istraživanja

Analiza upitnika obuhvata 34 pitanja, od kojih su 3 opšta, a ostalih 31-no pitanje su razvrstani u dve varijable: znanje (15 pitanja) i ponašanje (16 pitanja) korisnika IT-a. Pitanja koja ukazuju na znanje su: 3, 4, 5, 6, 10, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, a ponašanje: 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 22, 33 i 34.

Na osnovu ove dve varijable izabrana je statistička metoda za analizu prikupljenih podataka – χ^2 (Hi) kvadrat test nezavisnosti, koji testira povezanost između dva obeležja jednog skupa (Mann, 2009).

Prikupljeni zbirni rezultati upitnika su analizirani u SPSS (Analyze-Descriptive statistics-Crosstabs) programu za statističku obradu podataka.

Dihotomne¹ varijable – znanje i ponašanje, odn. njihove binarne vrednosti, u upitniku su kodirane sa: 1 (jedan) – za odgovor DA i 0 (nula) – za odgovor NE. Njihove ukupne i zbirne vrednosti, kao i uzajamni odnosi, prikazani su u tabeli 3.

U varijabli znanje, odgovori kodirani 1 pokazuje da postoji znanje, a 0 kada na postavljeno pitanje ne postoji znanje tj. odgovor nije tačan. Analogno tome, u varijabli ponašanje, oznakom 1 je

ocenjeno pozitivno ponašanje u određenoj situaciji, odnosno oznakom 0 negativno ponašanje. Kod ove varijable je izvršeno rekodiranje, jer su neki odgovori u upitniku koji su označeni sa 1 mogli ukazivati na pozitivno odn. negativno ponašanjem.

Tabela 3 – Dihotomne varijable – znanje i ponašanje

			PONAŠANJE		Zbir
			1 – DA	0 – NE	
Z N A N J E	1 – D A	Ukupno	222	396	618
		% znanje	35,9%	64,1%	100,0%
		% ponašanje	34,5%	43,9%	40,0%
		% od ukupnog	14,4%	25,6%	40,0%
N J E	0 – N E	Ukupno	421	506	927
		% znanje	45,4%	54,6%	100,0%
		% ponašanje	65,5%	56,1%	60,0%
		% od ukupnog	27,2%	32,8%	60,0%
Zbir		Ukupno	643	902	1545
		% znanje	41,6%	58,4%	100,0%
		% ponašanje	100,0%	100,0%	100,0%
		% od ukupnog	41,6%	58,4%	100,0%

2.4. Diskusija rezultata

Iz tabele 3, iz pojedinačnih i unakrsnih rezultata može se zaključiti sledeće:

- 35,9% onih koji su pokazali viši nivo znanja (svesti) je istovremeno iskazao i viši nivo bezbednosne kulture, dok je njih 64,1%, naprotiv pokazao niži nivo bezbednosne kulture;
- 45,4% onih koji su pokazali niži nivo bezbednosnog znanja (svesti) je pokazao viši nivo bezbednosne kulture, dok je njih 54,6% pokazao istovremeno i niži nivo bezbednosne kulture.
- Od ukupnog broja ispitanika 40,0% je pokazalo viši nivo znanja, a nasuprot tome 60,0% niži nivo znanja ili bolje reći neznanja pojedinih termina ili pojava u oblasti informacione bezbednosti;
- Sa druge strane 41,6% je pokazalo pozitivno ponašanje u određenim bezbednosnim

¹ „Uglavnom zavisna varijabla sa dve moguće vrednosti, često označene nulom i jedinicom.“ (Metodologija)

situacijama, tj. viši nivo bezbednosne kulture, dok je 58,4% pokazalo niži nivo bezbednosne kulture.

Generalno ove zaključke potvrđuju neke druge studije (Kaspersky, 2014): „i pored straha, korisnici i dalje imaju tendenciju da budu nebezbedni u svojim ponašanjima, jer mnogi ne samo da nemaju instalirana bezbednosna rešenja na svojim uređajima, već ih i ne štite lozinkama, a samo mali broj korisnika su svesni i mogu se suočiti sa pretnjama na netu.“

Takođe, korisnici na društvenim mrežama, bez obzira na to što su upoznati sa činjenicom da su im lični podaci zloupotrebljeni (The Guardian, 2018), nisu značajno promenili svoja ponašanja, kao ni postavke privatnosti (Engadget, 2018b).

Dok se iz tabele 4 može konstatovati da su ispunjene osnovne pretpostavke Hi kvadrat testa, jer je očekivana učestalost u svim ćelijama veća je od 5, tj. u ovom konkretnom slučaju je 257,20.

Tabela 4 – Hi kvadrat test

	Value	df	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	13,753 ^a	1		
Continuity Correction ^b	13,365	1		
Likelihood Ratio	13,840	1		
Fisher's Exact Test			0,000	0,000
Linear-by-Linear Association	13,744	1		
N of Valid Cases	1545			
a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 257,20.				
b. Computed only for a 2x2 table				

Takođe, iz tabele 4 se može konstatovati da je značajna vrednost Hi kvadrata, tj. njegova korigovana vrednost (*Continuity correction*), s obzirom da postoje samo dve kategorije: znanje i ponašanje.

Korigovana vrednost Hi kvadrata je 13,365 sa statističkom značajnošću $p=0,0001$, što je manje od 0,05 (Mann, 2009). Ova vrednost Hi kvadrata

pokazuje statistički značajne razlike između znanja i ponašanja ispitanika.

Tabela 5 – Fi koeficijent korelacije

		Value	Asymp. Std. Error ^a	Approx. T ^b
Nominal by Nominal	Phi	-0,094		
	Cramer's V	0,094		
Interval by Interval	Pearson's R	-0,094	0,025	-3,723
Ordinal by Ordinal	Spearman Correlation	-0,094	0,025	-3,723
N of Valid Cases		1545		
a. Not assuming the null hypothesis.				
b. Using the asymptotic standard error assuming the null hypothesis.				

Ovo je potvrđeno i Fi koeficijentom (Tabela 5) koji predstavlja koeficijent korelacije između dve dihotomne varijable.

Naime vrednost od -0,094 ukazuje na neznatnu i to negativnu korelaciju.

Ovako nizak i to negativan koeficijent korelacije može se tumačiti na sledeći način:

- Ispitanici koji su pokazali viši nivo znanja, a nasuprot tome niži nivo bezbednosne kulture, zapravo to znanje nisu suštinski usvojili i pretvorili ga u svest o potrebi zaštite i potencijalnim opasnostima u digitalnom svetu;
- Ispitanici koji su pokazali niži nivo znanja i pri tome imaju ocenjen viši nivo bezbednosne kulture, zapravo slabije koriste IT, pa time i nisu u prilici da iskažu negativno ponašanje tj. niži nivo bezbednosne kulture;
- Naposljetku, može se reći da su ovakvi rezultati i posledica metode ocenjivanja tj. njene ograničenosti obzirom da ona ocenjuje prisustvo, odnosno odsustvo obeležja koje se istražuje bez daljih kvalifikacija.

3. ZAKLJUČAK

I pored svih ograničenja, ovo istraživanje je pokazalo postojanje nedoslednosti između stečenih znanja (svesti) o informaciono-bezbednosnim rizicima i ponašanju ispitanika što

generalno ukazuje na probleme u srpskom obrazovnom kontekstu tj. da se stečena saznanja ne pretvaraju u praktična znanja koja bi vodila podizanju svesti i time uticala na ponašanja odn. na bezbednosnu kulturu i kulturu u najopštijem smislu.

U tom smislu autor se slaže sa Ejdušom i ostalima (2009) da 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 njihov nivo bezbednosne kulture. 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.

CITIRANI RADOVI

BBC (2018.), preuzeto 20. 8. 2018., sa <https://www.bbc.com/news/world-asia-india-45140158>

Bjelajac, Ž., Zirojević M., (2014), Bezbednosna kultura u eri globalizacije, Institut za međunarodnu politiku i privredu Beograd. Preuzeto 20.8.2018., sa <http://kpolisa.com/KP23/kp23-II-3-BjelajacZirojevic.pdf>

Business reporter (2016), preuzeto 20.8.2018., sa <http://business-reporter.co.uk/2016/05/26/5-costly-types-cyber-crime-2015/?getcat=2>

Business reporter (2016), preuzeto 20.8.2018., sa <http://business-reporter.co.uk/2016/05/26/two-five-consumers-unaware-ransomware-threat-survey-finds/?getcat=2>

Deloitte (2014), preuzeto 20.8.2018., sa <http://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-phishing-awareness.pdf>

Digital attack map, preuzeto 20.8.2018., sa <https://www.digitalattackmap.com/understanding-ddos/>

Ejduš, F., Unijat, J., Milošević M., (2009), Istraživanje i podizanje nivoa bezbednosne kulture mladih, preuzeto 20.8.2018., sa <http://www.bezbednost.org/Svi-projekti/700/Istrazivanje-i-podizanje-nivoa-bezbednosne.shtml#sthash.IRucHXPN.dpuf>

Engadget (2018a), preuzeto 20.8.2018., sa <https://www.engadget.com/2018/06/30/facebook-shared-user-data-with-52-tech-companies/>

Engadget (2018b), preuzeto 20.8.2018., sa <https://www.engadget.com/2018/04/13/facebook-users-aren-t-changing-privacy-settings/>

Kaspersky, Consumer security risks survey 2014: multi-device threats in a multi-device world. Preuzeto 20.8.2018., sa http://media.kaspersky.com/en/kaspersky_lab_consumer_security_risks_survey_2014_eng.pdf

Kuusisto, T., Ilvonen, I. (2003), Information security culture in small and medium size enterprises. *Frontiers of E-business Research*.

Lo, S., M., (2015), Preuzeto 20.8.2018., sa <http://www.mpn.gov.rs/prvo-razmisli-borba-protiv-digital/>

Mann S. P., (2009). Uvod u statistiku, Šesto izdanje, Ekonomski fakultet, Beograd.

Metodologija sa statistikom, Fakultet za specijalnu edukaciju i rehabilitaciju, Univerzitet u Beogradu, preuzeto 20.8.2018., sa <http://metodologija.org/doktorske/tipovi-varijabli/>

Norton, preuzeto 20.8.2018., sa <http://www.pctools.com/security-news/zero-day-vulnerability/>

Roer K., (2015), Build a Security Culture, IT Governance Publishing, United Kingdom, pp.14.

- The Guardian, (2018), preuzeto 20.8.2018., sa
<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- Thomson, K., Solms, R., Louw, L. (2006), Cultivating an organizational information security culture. *Computer Fraud & Security*. 10:7-11.
- Vroom, C., Solms, R., (2004), Towards information security behavioral compliance. *Computers & Security*, 23(3): 191-198.
- Zdnet, (2016), preuzeto 20.8.2018., sa
<http://www.zdnet.com/article/its-2016-and-we-dont-know-who-has-our-personal-data/>

Datum prve prijave:	28.08.2018.
Datum prijema korigovanog članka:	19.03.2019.
Datum prihvatanja članka:	27.03.2019.

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

Style – *APA Sixth Edition*:

Milanović, Z. (2019, 04 15). Informaciono-bezbednosna kultura mladih u Srbiji. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 110-118. doi:10.12709/fbim.07.07.01.13

Style – *Chicago Sixteenth Edition*:

Milanović, Zoran. 2019. „Informaciono-bezbednosna kultura mladih u Srbiji.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 110-118. doi:10.12709/fbim.07.07.01.13.

Style – *GOST Name Sort*:

Milanović Zoran Informaciono-bezbednosna kultura mladih u Srbiji [Časopis] // *FBIM Transactions* / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 110-118.

Style – *Harvard Anglia*:

Milanović, Z., 2019. Informaciono-bezbednosna kultura mladih u Srbiji. *FBIM Transactions*, 15 04, 7(1), pp. 110-118.

Style – *ISO 690 Numerical Reference*:

Informaciono-bezbednosna kultura mladih u Srbiji. **Milanović, Zoran**. [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, *FBIM Transactions*, T. 7, str. 110-118.



KRIPTOVALUTE – NOVI MODEL POSLOVANJA

CRYPTOCURRENCIES - A NEW MODEL OF BUSINESS

Ljubomir Miljković

Poslovni i pravni fakultet „Union – Nikola Tesla“ univerziteta, Beograd, Srbija

Dragana Trnavac

Poslovni i pravni fakultet „Union – Nikola Tesla“ univerziteta, Beograd, Srbija

Kristijan Ristić

Poslovni i pravni fakultet „Union – Nikola Tesla“ univerziteta, Beograd, Srbija

©MESTE

JEL kategorija: **E41, E51, L86**

Apstrakt

Razvoj tehnologije doveo je do stvaranja novih fenomena u finansijskom svetu. Jedan od tih fenomena su kriptovalute, digitalne decentralizovane valute kreirane za „svet budućnosti - koji je globalan i virtuelan, zasnovan na visokosofisticiranim tehnologijama i matematičkim algoritmima. Kriptovalute predstavljaju globalni fenomen novog doba koji je izazvao brojne kontraverze, osude i oduševljenja. Nakon skoro deceniju postojanja, i dalje se ne smiruju strasti podrške i osude kriptovaluta. Nesporna je činjenica da su pored svih osuda i osporavanja kriptovalute opstale, i ne samo to, već zadnjih godina doživljavaju nagli razvoj. Internet i globalizacija su vetar u leđa njihovom razvoju. Svet finansija nema više granica, sve je digitalizovano i u određenoj meri virtuelno. Kriptovalute su nastale kao odgovor na potrebe kreirane trendovima koje donosi budućnost. Kriptovalute danas više nisu naznaka daleke budućnosti, nego realno sredstvo plaćanja sa stvarnim posledicama. Bitcoin i altcoins su u svega par godina postali nosioci jednog novog vremena za trgovinu u kojoj nije potreban posrednik i čije su transakcije gotovo u potpunosti anonimne, što čini veliko odstupanje od dobro poznate prakse. Ne treba preterivati i reći da su postali zamena za novac i dosadašnju poslovnu praksu, ali je njihov uticaj na elektronsku trgovinu sve veći. Prva i najpoznatija kriptovaluta bitcoin obezbedila je svoje mesto u svetu finansija uprkos brojnim osporavanjima. Rast vrednosti bitcoina, njegova sve veća primena i priznavanje od strane određenih zemalja kao sredstva plaćanja otvara put prihvatanju kriptovaluta kao nove generacije valuta, valute budućnosti.

Ključne reči: kriptovaluta, bitcoin, digitalna valuta, internet, međunarodno poslovanje

Abstract

Adresa autora zaduženog za korespondenciju:

Ljubomir Miljković

ljubomir.miljkovic@ppf.edu.rs

The development of technology has led to the creation of new phenomena in the financial world. One of these phenomena is crypt, digitally decentralized currencies created for the "world of



the future - which is global and virtual, based on highly sophisticated technologies and mathematical algorithms. Cryptocurrency represent the global phenomenon of the new era, which has caused numerous controversies, condemnation and enthusiasm. After almost a decade of existence, the passions of support and the condemnation of the crypt are still not calmed down. It is an indisputable fact that in addition to all convictions and denial of the defendant, they have survived, and not only that, in recent years they have experienced rapid development. The Internet and globalization are the backbone of their development. The world of finance has no limits, everything is digitized and to a certain degree virtual. The crypto-logs were created in response to the needs created by the future trends. Crypto-calenders today are no longer a sign of a distant future, but a real means of payment with real consequences. In just a few years Bitcoin and Altcoins have become the bearers of a new time to trade in which no intermediary is needed and whose transactions are almost entirely anonymous, which makes a big departure from well-known practice. It should not be overstated and say that they have become a substitute for money and current business practice, but their impact on e-commerce is growing. The first and most famous bitcoin crypto has provided its place in the world of finance despite numerous denials. The rise in the value of bitcoin, its growing application and recognition by certain countries as a means of payment opens the way to accepting crypts as a new generation of currencies, the currency of the future.

Keywords: cryptocurrency, bitcoin, digital currency, internet, international business

1 KRIPTOVALUTE – SLEDEĆI STEPENIK U EVOLUCIJI NOVCA

Osnovni mehanizam poslovanja i razmene stvari između ljudi čine transakcije. Svi današnji servisi i usluge su zasnovani na tom konceptu. Sa druge strane, ključni problem koji realizacija transakcija sa sobom nosi jeste nepoverenje. Rešenje tog problema je kroz istoriju pronalazeno u posredovanju, a najčešće su to bile banke. Unapređivanje usluge transakcija je vršeno uvek dodatnom zakonskom regulacijom te oblasti i povećavanjem ingerencija posrednika. Ograničavanje moći posrednika, makar delimično, je na sebe preuzimala država. Svedoci smo da su u poslednje vreme pojedine banke postale veće i moćnije od pojedinih država. Globalizacija tržišta je omogućila širenje izvan granica država.

Kriptovalute su digitalne decentralizovane valute, zasnovane na kriptografiji. Kriptografija putem korišćenja šifre i digitalnog potpisa obezbeđuje sigurnost i sprečava moguće falsifikovanje ovih valuta. Glavno obeležje kriptovaluta je činjenica da nijedna institucija ili centralna banka nisu emitenti ovih valuta i ne mogu da utiču na njihov promet. Emisija kriptovaluta je bazirana na kompjuterskom algoritmu koji definiše maksimalno mogući broj emitovanih jedinica neke kriptovalute i uslove povećanja broja jedinica koje su u opticaju. Tvorac algoritma kriptovalute može unapred da definiše i druge karakteristike i ponašanje kriptovalute. Komplexna tehnologija, matematički algoritmi i način na koji funkcioniše su razlozi zbog kojih je skoro nemoguće falsifikovanje. Cena kriptovaluta se formira na osnovu ponude i tražnje i služe za razmenu vrednosti usluga i roba.

Tabela 1. Kriptovalute sa najvećom tržišnom kapitalizacijom na dan 28.03.2019

Naziv kriptovalute	Tržišna kapitalizacija [USD]	Vrednost [USD]
Bitcoin (BTC)	71.759.015.998	4.073,94
Ethereum (ETH)	14.736.097.787	139,78
XRP (XRP)	12.882.502.443	0,308884
EOS (EOS)	3.867.573.212	4,27
Litecoin (LTC)	3.747.415.517	61,35
Bitcoin Cash (BCH)	3.001.485.192	169,61
Binance Coin (BNB)	2.366.150.992	16,76
Stellar (XLM)	2.062.346.565	0,107201
Tether (USDT)	2.052.775.315	1,01
Cardano (ADA)	1.712.422.084	0,066048

Izvor: <https://coinmarketcap.com/all/views/all/>

Kriptovalute danas više nisu naznaka daleke budućnosti, nego realno sredstvo plaćanja sa stvarnim posledicama. Bitcoin i altcoins su u svega par godina postali nosioci jednog novog vremena za trgovinu u kojoj nije potreban posrednik i čije su transakcije gotovo u potpunosti anonimne, što čini veliko odstupanje od ustaljene prakse. Naravno, ne treba preterivati i reći da su postali zamena za novac i dosadašnju poslovnu praksu. Upravo je i cilj rada videti koliki je stvarni uticaj kriptovaluta i srodnih tehnologija na poslovnu klimu, odnosno, konkretno na međunarodno poslovanje.

Kriptovalute sa najvećom tržišnom kapitalizacijom prikazane su u tabeli 1. Najvišu vrednost na tržištu trenutno ima bitcoin sa 4.073 USD (na dan 28.03.2019) dok ostale kriptovalute po ceni osetno zaostaju. Za kriptovalute se može reći da u jednom delu predstavljaju sporno područje, budući da su pogodne za obavljanje nezakonitih aktivnosti zbog nedostatka jedinstvene regulacije, odnosno nepostojanja institucije zadužene za upravljanje. Budući da nema regulacije i da kriptovalute omogućuju visoku mogućnost privatnosti, često se povezuju sa ilegalnim aktivnostima, pa je u nekim zemljama zabranjeno njihovo korišćenje.

2 BITCOIN – NAJPOZNATIJA KRIPTOVALUTA

Bitcoin (Nakamoto, 2009) je prva kripto valuta (crypto-currency) nastala na blockchain

tehnologiji. Tačnije, objavljeni su istovremeno 2009. godine, od strane anonimnog autora. Nešto kasnije je uočeno da blockchain kao tehnologija može da bude iskorišćen i za druge namene, osim realizacije kripto valuta. Bitcoin je programiran tako da postoji konačna količina novčića koja će moći da bude rudarena, te neće biti moguće dodatno štampanje novčića i veštačko izazivanje inflacije. Algoritam blockchain-a praktično sprečava mogućnost duplog trošenja novca. Za razliku od prethodnih sistema za digitalni novac, kod Bitkoina praktično ne postoji novac. Postoji blockchain koji se ponaša kao javno dostupna glavna knjigovodstvena knjiga, u kojoj su zapisane sve transakcije ikada realizovane. Do informacije o tome koliko koji korisnik poseduje novca, i može li deo tog novca proslediti dalje, dolazi se praktično izračunavanjem svih prethodnih transakcija, koje su javno dostupne. Ukoliko pokušamo trošenje novca koji nemamo, rudari neće validirati našu transakciju i ona će biti odbijena. Anonimnost korisnika je obezbeđena time što u transakcijama učestvuju takozvani novčanici (wallet), koji se predstavljaju parom javnih i privatnih ključeva. Samo posedovanje privatnog ključa za novčanik omogućuje dalju manipulaciju sredstvima. Tu leži i najveći rizik po krajnje korisnike – ukoliko iz bilo kog razloga izgubimo privatne ključeve svog novčanika, ili nam ih neko ukrade, ne postoji više mogućnost da povratimo kontrolu nad svojim sredstvima. (Minović, 2017)



Slika 1. Kretanje cene bitkoina

Izvor: (coindesk, 2019)

Godine 2009. kad je BTC plasiran, nije bilo sasvim jasno kako i gde se može trošiti. Sada se može kupiti praktično sve. Na primer, velike kompanije kao što su Microsoft i Dell primaju uplate u BTC-u za niz svojih proizvoda i digitalnog sadržaja. Možete leteti sa aviokompanijama kao što su AirBaltic i Air Lithuania, kupiti karte za pozorište putem engleskog Theatre Tickets Direct, uzeti nekoliko boca zanatskog piva od Honest Brew pivare itd. Ostale opcije uključuju plaćanje hotela i kupovinu imovine, namirivanje računa u različitim barovima i restoranima, priključivanje sajtovima za upoznavanje, kupovinu poklon vaučera, kladenje u onlajn kazinu i dobrotvorne donacije. Postoji takođe niz različitih onlajn tržišta koji trguju sa svim, od ilegalnih supstanci do vrhunskih, luksuznih predmeta. Bitcoin je relativno nov i prilično složen proces plaćanja. Prirodno je što su potrošačke opcije i dalje ograničene, ali svakog dana sve više preduzeća - od malih, lokalnih kafića do industrijskih giganta - prihvata plaćanje u bitcoinu.

3 BLOCKCHAIN TEHNOLOGIJA

Kriptovalute se zasnivaju na tehnologiji pod nazivom blockchain, koja je okosnica cele priče. Blockchain je digitalna knjiga koja sadrži sve transakcije ikad napravljene u mreži i garantuje da su one legitimne i tačne. Bezbednost je garantovana i upotrebom kriptografskih ključeva. Zapis blockchain transakcije se ne može retroaktivno menjati bez promene svih narednih blokova što zahteva dogovor unutar mreže čime je neizvesnost učesnika u pogledu bezbednosti podataka marginalna. Blockchain se često definiše kao protokol za razmenu vrednosti, koja zasnovana na blokovima može biti brža, sigurnija i jeftinija nego kod tradicionalnih sistema. Ova tehnologija se bazira na ideji da više nije potrebna jedna ustanova koja će sve transakcije procesuirati, već je celi sistem decentralizovan i transparentan. Upotreba blockchain tehnologije je inovativna i nudi veliki broj zanimljivih i efikasnih rešenja, a primenjiva je u različitim oblastima. (Bojić, 2017) Organizovana je u formi jednostruko spregnute liste (lanac), gde su čvorovi blokovi sa podacima o transakcijama, koji se posle grupisanja štite kriptografskim metodama. Otuda i naziv blockchain. U pitanju je sistem koji omogućuje realizaciju digitalnih transakcija bez

posrednika. Zasnovana je na P2P arhitekturi, gde čvorovi koji učestvuju u realizaciji servisa poseduju kopiju svih zapisa, te stalno međusobno komuniciraju i sinhronizuju zapise. Pored toga, uloga pojedinih čvorova je i da stalno vrše verifikaciju autentičnosti zapisa koji se nalaze u lancu, te da odbace predložene blokove podataka, ukoliko ne prođu verifikaciju. Po tom modelu, neophodno je da 51% mreže radi svoj posao, i mreža ne može biti ugrožena plasiranjem lažnih podataka. Sa druge strane, preuzimanje većeg broja čvorova u mreži bi bio izuzetno komplikovan i skup poduhvat, te bi naponi za to daleko prevazišli napore potrebne da se ugrozi bilo koji centralizovan servis. Stoga se ovakav pristup čuvanju podataka smatra daleko bezbednijim u odnosu na centralizovane baze podataka. Podaci u lancu mogu biti javno dostupni, kakav je slučaj sa Bitcoin mrežom, ili pak mogu biti zaštićeni ili privatni (kod poslovnih sistema). Rudari (miners) su čvorovi mreže koji poseduju dosta računarskih resursa, koje stavljaju na raspolaganje za verifikaciju blokova. Oni praktično proveravaju na osnovu prethodnih transakcija da li pošiljalac poseduje dovoljno sredstava na računu. Kako bi se obezbedila demokratskost u procesu validacije, odnosno mogućnost da baš svaki rudar dobije priliku da njegov čvor bude uzet kao validan, oni dobijaju i računarski intenzivan zadatak, koji moraju da reše. Upravo na njega i troše najveći deo svojih resursa. Nagradu dobija onaj koji prvi pošalje validiran blok sa rešenim zadatkom. Ovakav pristup odabiru inicijalno validnog bloka transakcija se naziva dokaz-posla (proof-of-work) i praktično štiti mrežu od zloupotreba. Osnovni nedostatak ovog pristupa jeste velika potrošnja struje, kao i brzina. Tehnologija implementirana za Bitcoin lanac omogućuje maksimalno 7 transakcija po sekundi. Novije implementacije lanaca implementiraju i novije algoritme, koji omogućuju brži i efikasniji izbor kandidata. Na kraju, validiran blok dobija svoju jedinstvenu vremensku oznaku (timestamp) i potpis (hash), te se kao takav propagira na ostale čvorove u mreži. Pri dodavanju svakog narednog validiranog bloka, inkrementira se brojač potvrda za prethodno upisane blokove, te se dalje smanjuje verovatnoća da su oni lažni. Dakle, protokom vremena raste pouzdanost zapisanih podataka.

4 KRIPTOVALUTE I MEĐUNARODNO POSLOVANJE

Činjenica koja ne ide u prilog mogućnosti inflacije kriptovaluta jeste činjenica da se kriptovalute dele gotovo do nule. S obzirom na to da je količina određene kriptovalute ograničena nije moguća inflacija koja bi predstavljala gubitak vrednosti zbog pojave novoskovanih istih valuta u kratkom vremenu. U skladu sa tim, kriptovalute nisu klasična valuta, već predstavljaju imovinu, sličnu zlatu. S tim u vezi, za „uspeh” i „propast” kriptovaluta ne garantuje nijedna institucija. Alternativu im je moguće naći izborom bilo koje od drugih kriptovaluta. Prema tome, konkurencija kriptovaluta liči na konkurenciju među društvenim mrežama. One, baš kao i najpoznatije kriptovalute, zbog određenih karakteristika i imidža, imaju mnogo korisnika. Osim toga, kod kriptovaluta postoji velika mogućnost arbitraže u smislu trgovine na različitim berzama ili prelaska u druge kriptovalute što odgovara profesionalnim investitorima. Najšira upotreba kriptovaluta je u vidu online plaćanja. Danas su, uz plaćanje kreditnim karticama i preko Paypal sistema, najpopularniji oblici plaćanja na internetu upravo kriptovalute. (Meisser, 2013) Kao prirodan nastavak online plaćanja, a bez obzira na navedene rizike, dve kompanije mogu da naprave svoje kriptovalutne „novčanike” koje će koristiti kao pravne osobe. Naime, pravna lica mogu da ugovore koji će servis koristiti tako da se posle transakcije kriptovaluta prebacuje na račun banke baš kao i standardna valuta. Kriptovalute i postojeća tehnologija predstavljaju novo doba u svetskoj ekonomiji, trgovini i finansijskom tržištu. Iako se zabeleženi napredak nadovezuje na prednosti koje je tehnologija napravila po pitanju fizičkih osoba, u vidu raznih mobilnih i s internetom povezanih načina plaćanja i komunikacije, kriptovalute ipak imaju određeni segment rezervisan isključivo za međunarodno poslovanje među pravnim osobama. Jednako kako su mnogi loše procenili uticaj koji će imati bitcoin u svetu te samim time propustili priliku za zaradom, postoje naznake da je slično moguće u trenutku u kojem kompanije trebaju usvojiti kriptovalute te blockchain u svoje poslovanje. Doduše, pojedinci unutar kompanija i institucija poučeni prošlošću ovaj put ne skrivaju svoj interes za aktivnim učestvovanjem u revolucionizaciji međunarodnog poslovanja. Danas su najpopularniji oblici plaćanja na internetu kreditne kartice, koje se nisu znatno unapredile u zadnjih

20 godina pa su podložne prevari. Drugi popularan način je Paypal, ali pati od sličnih problema. Naravno, to se najčešće odnosi na transakcije pojedinaca, ali nije uvek tako. Business to business transakcije (B2B) često su komplikovanije. Glavni razlog za to je duži proces završetka same transakcije, što zbog dogovorenog načina plaćanja, što zbog same verifikacije plaćanja. Nezavisno o tome, ne postoji razlog zašto se šema plaćanja ne bi odvila uz pomoć kriptovaluta. Dve kompanije otvore svoje kriptovalutne lisnice koje će koristiti kao pravne osobe. Kompanije se dogovore koji će online servis isplate kriptovaluta koristiti, prilikom čega se kriptovaluta prebacuje na bankovni račun baš kao i standardna valuta. Dobije se potvrda o završetku transakcije, a sve je obavljeno bez komplikacija u vidu posebnih pinova, chipova ili terminala. (Turudić, Milić, & Štulina, 2017) Dobar temelj za korišćenje kriptovaluta u međunarodnom poslovanju bi se sagradio u slučaju stvaranja kriptovalute pod državnim pokroviteljstvom. Prema Deloitteovoj studiji delovalo bi slično kao bitcoin. Platiodci bi mogli koristiti elektroničku lisnicu na pametnom telefonu ili računaru za slanje novca prema javnim adresama primaoca.

5 ZAKLJUČAK

Tehnologija je omogućila slobodu i brzinu koja se više ne može zaustaviti. Ljudi ne žele da neko ograničava njihovo raspolaganje vlastitom imovinom ili da im je oduzima i umanjuje vrednost kada on hoće. Digitalno doba briše granice i zabrane, a u skladu sa tim traži i temeljne izmene u svim sferama života, pa tako i u finansijama i monetarnoj ekonomiji. Nasuprot potreba i tražnje koju je donela tehnologija, imamo finansijske i političke centre moći koji vekovima kroz kontrolu novčane mase, odnosno valuta, upravljaju celim svetom. Blockchain tehnologija na kojoj se zasnivaju kriptovalute predstavlja srž digitalne revolucije i izuzetno je važna za finansijsku industriju. Ova tehnologija zbog načina na koji funkcioniše mogla bi da promeni percepciju shvatanja vrednosti, te načina i mogućnosti kako se neka vrednost može imati i prenositi. Budućnost nosi velike promene i velike turbulencije, a pojava i razvoj kriptovaluta je samo početak novina koje bi budućnost mogla doneti pre svega u poslovanju kompanija.

Bitcoin predstavlja specifičnu valutu koja se po svojim karakteristikama razlikuje od svih svojih prethodnika. Otkad se pojavila pokrenula je niz

kontroverzi vezanih za pozitivne i negativne efekte njene primene. Emisija ove valute je kompjuterski programirana i ograničena, zasnovana na „peer-to-peer“ tehnologiji i tehnologiji enkripcije podataka čime se faktički eliminiše mogućnost dvostrukog plaćanja, falsifikovanja i sličnih zloupotreba. To je ujedno i jedan od glavnih razloga zbog čega se ova valuta smatra sigurnom iako ne postoji centralna emisiona institucija. Transakcioni troškovi su veoma niski, gotovo su zanemarljivi, ali same transakcije nisu reverzibilne, što se može oceniti značajnim nedostatkom ove valute.

Međutim, s obzirom na činjenicu da je makroekonomski značaj bitcoina zanemarljivo mali, čak i manji šokovi mogu negativno uticati na njegovu stabilnost i izazvati drastične fluktuacije deviznog kursa. Pritom, ne postoji centralna institucija koja bi mogla svojim merama pozitivno da utiče na njegovu stabilizaciju, a što može predstavljati značajnu prepreku za masovnije korišćenje ove valute.

Kakva će biti budućnost bitcoina i sličnih kriptovaluta zavisice kako od regulacije ovakvih valuta, tako i od njihove sigurnosti i stabilnosti.

CITIRANA DELA

- Bojić, B. (2017). Stanje i perspektive kriptovaluta. *Naučno-stručni časopis STVAROG*(15), 185-186.
- coindesk. (2019, 03 18). *Bitcoin Price (BTC)*. Preuzeto sa coindesk: <https://www.coindesk.com/price/bitcoin>
- Meisser, L. (2013). *Bitcoin - A Promise of Freedom*. Next Generation Finance.
- Minović, M. (2017). *Blockchain tehnologija: Mogućnosti upotrebe izvan kripto valuta*. Arandjelovac: INFOTECH.
- Nakamoto, S. (2009). *Bitcoin - A Peer-to-Peer Electronic Cash System*. Preuzeto sa <https://bitcoin.org/bitcoin.pdf>
- Turudić, A., Milić, J., & Štulina, K. (2017). Korišćenje kriptovaluta u međunarodnom poslovanju. *Zbornik sveučilišta Libertas*(1-2), 199-202.

Datum prve prijave: 09.09.2018.
Datum prijema korigovanog članka: 18.03.2019.
Datum prihvatanja članka: 27.03.2019.

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

Style – APA Sixth Edition:

Miljković, L., Trnavac, D., & Ristić, K. (2019, 04 15). Kriptovalute – novi model poslovanja. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 119-124. doi:10.12709/fbim.07.07.01.14

Style – Chicago Sixteenth Edition:

Miljković, Ljubomir, Dragana Trnavac, i Kristijan Ristić. 2019. „Kriptovalute – novi model poslovanja.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 119-124. doi:10.12709/fbim.07.07.01.14.

Style – GOST Name Sort:

Miljković Ljubomir, Trnavac Dragana i Ristić Kristijan Kriptovalute – novi model poslovanja [Časopis] // *FBIM Transactions* / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 119-124.

Style – Harvard Anglia:

Miljković, L., Trnavac, D. & Ristić, K., 2019. Kriptovalute – novi model poslovanja. *FBIM Transactions*, 15 04, 7(1), pp. 119-124.

Style – ISO 690 Numerical Reference:

Kriptovalute – novi model poslovanja. **Miljković, Ljubomir, Trnavac, Dragana i Ristić, Kristijan**. [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, *FBIM Transactions*, T. 7, str. 119-124.



USVOJEN ZAKON O NACIONALNOM DNK REGISTRU U REPUBLICI SRBIJI

ADOPTION OF THE LAW ON NATIONAL DNA REGISTER IN THE REPUBLIC OF SERBIA

*Rad je napisan u pomen na prof. dr Slobodana Batu Petrovića, ex dekana KPA
The paper is written in the mention of prof. dr Slobodan Bata Petrović, ex dean of the KPA*

Željko Nikač

Kriminalističko-policijski univerzitet, Beograd, Srbija

© MESTE

JEL kategorija: **K14**

Apstrakt

Narodna skupština Republike Srbije usvojila je sredinom prošle godine novi Zakon o nacionalnom DNK registru koji je najvažniji pravni izvor za forenzičke analize i veštačenja, pre svega u kontekstu otkrivanja i rasvetljavanja najtežih krivičnih dela i izvršilaca. U pitanju je propis koji je od izuzetnog značaja za procesuiranje krivičnih dela i izvršilaca, donošenje merodavnih sudskih odluka i sankcionisanje izvršilaca. DNK Registar je uspostavljen radi utvrđivanja identiteta nestalih i nepoznatih lica, utvrđivanje identiteta leševa i delova tela. Baza DNK profila koja je uspostavljena sadrži profile nespornih i spornih bioloških uzoraka, koji su utvrđeni u krivičnom postupku i dostavljeni centralnoj laboratoriji NKTC MUP RS. Podaci koji se nalaze u DNK Registru su pre svega lični i stoga treba iskazati veliku senzibilnost i obazrivost u postupanju, ne sme narušiti integritet ličnosti i mora se obezbediti njihovo zakonito korišćenje. U kontekstu poznate Prum konvencije (tzv. Šengen III/ i aplikacije Srbije za prijem u EU, autor sugeriše uspostavljanje trajne baza DNK podataka i unapređenje postupka veštačenja i uz poštovanje nacionalne legislative.

Ključne reči: DNK Registar, baza podataka, rasvetljavanje krivičnih dela, identifikacija izvršilaca, leševa, nestalih i nepoznatih lica, Srbija i EU.

Abstract

In the middle of last year, the National Assembly of the Republic of Serbia adopted a new Law on the National DNA Registry, which is the most important legal source for forensic analysis and expertise, primarily in the context of the detection and clarification of the most serious crimes and perpetrators. This is a regulation that is of great importance for the prosecution of criminal offenses and perpetrators, the adoption of relevant court decisions and the sanctioning of perpetrators. The DNA was established to establish the identity of the missing and unknown persons, identify the identity of the bodies and parts of the body. The DNA profile database that has been established contains profiles of

Adresa autora:

Željko Nikač

zeljko.nikac@kpu.edu.rs



uncontested and controversial biological samples, which were established in the criminal procedure and submitted to the central laboratory of the NCTC MOI RS. The data contained in the DNA register are primarily personal and therefore should show great sensitivity and caution in the treatment, must not violate the integrity of the personality and must be ensured their legal use. In the context of the famous Prum Convention (the so-called Schengen III) and the application of Serbia for admission to the EU, the author suggests the establishment of a permanent database of DNA data and the improvement of the expert procedure and with respect to national legislation.

Keywords: DNA Register, databases, clarification of criminal offenses, identification of perpetrators, corpses, missing and unknown persons, Serbia and EU.

1 UVOD

Borba protiv terorizma, organizovanog kriminala i drugih najtežih pojava oblika **kriminaliteta**, u današnje vreme, nije moguća bez adekvatne legislativne osnove, specijalizovanih agencija za primenu zakona, edukovanih kadrova, međunarodne i multiagencijske saradnje, savremene opreme i upotrebe naučnih metoda. Vodeće službe razvijenih država poput američkog FBI-a, Interpola i Europol koriste rezultate tehničko-tehnološkog napretka u svetu u borbi protiv zločina, njegovoj prevenciji i procesuiranju izvršilaca krivičnih dela.

U tom kontekstu posebno mesto danas zauzima **forenzika** koja je postala izuzetno popularna poslednjih decenija minulog i početkom ovog veka, kada je dostignut izuzetno visok nivo razvoja informacionih tehnologija. U pitanju su veliki informacioni sistemi koji su omogućili prepoznavanje lica, tragova i materijala od interesa za kriminalističke istrage. Savremena forenzika je specifična multidisciplinarna oblast u kojoj se primenjuju metodi fundamentalnih i primenjenih nauka s ciljem identifikacije tragova od značaja za procesuiranje zločina i zločinaca. Poznavanje naučnih metoda je važan prvi korak u forenzičkoj obradi kriminalnih događaja koji omogućava potrebne analize, pouzdane identifikacione rezultate i njihovo tumačenje na sudu. Primena forenzičkih metoda obuhvata nekoliko oblasti: kriminalističku, državnu i komercijalnu. (Grupa autora, 2011).

Na prostorima nekadašnje SFRJ, njenih država naslednica i Republike Srbije primena forenzike i posebno DNK (dezoksiribonukleinske kiseline) veštačenja nije bila dugo praktikovana zbog

nedovoljnog poznavanja metoda, postojanja oskudnih materijalnih resursa svake od zajednica, a u konačnici i zbog velikih troškova. Šira javnost nije bila upoznata s mogućnostima **DNK veštačenja**, dok se u stručnim krugovima pojavilo nekoliko pionirskih radova iz ove oblasti u kojima je ukazano na primenu u sudskim procesima (Obradović, 2000, 99-150). S društvenim promenama i reformama koje su pokrenute u Srbiji i ostalim državama ex Jugoslavije aktuelizovano je i pitanje upotrebe ove tehnologije u funkciji identifikacije izvršilaca krivičnih dela i prepoznavanja lica na osnovu biometrijskih karakteristika, lešnih i koštanih ostataka, tragova s mesta događaja kao i ispitivanja psihološkog, socijalnog i pravnog aspekta ličnosti (Miljković, 2000, 151-171).

Legislativni okvir za DNK i druga forenzička veštačenja po prvi put je utvrđen odredbama ranijeg Zakonika o krivičnom postupku (ZKP) iz 2001.godine.¹ Nakon prestanka postojanja Državne zajednice Srbije i Crne Gore 2006. godine nove nezavisne države regulisale su ovu materiju nacionalnim propisima. Republika Srbija je već u noveliranom ZKP 2011 i kasnijim izmenama i dopunama usvojila jedan broj rešenja u kojima se predviđa forenzičko veštačenje. Tako se u čl.130 predviđa **forenzičko-genetička analiza**² materijala i otisaka papilarnih linija pri obdukciji leša, zatim kod uviđaja (čl.133) i kada se angažuju stručna lica forenzičke, saobraćajne, medicinske ili druge struke, kod uzimanja biometrijskih uzoraka (čl.140 forenzička registracija osumnjičenog) te kod uzimanja uzoraka za forenzičko-genetičku analizu (čl.142).³ Pored propisa iz oblasti pravosuđa pitanja

¹ ZKP (stari), "Službeni list SRJ" br.70/01 i "Službeni glasnik RS" br.58/04, 85/05, 115/05, 49/07, 20/09, 72/09.

² Vidi više: (Primorac & Schanfield, 2016)

³ ZKP (važeći), "Sl.glasnik RS" br.72/11, 101/11, 121/12, 32/13, 45/13 i 55/14.

forenzičkih i drugih veštačenja dopunski su regulisana odredbama policijskih propisa kao što su bili ranije doneti Zakon o policiji⁴ i podzakonski akti poput Pravilnika o policijskim ovlašćenjima.⁵

Veliki značaj je imalo i usvajanje Zakona o posebnim merama za sprečavanje vršenja krivičnih dela protiv polnih sloboda prema maloletnim licima,⁶ posebno u delu koji se odnosi na posebne evidencije koje sadrže pored ostalog i DNK profile osuđenih lica. U pitanju je propis poznat u srpskoj javnosti pod kolokvijalnim nazivom *Marijin zakon* donet po pokojnoj devojčici M.J. (staroj 8 godina) iz Starih Ledinaca kod Novog Sada, koja je brutalno ubijena 26.06.2010. godine od strane višestrukog povratnika osuđivanog za seksualne delikte prema deci i maloletnicima.

U minule dve decenije ovog veka beležimo znatan porast obavljenih sudskih i drugih veštačenja za potrebe organa pravosuđa i policije, među kojima se posebno ističu forenzička biološka veštačenja (Obradović, 2004, 138-156). Potreba za DNK veštačenjima postoji zbog povećanja broja krivičnih dela i njihove prirode, kao i zahteva da dela budu otkrivena i izvršiocu procesuirani uz valjane dokaze. Krajnji cilj je sudski epilog i adekvatne sankcije za počinioce, dok bi žrtve trebale da dobiju adekvatnu satisfakciju. U tom smislu je grupa naših eksperata svojevremeno pokrenula pitanje izgradnje **baze DNK podataka** na osnovu koje bi se u toku veštačenja vršila upoređivanja materijala te bi se moglo doći do veze između lica i predmeta (Simonović, 2012).

2 ZAKON O NACIONALNOM DNK REGISTRU – sistematika i važnija rešenja

U istorijskom osvrtu treba podsetiti da je zakonodavna aktivnost na izradi ovog propisa počela znatno ranije. Tako je još 2004. godine osnovana Radna grupa za pripremu Nacrta Zakona o Agenciji za vođenje DNK registra. Posle kratkog perioda delovanja Radnu grupu je zamenila Komisija za reformu pravosuđa RS, koja je dalje formirala *ad hoc* Radnu grupu. Radna

grupa je relativno brzo završila rad, pripremila i predala Ministarstvu pravde 2006. godine *Nacrt Zakona o Agenciji za vođenje DNK registra*. Radna grupa je uvažila prethodni Nacrt koji je pripremila Komisija i sačinila radni tekst koji je u znatnoj meri bio harmonizovan s normama nacionalnog krivičnog zakonodavstva – KZ, ZKP, Zakonom o izvršenju krivičnih sankcija i Zakonom o maloletnim učiniocima krivičnih dela i krivično-pravnoj zaštiti maloletnih lica (Obradović, 2018, 18-21). Nakon toga rad na izradi finalnog teksta i usvajanju ovog propisa je potpuno zamro iz nepoznatih razloga. Pretpostavljamo da je osnovi razlog činjenica da isti propis nije bio među prioritetima u agendi propisa.

U Republici Srbiji je nedavno usvojen **Zakon o nacionalnom DNK registru**⁷ kao *lex specialis* propis u ovoj materiji. Zakon je od izuzetnog značaja za postupanje nadležnih organa u procesuiranju krivičnih dela i osumnjičenih (optuženih, okrivljenih) u sudskim postupcima, posebno gde je potrebno sofisticirano dokazno sredstvo koje može da pruži baza DNK podataka.

Sa stanovišta pravne tehnike novi Zakon o nacionalnom DNK registru je kratak i relativno jezgrovit zakonski tekst. U pitanju je propis koji ima ukupno jedanaest (11) odredaba koje uslovno možemo podeliti u tri kratka dela: uvodni, centralni i zaključni.

2.1 Uvodni deo

U uvodnom delu zakonodavac je ukazao na predmet zakona, značenje pojedinih izraza i upotrebu rodno osetljivog jezika (čl.1-3).

Predmet Zakona je uspostavljanje i sadržina nacionalnog registra koji je rezultat forenzičko-genetičke analize DNK za potrebe krivičnog postupka, utvrđivanja identiteta nestalih ili nepoznatih lica i leševa, delova tela, kao i obrada podataka dobijenih forenzičko-genetičkom analizom kao i druga pitanja od značaja za vođenje Registra. Pomenuto određenje u čl.1 je ekstenzivno i smatramo ga kao dobro rešenje jer se njime, pored normi krivičnog prava, uređuje uspostavljanje i sadržina registra od značaja za

⁴ Zakon o policiji (stari), „Sl.glasnik RS“ br.101/05, 63/09, 92/11,92/11,64/15.

⁵ Pravilnik o policijskim ovlašćenjima, „Sl.glasnik RS“ br.54/06. Više: (Nikač Ž. , 2008)

⁶ Zakon o posebnim merama za sprečavanje vršenja krivičnih dela protiv polnih sloboda prema maloletnim licima, „Sl. glasnik RS“ br.32/13, 55/2014 (čl.13).

⁷ Zakon o nacionalnom DNK registru, „Sl.glasnik RS“ br.24/18.

utvrđivanje identiteta nestalih ili nepoznatih lica, leševa ili delova tela.⁸

Dalje se u čl.2 podrobnije određuju stručni izrazi, pojmovi i termini od značaja za primenu zakona, pa ukazujemo na važnije: a) *DNK analiza* je određena kao forenzičko-genetička analiza biološkog materijala, izvršena za potrebe krivičnog postupka ili postupka utvrđivanja identiteta, kojom se dobijaju DNK profili, koji se unose u Registar; b) *lokus* je određeni specifični deo molekula DNK; c) *alel* je varijanta određenog lokusa; d) *DNK profil* je podatak koji predstavlja rezultat DNK analize. Jedinstveni DNK profil je DNK profil utvrđen analizom nespornog ili spornog biološkog uzorka poreklom od jedne osobe, dok je mešani DNK profil utvrđen analizom biološkog uzorka poreklom od više od jedne osobe; e) Evropski standardni set (ESS) označava međunarodno usvojeni skup lokusa; f) *Interpolov standardni set lokusa (ISSOL)* je međunarodno usvojeni skup lokusa koji koristi Interpol; g) *biološki uzorak*, u smislu ovog zakona, je svaki biološki materijal humanog porekla, koji se može dovesti u vezu sa krivičnim delom ili uzorak uzet u cilju utvrđivanja identiteta, na kojem se može izvršiti odgovarajuća DNK analiza; h) *nesporni* biološki uzorak je biološki materijal uzet od lica ili leša kome je prethodno utvrđen identitet; i) *sporni* biološki uzorak je biološki materijal nepoznatog porekla.⁹

Mišljenja sam da je možda bilo oportuno opterećivati tekst propisa tehničkim normativima kao što su Evropski standardni set i Interpolov standardni set, jer se radi o tehničkim standardima koji su promenljivog karaktera s obzirom da je forenzička genetika veoma dinamična. U svakom slučaju ovaj nomotehnički "višak" nije od posebnog značaja jer je propis relativno kratak, dok u primeni preovlađuje ekspertski pristup stručnjaka za DNK analize.

2.2 Centralni deo

Centralni deo zakona obuhvata odredbe od čl.4 do čl.8 koje se odnose na uspostavljanje, vođenje,

cilj i svrhu uspostavljanja Registra, sadržinu Registra, prikupljanje rezultata DNK analize, upoređivanje DNK profila i čuvanje podataka u Registru.

Predviđeno je da Registar DNK vodi MUP RS preko nadležne forenzičke službe koja je odgovorna za čuvanje i tačnost podataka.¹⁰ Forenzička služba je sastavni deo Direkcije policije MUP RS – Uprave kriminalističke policije (UKP), tačnije dela poznatog pod nazivom *Nacionalni kriminalističko tehnički centar* (NKTC). Posebnom odlukom Nacionalnog akreditacionog tela RS od 28.08.2014. godine, NKTC je akreditovan kao nacionalna referentna ustanova.¹¹ Sertifikat predstavlja verifikaciju o usklađenosti uvedenog sistema kvaliteta sa zahtevima međunarodnog standarda SRPS ISO/IEC 17025:2006, koji je identičan standardu ISO/IEC 17025:2005 (Nesic L. et al, 2016).

Pored laboratorije MUP RS u prethodnom periodu korišćene su i pojedine druge laboratorije u okviru: BU (Medicinski i Biološki fakultet), KC Niš i Novi Sad, pojedine privatne laboratorije i laboratorija BIA. Sada je DNK laboratorija NKTC MUP RS uspostavljena kao referentna nacionalna ustanova u ovoj materiji, u skladu sa čl.140 – 143. ZKP, u vezi sa čl.279 istog zakona, koji predviđa da se aktom Vlade RS uređuje vođenje evidencija o uzetim uzorcima za forenzičko-genetičku analizu, njihovo čuvanje i uništavanje.¹²

Svrha uspostavljanja Registra je vođenje krivičnog postupka i utvrđivanja identiteta nestalih ili nepoznatih lica i leševa i delova tela.¹³ Podaci iz Registra mogu se obrađivati samo na način da bi se postigla svrha obrade za koju su podaci prikupljeni, odnosno nije dozvoljena obrada podataka na osnovu koje se mogu ustanoviti fizičke, biohemijske, fiziološke ili psihološke karakteristike, odnosno specifične nasledne osobine.¹⁴

U delu stručne javnosti su se pojavile sumnje u poziciju DNK laboratorije NKTC kao jedine referentne laboratorije po ovom zakonu, posebno

⁸ Op.cit. u nap.7, čl.1.

⁹ *Ibid*, čl.2.

¹⁰ *Ibid*, čl.4.

¹¹ Sertifikat o akreditaciji NKTC br.01-413 od 28.08.2014.g.

¹² Op.cit. u nap.3. Postupak obuhvata uzimanje biometrijskih uzoraka (čl.140 ZKP), uzimanje uzoraka biološkog porekla (čl.141) i uzimanje uzoraka za forenzičko-genetičku analizu (čl.143).

¹³ *Ibid*, čl.4.st.3

¹⁴ *Ibid*, čl.4.st.4.

u smislu potencijalnih zloupotreba podataka. Stav se dalje obrazlaže time da experti MUP RS učestvuju u fazi predistražnog postupka i da Centar poseduje osetljive podatke, pa to daje osnova za sumnju u nepristrasnost u radu i moguće "curenje" podataka (Obradović, 2018, 20). Mišljenja smo da ova primedba ne stoji jer se ne može *a priori* unapred, bez početnih indicija i činjenica, sumnjati u status Centra i rad njegovih eksperata koji imaju relevantne reference i akreditaciju nadležnog tela RS.

U pogledu vođenja Registra predviđeno je da se ažuriranje i brisanje, rokovi čuvanja i mere zaštite podataka u Registru detaljnije regulišu posebnim zakonom, kojim se uređuju evidencije i obrada podataka u oblasti unutrašnjih poslova. Zakon pod istim nazivom je usvojila NS RS i isti je objavljen u oficijelnim novinama.¹⁵ Tako se u čl.45 pomenutog zakona predviđa uzimanje materijala radi utvrđivanje identiteta, daktiloskopiranje, fotografisanje (forenzička registracija) i uzimanje drugih uzoraka, zatim forenzička veštačenja i analize i vođenje Nacionalnog DNK registra. Postoji pravna praznina u ovom delu zakona jer nisu predviđena pravna rešenja za važna otvorena pitanja, kao što su brisanje uzetog biološkog materijala kada protiv osumnjičenog lica nije pokrenut krivični postupak, ili je isti obustavljen zbog zakonskih razloga i kada nije podignuta optužnica protiv prijavljenog lica. I dalje od toga, postoji opasnost od podnošenja tužbi ESLJP (Evropski sud za ljudska prava, Strazbur), potencijalnih gubitaka sporova i naknade štete.

Podaci iz Registra mogu se razmenjivati i prenositi međunarodnim organizacijama odnosno državama, u skladu s ovim i drugim zakonom.¹⁶ To je posebno važno danas u borbi protiv terorizma, organizovanog kriminala i drugih najtežih pojava oblika kriminala koji ima nesporno transnacionalni karakter.¹⁷ U ovoj oblasti najdalje je otišla poznata Prumska konvencija (CEU, 2005) (tzv. Šengen 3) koja predviđa poboljšanje prekogranične saradnje država u borbi protiv terorizma, prekograničnog

kriminala i ilegalnih migracija.¹⁸ Konvencija dalje omogućava razmenu podataka iz nacionalnih baza DNK, razmenu podataka koji se tiču otisaka prstiju i razmenu informacija o vozilima (Nikač, 2015, 169-171). To je značajno zbog međunarodne policijske saradnje generalno (Interpol, regionalno, bilateralno) i posebno pozicije Srbije zbog aplikacije za prijem u EU, saradnje s državama članicama i Europolom. Dalji doprinos saradnji u ovoj oblasti dali su posebna strukovna udruženja forenzičara kao što je ENFSI (*European Network of Forensic Science Institutes*) (ENFSI, 2018), koji ima 17 ekspertskih radnih grupa i među njima WG za DNK materijale. Na nivou EU postoji uže udruženje Euroexpert (*EE- EuroExpert*) kao asocijacija forenzičara, forenzičkih laboratorija i sudskih veštaka (Nikač, 2015, 210-212).

Sadržina Registra obuhvata sledeće baze podataka DNK profila: a) utvrđenih iz nespornih bioloških uzoraka, b) utvrđenih iz spornih bioloških uzoraka i c) utvrđenih u krivičnim postupcima dostavljenih iz svih DNK laboratorija iz RS.¹⁹

Baza DNK profila utvrđenih iz *nespornih* bioloških uzoraka sadrži zbirke DNK profila: lica nad kojima je izvršena forenzička registracija; lica kojima je sud odlukom o izricanju krivične sankcije odredio uzimanje uzorka; lica osuđenih za krivična dela određena u zakonu kojim se uređuju posebne mere za sprečavanje vršenja krivičnih dela protiv polne slobode prema maloletnim licima; koji su dostavljeni od strane nadležnih organa u okviru međunarodne policijske ili pravosudne saradnje i profila utvrđenih radi eliminacije sumnje.²⁰

Baza DNK profila utvrđenih iz *spornih* bioloških uzoraka sadrži sledeće zbirke dokumenata: jedinstvenih DNK profila lica kojima se utvrđuje identitet i drugih lica dostavljenih u svrhu njihove identifikacije; jedinstvenih DNK profila leševa kojima se utvrđuje identitet; jedinstvenih DNK profila koji su dobijeni iz spornih bioloških uzoraka; DNK profila koji su dostavljeni od strane nadležnih organa u okviru međunarodne

¹⁵ Zakon o evidenciji i obradi podataka u oblasti unutrašnjih poslova, "Sl.glasnik RS" br.24/18.

¹⁶ Op.cit. u nap.7, čl.4 st.4-5.

¹⁷ Vidi više: (Božić & Nikač, 2016)

¹⁸ Vidi više: (Nikač & Božić, 2017, str. 165-180)

Vidi i: (Božić & Nikač, 2018)

¹⁹ Op.cit. u nap.7. čl.5

²⁰ *Ibid*, čl.5

policijske ili pravosudne saradnje i Zbirku mešanih DNK profila.²¹

Baza DNK profila utvrđenih u *krivičnim postupcima* dostavljenih iz svih DNK laboratorija iz Republike Srbije sadrži zbirke: registrovanih DNK laboratorija; utvrđenih DNK profila iz nespornih bioloških uzoraka u trenutku dostavljanja podataka u Registar i utvrđenih jedinstvenih DNK profila iz spornih bioloških uzoraka u trenutku dostavljanja podataka u Registar.²²

Zbirke sadrže posebne evidencije identifikacionih podataka kao što su: DNK profili, personalni podaci lica, naziv organa koji vodi postupak sa brojem predmeta, laboratorijski delovodni broj, podatke o poreklu uzorka, podaci o tehničarima i analitičarima koji su obrađivali biološke uzorke iz kojih su dobijeni DNK profili, naziv i sedište postupajuće laboratorije.

Prikupljanje rezultata DNK analiza (čl.6) obuhvata obavezu postupajuće laboratorije, koja je izvršila DNK analizu po naredbi organa postupka, da uz zapisnik o veštačenju dostavi utvrđene DNK profile nadležnom organu i dostavi MUP raspoložive identifikacione podatke radi unosa u Registar.²³ Dalje se predviđa situacija kada se za potrebe vršenja DNK analize u okviru krivičnog postupka, kao nesporni biološki uzorak (bukalni bris) uzima posredstvom neakreditovane DNK laboratorije. Tada se zahteva da laboratorija obavlja analizu u skladu sa standardom SRPS ISO/IEC 17025:2006 ili odgovarajućem standardu po kom se akredituju forenzičke laboratorije, sve u funkciji tačnosti podataka koji se unose u Registar. Ako laboratorija nije u mogućnosti da uzme bukalni bris dužna je dostaviti MUP krv ili drugi biološki materijal koji je podoban za DNK analizu.²⁴

Podaci o akreditovanim DNK laboratorijama u Republici Srbiji su dostupni javnosti u okviru registra koje vodi nadležno telo, u skladu sa zakonom kojim se uređuje akreditacija.²⁵

Upoređivanje DNK profila je kao mogućnost predviđena prema čl.7. istog zakona. Nadležni organ može zahtevati pretraživanje Registra radi upoređivanja DNK profila dobijenog analizom, s podacima koji se već nalaze u Registru i bez odlaganja. Zahtev se podnosi po pravilu u pisanoj formi, a izuzetno usmeno, uz obavezu naknadnog dostavljanja pisanog zahteva.²⁶

Postoji pravna dilema da li je u postupanju nadležan organ Javno Tužilaštvo (JT) ili nadležna linija rada policije koja u predistražnom postupku deluje samostalno, po zahtevu tužioca ili suda. Mišljenja smo da treba prihvatiti ekstenzivno tumačenje s obzirom da policija po pravilu postupi po nalogu JT. Sledeća dilema odnosi se na pravnu formu zahteva, naime, ZKP poznaje formu naredbe za veštačenje u toku predistražnog postupka policije ili istrage JT.²⁷ Kao subjekt postupka u ovom delu može se pojaviti i sud, ali u toku glavnog pretresa. Mišljenja smo da treba prihvatiti naredbu kao prepoznatljivu pravnu formu zahteva koja je utvrđena prema ZKP, na koji način bi se izbegli potencijalni prigovori nezakonitosti.²⁸

Dalje postoji dilema i povodom molbe strane države ili međunarodnih organizacija za dostavu pomenute vrste podataka, kao vid međunarodne krivičnopravne pomoći. Mišljenja smo da treba postupati u skladu sa Prum konvencijom i intresima RS povodom aplikacije za prijem u EU, ali to treba da bude na obrazloženi pisani zahtev stranog organa i shodno načelu uzajamnosti i potpisanim međunarodnim sporazumima. Postoje i nedoumice u pogledu rokova za dostavljanje pismenih zahteva za pribavljanje podataka, što pak nije precizirano odredbama propisa.

Čuvanje podataka u Registru se vrši u elektronskom obliku i to primenom informaciono-komunikacione tehnologije. Pored toga predviđena je i primena mera fizičke i tehničke zaštite, što je razumljivo jer mere Informacijskog tehničkog sistema (ITS) nisu dovoljne.

²¹ *Ibid*, čl.5

²² *Ibid*, čl.5

²³ *Ibid*, čl.6, st.1-2.

²⁴ *Ibid*, čl.6, st.4.

²⁵ *Ibid*, čl.6, st.3.

²⁶ *Ibid*, čl.7, st.1-2.

²⁷ *Op.cit.* u nap.3.

²⁸ *Ibid*, čl.140-141 ZKP.

Uzimanje biometrijskih uzoraka (bukalni bris) i uzoraka biološkog porekla za forenzičko genetičke analize, obavlja se isključivo po naredbi JT ili suda. Shodno tome, i poređenje DNK profila treba obavljati po naredbi ovlašćenih organa.

Pristup podacima iz registra je dozvoljen samo ovlašćenim licima NKTC (forenzičke službe) MUP, uz primenu pomenutih zaštitnih mera.

Obrada podataka u Registru se evidentira u posebnoj evidenciji koja sadrži podatke o postupajućem ovlašćenom službenom licu, datumu i vremenu obrade kao i vrsti i predmetu obrade.

Arhiviranje podataka u Registru se vrši na način da se obezbedi njihovo čuvanje od gubitka i oštećenja.²⁹

2.3 Završni deo

Završni deo obuhvata odredbe od čl.9 do čl.11 i odnosi se na nadzor nad sprovođenjem zakona i donetih podzakonskih propisa za njegovu primenu, zatim na rokove za uspostavljanje Registra i usvajanje podzakonskih akata u vezi s tim i, na kraju, uspostavljanje Registra u narednom roku od dve (2) godine od stupanja na snagu zakona.

U završnim odredbama se obavezuju sve DNK laboratorije na teritoriji RS da dostave MUP u elektronskoj formi DNK raspoložive profile i identifikacione podatke dobijene tokom krivičnog postupka, postupkom utvrđivanja identiteta nestalih ili nepoznatih lica, leševa i delova tela, a najkasnije u istom roku kao gore (2 godine). Završna odredba odnosi se na datum stupanja na pravnu snagu zakona i rok od osam (8) dana od stupanja na pravnu snagu (vacatio legis).³⁰

3 ZAKLJUČAK

Usvajanje Zakona o nacionalnom DNK registru je nesporno važan korak u harmonizaciji normi nacionalnog zakonodavstva Srbije s pravom EU, posebno u kontekstu aplikacije naše zemlje za prijem u Uniju. U pitanju je ispunjavanje uslova iz

Poglavlja br.23 i 24 u procesu pridruživanja EU i s tim u vezi obaveza koje proističu za našu zemlju, pravosuđe i organe unutrašnjih poslova.

Novi legislativni okvir u ovoj oblasti u skladu je s međunarodnim dokumentima EU, pre svih sa Prum konvencijom, na osnovu koje je razvijena međunarodna krivičnopravna i policijska saradnja u formi razmene podataka iz nacionalnih DNK baza podataka. To je u funkciji saradnje u zajedničkoj borbi protiv terorizma i organizovanog kriminala, sprečavanju ilegalnih migracija i prekograničnog kriminala.

U radu su detaljnije i kritički analizirana nova zakonska rešenja u ovoj veoma osetljivoj oblasti. Istaknuti su po našem mišljenju pozitivni aspekti novog zakona, ali je i ukazano na određene nedoumice koje mogu nastupiti u svakodnevnoj primeni i to usled nedovoljno preciznih odredaba. Mišljenja smo da pomenuti zakon u primeni treba da se u celosti oslanja na ZKP kao najvažniji procesni legislativni okvir u krivičnom postupku. U skladu s tim su i manje mogućnosti za potencijalne povrede ljudskih prava i građanskih sloboda. U primeni zakona valja biti veoma obazriv kada su u pitanju ranjive socijalne grupe i među njima maloletnici koji su u sukobu sa zakonom. Isto tako, u primeni zakona treba uvažiti pozitivna iskustva razvijenih država i praksu Evropskog suda za ljudska prava (ESLJP) u ovoj oblasti.

Da rezimiramo, zbog kratkog roka od stupanja na snagu novog zakona i nedostatka konkretnijih početnih rezultata za sada nije moguće dati neku sveobuhvatniju analizu usvojenih odredaba. Mišljenja smo da valja sačekati protek primerenog roka od minimalno godinu dana, nakon čega se onda mogu dati preliminarne ocene i predlozi za unapređenje normativnog okvira, kao i prakse u radu organa za primenu zakona.

CITIRANA DELA

Božić, V., & Nikač, Ž. (2016). Criminal incriminations based on the United Nations Convention Against Transnational Organized Crime in the criminal legislation of the Republic of Croatia and the Republic of Serbia. *St. Clements's messages for ethics, morality and values* (str. 89-111). Skopje: Faculty of Security.

Božić, V., & Nikač, Ž. (2018). Međunarodni kaznenopravni odgovori na aktualnu migrantsku krizu. *Pravna riječ* br. 56, 167-186.

²⁹ Ibid, čl.8.

³⁰ Ibid, čl.9-11.

- CEU. (2005, 07 07). *Prüm Convention 10900/05*. Preuzeto sa Council of the European Union: register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010900%202005%20INIT
- Council of the European Union, Prüm Convention, 10900/05.
- ENFSI. (2018, 12 18). *History*. Preuzeto sa ENFSI: www.enfsi.eu
- Grupa autora (2011), *Primena forenzičkih metoda u kriminalistici*, KPA, Zbornik radova, Beograd.
- Miljković J (2000), *Veštačenje DNK otisaka u krivičnim postupcima kod krivičnih dela silovanja iz čl.103. KZ RS*, Bilten sudske prakse Vrhovnog suda Srbije br.02/00, str.151-171
- Nešić L, Vučković J, Marić A (2016), *Uvođenje sistema kvaliteta u Nacionalni kriminalističko-tehnički centar MUP RS u skladu sa međunarodnim standardom SRPS ISO/IEC 17025:2006 (ISO/IEC 17025:2005)*, Zbornik sa Projekta, KPA, Beograd.
- Nikač, Ž., & Božić, V. (2017). *Međunarodna policijska i krivičnopravna saradnja država EU u borbi protiv terorizma s osvrtnom na Republiku Srbiju kao kandidata za članstvo*. U Ž. Nikač, & V. Božić, *Tematska monografija "Integralna bezbednost Republike Srbije"* (str. 165-180). Beograd: Fakultet za poslovne studije i pravo.
- Nikač, Ž. (2008). *Zbirka propisa iz oblasti unutrašnjih poslova*. Beograd: MUP RS, Interno izdanje.
- Nikač, Ž (2015). *Međunarodna policijska saradnja*, KPA, Beograd.
- Obradović D (2000), *Veštačenje DNK u krivičnom postupku*, Bilten sudske prakse Vrhovnog suda Srbije br.2/00, Beograd, str.99-150
- Obradović D (2004), *Biloška veštačenja – značaj, primena i perspektiva u sudskim postupcima kod nas*, Bilten Vrhovnog suda Srbije br.3/04, Beograd, str.138-156.
- Obradović D (2018), *Osvrt na pojedine odredbe Zakona o DNK registru*, Pravni informator br.04/18, Beograd, str.18-21.
- Pravilnik o policijskim ovlašćenjima, „Sl.glasnik RS“ br.54/06.
- Primorac, D., & Schanfield, M. (2016). *Forensic DNA Analysis: An Interdisciplinary Approach (Forenzična analiza DNA: Interdisciplinarni pristup)*. Zagreb: Školska knjiga.
- Sertifikat o akreditaciji NKTC br.01-413 od 28.08.2014.g.
- Simonović B (2012), *Kriminalistika*, III izmenjeno i dopunjeno izdanje, Pravni fakultet Kragujevac.
- Zakon o nacionalnom DNK registru, „Sl.glasnik RS“ br.24/18.
- ZKP (stari) - Zakonik o krivičnom postupku, "Službeni list SRJ" br.70/01 i "Službeni glasnik RS" br.58/04,85/05,115/05,49/07,20/09,72/09.
- ZKP, Zakonik o krivičnom postupku, važeći "Sl.glasnik RS" br.72/11, 101/11, 121/12, 32/13, 45/13 i 55/14.
- Zakon o policiji (stari), „Sl.glasnik RS“ br.101/05, 63/09, 92/11,92/11,64/15.
- Zakon o policiji (novi), „Sl.glasnik RS“ br.06/16, 24/18.
- Zakon o posebnim merama za sprečavanje vršenja krivičnih dela protiv polnih sloboda prema maloletnim licima, "Sl. glasnik RS" br.32/13,55/2014.
- Zakon o evidenciji i obradi podataka u oblasti unutrašnjih poslova, "Sl.glasnik RS" br.24/18.
- www.enfsi.eu, about ENFSI, History (18.12.2018).

NAPOMENA

Rad je rezultat istraživanja u okviru Projekta "Inoviranje forenzičkih metoda i njihova primena" br.34019, koji podržava Ministarstvo prosvete, nauke i tehnološkog razvoja RS.

NOTE

The paper is the result of research on the Project "Innovation of forensic methods and their application" No. 34019, which is supported by the Ministry of education, science and technology development of the RS.

Datum prve prijave: 03.09.2018.
Datum prijema korigovanog članka: 19.03.2019.
Datum prihvatanja članka: 27.03.2019.

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

Style – **APA Sixth Edition:**

Nikač, Ž. (2019, 04 15). Usvojen zakon o nacionalnom dnk registru u Republici Srbiji. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 125-133. doi:10.12709/fbim.07.07.01.15

Style – **Chicago Sixteenth Edition:**

Nikač, Željko. 2019. „Usvojen zakon o nacionalnom dnk registru u Republici Srbiji.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 125-133. doi:10.12709/fbim.07.07.01.15.

Style – **GOST Name Sort:**

Nikač Željko Usvojen zakon o nacionalnom dnk registru u Republici Srbiji [Časopis] // *FBIM Transactions* / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 125-133.

Style – **Harvard Anglia:**

Nikač, Ž., 2019. Usvojen zakon o nacionalnom dnk registru u Republici Srbiji. *FBIM Transactions*, 15 04, 7(1), pp. 125-133.

Style – **ISO 690 Numerical Reference:**

Usvojen zakon o nacionalnom dnk registru u Republici Srbiji. **Nikač, Željko.** [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, *FBIM Transactions*, T. 7, str. 125-133.



PRIMENA INTELIGENTNIH TEHNOLOGIJA PRI UPRAVLJANJU LANCIMA SNABDEVANJA

APPLICATION OF INTELLIGENT TECHNOLOGIES IN THE MANAGEMENT OF SUPPLY CHAINS

Dušan Regodić

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

Marija Matotek

Visoka tehnička škola strukovnih studija, Zrenjanin, Srbija

Radomir Regodić

Zavod za izdavanje udžbenika, Beograd, Srbija

©MESTE

JEL Category: **O18, R41**

Apstrakt

Cilj ovog rada je da se prikaže da efektivna implementacija savremenih informacionih sistema u kompanijama i njihova dostupnost putem Interneta (cloud computing) omogućavaju racionalnije i kvalitnije upravljanje lancima snabdevanja. Primenom novih informacionih sistema, računarstva u oblaku, elektronskog poslovanja i sistema za podršku odlučivanju povećavaju se efikasnost i efektivnost. Kompanije kvalitetnije, jednostavnije, brže i uz manje troškove rešavaju složene procese savremenog razvoja, nove integracije tržišta, zahteve klijenata, različitih razvojnih i proizvodnih lokacija, dobavljača i proizvođača, projektovanja i proizvodnje. Cloud computing, kao nova web tehnologija, sve više se koristi u poslovnom svetu. Efekti korišćenja ove tehnologije u poslovanju su brojni. Cloud computing se može implementirati u širokom spektru poslovnih procesa, u cilju efikasnog upravljanja. Brojne veze aktera u e-lancu snabdevanja, e-proizvodnji i e-trgovini zahtevale su nove softvere za skladištenje, obradu, upravljanje, saradnju, analizu, kreiranje i simulaciju. Razvijaju se inteligentni softverski sistemi koji obezbeđuju autonomnost svim akterima pri pregovaranju oko složenih procesa u lancu snabdevanja i simulacije ovih procesa u virtuelnom svetu. Na nivou 6PL, uslovi interakcije učesnika u logističkom lancu snabdevanja se formiraju u integrisanom informacionom okruženju. Softverska platforma 6PL može se koristiti u logističkim sistemima. U radu su prikazani rezultati analize savremenih nivoa logističkih usluga. Primenom savremenih informacionih i komunikacionih tehnologija ostvarena je virtuelizacija interakcije između učesnika u lancu snabdevanja.

Adresa autora zaduženog za korespondenciju:

Dušan Regodić

 dusanregodic5@gmail.com

Ključne reči: cloud computing, informacioni sistem, logistički operator, lanac snabdevanja, sistem za podršku odlučivanju.



Abstract

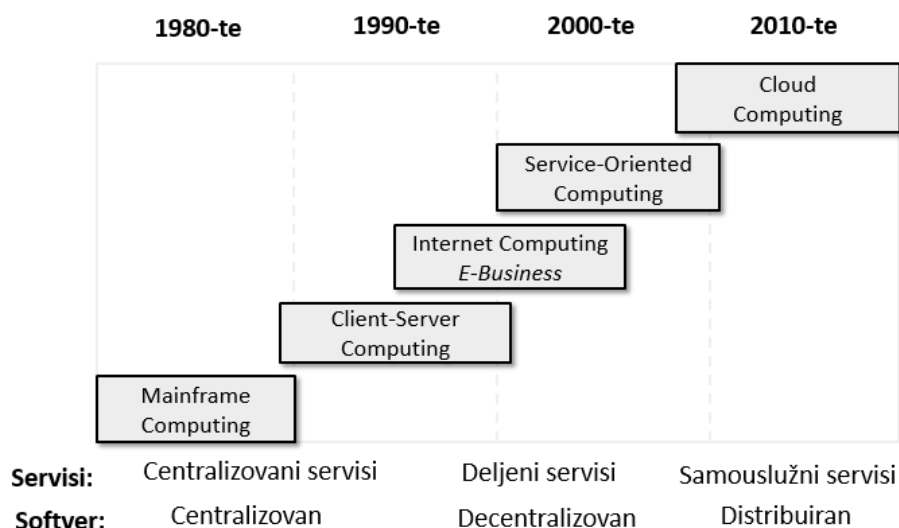
The aim of this paper is to demonstrate that the effective implementation of modern information systems in companies, as well as their availability through cloud computing, enable higher quality management of supply chains. The use of new information systems, such as cloud computing, e-business, and decision support systems, increases the company's efficiency and effectiveness. Companies can now address multifaceted processes, new market integrations, and customer requirements in a faster, simpler and more affordable way. Cloud computing, as a new web technology, is becoming increasingly popular in the business world. The effects of using this technology in today's business environment are numerous. Interwoven relationships between participants in the e-supply chain, e-production and e-commerce required the creation of new software for storage, processing, management, collaboration, analysis, creation, and simulation. Intelligent software systems are being developed to ensure autonomy for all stakeholders in the supply chain, as well as to simulate process development in the virtual world. At the level of the software platform 6PL, the conditions of the interaction of the participants in the logistics supply chain are formed in an integrated information environment. The 6PL software platform can be used in logistics systems. Furthermore, this paper presents the results of the analysis of modern level logistics services. Virtualization of the interaction between the participants in the supply chain was realized using modern information and communication technologies.

Keywords: cloud computing, information system, logistic operator, supply chain, decision support system.

1 UVOD

Kompleksnost procesa savremenog razvoja i proizvodnje zahteva nove integracije tržišta, različitih razvojnih i proizvodnih lokacija, dobavljača i proizvođača, projektovanja i proizvodnje, više proizvođača hardverskih i softverskih komponenti. Cloud computing

transformiše sve sfere našeg sveta od privrednog života, zabave, kulture, društva, obrazovanja, itd. (Quinn, Strauss, & Kristandl, 2014). Ova tehnologija utiče i na sve aspekte poslovanja, i pronalazi svoju primenu u istraživanju, dizajnu proizvoda i usluga, proizvodnji, logistici, marketingu i finansijama, slika 1.



Slika 1: Razvoj softvera i servisa

U savremenom poslovanju termin "cloud" se poistovećuje sa dostupnošću, lakoćom i brzinom upravljanja podacima (Hui & Yu, 2010). Reč je o savremenoj tehnologiji koja u značajnoj meri može da unapredi efikasnost poslovnih procesa i redukuje troškove. U razvijenim ekonomijama,

sve veći broj preduzeća uviđa prednosti korišćenja ove tehnologije u poslovanju. Tokom dvadesetog veka (70-ih godina) u SAD je pokrenut projekat integrisane proizvodnje pomoću računara (ICAM). Realizacijom tog projekta tokom 1983. godine su definisani osnovni problemi

tadašnje industrijske automatizacije: sistemi i funkcionalne jedinice nisu integrisani, nemogućnost lakog upravljanja informacijama od strane korisnika, zahtevane promene su skupe i dugotrajne, i kvalitet podataka nije pogodan za integraciju.

Tokom kraće primene 90-tih godina dvadesetog veka identifikovane su prednosti integracije kroz bazu podataka: mogućnost komunikacije između različitih funkcionalnih jedinica proizvodnog sistema, tačan prenos podataka unutar i između sopstvenih proizvodnih pogona, brža reakcije na zahtevane promene, povećana fleksibilnost u smislu uvođenja novih proizvoda, povećanje preciznosti i kvaliteta u proizvodnim procesima, povećanje kvaliteta proizvoda, efikasna kontrola i upravljanje tokovima podataka između različitih funkcionalnih jedinica, smanjenje vremena razvoja i proizvodnje i unapređenje proizvodnog toka od narudžbe do isporuke. Osetila se potreba za povezivanjem eksternog toka materijala, informacija, novca i usluga, od dobavljača sirovina, preko proizvodnje, skladištenja, pa sve do krajnjeg kupca. Tako je prvobitno nastao lanac snabdevanja koji obuhvata organizacije i procese koji kreiraju i isporučuju proizvode, usluge i informacije krajnjim kupcima. Danas su razvijeni generički modeli arhitekture lanaca snabdevanja u e-okruženju, koji obuhvata e-organizacije, e-nabavku, e-trgovinu i e-saradnju, može poslužiti kao dobra osnova za razvoj specifičnih modela za učesnike na različitim nivoima u mreži lanaca snabdevanja i za različite proizvodne i uslužne organizacije (Turban, Aronson, Liang, & Sharda, 2010).

Razvoj Interneta kao globalne računarske mreže uslovio je nastanak računarstvo u oblaku (cloud computing). Ovaj koncept u računarstvu je omogućio da se računarski resursi isporučuju korisnicima na osnovu njihovog zahteva u vidu usluge, i putem Interneta. Cloud computing se zasniva na tehnologiji virtuelizacije i podrazumeva da se servisi i podaci hostuju u deljenom, dinamički skalabilnom skupu resursa provajdera. Popularnost ove tehnologije raste i u Srbiji. Javljaju se kompanije koje nude usluge cloud computing-a. Efektivna implementacija savremenih informacionih sistema u kompanijama i njihova dostupnost putem Interneta (cloud computing) omogućava primenu savremenih alata za:

- Transformaciju podataka i informacija: grupa podataka iz različitih mašina i procesa postoji na različitim nivoima. Alat za smanjenje podataka, njihovo predstavljanje i usvojena predviđanja za operacione podatke mora da bude razvijen.
- Predviđanje: napredne metode i prediktivni alati moraju da budu razvijeni da bi mogli da otkriju degradacije, greške performansi ili trend "failure not faults", defekte itd.
- Optimizaciju: u okruženju e-proizvodnje podacima se može pristupiti bilo kad i bilo gde. Alati bi trebalo da budu sposobni da upoređuju višestruke, bazne parametre performansi kroz optimalni prikaz kao i da upoređuju proizvodne performanse kroz mrežni monitoring (Network).
- Sinhronizaciju: sinhronizujući elementi obezbeđuju potrebnu integraciju sa sistemima e-poslovanja uključujući CRM, SCM, B2B, sisteme e-trgovine. Sinhronizacije elemenata predviđa integraciju sa e-poslovnim sistemima uključujući CRM, SCM i B2B e-trgovinu.

Teorijski, ova tehnologija predstavlja pogodno rešenje za realizaciju infrastrukture poslovnih sistema, uz smanjenje troškova ulaganja u infrastrukturu i postizanja visokog stepena skalabilnosti i dostupnosti (Armbrust, et al., 2010).

Uloge koje se mogu uočiti u cloud computing-u su:

- Prodavac - preduzeće koje kao posrednik prodaje cloud usluge krajnjim korisnicima.
- Provajder - preduzeće koje je vlasnik cloud servisa, koje nudi korisnicima.
- Korisnik - pojedinac ili preduzeće koje koristi cloud servise.

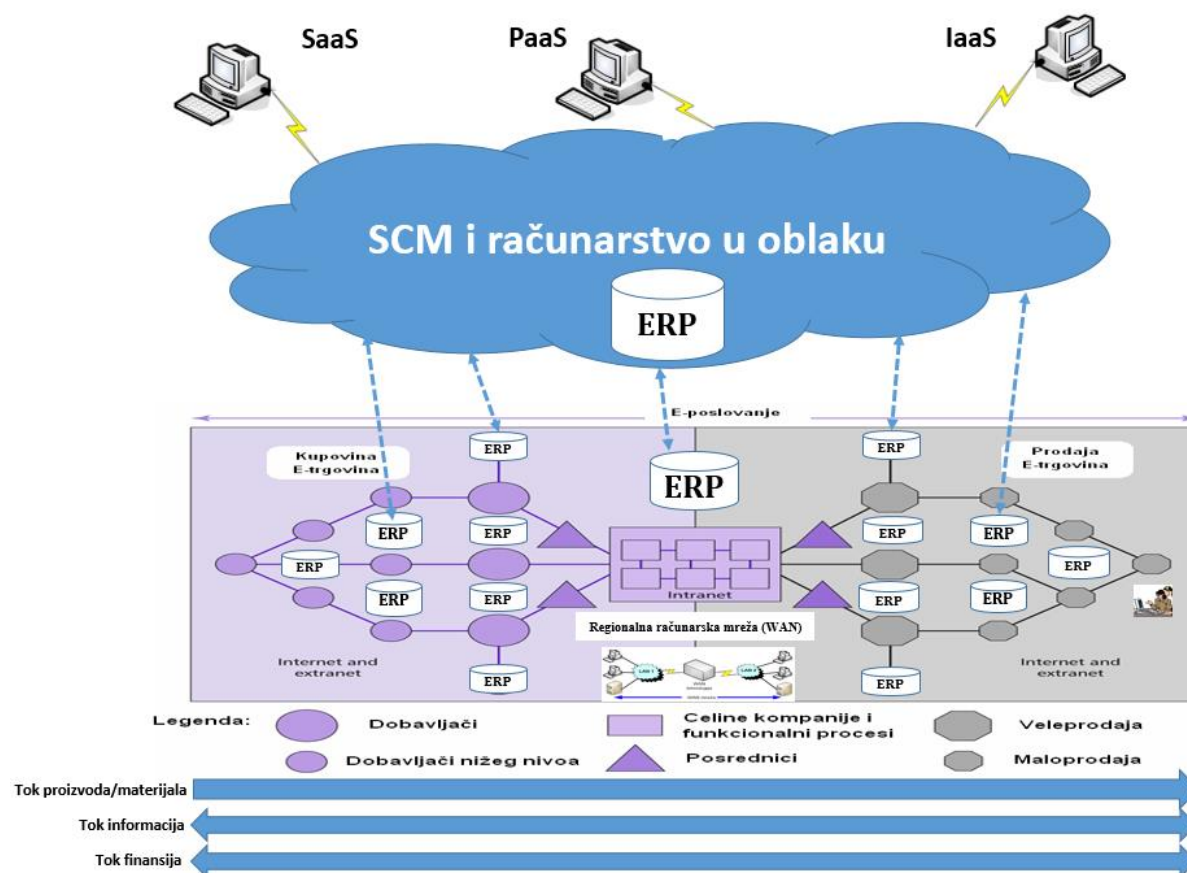
Danas se putem Interneta i web browser-a može bez problema pristupiti hardverskim i softverskim resursima koji se nalaze na lokacijama koje su izvan fizičkih granica kompanije. U teoriji postoje brojne definicije cloud computing-a, ali nijedna od njih ne može se smatrati opšte prihvaćenom. Kao jedna od najpotpunijih definicija, uzima se ona koju je dao Nacionalni institut za standarde i tehnologiju Sjedinjenih Američkih Država (NIST), prema kojoj je cloud computing "model koji omogućava pogodan pristup po zahtevu" mreži zajedničke grupe podesivih računarskih resursa (npr. mreža, serveri, skladišta, aplikacija i usluga) koje mogu brzo snabdevati korisnike uz

minimalan napor upravljanja ili interakcije sa provajderom usluge. NITS je takođe definisao i osnovne karakteristike cloud computing-a, a one uključuju (Mell & Grance, 2011): pružanje usluga na zahtev korisnika, širok mrežni pristup, udruživanje resursa, brzu elastičnost i merljivu upotrebu. Pružanje usluga na zahtev korisnika (*on-demand self-servis*) podrazumeva da korisnici mogu samostalno da odaberu i pokrenu kompjuterske resurse koji su im neophodni. Široki pristup mreži (*broad network access*) podrazumeva da su usluge dostupne preko mreže, a njima se može pristupiti putem standardnih uređaja, kao što su mobilni telefoni, tablet računari, laptopovi, itd. Udruživanje resursa (*resource pooling*) kompjuterski resursi provajdera spajaju se uz pomoć tzv. *Muli-Tenant* modela kako bi više korisnika istovremeno moglo da koristi cloud usluge, sa različitim fizičkim i virtuelnim resursima, koji se dodeljuju i uklanjaju na zahtev korisnika. Brza elastičnost (*rapid*

elasticity) cloud computing usluge mogu biti brzo i elastično pokrenute, nekada i automatski, kako bi se resursi prilagodili trenutnim potrebama korisnika. Dostupni kapaciteti su često bez ograničenja i može im se pristupati u bilo koje vreme. Merljiva upotreba (*measured service*). Cloud sistemi automatski kontrolišu i optimiziraju korišćenje resursa. Korišćenje resursa može biti praćeno, kontrolisano i o njemu se mogu kreirati izvještaji, koji omogućavaju transparentnost za provajdera i korisnika usluge.

2 RAZVOJNI MODELI RAČUNARSTVA U OBLAKU

Računarstvo u oblaku omogućava tri osnovna tipa razvojnih modela, u zavisnosti od tipa usluge koja se isporučuje korisniku: infrastruktura kao servis, platforma kao servis i softver kao servis, slika 2 (Mell, & Grance, 2011).



Slika 2: SCM računarstvo u oblaku

Infrastruktura kao servis (IaaS). Računarski i mrežni resursi, kao što su procesorska snaga, prostor na disku, memorija, mrežni kapacitet,

ruteri, fajervol, i sl. korisniku se isporučuju kao usluga; instalacija i konfiguracija sistema su u nadležnosti korisnika. Korisnik može kod

provajdera oblaka rezervirati resurse koji su mu potrebni i dinamički menjati te resurse u skladu s potrebama. Korisnik provajderu plaća za infrastrukturu koju koristi na sličan način kao što plaća račun za električnu energiju ili za mobilni telefon. Iznos računa zavisi od potrošnje i/ili od predefinisano tarifynog paketa.

Međutim, da bi IaaS bio dostupan korisnicima, neophodan je softver koji provajderima oblaka omogućava administraciju infrastrukture, jednostavno dodeljivanje resursa korisnicima, upravljanje infrastrukturom i merenje performansi. Neki od alata za upravljanje oblakom su: OpenStack, OpenNebula, Eucalyptus, AppLogic i drugi. Kao globalni provajderi oblaka ističu se: Amazon AWS i Rackspace. Brojni lokalni provajderi Internet ili telekomunikacionih usluga proširuju svoju ponudu nudeći infrastrukturu kao servis.

Platforma kao servis (PaaS). Platforma omogućava korisniku skup alata i aplikativnih programskih interfejsa (API) koji se mogu koristiti za razvoj aplikacija. Korisnik ne može da upravlja hardverskim resursima na kojima se aplikacija izvršava, već samo ima kontrolu nad aplikacijom koju razvija. Primeri platformi su: Google AppEngine i Microsoft Azure.

Softver kao servis (SaaS). Korisniku se omogućava da koristi gotov softver koji je razvio provajder. Softver se pokreće na cloud computing infrastrukturi, a korisnik mu pristupa najčešće kroz veb-brauzer. Brojni su primeri softvera koji se korisnicima nudi kao servis, besplatno ili kao freemium model: elektronska pošta (Gmail, Hotmail, Yahoo, i drugi), čuvanje podataka (Dropbox, Google Drive, Microsoft OneDrive, iCloud i drugi), ali i onih koji nude softver za različite poslovne funkcije, kao što su:

- Aplikacije za kancelarijsko poslovanje (Microsoft Office, Google Apps for Business, Zoho Office).
- ERP rešenja (Netsuite, Epicor).
- Upravljanje odnosima s klijentima i korisnička podrška (SalesForce).

U zavisnosti od vlasništva, postoje četiri modela razvoja cloud computing infrastrukture:

1. Privatni oblak. Preduzeće koristi koncepte računarstva u oblaku za organizaciju sopstvene računarske infrastrukture. Ovaj

pristup najčešće nije pogodan za mala i srednja preduzeća.

2. Javni oblak. Resursi se dinamički dodeljuju korisnicima, pri čemu korisnik ne zna gde se podaci fizički čuvaju, niti ima potpunu kontrolu nad njihovom zaštitom.
3. Hibridni oblak. Kombinacija javnog i privatnog oblaka, u smislu da se deo podataka drži u privatnom a deo u javnom oblaku.
4. Zajednički oblak. Više organizacija deli istu cloud infrastrukturu. Oblakom upravlja jedna od tih organizacija, ili neko treće lice.

3 POJAM I DEFINICIJA LOGISTIČKOG OPERATERA

Logistički operater je činioc koji uspešno dizajnira i optimizira logističku mrežu koja je sve više integrisana u globalni privredni sistem te obavlja razne logističke aktivnosti od dobavljača do tačke prijema i uz minimalne uložene resurse maksimalno zadovoljava zahteve tržišta. Aktivnosti logističkog operatera možemo najbolje prikazati kroz lanac snabdevanja. Sistem lanca snabdevanja obuhvata međudelovanje uključenih subjekata, kao što su: kupci, dobavljači sirovina i repromaterijala, proizvođači finalnih proizvoda, distributeri (veletrgovci), maloprodajni trgovci, logistički operatori i prevoznici. Međudelovanje se ogleda u odvijanju tokova roba, informacija i finansijskih sredstava između i unutar pojedinih faza lanca snabdevanja.

U uslovima globalizacije prioritet imaju mega logistički operatori, koji se mogu potpuno i vrlo fleksibilno vertikalno integrisati. Proces globalizacije, nameće potrebu razvika nacionalnih do svetskih tržišta, privrede i društva, uklanjaju se trgovinske barijere, jačaju međunarodna konkurencija, tehnologije. Danas u logistici postoji šest koncepata logističkih operatera:

- 1PL (First Party Logistics) operatera,
- 2PL (Second Party Logistics) operatera,
- 3PL (Third Party Logistics) operatera,
- 4PL (Fourth Party Logistics) operatera,
- 5PL (Fifth Party Logistics) operatera, i
- 6PL (Sixth Party Logistics) operatera.

Koncept 5PL koristi se u transformaciji lanca snabdevanja u mrežu. Posедуje modernu IT platformu sa fokusom na inovacije. 5PL logistički

operator upravljaju mrežom različitih lanaca snabdevanja (Ivaschenko, 2014).

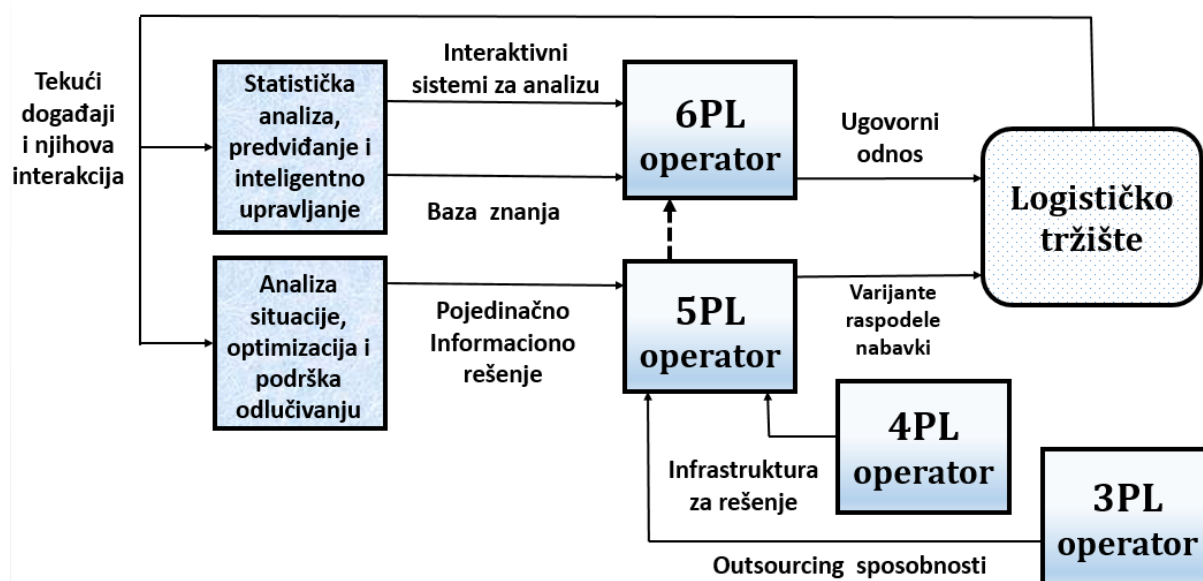
Oni su često povezani putem e-poslovanja zbog čijeg se uticaja razvila elektronska logistika (e-logistika). E-logistika kao aktivnost označava koordinirani, konzistentni i računarski upravljani (podržani, organizirani i kontrolisani) skup složenih intra i interorganizacijskih logističkih fenomena za sve aspekte poslovnih aktivnosti, kojim se može upravljati i voditi putem računarske Internet mreže. Dakle, 5PL operator uglavnom kontroliše protok informacija o naredbama, resursima, planovima i stvarnom stanju transportne mreže. Operator 5PL se uglavnom zasniva na korišćenju modernih informacionih i komunikacionih tehnologija i dovodi do pojave sledećih trendova u upravljanju resursima:

- saradnja kompanija koje učestvuju u lancu snabdeva i široka primena principa outsourcinga;

- pretežno informativna interakcija kupaca i izvršilaca;
- podrška za model SaaS (Softver kao a usluga) na tehničkom i ekonomskom nivou;
- stroga kontrola izvršenja naloga trenutni račun za nadzor statusa;
- distribucija i decentralizacija procesa donošenje odluka.

Ažurirane informacije o procesu isporuke mogu biti stalno obezbeđene. Dakle, 5PL operator uglavnom kontroliše protok informacija o naredbama, resursima, planovima i stvarnom stanju transportne mreže.

Na nivou 6PL, su ostvareni uslovi za interakciju učesnika u lancu snabdevanja snabdevanje u integrisanom informacionom okruženju (Ivaschenko & Peysakhovich, 2014). Ovi uslovi su izraženi u obliku ugovornih odnosa koji odražavaju stabilnu interakciju između učesnika. Na slici 3. je ilustracija predloženog rešenja.



Slika 3: Interakcija operatora u lancima snabdevanja

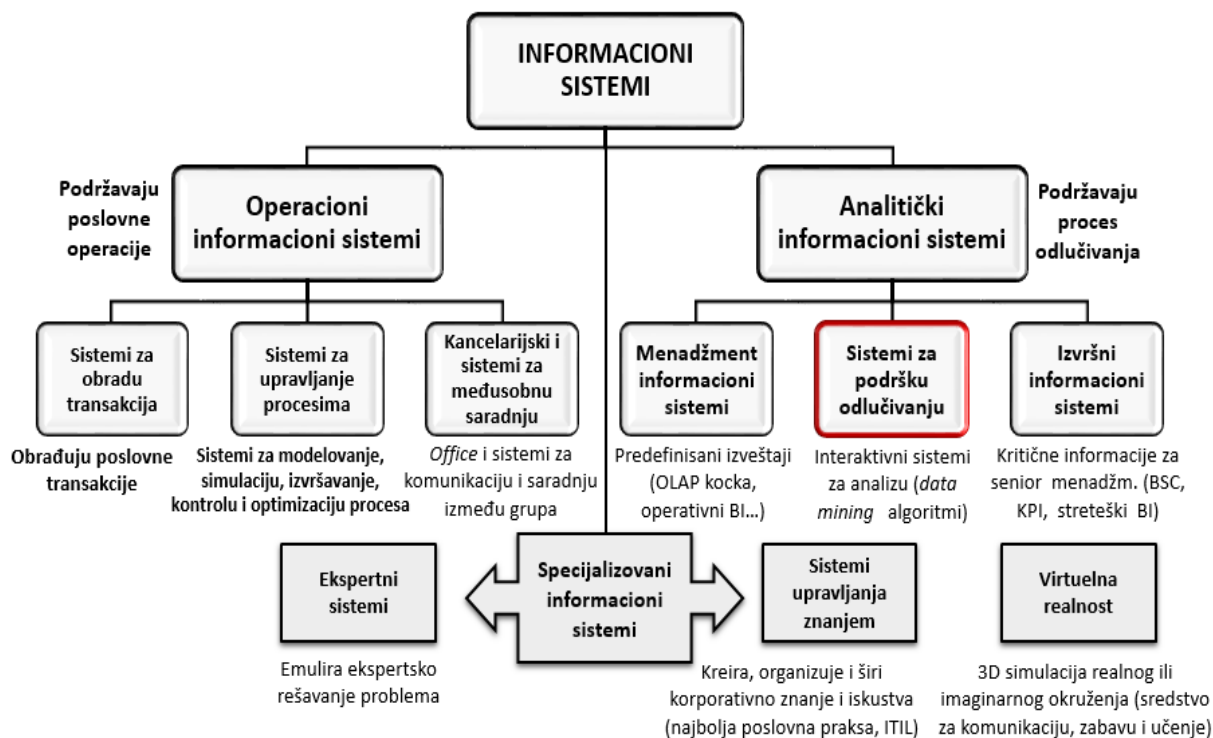
Operator 5PL poseduje softverske platforme za implementaciju interakcija učesnika u lancu snabdevanja snabdevanje u jedinstvenom informacionom prostoru. Optimizacijom se definišu opcije za izvršavanje naloga i nude ih učesnicima. Operator 5PL implementira upravljanje informacijama. Predlozi se formiraju na osnovu analize trenutne situacije operativnim upravljanjem interakcijama između učesnika. Operator 6PL bazira svoj rad na softveru koji se

primenjuje na upravljanju sa sistemskim interakcijama. Ovaj softver realizuje sve statističke analize tih interakcija. Predloženi model 6PL-operatora uključuje informaciono okruženje operatora 5PL. Osnova za formiranje održivih interakcija je operativna interakcija na nivou infrastrukture odlučivanja 4PL, a na osnovu informacija iz lanaca snabdevanja. Rezultat predloženog modela su ugovoreni odnosi kao i operativne informacije interakcija.

4 SISTEMI ZA PODRŠKU ODLUČIVANJU

Razvojem hardvera postojala je sve veća potreba za razvojem operacionih, analitičkih i specijalizovanih informacionih sistema, slika 4.

DSS sistemi kao takvi su složeni i imaju veliki broj različitih implementacija. DSS predstavlja skup procedura zasnovan na modelima za obradu i tumačenje informacija koje daju podršku menadžeru u donošenju odluka. Ne postoji opšte prihvaćena definicija.



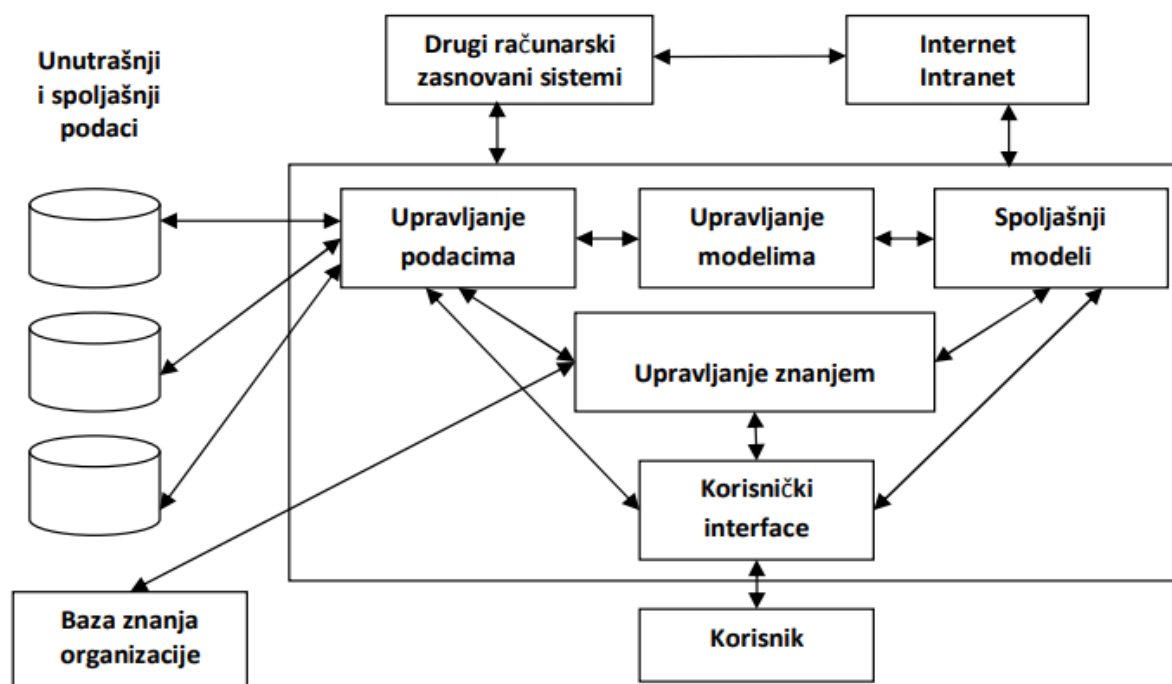
Slika 4: Pozicija DSS u razvoju informacionih sistema

Neka od značenja DSS (Miškovic, 2013):

1. Interaktivni (računarski zasnovan) sistemi ili podsistemi za pomoć donosiocima odluka u:
 - korišćenju komunikacionih tehnologija, podataka, dokumenata, znanja i/ili modela,
 - identifikaciji, rešavanju problema i izvršavanju zadataka u procesu odlučivanja i
 - donošenju odluka.
2. Opšti izraz za računarske aplikacije, koje poboljšavaju ličnu ili grupnu sposobnost donošenja odluka.
3. Intraktivni kompjuterski sistemi za ciljem da pomognu menadžerima ili donosiocima odluka da identifikuju, strukturiraju, i/ili reše polustrukturirane i nestrukturirane probleme i da naprave izbor među alternativama.
4. Naziv akademskog područja, koje istražuje i proučava sisteme za podršku odlučivanju u kontekstu njihove upotrebe.

Odluka jeste rezultat procesa odlučivanja, koja treba delotvorno da reši problem, ali odluka je samo jedna faza kompletnog procesa rešavanja problema. Zato ona mora da bude realna i precizna, nedvosmislena i donešena na vreme. Podrška ne mora biti samo računarska. Prednosti računarske podrške su (Miškovic, 2013):

- Brzina - veliki broj računanja, brzo i po niskoj ceni;
- Prevazilaženje ograničenja u obradi i memorisanju podataka, koja mogu smanjiti sposobnost rešavanja problema (npr. loše pamćenje);
- Tehnička podrška u memorisanju, pretraživanju i prenosu podataka, brže i jeftinije;
- Kvalitet podrške, kroz bolje odluke, obradu više alternativa, analizu rizika i ekspertsku podršku;
- Smanjenje cene koštanja podrške; i
- Agilnost podrške - brzo donošenje dobrih odluka.



Slika 5: Komponente današnjih DSS

Pojam neizvesnosti se odnosi na nedostatak informacija o objektu i trenutku kada treba doneti odluku. Svaki problem karakteriše nedostatak informacija ili njihova nepouzdanost. Komponente današnjih DSS su podsistemi za, slika 5.: upravljanje podacima, upravljanje modelima, korisnički interfejs i upravljanje znanjem (Mišković, 2013).

Podsistem za upravljanje podacima obuhvata: bazu podataka koja sadrži relevantne podatke o problemu, Sistem za upravljanje podacima (DBMS - Database Management System), rečnik podataka i upite.

Podsistem za upravljanje modelima se sastoji iz: baze modela, Sistema za upravljanje bazom modela (MBMS – Model Base Management System), rečnik modela, direktorijuma modela i izvođenja modela, integracije i komandnog procesora.

Podsistem – korisnički interface pokriva sve aspekte komunikacije između korisnika i DSS-a. On se ne odnosi samo na hardver i softver već i na faktore koji se tiču lakoše korišćenja i pristupačnosti sistema i faktore vezane za interakciju čovek-mašina. Jedan od glavnih razloga zašto menadžeri ne koriste kompjutere i kvantitativne analize, onoliko koliko bi one mogle da se koriste, je težak korisnički interfejs. Aktuelnom DSS-u pristupa se preko web browsera,

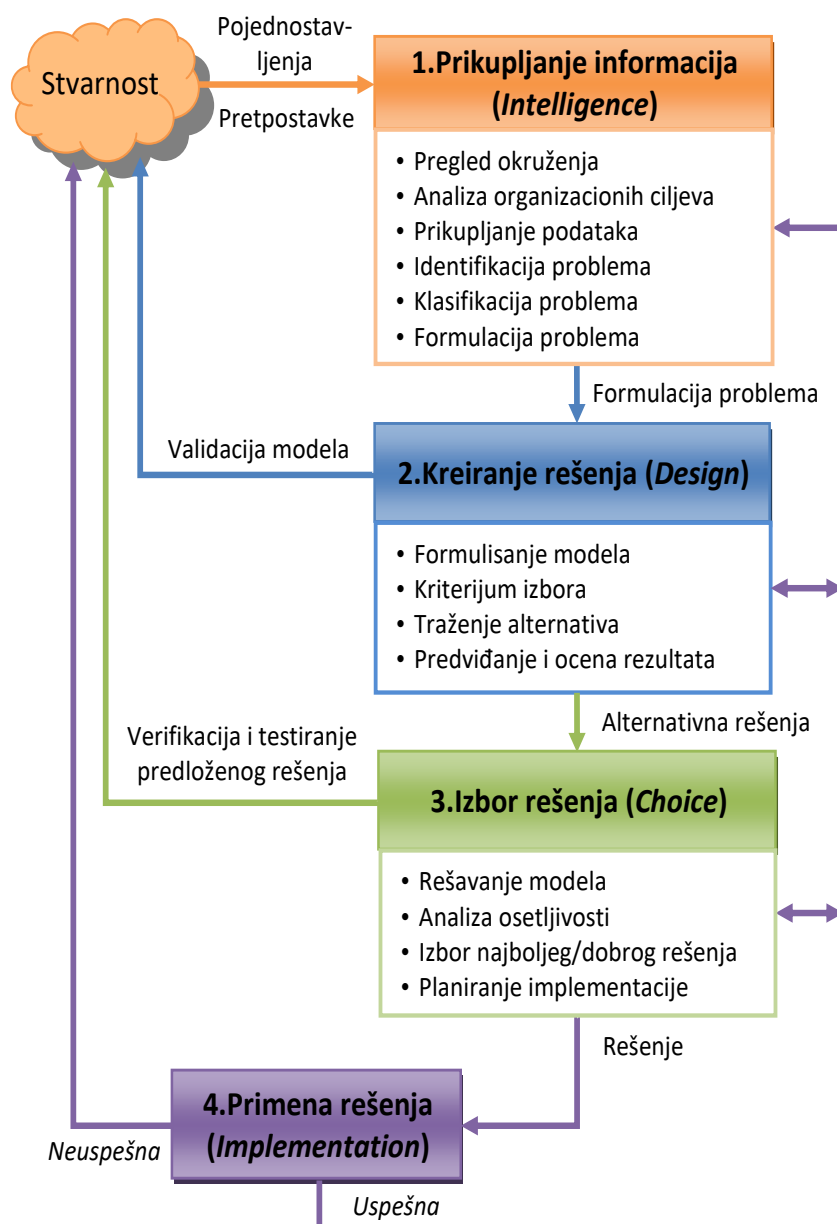
efektivnog grafičkog korisničkog interfejsa (GUI), uključujući i glasovne inpute i outpute, portabl uređaje i direktno očitavanje sa uređaja. Web browser je fleksibilan, naklonjen korisnicima i gateway skoro svim izvorima neophodnih podataka i informacija. Korisnički interfejs savremenog DSS-a obezbeđuje interakciju sa bazom podataka i bazom modela, dozvoljava da se više funkcija izvršava istovremeno, predstavlja podatke u različitim formatima, obezbeđuje učenje kroz primere itd., što u velikoj meri olakšava rad korisnicima (zaposlenima na svim nivoima u organizaciji) i doprinosi velikoj upotrebi DSS-a.

Podsistem za upravljanje znanjem (Mišković, 2013) može da podržava bilo koji podsistem ili da deluje kao samostalna komponenta. Glavna karakteristika koja izdvaja ovaj podsistem od ostalih je postojanje baze znanja, što omogućava korisniku ekspertizu o postavljenom problemu.

Komponente podsistema mogu se obezbediti putem ekspertnih sistema, neuronskih mreža, inteligentnih agenata, fazi logike itd. DSS koji poseduje ovaj podsistem naziva se inteligentni DSS ili DSS baziran na znanju (knowledge-based DSS). Osnovne faze u procesu donošenja odluka (Simon, 1960) su: prikupljanje informacija (*intelligence*); kreiranje rešenja (*design*), model; izbor rešenja (*choice*); primena rešenja (*implementation*), slika 6.

U okviru nauke o menadžmentu razvijen je veliki broj metoda za rešavanje važnih praktičnih problema: linearno programiranje, mrežna

optimizacija (*network optimization*), teorija repova (*queueing theory*), teorija igara (*games theory*).



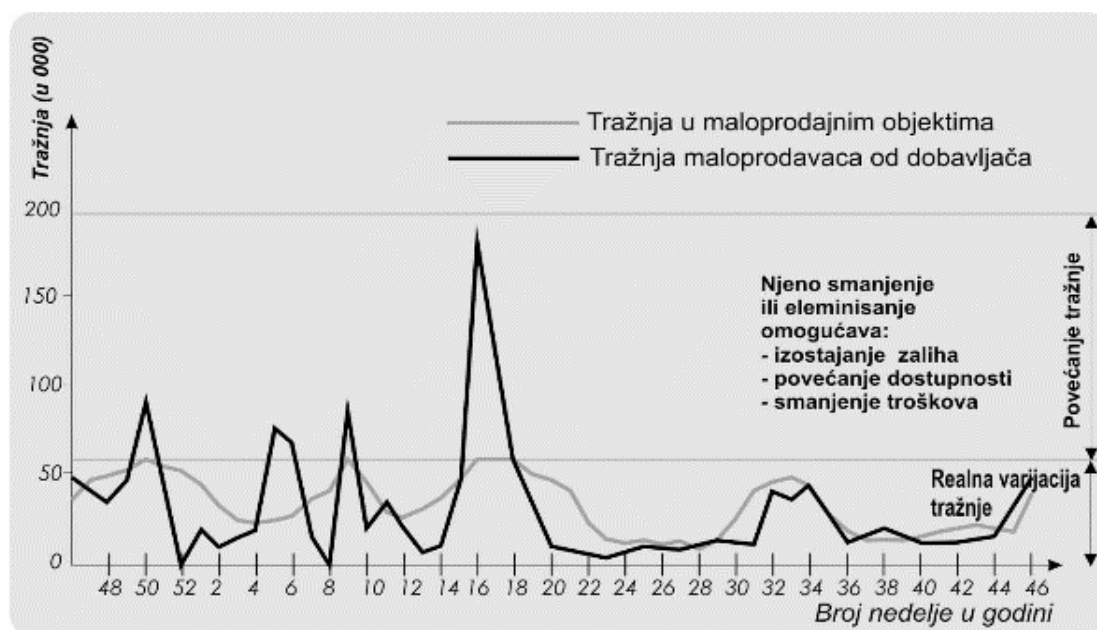
Slika 6: Osnovne faze u procesu donošenja odluka

Mnogi problemi optimizacije se mogu pogodno formulisati za rešavanje metodom linearnog programiranja i njegovim generalizacijama. Prikazaće se dva pristupa rešavanju poznatog problema upravljanja zalihama (*inventory management*): jednostavno analitičko rešenje i složenija računarski zasnovana rešenja.

4.1 Primena DSS pri upravljanju sa zalihama

Zalihe su sve količine materijala, energije i informacija koje su određeno vreme isključene iz

procesa proizvodnje ili upotrebe (potrošnje) sa ciljem da se u datom trenutku ukazane potrebe mogu iskoristiti (Regodić, 2014). Pri upravljanju zalihama postoje brojni i različiti problemi odlučivanja: Koje i kolike zalihe su potrebne? Kako ih formirati? Kako ih pratiti i kontrolisati? Kako ih popunjavati u vremenu? Koji su faktori koji ih limitiraju i na koji način? Upravljanje zalihama ima uticaj na sve poslovne funkcije, posebno proizvodnju, marketing i finansije.



Slika 7: Povećanje varijacija tražnje i pojava efekta jakog biča (Regodić, 2014).

Zalihe osiguravaju uslugu potrošačima, što je od životnog interesa za marketing. Nepravilno upravljanje zalihama dovode do efekta jakog biča (*bulwhip effect*), slika 7.

Kvalitetno upravljanje zalihama je ključ za profitabilnost firme. Optimalne zalihe predstavljaju onaj obim robe na skladištu koji uslovljava najniže troškove nabavke, skladištenja i prodaje po jedinici. To je najpoželjniji nivo zaliha jer je za trgovinu najekonomičniji. Optimalni nivo može da se poklapa i sa minimalnim i sa maksimalnim zalihama, ali češći je slučaj da se nalazi negde između njih.

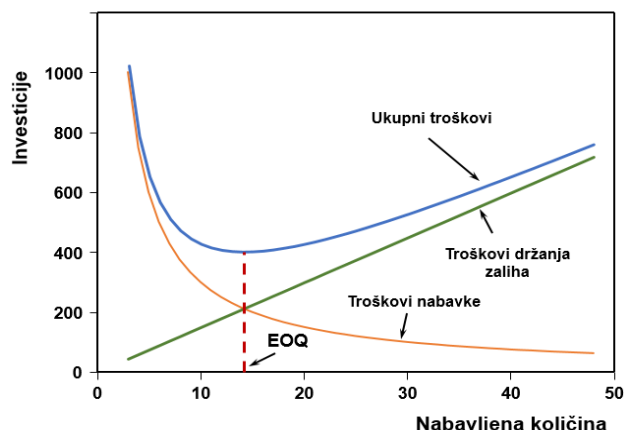
Ukupne troškove, počev od nabavne cene robe, pa do poslednjeg troška u vezi sa skladištenjem, moguće je podeliti u dve grupe, slika 8. (Regodić, 2014):

- troškovi nabavke (T_n),
- troškovi držanja zaliha (T_{dz}).

Troškove zaliha teško je proceniti, ali je ipak moguće i dovoljno za donošenje odluka. Najvažnije komponente troškova nabavke su troškovi naručivanja i dopreme. Troškovi naručivanja vezani su za naručivanje serije ili partije proizvoda. Troškovi naručivanja su uglavnom fiksnog karaktera, s obzirom da vrlo malo zavise od naručene količine. Ovi troškovi uključuju troškove pisanja narudžbe i otpreme, troškove prevoza, troškove preuzimanja partije.

Takođe, postoje troškovi vezani za izvršenje narudžbe koji su nezavisni od broja izrađenih predmeta. Troškovi izmene uključuju administrativne troškove potrebne za pripremu proizvodne opreme za izradu serije, troškovi kvalitativnog i kvantitativnog prijema robe, lični dohoci nabavne službe i sl. Ovi troškovi se često smatraju fiksnim, a mogu se smanjiti promenom načina na koji je proizvodnja zasnovana. Troškovi predmeta predstavljaju troškove proizvodnje ili kupovine pojedinih predmeta za zalihe. Trošak predmeta je izražen kao trošak po jedinici proizvoda pomnožen nabavljenom ili proizvedenom količinom. Ponekad se na trošak daje popust, ako se odjednom kupi dovoljna količina jedinica. Troškovi dopreme su uglavnom proporcionalnog karaktera. Ovde spadaju troškovi prevoza, utovara, pretovara, istovara, osiguranja, kalo, lom, rastur i ostali gubici na kvalitetu i kvantitetu robe, koji mogu nastati za vreme njenog transporta. Zajedno uzeti, troškovi naručivanja i dopreme najčešće imaju relativno fiksni karakter, ali se radi njihovog lakšeg grafičkog prikazivanja obično pretpostavlja da su proporcionalni sa brojem narudžbina.

Troškovi držanja zaliha sastoje se od kamata na angažovana obrtna sredstva, troškova amortizacije, zastarevanja, kirija, svetla, ogreva, poreza i troškova manipulacije sa robom na zalih.



Slika 8: Odnos troškova držanja zaliha i troškova nabavke (Regodić, 2014).

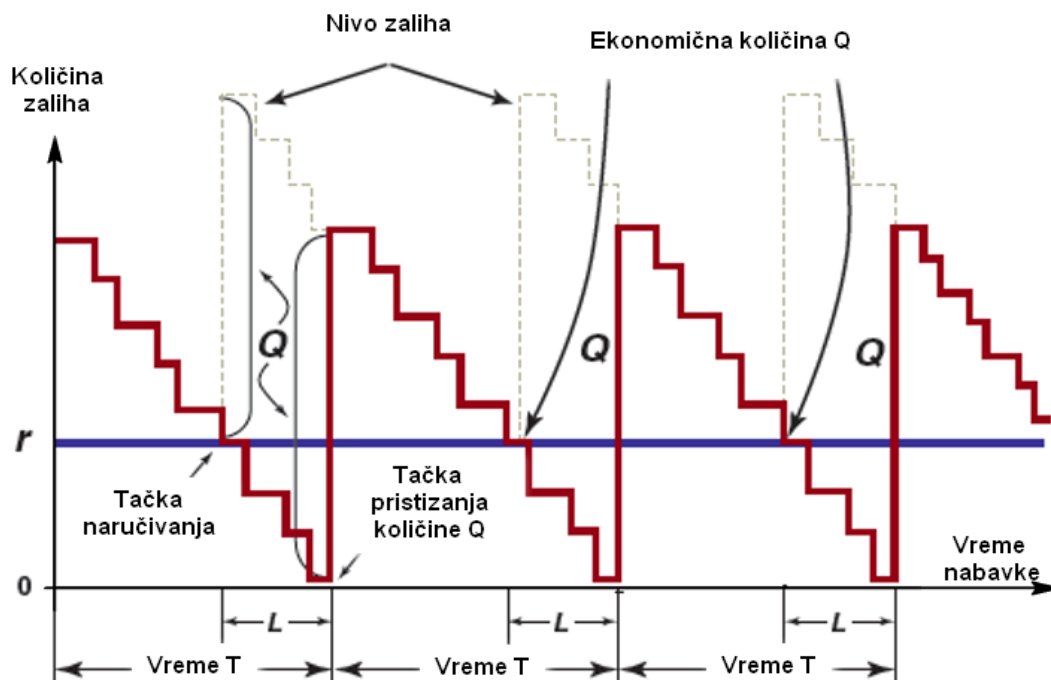
Troškovi čuvanja ili održavanja - vezani su sa držanjem predmeta na zalihama tokom nekog vremenskog perioda. Troškovi održavanja zaliha sastoje se od tri komponente: troškovi kapitala, troškovi skladištenja i troškovi zastarevanja, kvarenja i gubitaka. Značajne komponente troškova držanja zaliha su tzv. oportunitetni troškovi i troškovi zastarevanja. Zbir ovih troškova čini konačnu cenu koštanja robe, a optimalnim nivoom zaliha smatra se onaj nivo pri kojem je zbir

ovih troškova najniži. Oportunitetni troškovi se donose na:

- izgubljeni prihod od mogućeg angažovanja sredstava koja su zarobljena u zalihama a da nisu, i
- izgubljeni prihod od prodaje proizvoda kojih nema a kada bi ih bilo na zalih.

4.2 Utvrđivanje potreba za zalihama i ekonomična količina narudžbe

Različiti normativi i nivoi zaliha su usloveli i različite postupke za utvrđivanje nivo zaliha. Stohastički postupak se primenjuje za utvrđivanje potreba za zalihama repromaterijala i poluproizvoda (Regodić & Stojanović, 2017). Deterministički postupak određivanja potrebnih količina zaliha zasniva se na planovima proizvodnje. Detaljan plan proizvodnje i precizne sastavnice svakog proizvoda su uslov dobrih planova nabavki i zaliha. Sastavnice mogu biti količinske (lista elemenata), strukturne (podaci o strukturi proizvoda) i modularne (za podsklopove). Ovaj postupak zahteva i definisanje normativa zaliha: minimalnih, standardnih, signalnih, optimalnih i maksimalnih.



Slika 9: Kontinualna popuna količinama $Q=EOQ$

Deterministički modeli upravljanja zalihama su se razvijali u dva pravca (Regodić & Stojanović, 2015): klasični i dinamički. Klasični modeli nabavke se zasnivaju na vrednosti ekonomske

količine nabavke (EKN) koju je moguće dobiti kroz dva kontradiktorna zahteva. Prvi je: veća količina nabavki, niže cene po jedinici nabavljene robe i niži troškovi utovara/istovara i transporta. Drugi je

što manje nabavke, manje novčanih sredstava, niži troškovi skladištenja i kamata na angažovana sredstva. Klasični model se razvijao u dva pravca. Prvi podrazumeva naručivanje (obnavljanje) zaliha u poznatim vremenskim intervalima. Drugi podrazumeva naručivanje zaliha posle svake promene stanja. Razlikujemo periodični (P-sistem) i kontinualni sistem (Q-sistem).

Godine 1915. godine F.W. Harris razvio je formulu ekonomične količine narudžbe (EKN, economic order quantity, EOQ) koja je stekla široku primenu u industriji, slika 9. (Regodić, 2014).

Model za proračun EKN ima mnogo ograničenja (Regodić, 2014):

- za potražnju se pretpostavlja da je konstanta, dok u mnogim realnim situacijama ona značajno varira,
- za jedinične troškove se pretpostavlja da su konstantni, mada u praksi često postoje popusti na količinu kod velikih kupovina,
- za materijal u seriji pretpostavlja se da dolazi odjednom, mada će se u nekim slučajevima kontinuirano smeštati u zalihe zavisno od toga kako se proizvodi,
- pretpostavlja se samo jedan proizvod, mada se od dobavljača nabavlja nekoliko predmeta koji se svi otpremaju u isto vreme,
- troškovi pripreme uzimaju se kao fiksni, dok se često oni mogu smanjiti.

EKN se može izračunati na bazi minimizacije troškova skladištenja i narudžbe. Optimalan broj nabavki se dobija kao odnos planirane potrebe i ekonomične količine nabavke (Regodić, 2014).

$$EKN = \sqrt{\frac{200 \cdot P \cdot Tn}{Nc \cdot Sz}} = \sqrt{\frac{2 \cdot P \cdot Tn}{Nc \cdot sz}}$$

gde su:

- P – procenjena (fiksna) potreba za materijalom/delovima za određeni period/godišnje;
- Tn – procenjeni (fiksni) troškovi nabavke po jednoj nabavci;
- Nc – nabavna cena;
- Sz – stopa troškova držanja zaliha, izražena u % (0 do 100);
- sz – stopa troškova držanja zaliha, izražena u procentima (0 do 1).

Optimalno vreme između narudžbi (trajanje ciklusa narudžbe):

$$T_{VQEOQ} = \frac{EKN}{P}$$

Trenutni troškovi skladištenja proizvoda x:

$$T_z = \bar{Z} \cdot Nc \cdot sz + \frac{P}{Z} \cdot Tn$$

gde su:

- Tz – ukupni troškovi;
- $\bar{Z}$ – prosečan nivo zaliha na skladištu:

$$\bar{Z} = \frac{Z_{max} + Z_{min}}{2} = \frac{EKN}{2} + Z_{sig} = \frac{EKN}{2} + Z \cdot \sigma_L$$
- P – procenjena (fiksna) potreba za materijalom/delovima za određeni period/godišnje;
- Tn – procenjeni (fiksni) troškovi nabavke po jednoj nabavci;
- Nc – nabavna cena;
- Zmax – m, maksimalni nivo zaliha u skladištu (EKN+Zsig);
- Zmin – minimalni nivo zaliha u skladištu predstavlja očekivanu prodaju/potrebu (P) u jedinici vremena (danu, mesecu) i vremena (V) $Z_{min} = P \cdot V$;
- Z=Q – količina koja se isporuči tokom jedne porudžbine (EKN);
- Sz – stopa troškova držanja zaliha, izražena u % (0 do 100);
- sz – stopa troškova držanja zaliha, izražena u procentima (0 do 1);
- σ_L – standardno odstupanje potreba (potražnje);
- z – standardizovana slučajna promenljiva.

Teži se iznalaženju modela po kojem nisu fiksne količine nabavke, vreme ponovne narudžbe, niti potrebe. Po metodu promenljivih količina nabavke EKN je u tački gde su troškovi skladištenja i troškovi nabavke minimalni – tački njihovog preseka.

$$EKN = \sqrt{\frac{2 \cdot P \cdot (Tn \cdot Qtn)}{Nc \cdot q \cdot (1 \cdot usr / isr)}}$$

Ukoliko se u izračunavanje EKN uvrste cene koje su pod uticajem nabavljene količine, onda EKN izgleda ovako:

$$EKN = \sqrt{\frac{2 \cdot P \cdot (Tn \cdot Qtn)}{C \cdot q}}$$

gde su:

- P – nije prosečna potreba, već klizna potreba (potreba koja se menja po periodu);

- T_n – troškovi nabavke;
- Nc_q – nabavna cena po jedinici koja nije jednaka za svaku jedinicu;
- q – broj jedinica po nabavci;
- usr – ulazna skladišna rata;
- isr – izlazna skladišna rata;
- C – cene zavisne od količina;
- Q_{tn} – operativni troškovi nabavke (fiksni).

Momenat ponovne nabavke (MPN) se dobija kada se pomnoži vreme izvršenja narudžbe sa dnevnom potrebom. Ovakav način računanja MNP je optimalan kada je konstantna upotreba zaliha. Ukoliko upotreba zaliha nije konstantna, tj. njihova upotreba je neizvesna, onda MPN izgleda ovako:

$$MPN = P \cdot T + F_{nz} \sqrt{P \cdot q \cdot T}$$

gde su:

- P – planirana potreba;
- T – vreme izvršenja nabavke;
- F_{nz} – faktor prihvatljivog nedostatka zaliha;
- q – prosečan broj jedinica po jednoj nabavci.

Optimalno vreme skladištenja se dobija na osnovu sledeće formule (Regodić, 2014):

$$OVN = \sqrt{\frac{2 \cdot T_n}{Nc/q \cdot P \cdot q}}$$

gde su:

- P – procenjena potreba za svaki period;
- T_n – procenjeni (fiksni) troškovi nabavke po jednoj nabavci;
- Nc/q – nabavna cena zaliha po jedinici (jednaka za svako pakovanje);
- T_{dz} – prosečan broj jedinica po jednoj nabavci.

Moderni DSS računaju EOQ na osnovu raspoloživih informacija. Uzimaju u obzir dodatne promenljive, kao što je raspoloživi prostor skladišta ili ograničenja dobavljača, povezana s mogućnošću kreditiranja. Na osnovu tih dodatnih informacija, savremeni softver pomaže menadžerima u donošenju boljih odluka u upravljanju zalihama (Mišković, 2013):

1. Analitičko rešenje (EOQ) i rešenje korišćenjem MS Excel Solvera;
2. Microsoft Office osnovni EOQ model; i
3. Inventory Management DSS.

Tabela 1. Sistem jednačina, pregled upotrebljenih oznaka i ulazni podaci u Excel Solver modelu

	Data			Results	Range Name	Cell
$d = P$	6000	(demand/year)	Reorder Point	216	Annual Holding Cost= $h \cdot (Q/2)$	G7
$K = T_n$	\$115	(setup cost)			Annual Setup Cost= $K \cdot (d/Q)$	G6
$h = Nc$	\$4.20	(unit holding cost)	Annual Setup Cost	\$1,203.74	d	C4
$L =$	9	(lead time in days)	Annual Holding Cost	\$1,203.74	h	C6
$WD =$	250	(working days/year)	Total Variable Cost	\$2,407.49	K	C5
					L	C7
	Decision				Q	C11
$EOQ=Q$ $= \sqrt{\frac{2 \cdot P \cdot T_n}{Nc \cdot Sz}}$	573.2115				ReorderPoint $=d \cdot (L/WD)$	G4
					TotalVariableCost $=K \cdot (d/Q) + h \cdot (Q/2)$	G8
					WD	C8

Primer 1: Analitičko rešenje (EOQ=EKN) i rešenje korišćenjem MS Excel Solvera.

Izračunati ekonomičnu količinu naručivanja ako je poznato:

- Predviđena mesečna potražnja: $P = 11.107$ jedinica;
- Procenjeni (fiksni) troškovi nabavke po jednoj nabavci: $T_n = \$10$ po porudžbini;

- Nabavna cena: $Nc = \$0,11$ po jedinici;
- Stopa troškova držanja zaliha, izražena u % (0 do 100): $Sz = 20\%$ godišnje;
- Standardna devijacija greške predviđanja: $S_d = 3.099$ jedinica;
- Vreme izvršenja dopunjavanja: $LT = 1,5$ mesec; i
- Verovatnoća da će stavka biti na lageru tokom vremena izvršenja: $P=75\%$.

Ekonomična količina za ponovno poručivanje je:

Programsko rešenje dato je u tabeli 1 i na slici 10.

$$EOQ = \sqrt{\frac{2 \cdot P \cdot T_n}{N_c \cdot S_z}} = \sqrt{\frac{2(11,107)(10)}{(0,11)\left(\frac{0,20}{12}\right)}} = 11,00 \text{ jedinica}$$

MS Excel Solver model pronalazi optimalni Q tako da minimizuje *Total Variable Cost* (Hillier, 1998)

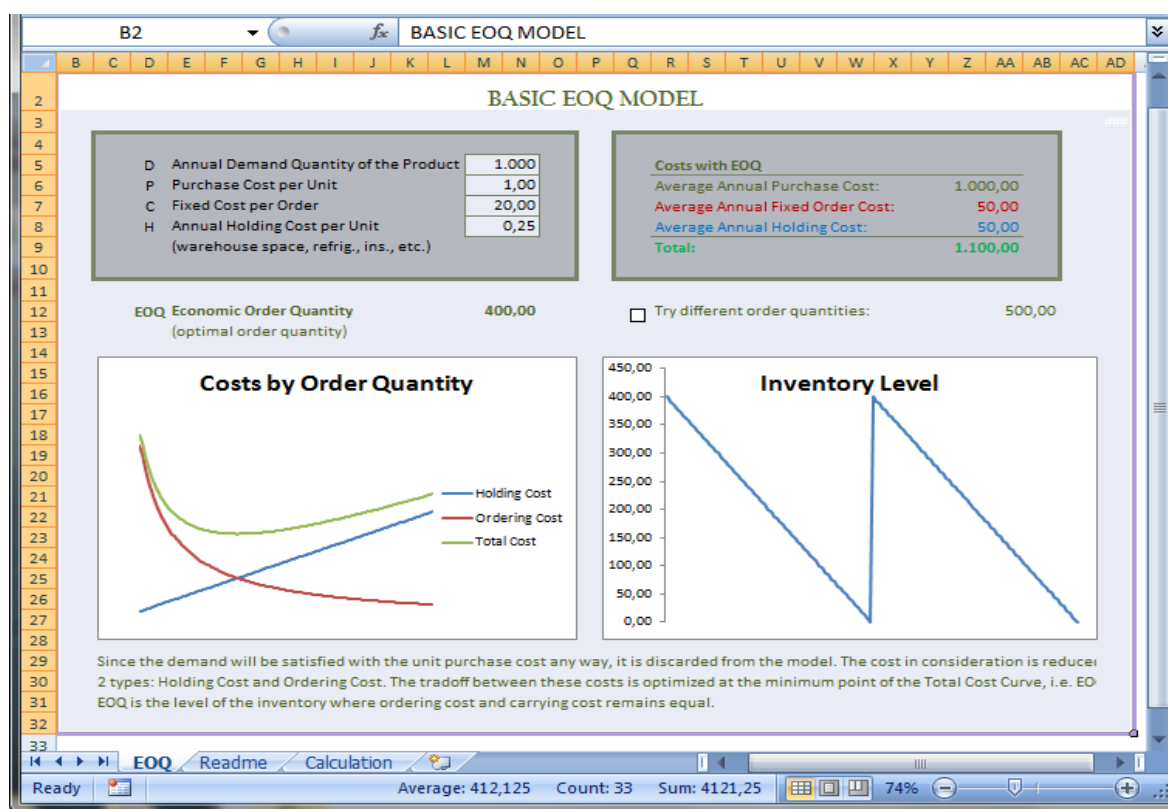
Basic EOQ Model (Analytical Version)	
Data	
d = 6000	(demand/year)
K = \$115	(setup cost)
h = \$4.20	(unit holding cost)
L = 9	(lead time in days)
WD = 250	(working days/year)
Decision	
Q = 573,212	(optimal order quantity)
Results	
Reorder Point	216
Annual Setup Cost	\$1,203.74
Annual Holding Cost	\$1,203.74
Total Variable Cost	\$2,407.49

Range Name	Cell
AnnualHoldingCost	G7
AnnualSetupCost	G6
d	C4
h	C6
K	C5
L	C7
Q	C11
ReorderPoint	G4
TotalVariableCost	G8
WD	C8

Slika 10. MS Excel Solver model

Primer 2: Microsoft Office osnovni EOQ model, slike 11 i 12.

Prikaz je dat na: <http://office.microsoft.com/en-us/templates/basic-eoq-model-TC010370172.aspx>.



Slika 11. Prikaz Microsoft Office osnovni EOQ model



Slika 12. MS Excel osnovni EOQ model

5 DISKUSIJA REZULTATA, PREDNOSTI I NEDOSTACI RAČUNARSTVA U OBLAKU

Primenom 6PL operatora su ostvareni uslovi za interakciju učesnika u lancu snabdevanja snabdevanje u integrisanom informacionom okruženju. Ovi uslovi su izraženi u obliku ugovornih odnosa koji odražavaju stabilnu interakciju između učesnika. Kao osnovne prednosti *cloud computing*-a mogu se navesti:

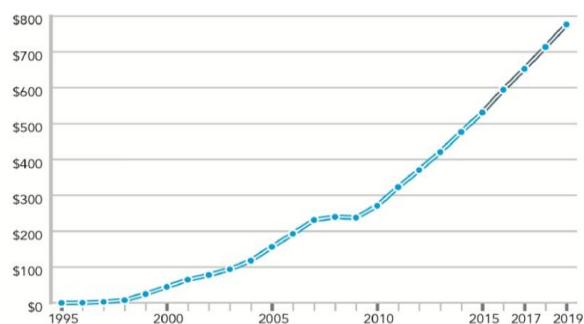
- Servisi na zahtev-resursi se koriste samo onda kada su potrebni.
- Visoko apstrahovana infrastruktura-računarske resurse korisnici koriste ne znajući gde se ti resursi nalaze niti kako su fizički organizovani.
- Elastičnost-resursi se fleksibilno obezbeđuju i oslobađaju, u zavisnosti od potreba.
- Merljivost-korišćenje resursa se može izmeriti i naplatiti po utrošku.
- Skalabilnost-infrastruktura može pratiti rast poslovnih potreba u realnom vremenu.
- Bolja iskorišćenost resursa-iste resurse može koristiti veći broj korisnika bez međusobnih uticaja.

Osnovni nedostaci *cloud computing* pristupa odnose se na još uvek neadekvatnu pravnu regulativu i nejasnoće u nadležnostima. Na primer, preduzeća iz jedne države mogu koristiti usluge provajdera oblaka iz druge države, a podaci se mogu fizički čuvati u računarskom centru lociranom u trećoj državi (Regodić & Stojanović, 2017). Takođe, postoji nedostatak jasnoće u pogledu licenci za softver, problemi u

upravljanju digitalnim identitetima i pristupom, kao i problemi u garanciji dostupnosti servisa od strane provajdera (Matotek, Barać, Regodić, Grubor, 2015). Studija koju je sprovedla kompanija *Aberdeen Group* pokazala je da organizacije koje koriste *cloud* usluge mogu da reše određene problem u prosečnom roku od 2.1 sata, dok je ostalim kompanijama potrebno u proseku oko 8 sati (SalesForce, 2014). Jedna od glavnih prednosti *cloud computing*-a je pristupačnost. Za razliku od tradicionalnih softvera, *cloud* softver je dostupna sa bilo kojeg računara, tableta ili smart telefona sa bilo koje lokacije. Za povezivanje *cloud* softvera sa korisnikom neophodna je samo Internet veza. Broj korisnika servisa se može menjati, a trošak se ne povećava rastom broja korisnika. *Cloud computing* usluge su obično po sistemu "pay as you go", tako da skoro i da nema potrebe za kapitalnim troškovima. *Cloud computing* povećava kolaboraciju između zaposlenih, gde god da se nalaze, i omogućava sinhronizaciju i rad na zajedničkim dokumentima i aplikacijama istovremeno. Istraživanje koje je sprovedla kompanija *Frost & Sullivan* pokazalo je da su kompanije koje su investirale u tehnologiju za kolaboraciju imale povrat od 400% na investiciju (SalesForce, 2014). Preduzeća koja koriste *cloud computing*, zakupljuju samo resurse koji su im neophodni, i na taj način smanjuju troškove poslovanja, kao i negativan uticaj na životnu sredinu. Pored brojnih prednosti koje nosi upotreba *cloud computing*-a u poslovanju, neizbežno se javljaju i problemi i zazovi korišćenja ove tehnologije. Problemi korišćenja *cloud computing*-a u poslovanju se najčešće odnose na

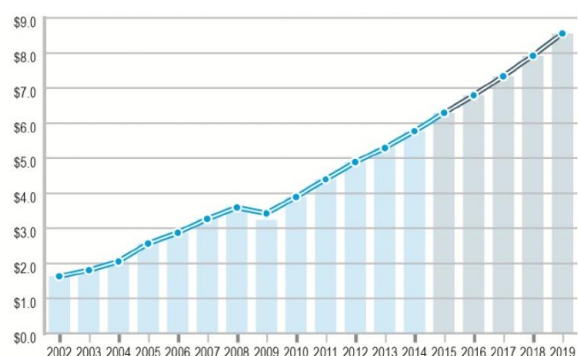
sigurnost čuvanja informacija o poslovanju. *Cloud computing* sa sobom nosi značajne rizike koji se odnose na privatnost i pouzdanost podataka koji se čuvaju u *cloud-u*.

Ulaganja u *cloud computing* usluge se konstantno povećavaju. International Data Corporation (IDC) predviđa da će ulaganja u cloud IT usluge iznositi 107 milijardi dolara u 2017, što je značajno povećanje u odnosu na 2013. kada su ulaganja iznosila 47.4 milijardi dolara (International Data Corporation, 2014). Cloud usluge menjaju način poslovanja i taj trend će se održati i u narednim godinama. Najzastupljeniji oblici e-trgovine su: Business-to-Consumer (B2C), Business-to-Business (B2B), Consumer-to-Consumer (C2C), Social e-commerce, Mobile e-commerce (M-commerce) i Local e-commerce. Na slici 13. (Laudon & Traver, 2016) je dat prikaz rasta prihoda B2C e-trgovine na globalnom nivou za period od 2000. do 2019. godine.



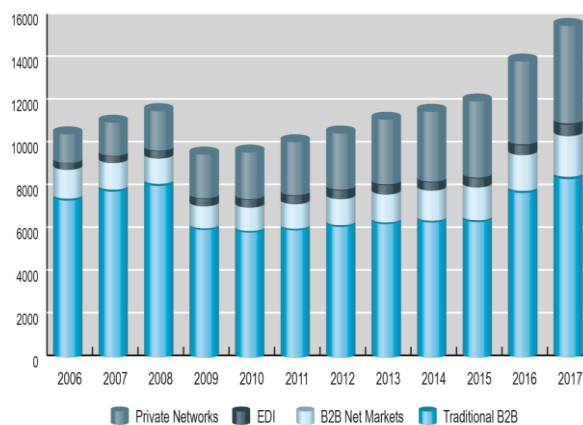
Slika 13: Prikaz prihoda B2C e-trgovine u milijardama USD za period od 2000. do 2019. godine.

Za period 2012-2017.godine B2B e-trgovina je porasla sa 4,1 na 6,6 trilionu dolara ili sa 40 na 42% od ukupne trgovine između kompanija, slika 14. Privatne industrijske mreže imaju primarnu ulogu u B2B e-trgovini (Laudon & Traver, 2016).



Slika 14: Prikaz prihoda B2B e-trgovine u milijardama USD za period od 2000. do 2019. godine.

EDI trgovina ima i dalje značajnu ulogu. Na slici 15. je prikazano da je ne-EDI najbrže rastuća vrsta B2B e-trgovine, a EDI je zastupljena ali se vremenom smanjuje. Slika 15. (Laudon & Traver, 2014) pokazuje da će elektronska tržišta postati dominantna oblik B2B e-trgovine.



Slika 15: Prikaz različitih tehnologija B2B e-trgovine za period od 2006. do 2017. godine u milijardama USD

Posebna poboljšanja nastala kao posledica B2B trgovine su: unapređena je saradnja između kupca i prodavca, poboljšana kvaliteta proizvoda, skraćeno je vreme proizvodnje, povećana je transparentnost cena, povećana vidljivost proizvoda i unapređena razmena informacija u realnom vremenu. Sa rešenjima lanca snabdevanja u oblaku, SaaS ERP brzo raste i brojne organizacije prihvataju ovo rešenje.

6 ZAKLJUČNA RAZMATRANJA

Promene u okruženju savremenih kompanija, posebno nove, informacione tehnologije, uslovljavaju razvoj novog koncepta inovativne organizacije koja ima sledeće karakteristike: oslanjanje na tehnologije kao vitalnog resursa konkurentnosti; inovativna organizaciona kultura; jak (izražen) poslovni fokus; adaptibilnost; organizaciona kohezivnost; osećaj integriteta; angažovan top menadžment; plice organizacione hijerarhije i viši stepen participativnosti (Regodić & Cvetković, 2011).

Razvojem hardvera postojala je sve veća potreba za razvojem operacionih, analitičkih i specijalizovanih informacionih sistema. Cloud lanac snabdevanja informacioni sistem postaje faktor na osnovu kojeg jača konkurentna prednost kompanije. Osnovna prednosti cloud-a u SC jeste povećanje efikasnosti i efektivnosti

sistema. Cloud donosi značajan broj kvalitetnih rešenja: integralnost u unošenju podataka, transparentnost u poslovanju, poboljšanom finansijskom izveštavanju, smanjenje operativnih troškova, smanjenju administracije u obavljanju ovih operacija, kao i boljoj usklađenost procesa u celokupnom poslovanju. Softver Platforma 6PL se može koristiti u sistemima za upravljanje lancima snabdevanja zaliha, sistema planiranja proizvodnje, internet portala, kontrolnih sistema posrednička aktivnost. Softver 6PL platforma omogućava simulaciju procesa interakcije učesnika lanca snabdevanja, analizira statistiku interakcije i formira uslove interakcije, uzimajući u obzir autonomiju aktera. Primenom DSS Ekonomični model nabavke (EOQ, *Economic Order Quantity*) daje analitičko rešenje naručivanja neophodnih stavki i troškova držanja zaliha. Prednosti su u optimizaciji procesa u lancu

snabdevanja. Autori su pokazali primenu modela upravljanja zalihama. Posebna pogodnost modela je u pojedostavljenju i racionalizaciji procesa nabavke.

Primenom 5PL logističkog operatera upravlja se mrežom različitih lanaca snabdevanja koji su povezani putem e-poslovanja. U budućnosti možemo očekivati razvoj postojećih i stvaranje novih logističkih tehnologija (operteri od 7PL do 10PL). Iz navedenog na evropskom tržištu preko logističkog operatera obavlja se 61% ukupnog transporta, 35% skladištenja, 25% informacijskih sistema, 15% obrnute logistike, 13% menadžmenta materijalima, 11% prilagođavanje kupcima, 8% menadžment zaliha, 6% procesa narudžbi, 5% podrške klijenata te 18% ostalih logističkih aktivnosti, s tendencijom daljnjeg povećanja učešća.

CITIRANA DELA

- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50-58.
- Hillier, M. (1998, 09 28). *Basic EOQ (Analytical)*. Preuzeto sa University of Nebraska-Lincoln: [http://www.math.unl.edu/~tshores1/Public/Math428S08/Week16/Basic%20EOQ%20\(Analytical\).xls](http://www.math.unl.edu/~tshores1/Public/Math428S08/Week16/Basic%20EOQ%20(Analytical).xls)
- Hui, D., & Yu, C. (2010). Cloud Computing, Accounting, Auditing, and Beyond. *CPA Journal*, 80(10).
- Ivaschenko A. (2014). *Multi-agentsko rešenje za upravljanje poslovnim procesima transportnog provajdera 5PL*. Predavanja u obradi poslovnih informacija, Springer Intern. Publ., vol. 170, str. 110-120.
- Ivashchenko, A.V., & Peysakhovich, D.G., (2014). Metod proaktivnoy dispetcherizatsii v informatsionnoy srede dlya transportnykh operatorov 5PL. *Informatsionnyye tekhnologii*, (3), 49-54.
- Laudon K.C., & Traver C.G. (2014). *E-commerce, business, technology, society, 6th Ed*. Addison-Wesley Pub (Sd).
- Matotek, M., Barać, I., Regodić, D., & Grubor, G. (2015). Supply Chain Risk Management Using Software Tool, *Acta Polytechnica Hungarica*, doi: 10.12700/APH.12.4.2015.4.10.
- Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. Preuzeto sa <http://csrc.nist.gov/publications/nistpubs/800-145/SP800>
- Mišković, V. (2013). *Sistemi za podršku odlučivanju*. Beograd: Univerzitet Singidunum.
- Quinn, M., Strauss, E., & Kristandl, G. (2014). The effects of cloud technology on management accounting and business decision-making. *Financial Management*. August. 54-55.
- Regodić, D., & Stojanović M., (2017). The Significance of the Integrated Multicriteria ABC-XYZ Method for the Inventory Management Process, *Acta Polytechnica Hungarica*, 14(5), 29-48. doi: 10.12700/APH.14.5.2017.5.3

- Regodić, D., & Stojanović M. (2015). *Uticaj informaciono-komunikacionih tehnologija na ekonomski rast*. Zbornik radova Sinergija 2015, pp. 105-108. Bijeljina: Univerzitet Sinergija. doi:10.7251/ZRSNG1501105S
- Regodić, D., & Stojanović M., (2016). *The Improvement of the Inventory Process in the Company "Benlian Food" Niš by Applying the Pom-Qm 4.0 Software*. Sinteza 2016, doi: 10.15308/Sinteza-2016-257-264, pp. 257-264. Univerzitet Singidunum.
- Regodić, D. (2014) *Logistika-lanci snabdevanja*, Beograd: Univerzitet Singidunum, ISBN 978-86-7912-564-4.
- Regodić, D., & Cvetković, D. (2011). *Automatizacija, proizvodni sistemi i računarski integrisana proizvodnja*. Beograd: Univerzitet Singidunum, ISBN 978-86-7912-367-1.
- Turban, E., Aronson, J.E., Liang, T., & Sharda, R., (2010). *Decision Support and Business Intelligence Systems, 9th Ed*. Pearson Education, Inc.

Datum prve prijave: 16.03.2018.
Datum prijema korigovanog članka: 12.09.2019.
Datum prihvatanja članka: 27.03.2019.

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

Style – APA Sixth Edition:

Regodić, D., Matotek, M., & Regodić, R. (2019, 04 15). Primena inteligentnih tehnologija pri upravljanju lancima snabdevanja. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 134-151. doi:10.12709/fbim.07.07.01.16

Style – Chicago Sixteenth Edition:

Regodić, Dušan, Marija Matotek, i Radomir Regodić. 2019. „Primena inteligentnih tehnologija pri upravljanju lancima snabdevanja.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 134-151. doi:10.12709/fbim.07.07.01.16.

Style – GOST Name Sort:

Regodić Dušan, Matotek Marija i Regodić Radomir Primena inteligentnih tehnologija pri upravljanju lancima snabdevanja [Časopis] // *FBIM Transactions* / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 134-151.

Style – Harvard Anglia:

Regodić, D., Matotek, M. & Regodić, R., 2019. Primena inteligentnih tehnologija pri upravljanju lancima snabdevanja. *FBIM Transactions*, 15 04, 7(1), pp. 134-151.

Style – ISO 690 Numerical Reference:

Primena inteligentnih tehnologija pri upravljanju lancima snabdevanja. **Regodić, Dušan, Matotek, Marija i Regodić, Radomir**. [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, FBIM Transactions, T. 7, str. 134-151.



IT VEŠTAK IZMEĐU SCILE I HARIBDE

IT COURT EXPERT BETWEEN SCYLLA AND CHARYBDIS

Boško S. Rodić

Visoka škola akademskih studija „Dositej“ Beograd

©MESTE

JEL kategorija: **K11, K14, K24**

Apstrakt

Prihvatajući se veštačenja u IT sudski veštak se susreće¹ sa brojnim moralnim, stručnim, i, razume se objektivnim problemima. U ovom radu pokušaćemo da dodirujemo spomenute probleme nudeći rešenja iz sopstvenog iskustva. Prvi problem jeste – dobiti posao, drugi uraditi posao i treći – naplatiti posao. Posao se dobija pre svega direktno preko sudova. Veštake predlažu i individue – učesnici u pravosudnom postupku: tuženi, tužioci i/ili njihovi opunomoćenici. Stranke (tuženi i/ili tužilac) mogu iz raznih razloga da ne prihvate veštaka koje predlaže neko mimo njih. Da bi posao veštačenja bio uspešno realizovan, već spomenuto na početku ovog teksta, veštak mora da savlada brojne Scile i Haribde. Ipak karakterističan problem za srpsko pravosuđe u odnosu na veštake jeste plaćanje, bolje rečeno – neplaćanje. Prema (Derikonjić, 2017) veštacima se duguje oko pola miliona evra. I ako budu isplaćeni, što zbog inflacije, što zbog pravila „bolje danas hiljadu, nego za godinu dana – deset hiljada“, veštaci su stalno u problemu. Poseban problem je realno vrednovanje – valorizacija nečijeg rada prilikom veštačenja. Saglasimo se da je IT veštačenje u domenu visokotehnološkog kriminala gde se zahteva najviši mogući stepen stručnosti – znanja. Kako platiti to znanje?

Ključne reči: IT, zakoni, veštačenje, nalaz i mišljenje, naplata veštačenja.

Abstract

Accepting expertise in IT, the court expert encounters with numerous: moral, professional, and is understood by objective problems. In this paper we will try to explain the mentioned problems by offering solutions from our own experience. The first problem is to get a job, then to do the job, and the third, to charge the services. This job is primarily obtained through courts. Experts also suggest individuals – participants in the judicial process: the defendants, prosecutors and/or their plenipotentiaries. The parties (the respondent and/or the prosecutor) may for various reasons not accept expert witnesses

Adresa autora:

Boško S. Rodić

 bosko.rodic@gmail.com

¹ Kad je u pitanju IT veštačenje malo je reći da se IT veštak nalazi između dva „čudovišta“. Slično, kao u satiri „Jazavac pred sudom“, glavni junak David Štrbac nije na „četiri“ ćoška, nego na – „dvadeset četiri“. Pored otpora suprotstavljenih strana, veštak je posebno opterećen zahtevom za poznavanjem predmeta veštačenja. Kad je u pitanju informaciona tehnologija (IT) ovaj problem se višestruko uvećava. Naime, u pitanju je tehnologija koja ima najbrži stepen promena – usavršavanja. Veštak, hteo – ne hteo, da bi bio u toku sa promenama, mora stalno da uči.



suggested by someone past them. For this work to be successfully realized, already mentioned at the beginning of this text, the expert has to master numerous Scylla and Charybdis. Still, a typical problem for the Serbian judiciary in relation to experts is payment, or rather - non-payment. According to Derikonjic (2017) courts owe the experts about half a million euros. And if they are paid out, because of the inflation, because of the rules "better today thousand, then for a year - ten thousand", experts are constantly in trouble. A particular problem is realistic valuation - the valorization of someone's work in the artificial experiment. Let's agree that IT is an expertise in the domain of high-tech crime where the highest possible level of expertise - knowledge is required. How to pay this knowledge?

Keywords: IT, Laws, Expertise, Finding and Opinion, Expertise Collection.

1 DOBIJANJE POSLA VEŠTAČENJA

Da bi neko bio angažovan kao sudski veštak mora da ima „licencu“, formalno pravo, koje se reguliše odgovarajućim dokumentom – Rešenjem koje izdaje Ministarstvo pravde. U preambuli Rešenja stoji „na osnovu člana 13. stav 1. Zakona o sudskim veštacima („Sl. glasnik Republike Srbije“, broj 44/2010) i člana 192. stav 1. Zakona o opštem upravnom postupku („Sl. List SRJ“, br.33/97 i 31/2001 i „Sl. glasnik Republike Srbije“, broj 30/2010) rešavajući po zahtevu koji je podneo NN za imenovanje sudskog veštaka, ministar pravde doneo je REŠENJE...

Razume se da se moraju ispunjavati brojni uslovi koje kandidat za sudskog veštaka mora da zadovolji da bi stekao pravo za imenovanje.

Veštak će se angažovati – ako za to postoji potreba. Veštaka predlažu fizička i/ili pravna lica (njihovi opunomoćenici), pa i sami sudovi. Zakonom o parničnom postupku, („Sl. glasnik RS“, br. 72/2011), trenutno važeća verzija, tačka 5, članovima 259. do 275, zaključno, definiše se angažovanje veštaka. Naime, član 259: „Sud će da izvede dokaz veštačenjem ako je radi utvrđivanja ili razjašnjenja neke činjenice potrebno stručno znanje kojim sud ne raspolaže.“

1.1 Primeri iz prakse

Već je spomenuto da se veštak angažuje (po potrebi) na predlog strana u sporu i/ili na predlog suda. Prvo veštačenje ovog veštaka bilo je upravo na predlog stranke, građanina FZ iz Beograda u (mogućem) sporu u periodu februar – mart 2007. Oštećeni – predlagač, je tražio da se izvrši procena štete po elektrotehnici na objektima u

kojim su se navodno proizvodile sintetičke droge². Objekti su bili u selu U. Naime, nakon što su organi unutrašnjih poslova preuzeli „staranje“ nad objektima u selu došlo je do oštećivanja istih praćeno pljačkom svega i svačega što se moglo izneti iz objekata i, pre svega, iskoristiti. Ono što nije moglo da se koristi (oprema, infrastruktura) uništeno je do stepena pretvaranja pokretnih sredstava u furdu. Da bi se veštačenje „formalno pokrilo“ oštećeni je samo pitao veštaka da li poseduje dokument (rešenje) po kojem je ovlašćen da veštači i na elektrotehničkoj opremi. Veštak je odgovorio pozitivno. Grubo uzevši veštak je dobio posao „na reč“.



Slika 1. Deo (uništenog) magacinskog prostora

Posebna je priča u vezi sa realizacijom zahteva oštećenog. Veštak se našao pred više problema. Kako popisati svu oštećenu elektrotehničku opremu sa potpunim i preciznim opisom oštećenja na istoj? Kako definisati potrebne radnje da se oštećena oprema popravi (zameni, ugradi...) do pune funkcionalnosti? Proceniti troškove za revitalizaciju celog sistema. Posebno

² Reč je o jedinjenjima koji sadrže amfetamin-sulfat, piperonal, difenil, formamid...

sa aspekta „izgubljene dobiti“ !!!³. Epilog: veštak je uspešno rešio zahtev oštećenog.



Slika 2. Jedan od mnogobrojnih uništenih/opljačanih razvodnih ormarića za struju

Napominjem da je prilikom izvođenja konačne – ukupne „vrednosti“ štete veštak u prvi mah pogrešio. Greška je vrlo brzo otklonjena. Ova greška, kao iskustvo, obavezuje veštaka da više puta proveriti zaključke do kojih je došao.

Poslednja 2-3 veštačenja veštak je dobio preko udruženja „IT veštak“.

2 URADITI POSAO

„Uraditi posao“ – znači, u skladu sa zadatkom veštačenja koji definiše predlagač, uraditi nalaz i na osnovu istog dati mišljenje. Veštak je tokom „karijere“ uradio 17 nalaza iz oblasti elektrotehnike/elektronike i 113 nalaza iz oblasti IT. Vrednosti parnica su se kretale i preko 250.000.000,00 EUR.

Svi predmeti su imali manju ili veću dozu specifičnosti. Šta više, neki su, u prvi mah, bili potpuno strani – nepoznati veštaku, barem u odnosu na predmet veštačenja. Na primer, veštačenje štete (2008/2009) na automobilu zbog (ne)ispravnog funkcionisanja tzv. „potapajućih“ stubića, Slika 3. Tužilac je bio fizičko lice. Tužena je opština SM zbog toga što je zbog, navodno, neispravnosti stubića tužilac ošteti automobil.

Imenovani je pokušao da pređe na neregularan način (velikom brzinom) preko spuštenog stubića. Stubić je „odradio“ svoj „posao“ na regularan način – dočekao tužiočev automobil. Posledica se već pretpostavlja.

Veštak se, pre veštačenja, nikad ranije nije sretao sa tom tehnologijom. Barem ne kao problemom. U pitanju je tehnika koja je u funkciji sprečavanja nekontrolisanog ulaska vozila u zabranjene (pešačke) zone. Veštak je prilikom boravka u Francuskoj, u Kampijenu, 1996. godine prvi put video kako funkcionišu ti stubići.



Slika 3. Potapajući stubići



Slika 4. „Optuženi“ stubić

Ispitivanje, dokazivanje, „krivice“ stubića provereno je i putem eksperimenta. Simulacija – eksperiment je dokazao da je stubić funkcionisao u skladu sa ugovorom (deklaracijom) o ispravnosti sistema.

³ Da nije tužno, bilo bi – smešno. Kako govoriti o „dobiti“ od proizvodnje droga?

Veštak je, inače, u cilju izvođenja korektnog nalaza često pribegavao simulacijama – eksperimentu. U parnici, pod kodnim imenom „garaža“, praktično je proveravan sistem (polu)automatskog funkcionisanja (garažnih) vrata, Slika 5. Naime, jednom od korisnika zajedničke garaže, prilikom izlaska iz garaže, garažna vrata su izgrebala karoseriju. Vrata su se u skladu sa propisanom procedurom zatvarala prilikom prolaska oštećenog vozila.

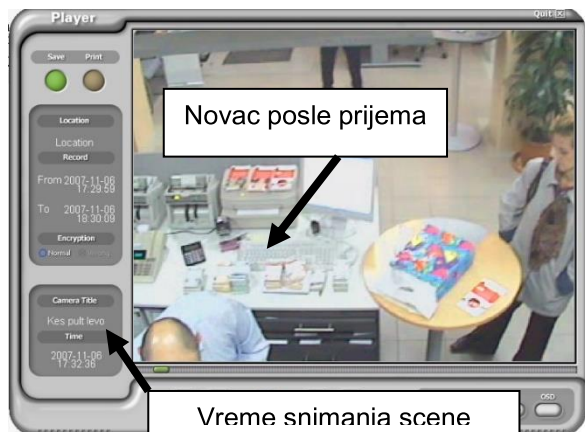


Slika 5. Provera sistema za upravljanje garažnim vratima

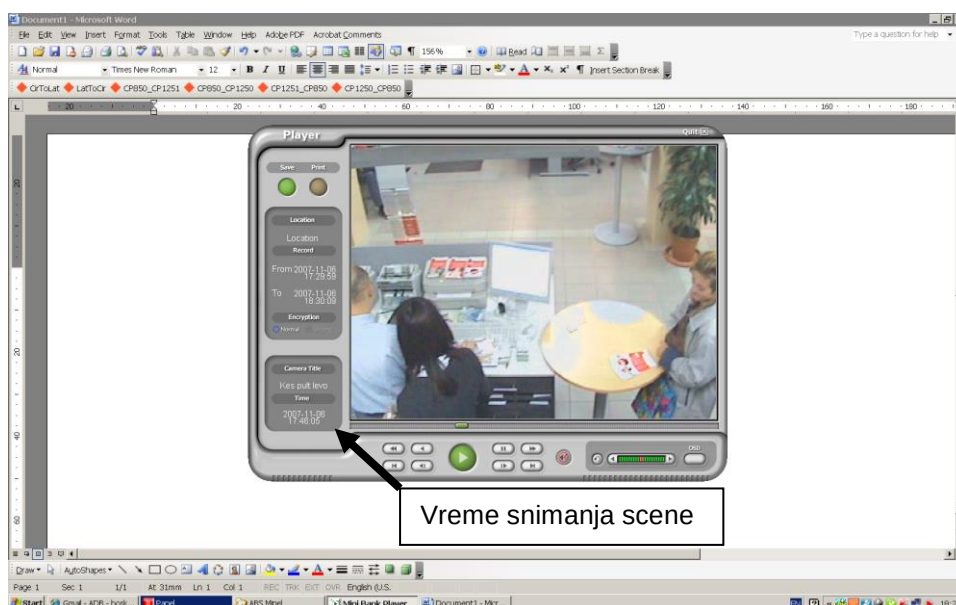
Proverom je dokazano da vrata nisu bila uzrok oštećivanja (grebanja) karoserije automobila, već nepravilno rukovanje sistemom od strane vlasnika (vozača) oštećenog vozila. U tom slučaju

veštak je utvrdio da odgovornost nije na strani tuženog kućnog saveta. Jedini propust kod vrata je učinio vlasnik – kućni savet, što nije obezbedio vidno upozorenje u vezi moguće štete izazvane nepravilnom upotrebom pomenutog sistema.

Veštačenje u oblasti IT, pored visokog nivoa stručnosti zahteva i veštinu korišćenja tehnike, „ostro oko“, itd. U parnici (2008/2012) koja je trebala da reši problem krađe novca veštak je zahvaljujući veštini doveo u sumnju mogućnost krađe novca od strane službenika banke – brojača novca. Naime, klijentu banke je tokom primopredaje novca u banci, u iznosu oko 100.000,00 EUR, nestalo oko 35.000,00 EUR. Slike 6, 7. i 8.



Slika 6. Privremeni raspored novca nakon predaje



Slika 7. Brojačica nosi novac levo, prva trećina pete sekunde



Slika 8. Brojačica nosi novac levo, druga trećina pete sekunde

Napominjemo da su sve ostale kamere bile isključene osim ove koja je zabeležila priložene snimke. Slučajno!?

Tokom veštačenja, pored razumljivih problema – utvrđivanja istine, veštak je imao problema zbog nekooperativnosti učesnika u parnici. To je sasvim razumljivo. Kako je, barem jedna strana, grešna (obično tužena), dešavalo se da veštak bude izložen pritiscima, uvredama. Bilo je i pokušaja nagodbe jedne od strana sa veštakom⁴. Doduše ne često.

Generalni problem bio je (ne)poznavanje tehnologije. Veštak je zbog toga pod stalnim pritiskom da uči nove tehnologije.

3 NAPLATA VEŠTAČENJA

Ovo je po ličnom iskustvu, a i prema (Derikonjić, 2017), najproblematičniji⁵ deo posla. Veštak se dva puta „opekao“ „zahvaljujući“ lažnim obećanjima advokata. Radi se o nemalim iznosima. Inače najneefikasnija naplata je od Višeg suda. Kasni i do godinu dana. Sa druge strane dobar primer je Privredni sud. Na osnovu uplaćenog depozita, po završenom suđenju, veštaku se odmah isplaćuje njegova naknada.

Otvoreno je pitanje visine naknade. Odnosno, da li je ista samerljiva sa troškovima i vrednošću nalaza koji je uradio veštak?

Koristim priliku da podsetim da je, ministar pravde, prema (Bodolo, 2018)], doneo novi Pravilnik o naknadi troškova u sudskim postupcima koji je objavljen u „Službenom glasniku RS“, broj 9 od 05.02.2016.godine. Novim Pravilnikom, između ostalog, propisani su uslovi za naknadu i visinu naknade koji u sudskim postupcima pripadaju veštaku.

Članom 5. navedenog Pravilnika utvrđeno je da troškovi učešća u postupku veštaka čine putni troškovi, troškovi za ishranu i prenoćište i izgubljena zarada.

Izgubljena zarada regulisana je članovima 10, 11. i 12, ista se nadoknađuje učesniku u postupku – veštaku koji je u radnom odnosu, s tim da poslodavac ima pravo da od suda koji vodi postupak zahteva naknadu iznosa koji je licu u radnom odnosu isplatio na ime zarade. Pravilnik ne navodi koja je to visina izgubljene zarade koja se nadoknađuje učesniku u postupku.

Neposredni troškovi veštačenja regulisani su članovima 14, 15. i 16, između ostalog se navodi da se veštaku nadoknađuju izdaci za utrošeni materijal i drugi stvarni izdaci.

⁴ Možda nije slučajno, radi se o istom licu.

⁵ Prema (Derikonjić, 2017), sudovi u Srbiji dužni su veštacima čak pola miliona evra. I, ne samo da im duguju novac, nego stručnjaci različitih profila koje sud

angažuje za iznošenje stručnog mišljenja u parničnim i krivičnim postupcima, na isplatu dugovanja čekaju mesecima, pa i godinama.

Visina nagrade učesnika u postupku regulisana je članovima 18. i 19. Veštaku se nagrada određuje tako što se osnovica za obračun nagrade deli brojem časova u mesecu koji je prethodio veštačenju, pa se tako dobijeni iznos množi brojem časova koji su bili neophodni za veštačenje⁶. Osnovica za obračun nagrade jeste dvostruki iznos prosečne mesečne zarade po zaposlenom u Republici Srbiji, bez poreza i doprinosa, isplaćene za mesec koji je prethodio veštačenju prema podacima organa nadležnog za poslove statistike.

Za veštačenja obavljena u otežanim uslovima, nagrada se uvećava za 100%, takođe je propisano da veštaku u krivičnom postupku u kome je posebnim zakonom određeno da postupa javno tužilaštvo posebne nadležnosti pripada nagrada koja može biti dvostruko visa od nagrade iz stava 1. i 2. člana 18.

Postupak zahteva za naknadu troškova i nagradu regulisani su članovima 31. i 32.

Pravilnik je stupio na snagu 13.02.2016.godine.

Prema prethodnom Pravilniku, osnovica za obračun nagrade koja je takođe bila definisana kao prosečna zarada u Republici, bez poreza i doprinosa i uvećavala se u određenom procentu, zavisno od školske spreme (više škole 150%, visoke 200%, magistrature 250% i doktorata 300%), novi Pravilnik definiše da osnovicu čini

dvostruki iznos prosečne mesečne zarade, nezavisno od školske spreme. Starim Pravilnikom bilo je dozvoljeno uvećanje nagrade za 100%, za posebno složene predmete, dok novi Pravilnik dozvoljava tu mogućnost samo za veštačenja obavljena u otežanim uslovima (noću, u izuzetno nepovoljnim vremenskim uslovima i sl.), i za veštačenja koja je neophodno obaviti nedeljom i praznikom.

Preporučujemo primenu Pravilnika o naknadi troškova u sudskim postupcima („Službeni glasnik“ Republike Srbije 09/16) u pogledu nagrade veštaka.

U praksi se mogu naći i drugi (drugačiji) primeri – načini obračuna naknada veštačenja. Na primer, „Cenovnik troškova i naknada veštačenja USVB⁷“

4 ZAKLJUČAK

U radu je dat, samo, mali deo „Scila i Haribdi“. Najproblematičnije bile su i ostale stručna znanja vezana za konkretni problem. Ovo stoga jer u prvosudnom postupku ne mogu da se dozvole dileme zbog nepotpunosti i/ili nepreciznosti iznošenja činjenica. Veštak nikako ne sme da dozvoli da zbog njegove nesposobnosti bude optuženo i okrivljeno lice koje je nevino, a ništa manje, da ne bude optuženo i okrivljeno lice koje nije nevino.

CITIRANA DELA

Bodolo, I. (2018, 11 29). *Cenovnik*. Preuzeto sa Udruženje sudskih veštaka "Vojvodina": <http://www.forensicexp-vojvodina.org.rs/docs/UVcenovnik.pdf>

Derikonjić, M. (2017, 05 30). *Zakon o rokovima izmirenja novčanih obaveza u komercijalnim transakcijama*. Preuzeto sa Vebsajt Politika: <https://www.paragraf.rs/dnevne-vesti/020617/020617-vest7.html>

Datum prve prijave: 14.08.2018.
Datum prijema korigovanog članka: 22.03.2019.
Datum prihvatanja članka: 27.03.2019.

⁶ Ovdje je stalno prisutna moralna dilema: preterati ili potceniti broj potrebnih sati. Takođe, „ozbiljno“

veštačenje često ulazi u sfere, ako ne naučnog rada, ono barem stručnog rada. Kako „valorizovati“ taj rad?

⁷ USVB – Udruženje sudskih veštaka Beograd.

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

Style – **APA Sixth Edition:**

Rodić, B. S. (2019, 04 15). IT veštak između Scile i Haribde. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 152-158. doi:10.12709/fbim.07.07.01.17

Style – **Chicago Sixteenth Edition:**

Rodić, Boško S. 2019. „IT veštak između Scile i Haribde.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 152-158. doi:10.12709/fbim.07.07.01.17.

Style – **GOST Name Sort:**

Rodić Boško S IT veštak između Scile i Haribde [Časopis] // *FBIM Transactions* / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 152-158.

Style – **Harvard Anglia:**

Rodić, B. S., 2019. IT veštak između Scile i Haribde. *FBIM Transactions*, 15 04, 7(1), pp. 152-158.

Style – **ISO 690 Numerical Reference:**

IT veštak između Scile i Haribde. **Rodić, Boško S.** [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, *FBIM Transactions*, T. 7, str. 152-158



IZAZOV ZLOUPOTREBE INFORMACIONIH TEHNOLOGIJA ZA JAVNO INFORMISANJE

CHALLENGE OF THE ABUSE OF INFORMATION TECHNOLOGIES FOR PUBLIC INFORMATION

Miroslav D. Stevanović

Akademija za nacionalnu bezbednost, Beograd, Srbija

Dragan Ž. Đurđević

Akademija za nacionalnu bezbednost, Beograd, Srbija

©MESTE

JEL Kategorija rada: **H19, H52, Y80**

Apstrakt

U ovom članku posmatramo informisanje kao proces činjenja javno dostupnim podataka i informacija, njihovom distribucijom u kiber prostoru. S obzirom da je informisanje osnovno pravo svake individue i obaveza javnih vlasti, pojava fenomena nazvanog „lažne vesti“ implicira da javne vlasti ne uspevaju, u savremenim uslovima, da obezbede pravo na objektivno i tačno informisanje. Problem koji fokusiramo je u kom obimu informacione tehnologije mogu biti instrumentalizovane za relativizovanje funkcije javnog informisanja. U navedenom kontekstu, cilj rada je da se izoluju mehanizmi zloupotrebe, kako bi ih bilo moguća blagovremeno prepoznati i suprotstaviti se štetnim posledicama u realnom prostoru. Metodološki, rad se zasniva na fenomenološkoj distinkciji značaja utiska naspram na faktičkog stanja, kako bi se došlo do realne vrednosne dimenzije informisanja. Pokazatelji dobijeni na taj način podvrgnuti su analizi sa aspekta potencijalnog strukturalnog i funkcionalnog uticaja sistematske instrumentalizacije informacionih tehnologija za nametanje mnjenja umesto informisanja. Rezultati analize ukazuju da postoji niz rizika koji proističu iz neuređene i nekontrolisane masovne primene informacionih tehnologija, a koji potiču iz neravnopravnog položaja učesnika u kiber prostoru. Nalazi daju osnova za zaključak da potencijalni rizici uključuju i moguće ofanzivno delovanje, te da zahtevaju uređenje preuzimanja i prenošenja informacija i podataka u nacionalnom kiber prostoru. U tom kontekstu, čini se da evaluacije informacionih tehnologija ne može biti prepuštena autarhičnim inicijativama, već da mora biti predmet sistematske ocene od strane relevantnih forenzičkih tela.

Ključne reči: percepcija, narativ, geoprostorno prikupljanje podataka, metapodaci, prikupljanje podataka o ljudskom domenu

Abstract

In this article, we view public information as a process of making available data and information through their distribution, primarily in cyberspace. Given that information is the fundamental right of every individual and obligation of public authority, the emergence of a phenomenon called "fake news"

Adresa autora zaduženog za korespondenciju:
Miroslav Stevanović
mstvnv297@gmail.com



implies that, in contemporary conditions, public authorities fail to secure the right to objective and accurate information. The problem we are focusing on is the extent to which information technology can be instrumentalised to relativise the public information function. In this context, the goal of the work is to isolate the abuse mechanisms, so that they can be timely identified and harmful consequences counteracted in the realm. Methodologically, the work is based on the phenomenological distinction between the importance of the impression and the factual situation in order to reach the real value dimension of information. The indicators obtained in this way are analysed from the perspective of the potential structural and functional impact of systematic instrumentalisation of information technologies to impose opinions instead of informing. The results of the analysis point to the existence of a number of risks arising from the unregulated and uncontrolled mass application of information technologies, which stem from the unequal position of the participants in the cyberspace. Findings provide a basis for the conclusion that potential risks include possible offensive action and require the organisation of the download and transmission of information and data in the national cyberspace. In this context, it seems that information technology evaluations cannot be left to autarchical initiatives, but must be subject to a systematic assessment by relevant forensic bodies.

Keywords: perception, narrativa, geospatial intelligence, metadata, human domain intelligence

1. UVOD

Informacione tehnologije, sa aspekta funkcije u informisanju, predstavljaju upotrebu računara da se arhiviraju, pronađu, prenose ili manipuliše, s jedne strane, nizom kvalitativnih i kvantitativnih promenljivih kao činjenicama koje su osnov za rezonovanje, raspravu ili kalkulaciju (podaci) i, s druge, oblicima i formama koje pružaju deo ili celovit odgovor na neke neizvesnosti, u smislu komunikacije ili dobijanja apstraktnih ili obaveštajnih saznanja (informacije). Ako se posmatra strukturalno, informacione tehnologije obuhvataju sve oblike tehnologije koje uključuju bilo kakav oblik digitalnih (elektronskih) podataka i informacija. Podaci i informacije, u kontekstu analize potencijalne zloupotrebe informacionih tehnologija u informisanju, odnosno kontekstualizovani sa aspekta učesnika u kiber informacionom prostoru, predstavljaju svaki stimulans koji za prijemnika ima neko značenje u određenom misaonom kontekstu.

U skladu sa navedenim, informacioni prostor se doktrinarno može odrediti prema različitim unutrašnjim pravilnostima. Ovaj pojam, s jedne strane, obuhvata set misaonih koncepata i uzajamnih odnosa između njih koje određeni informacioni sistem održava, u smislu kognitivnog prostora (Newby, 2001). U tom smislu, pojam informacioni prostor opisuje opseg mogućih vrednosti ili značenja koji podatak ili informacija mogu imati u okviru datih pravila i okolnosti. S druge strane, ovaj pojam istovremeno podržuje i tip informacionog dizajna u kojem su prenosioci predstave o podatku/informaciji

locirani u načelnom prostoru, odnosno prostoru u kojem njihova lokacija i smer imaju značenje tako da postoji mogućnost njihovog mapiranja i navigacije (MIT Artificial Intelligence Laboratory, 1998) U navedenom smislu, informacioni prostor bi predstavljao ono što nas informativno okružuje, te bi preuzimanje fajlova, korišćenje pretraživanja i ulazak na web stranice predstavljalo kretanje kroz informacioni prostor.

Pored navedenih određenja, koji se zasnivaju na sadržini (materijalistička), informacioni prostor je moguće odrediti i idealistički. Tako se, na primer, može posmatrati kao ukupni rezultat semantičke aktivnosti čovečanstva, kao svet prihvaćenih naziva i značenja, u sprezi sa ontološkim svetom. Kako je informacioni prostor izvorni koncept nemoguće ga je definisati precizno, osim da predstavlja dijalektičku suprotnost materijalnom, fizičkom, objektivnom prostoru. Idealistički posmatrano, informacioni prostor bi predstavljao konceptualni okvir za kodifikovanje, apstrakciju i prenošenje podataka i informacija kroz društveni sistem (Boisot, 1995).

U informacionom prostoru, zloupotreba informacionih tehnologija, apstrahujući sama značajska preferiranja budući da ona ne predstavljaju isključivo posledice takve zloupotrebe, može se odraziti kroz ograničavanje suprotnog mišljenja (regulatorno zarobljavanje), kroz skrivanje poruka (prikrivena cenzura) i kroz pojačavanje linije mišljenja. Sama zloupotreba se, suštinski, sastoji u tome da se informacione tehnologije, koje predstavljaju javni alat i sredstvo, postavljaju kao učesnici u komunikaciji,

ali bez interaktivnih odlika sa drugim učesnicima u javnom prostoru (Karatas; Zihni, 2010).

Na taj način preobražaj ka društvu znanja, kakvom se nominalno teži u informacionom dobu, praktično se podvrgava digitalnoj pristrasnosti. Problem se ispostavlja kao društveno-tehnički. Naime, kako se primećuje u teoriji, on obuhvata značaj, s jedne strane, informacionih tehnologija, odnosno transparentnost i neutralnost platformi i, s druge, administriranja i odgovornosti za informacioni prostor javnih vlasti (Reddick, 2012).

Ovaj problem je višedimenzionalan, budući da obuhvata preduzetničku, bezbednosnu i političku komponentu informacionih tehnologija u informacionom prostoru. Kako informacija ima javnu funkciju, u smislu da oblikuje mnjenje, činioци koji tome doprinose (uključujući informacione tehnologije) mora se posmatrati u kontekstu motivacije javnosti. Kako, sa aspekta korporativnih vlasnika platformi, podatak i informacija postaju roba na tržištu, empirijsko posmatranje je ograničeno na uticaje i stavove.

Informacione tehnologije ne funkcionišu u vakuumu ili izolovano od konteksta u kome se koriste te je neophodno odrediti radni pojam njihove zloupotrebe. U kontekstu ovog rada, pod zloupotrebom informacionih tehnologija podrazumeva se njihovo korišćenje (najčešće od strane korporativnih vlasnika tehnologija) radi uticaja na oblikovanje mnjenja u isključivom interesu nosilaca vlasti ili javnog sektora.

2. INFORMACIONE TEHNOLOGIJE U JAVNOM INFORMISANJU

Primeri naizgled organizovanog postavljanja poruka na mreži su široko opisani u literaturi i medijima i mnogi autori ovo smatraju kao realnost u kiber informacionom prostoru. Javni akteri, međutim, po pravilu negiraju da se pribegavaju takvoj praksi i tvrde da su isključivo posvećeni objektivnom informisanju. Informaciono doba je eksponiralo ulogu koju u distribuciji poruka, pored medija, imaju platforme koje su u vlasništvu i kojima upravljanju privatne korporacije, koje se formalno ne bave javnim informisanjem niti javnim politikama i naizgled su neutralni u procesu informisanja. Njihova uloga u informacionom prostoru proističe iz pozicije pružaoca tehnoloških usluga, posredstvom kojih imaju indirektan pristup učesnicima u na mreži i

direktan pristup njihovim metapodacima (Stevanović, Đurđević, 2018).

Zbog kontrolne uloge koju imaju u tehnološkoj strukturi kiber prostora, ove korporacije su u poziciji da utiču na sve koji se informišu u kiber prostoru, a posebno na učesnike u društvenim mrežama. Njihov uticaj na korisnike može biti indirektan, kroz promociju pozitivnih ili negativnih osećanja o određenoj temi, s jedne, i kroz izazivanje podložnosti određenim emocijama kod učesnika na mreži, s druge strane,. Sledstveno, ove korporaciji su u poziciji da mogu netransparentno da utiču na vrednosne afinitete i prijemčivost informacija na društvenom, pa čak i na porodičnom i privatnom nivou (Miltiadis, Novo-Corti, 2012). U tom, kontekstu, posebno se apostrofira značajan uticaj društvenih mreža na privatnost, povezanost i prijemčivost podataka i informacija, usled čega kompanija koja upravlja mrežom može praktično uticati na sadržaj života u realnom prostoru.

S obzirom da ove kompanije nisu odgovorne za informacije, niti su legitimni politički činioци, mogućnost da oblikuju narative može generisati izazove za demokratske procese i slobode. Osim uticaja vlasnika tehnologija na širenja narativa, umesto objektivnog informisanja, ove kompanije su u poziciji da iz diskursa u kiber informacionom prostoru neposredno eliminišu ili promovišu poruke određene sadržine i učesnike koji zagovaraju takav sadržaj.

Posmatrajući plasiranje narativa u kiber prostoru, može se konstatovati da su u kratkom periodu javno eksponirani mnogi primeri koji svedoče da je uticaj privatnih tehnoloških kompanija na informacioni prostor postao stvarnost.

Tokom predsedničke kampanje u Sjedinjenim Američkim Državama 2016. godine, Facebook je jednostrano gasio veliki broj naloga korisnika koji su agitovali za opozicionog kandidata, ali i onih koji su propagirali afirmativne stavove o nekim pitanjima za koja se taj kandidat zalagao (poput o vojsci, pravu na posedovanje oružja, kontroli granica i hrišćanstvu). Pomenuta kompanija je nastavila takav trend i nedavno uvela softversku aplikaciju na društvenoj mreži kojom upravlja, u svrhu "nezavisnei provjere činjenica", navodno sa ciljem da se eliminišu postovi koji pronose "lažne vesti", što se u praksi svelo skoro isključivo na one koji promovišu konzervativne stavove.

Tokom predizborne kampanje u Francuskoj, Facebook je samoinicijativno na svojoj društvenoj mreži ugasio 30.000 računa, uz obrazloženje da se radi o „lažnim računima“, ali isključivo onih koji su podržavali konzervativnu kandidatkinju (Ali; Associated Press, 2017).

Krajem 2017. i početkom 2018. godine, Twitter je na društvenoj mreži kojom upravlja sproveo kampanju za smanjenje autoriteta zagovornika konzervativne ideološke provenijencije (uključujući libertarijanske). Ova društvena mreža je prethodno, pod izgovorom da je obavezna da obezbedi primenu sopstvenih smernica protiv nasilja i maltretiranja, jednostrano, bez javno poznatih pravila i procedure, izbrisala neke automatske naloge i korisnike zbog navodnog kršenja pravila te mreže. Jedan od izvršnih menadžera Twitter-a svedočio je pred Komitetom za obaveštajne poslove Kongresa SAD, u novembru 2017. godine, da je kompanija smanjila rejting članka objavljenog na portalu, koji se nije uklapao u dominantni narativ i uprkos tome uspeo da zaobiđe algoritam i dospe na vrh opcije trendova (i kao takav privlači korisnike).

Google je pokrenuo niz aktivnosti sa ciljem da na pretraživaču kojem upravlja direktno promeni rezultate pretrage i blokira pristup određenim sajtovima. Ova kompanija je posebno značajna za najširi krug korisnika, jer kontroliše pretraživač koji je prvi dostupan korisnicima koji traže informacije na mreži. Stoga, manipulisanje rezultatima koje korisnici smatraju objektivnim stanjem predstavlja veštačko usmeravanje korisnika i održavanje predrasuda o temi.

Sa Google-om povezana kompanija Youtube takođe je iz svoje mreže uklanjala "desničarske" kanale, bez transparentnog postupka, samo na osnovu procene anonimnih tela unutar kompanije da su na njima prekršeni kompanijski uslovi usluge. S obzirom da se radi o privatnoj kompaniji, a da uklanjanje nije vršeno na osnovu zakonske obaveze, interesantna je opservacija da su neki od uklonjenih kanala imali milijardu pristupa i milione pretplatnika i bili na ovoj mreži više od jedne decenije, što implicira da odluka nije bila motivisana komercijalnom interesom. U oktobru 2017, zaposleni Youtube su priznali da je portal Infowars-a na ovoj mreži cenzurisani, u sklopu interne operacije kompanije uvedene radi uklanjanja objavljenih video zapisa

koji navodno šire lažne informacije, na osnovu žalbe privatne Kablovske mreže vesti (CNN).

Arbitrarnost i moć tehnoloških monopolista na mreži, koja predstavlja javno dobro, otvara, kada se radi o mreži kao informacionom prostoru, pitanje nepristrasnog rukovanja tehnologijom, koji ne bi omogućavao prikrivenu cenzuru. Empirijski posmatrano, vlasnici informacionih tehnologija imaju mogućnost da algoritamski, netransparentno, praktično vrše "izbor" propulzivnog sadržaja na Internetu, kontrolišu ideje u kiber informativnom prostoru, kao i da masovno ciljaju sa porukama. Ako je svrha informisanja stvaranje kompetentnog mnjenja, ove mogućnosti kompanijama predstavljaju izazov kao oblik propagande i dezinformisanja.

Čini se da u kiber informacionom prostoru, kada se radi o javnom informisanju, postoji nivo simbioze između korporativnih monopolista informacionih tehnologija i korporativnih medija sa globalnim domašajem, poput CNN. Naime, sposobnost postojećih softvera da praktično kreiraju sadržaj dostigla je nivo da je otežano da se u kiber prostoru percipira razlika između informacije/podatka od poluinformacija ili dezinformacija koje se plasiraju uklanjanjem sadržaja, upućivanjem, favorizovanjem ili drugim načinima zbunjivanja korisnika. Ova simbioza se posebno ogleda u favorizovanju i uvećanom prikazivanju dometa velikih medijskih sistema, čak i kada ankete ukazuju na nizak nivo poverenja u njihovo izveštavanje. Osnovni problem može se svesti na to da se informacioni prostor koristi kao medijum za kreiranje narativa, umesto za izveštavanje, što ga pretvara u poprište borbe za kontrolu informacija.

Suočeni sa tehnološkim monopolom, potencijalni izvori drugačijih informacija primorani su da povlađuju kompanijama čije tehnološke sisteme i usluge moraju da koriste kako bi obezbedili prisustvo u informacionom prostoru. Ukoliko te kompanije ograničavaju mogućnost predstavljanja drugačijih činjenica, takvo postupanje bi predstavljao udar na informacioni prostor na mreži. Naime, prisustvo na mreži je u informacionom dobu racionalno ponašanje. U tom kontekstu, sajтови postaju javni prostor, te uticaj na informisanje, posebno činilaca koji nemaju formalnu funkciju informisanja, ne bi smeo bitintransparentan i bez osnova u zakonu.

Velike tehnološke kompanije imaju monopol u oblasti informacionih tehnologija i nad medijima. Kako, danas, savremeni čovek sve više vremena provodi pred ekranom ili na mrežama, preko kojih dobija neophodne podatke i informacije, informacione tehnologije imaju objektivnu ulogu u informisanju javnosti.

3. OPŠTE FUNKCIJE UZURPACIJE

Informacije i podaci su, u savremenom svetu, vitalni element koji povezuje ideje, ljude, prostor, znanje i kapital. Informacioni prostor moguće je usmeravati alatima kojima se klasifikuju pojmovi i kontroliše vokabular. Demokratske implikacije mogućnosti da individua aktivno participira u kiber prostoru ogledaju se širenju prostora za razmišljanje i učešće, u smislu da reakcije na osnovu dostupnog sadržaja tvore novi informacioni prostor, u kome se istovremeno kristališe i javno mnjenje.

Sa aspekta tehnološkog uticaja na stvaranje i oblikovanje informativnog prostora u materijalnom smislu, mogu se izvesti četiri opšte funkcije instrumentalizacije kiber prostora za uzurpaciju informacionog prostora: a) masovna tehnološka kontrola mišljenja; b) oblikovanje nerealne percepcije; c) negativne kampanje protiv ideja i individua i d) sredstvo u igri moći (Chalmers, 2003).

a) Masovna tehnološka kontrola mišljenja

Specijalizovani softveri omogućili su da se prevaziđe problem praćenja ogromne količine dostupnih podataka. Inicijalno se radilo o praktičnim alatima za sistematsko praćenje tema, za potrebe specijalizovanih službi da pretražuju veliki broj dokumenata, grupisanjem tema. Ova tehnološka mogućnost daje kvalitativnu prednost korisnicima koji su u mogućnosti da takav softver koriste u kiber prostoru. Naime, praktični značaj ove mogućnosti za usmeravanje mnjenja i narativa može se uporediti sa zloupotrebom informacionog prostora plasiranjem podataka, informacija i narativa preko uticajnih medija, pod okriljem interesa nacionalne bezbednosti, a najočitije u situacijama sukoba. Primer simbioze obaveštajnih službi, medija i interneta u oblikovanju narativa je tokom NATO agresije na bivšu SR Jugoslaviju. Naime, CNN i Nacionalni javni radio (NPR) su priznali da su tokom vojne operacije u njima bile stacionirane jedinice za

psihološke operacije američke vojske. Činjenica da su vojni propagandisti bili u redakcijama medija koji su bili u funkciji propagande podriva pretpostavku o nezavisnosti privatnih informativnih medija.

Od uviđenja ovih softvera, posmatrano u širem kontekstu, kompanije poput Google, Amazon, Facebook i Twitter su demonstrirali moć svojih platformi, da manipulisanjem sadržaja na mreži kanališu emocije i svest korisnika u realnom svetu. Posledica prepoznavanja te moći, u kontekstu dizajniranja i kontrole narativa i javnog mnjenja, je to da su aktivnosti na mreži danas dobile široku primenu u političkim kampanjama.

b) Oblikovanje nerealne percepcije

Suočavanje u informacionom prostoru postalo je sastavni deo različitih vojnih i civilnih operacija. U tom kontekstu, društvene mreže su zbog svojih odlika, dometa i uticaja, postale nezaobilazne za organizovanje, mobilisanje i širenje ideja i za dolaženje do podataka i informacija. Domet društvenih mreža, posebno sa masovnom upotrebom mobilnih telefona, omogućava više kanala za prenos poruka, što ih čini pogodnim kao organizacioni mehanizam i moćno sredstvo za mobilisanja svesti.

Društvene mreže su pogodne za širenje dezinformacija ili kampanja za podrivanje morala ili uticaja i za pokretanje reakcija ciljane grupe. Relativno novi fenomen u tom kontekstu je konkurencija uticaja na percepcije na mreži (rat narativa). Javno poznata taktika u tom kontekstu je upotreba trolova da se započne diskusija i izazovu komentari, kako bi se pokrivali afirmativni i/ili napadali negativni stavovi (Đurđević; Stevanović, 2017). U oblikovanju narativa, sve značajniju ulogu imaju entiteti koji se oslanjaju na tehnologije veštačke inteligencije, preko kojih se pronose informacije ili dezinformacije ili poluinformacije (chat robots, Chatbots). Na primer, Google-ov tip četbot tehnologije reaguje u razgovorima po algoritmima, programiranim na bazi primera iz "trening-dijaloga". Facebook takođe ulaže u razvoj četbot tehnologija koje mogu da simuliraju razgovore ljudi u komunikaciji.

Sa povećanom ulogom društvenih mreža u informacionom prostoru, učesnici na mreži sve više ne moraju da istražuju vesti, jer su izloženi informacijama i tako se obaveštavaju preko drugih individua i društvenih mreža. Na taj način

su izloženi riziku da uverenja o javnim poslovima grade na indirektnom informisanju. Naime, informacioni prostor koji nudi širok spektar izbora *eo ipso* generiše izazov za demokratske procese, jer dovodi do produbljivanja praznina u političkom znanju na osnovu preferencija sadržaja, interesa i načina korišćenja. Pojedinci koji nasumično konzumiraju vesti ne mogu postići napredak u političkom znanju i pored količine informacija budući da, kako se u primećuje u teoriji, aktivno učenje nije srazmerno dostupnom medijskom sadržaju, već pravilnom odabiru informacija.

c) Negativne kampanje

Američka obaveštajna zajednica je upozorila na rizik od spoljnog "finansiranja akademskih institucija i neprofitnih organizacija koje se bave istraživanjem i obrazovanjem kako bi se sprečila istraživanja koja su nepovoljna po finansijere, kao taktike za podsticanje povoljnih stavova i autocenzure". Ova procena je relevantna u kontekstu zloupotreba informacionih tehnologija u kiber informacionom prostoru utoliko što implicira mogućnost zloupotrebe kreiranje mnjenja za obaveštajne, *ergo* i druge informativne operacije.

Kako se samo upozorenje izvodi iz kontemplacije, bez činjeničnih nalaza, čini se da je osnovni motiv upozorenja upravo vezan sa problem dometa velikih američkih kompanija koje pružaju usluge društvenih mreža. U tom smislu ukazuje navod iz izveštaja da kineska aplikacija WeeChat ima više od milijardu korisnika, što joj omogućava da se finansira na američkom tržištu novca. Kako američka obaveštajna zajednica procenjuje da kineski pružaoci ovih usluga imaju određenu kontrolu nad sadržajem i prikupljanjem ličnih podataka, po logici stvari sledi da i je imaju i američke kompanije u tom sektoru. Imajući u vidu da velike tehnološke kompanije iz Silikonske doline imaju ugovore sa američkim saveznim agencijama, posebno sa CIA i NSA, ne može se isključiti mogućnost da američku obaveštajnu zajednicu iritira konkurencija u kiber prostoru. Rezultat ovakvih manipulacija ilustruju brojni primeri. Tako je plasiran narativ kako se Iran fokusira na špijuniranje i kiber operacije protiv SAD i njenih saveznika, iako je u kiber prostoru apsolutna dominacija američkih kompanija i službi, te je taj diskurs notorno u funkciji stvaranja negativnog raspoloženja. Isto se može konstatovati i za rezultat istraživanja

sprovedenog u trenutku zategnutih odnosa sa Severnom Korejom, da 80% Amerikanaca smatra kao kritičnu pretnju sa kojim se suočava i severnokorejske operacije u kiber prostoru.

d) Sredstvo u igri moći

Društveni mediji prenose vesti, poput radija, štampe ili TV. Sa njihovim stalnim emitovanjem u informacioni prostor kod korisnika je rastuće uverenje da se podrazumeva da su informisani, iako ne ulažu ciljane napore u tom pravcu. Kada se kod građana postigne svest da bitne vesti dolaze same, smanjuje se verovatnoća da će oni aktivno tražiti ili proveravati raspoložive informacije. Tako se informisanje svodi na uticaj simboličke komunikacije, a važnu ulogu u tome imaju utisci koji dominiraju na društvenim mrežama.

Učesnici na mreži su danas sve više orijentisani na društvene mreže, a posebno mladi. Prema statistikama za 2017. godinu, evidentirano oko 2,6 milijardi korisnika društvenih mreža širom sveta. Takav nalaz, bez obzira na tačnost statistike, uslovljava da promocija na društvenim medijima postaje obavezna taktika u komunikaciji sa javnošću. Važnu ulogu u strukturiranju odgovarajućeg pristupa imaju Facebook, sa 2.01 milijardu korisnika mesečno, od kojih 88 odsto godišta između 18 i 29 i Twitter, sa 328 miliona korisnika mesečno, od kojih je 36 odsto između 18 i 29 godina. Interakcija mladih je važna pa su razvijene posebne aplikacije za komunikaciju unutar ove populacije, poput Snapchat (dostupan samo preko mobilnih telefona), koji dnevno ima oko 166 miliona korisnika, od kojih 56% između 18 i 29 godina, ili Facebook-ov, Instagram, koji je postao popularan među mladima.

4. RIZICI VEZANI ZA NAČIN KOMUNIKACIJE

Društveni mediji, uvodeći niz opcija koje omogućavaju i pružaju, nameću promene u načinu komunikacije. Kao sredstvo komunikacije, društvene imaju, najmanje, sledeća dejstva:

- doprinose stvaranju osećaja hitnosti i potrebe da se dele poruke (uključujući o privatim životima);
- omogućavaju ličnu predstavu o udaljenim mestima i nepoznatim događajima;
- promovišu opštu priču i detalje, ali ne fokusiraju relevantne informacije;

- donose vesti u živote mlađih generacija; i
- pružaju mogućnost emitovanja uživo i imaju mobilizacijski učinak.

Međutim, kada se radi o razumevanju širokog spektra vesti o političkim i javnim pitanjima, korišćenje društvenih mreža za informisanje ne može da nadomesti potrebu za tradicionalnim izveštavanjem. Izvori informacija u kiber prostoru stvaraju linije priča kroz različite vrste objavljive ličnih mišljenja i uvida. Kako raste popularnost i prihvatanje društvenih medija raste, više korisnika istražuje diskusiju o informacijama i podacima, čak i kada se radi o kriznim situacijama. Zbog toga je stvaranje strateških narativa u centru savremenih strategija komunikacije u poslovanju, politici i vojnim operacijama. Borba narativa postala je poluga i međunarodne politike, a u tom okviru društvene mreže postaju neophodni alat za nadmetanje.

Posledica društvenih mreža je da osnažuju individuu, tako što omogućavaju da deluje u mreži na načine koji nisu vidljivi. Kao takvi su ujedno pogodni za diversifikaciju i unapređenje propagandnih i psiholoških operacija, kao metoda uticaja na javno mnjenje.

Oblikovanja narativa, osim uticaja na prilagođavanje svesti, utiče i na institucionalni aspekt sistema nacionalne bezbednosti. Naime, promena percepcije o bezbednosno indikativnoj prirodi pojave ne menja činjenice, već samo njihovo značenje (poimanje). Otuda je oslanjanje na informacione tehnologije problematično, budući da one nemaju logički kapacitet, te efikasnost iziskuje da se prethodno odrede segmenti koji istim činjenicama daju novo značenje. Kako je nacionalna bezbednost vrednosno objektivna kategorija, ona zavisi od percepcije, zbog čega se kao problem ispostavlja blagovremeno prepoznavanje izazova i razumevanje i identifikovanje pretnji i rizika, što zahteva odgovarajući kapacitet za kreativno i vrednosno razmišljanje u procesu odlučivanja (Stevanović, Đurđević, 2015).

Jednostavnost korišćenja i pristupačnosti društvenih medija, te razvoj strategija digitalne manipulacije, prisiljavaju obaveštajne službe, vojne stratege i kreatore politike da se prilagode toj stvarnosti. Javno eksponiran skandal, vezano za političku konsultantsku kompaniju Cambridge Analytica (CA), otkrio je mogućnosti zloupotrebe

neovlašćenog prikupljanja podataka korisnika Facebook-a. CA je, naime, koristila nemoralne taktike kako bi se uticalo na izbore. To je, između ostalog, obuhvatalo Facebook ažuriranja, putem reklama, da bi stiglo do korisnika koji objavljuju poruke. Facebook je dopustio CA pristup podacima o svojim korisnicima i o njihovim prijateljima u toj mreži, čak i onima koji nisu instalirali aplikaciju, niti su prihvatili da dele svoje lične podatke, što je omogućilo programerima sa Univerziteta Kembridž da brzo kreiraju baze podataka i tajni uticaj na demokratske procese. Sa aspekta uticaja informacionih tehnologija na institucionalizaciju upravljanja informacijama i međuljudske odnose posebno treba imati u vidu mogućnost geoprostornog prikupljanja podataka, budući da predstavlja rizik za privatnost ličnih podataka na mreži.

Termin geoprostorni koristi se da izrazi kolektivitet podataka i prateće tehnologije sa geografskom ili lokacijskom komponentom, odnosno zapisa koji u skupu podataka sadrže lokacijske informacije vezane za njih (na primer, u obliku koordinata, adrese, grada). Geoprostorni podaci mogu poticati iz sistema u kojima se geografske informacije čuvaju i integrišu u geografske softverske programe tako da se mogu kreirati, čuvati, koristiti, analizirati i vizualizovati (mapirati). Sajtovi društvenih mreža, na primer, koriste "check-in" koji korisnicima omogućava da svoje statusne podatke označe geografski.

Za prikupljanje, manipulaciju i skladištenje geografskih podataka i informacija koriste se geoprostorne tehnologije. Radi se o opsegu alata koji omogućavaju geografsko mapiranje i analizu zemlje i ljudskih društava. Među takvima su:

- daljinska detekcija, kojom se dolazi do slike i podataka sa različitih kamera, uređaja i senzorskih platformi. Kako neki od ovih izvora pokazuju detalje od jednog metra ili manje, takve slike mogu biti zloupotrebljene za praćenje ljudskih potreba, navika i kršenje ljudskih prava.
- geografski informacioni sistem (GIS), što obuhvata skup softverskih alata za mapiranje i analizu geografski određenih podataka. GIS se može koristiti za utvrđivanje geografskih obrasca u drugim podacima, uključujući i vezano za ljudsko ponašanje i navike.
- sistem globalnog pozicioniranja (GPS) obuhvata mrežu satelita američkog Sekretarijata odbrane koja pruža precizne koordinatne lokacije civilnim i

vojnim korisnicima sa odgovarajućom opremom za prijem (sličan evropski sistem nazvan Galileo trebalo bi da postane operativan narednih godina dok ruski sistem funkcioniše, ali je ograničen).

- internet mapiranje obuhvata softverske programe (poput Google Earth) i aplikacije na mreži (poput Microsoft Virtual Earth) koje menjaju način razmišljanja i razmene geoprostornih podataka. Kretanje u korisničkom interfejsu omogućava dostupnost takvih tehnologija, zbog čega su te tehnologije podstakle mrežu nacionalnih bezbednosnih, naučnih i komercijalnih satelita. Visokokvalitetni hardver i podaci su sada široko dostupni, te je omogućeno prikupljanje niza geoprostornih podataka, bez adekvatne kontrole i regulative u pogledu korišćenja podataka, što predstavlja izazov za zaštitu podataka o ličnosti.

Geoprostorno prikupljanje podataka omogućava fuziju kartografskih podataka da konvencionalnim obaveštajnim podacima državnih agencija. Ono je zasnovano na aktivnosti i, posmatrano sa aspekta manipulacija u informativnom prostoru, pogodno je za istraživanje relevantnih obrazaca, odnosno istraživanje ljudskog domena.

Kiber prostor može biti zloupotrebljen ciljano, okupirajući ga informacijama, dezinformacijama i poluinformacijama, kako bi se neurofiziološki uticalo na ponašanje. U tom kontekstu, posebno je eksponirana zloupotreba metapodataka, odnosno podataka o sadržaju najčešće korišćenih klikova na mreži, što omogućava predstavu o individui i afinitetima i, u skladu sa tim, uticaj na percepciju.

Navedeno ukazuje da ključni nosioci komunikacionih tehnologija u kiber prostoru, funkcionalno, predstavljaju činioce koji imaju uticaj na izbor, dinamiku i promociju sadržaja, s jedne, kao i činioce uticaja na oblikovanje mnjenja u određenom periodu. Ova funkcionalna odlika može se konstatovati na primerima podrivanja tradicionalnih vrednosti (poput obojenih revolucija), kada cilj nisu institucije (zbog čega su pogodni nenasilni metodi), već nametanje odgovarajućih narativa u informativnom prostoru. Na primer, aplikacija društvene mreže Telegram, pokrenuta 2013. godine, omogućava razmenu poruka u grupama do 5.000 ljudi i bezbedno šifrovane komunikacije. Vlasti nekoliko zemalja (Rusija, Jermenija) ukazivale su da je ova mreža

korišćena u planiranju terorističkih napada i uličnih protesta. Takva funkcionalna uloga omogućava sistemsku instrumentalizaciju informacionih tehnologija, odnosno strukturalne pozicije vlasnika tih tehnologija u informisanju javnosti, iako njihova profesionalna aktivnost ne uključuje informisanje javnosti.

U navedenom kontekstu, informacione tehnologije mogu u informacionom prostoru biti zloupotrebljene, najopštije posmatrano, nelegitimnim korišćenjem (zloupotreba sistema) ili podrivanjem sistema (sistemska zloupotreba).

Kao zloupotreba sistema može se kvalifikovati korišćenje tehnologija na način koji obuhvata: neovlašćen pristup podacima; neovlašćeno korišćenje podataka ili informacija iz informacionih sistema; kršenje privatnosti ličnih podataka; neovlašćeno otkrivanje poverljivih ili osetljivih informacija; neovlašćeni pristup računarskim sistemim trećih strana; prenos neželjenih materijala; imitiranje drugog pojedinca preko mreže pomoću njihovog pristupa; prekomerno preuzimanje, skladištenje, datoteka ili podataka koji nisu direktno povezani sa zadatkom korisnika; Instaliranje neovlašćenog softvera, aplikacije ili dodataka, kao i preuzimanje nedozvoljenih materijala.

Kao sistemska zloupotreba mogu se smatrati operacije kojima se bilo neovlašćeno korumpira ili uništava informacioni sistem ili podaci tj. informacije, uključujući ubacivanjem računarskih virusa ili zlonamernog softvera kako bi se korumpirala računarska ili mrežna oprema, softver ili podaci, ili obezbedio neovlašćeni pristup korisničkom imenu, lozinkama ili identifikacionim detaljima.

Analizu opsega zloupotreba informacionih tehnologija u informacionom prostoru teško je posmatrati kao neutralnu pojavu. U tom smislu ukazuje primer kanadskog premijera, inače poznatog kao jednog od najzastupljenijih emitera poruka na Twitter-u i Instagram-u, koji je uprkos svojoj dominantnoj poziciji u informativnom prostoru Kanade javno zapretio direktorki Facebook-a u toj državi da će se suočiti sa „strožijom“ regulativom ukoliko ne reši objavljivanje statusa koje on smatra „lažnim“ (Boutilier, 2018). Istraživanja mogućih zloupotreba na koje ovaj primer ukazuje, do sada su obično potcenjivala nivo saradnje nacionalnih

sistema bezbednosti i tehnoloških monopolista u kreiranju javnog mnjenja. Ovakvo stajalište bi trebalo uvažavati, bez obzira na problem dokazivosti. Alford i Seker su, zahvaljujući dokumenatima dobijenim na osnovu Zakona o slobodi informisanja, uspeli da dokažu da je, na primer, američki sistem nacionalne bezbednosti, pre svih Centralna obaveštajna agencija (CIA) i generalštab (Pentagon) radio na više od osam stotina filmova holivudske produkcije i preko hiljadu televizijskih emisija (Alford; Secker, 2017). Ove snage su iz političkih razloga menjale scenarije, da se određene priče potisnu ili ubace u javni narativ. Kada pisac ili producent zatraže pristup imovini državnih agencija, moraju da podnesu scenario radi provere. Sekretarijat odbrane ima oficira za vezu za film i TV. Da bi se ostvarila saradnja, proizvođači moraju da potpišu sporazum o pomoći u produkciji, koji ih vezuje za odobrenu verziju scenarija. CIA nema formalni postupak provere scenarija, ali ima oficira za vezu za zabavu, koji je uspevao da se ubaci u rane faze pisanja nekih scenarija. Iako se, strogo posmatrano, ne radi o cenzuri, činjenica je da se koristi uticaj i netransparentan pritisak na narative i simboliku koji se emituju širom sveta (za Srbiju, ova knjiga je značajna jer ozbiljno preispituju uvrežene narative o Balkanu devedesetih). Kako se radi o državi koja otvoreno koristi svoju moć u inostranstvu, netransparentno oblikovanje popularne kulture za promovisanje načina razmišljanja trebalo bi posmatrati i sa aspekta hegemonije.

ZAKLJUČNA RAZMATRANJA

Veštačka inteligencija omogućava da stvarnost bude ono što algoritam predviđa. Stoga, monopol nad algoritmima nužno dovodi do mogućnosti nametanja odluka i, posledično, ograničava humanost. Kako je pokazano, Google, Facebook i Youtube već sad algoritamski ograničavaju dostupnu istinu, što predstavlja pravni problem, jer primenjuju subjektivne kriterijume i postupke u javnom prostoru.

Informisanje u praksi postaje zasnovano na aspektu programiranja i oblikovanja svesti umesto na činjenicama i događajima. Ako takvo informisanje postane prepušteno automatizmu i algoritmima, čitav sistem informisanja postaće u funkciji onih koji kontrolišu korporacije koje kontrolišu platforme. Opštije posmatrano, čini se

da postoji potreba uspostavljanja ravnoteže između antropocentričnog i tehnokratskog.

Tehnološke kompanije, po prirodi svog proizvoda, zavise od državnih sistema. U simbiozi administracija i tehnoloških monopolista razvija se direktna poluga nad distribucijom vesti u kiber prostoru. Tehnološke kompanije, pravno-logički posmatrano, ne mogu imati takvu moć. Naime, nije moguće preneti ovlašćenja kojima bi se pravo na informisanje ograničavalo voljom privatnih kompanija, kao ni država, u toj oblasti.

Navedeni primeri, pak, pokazuju da su decenije strateških integracija dovele do vertikalne tehnološke integracije, koja okupira informacioni prostor na mreži. Ukidanjem u tom prostoru, individua je onemogućena da postoji u kiber prostoru, odnosno postaje „nelice“, a ako je to zbog stavova, onda su i stavovi objekat cenzure. Mogućnost privatne ucene u tom prostoru svodi se na reketiranje (naplata zaštite od sopstvenog maltretiranja). Prihvatanje ove prakse bi podrazumevalo da privatni proizvođači struje mogu da ne isporuče struju korisnicima čiji im se šporeti ne sviđaju, ili vlasnici zemlje preko koje protiče potok da ograde tok jer im se ne sviđa bilje koje se gaji vlasnik susednog zemljišta.

Analizirane mogućnosti zloupotrebe informacionih tehnologija u kiber informacionom prostoru ukazuju da savremeno doba nameće potrebu da svi profesionalni akteri u tom prostoru imaju niz sposobnosti u funkciji efikasnosti zaštite objektivnog informisanja javnosti. Prema tipu izazova sa kojim se suočava, ove sposobnosti se mogu podeliti u tri kategorije: profesionalne, upravljanja informacijama i društvene. Izuzev profesionalne, druga dva tipa sposobnosti obuhvataju i one koji se bave nadzorom i kontrolom sistema informisanja, koji je preduslov funkcionalne demokratije.

U uslovima višeslojnih izvora i izloženosti obilju i brzini dostupnih podataka i informacija naglašena je potreba da profesionalci u informativnom sektoru znaju kako istraživati (uključujući i nekonvencionalnim metodima), kako dolaziti do podataka i informacija i odabrati one relevantne za analizu, proveravati njihov kvalitet i koristiti odgovarajuće analitičke metode, kako bi se obezbedio uvid i predviđanje i formirali zaključci i sinteza. Sposobnost da se odgovori na ključne probleme obezbeđivanja uvida javnosti u odluke i

događaje je osnovni uslov suočavanja sa izazovima delatnosti. Ova sposobnost iziskuje niz veština, u koje spadaju kritičko, logično i analitičko razmišljanje, veština posmatranja, tačnost, svest za detalje, racionalnost i intelektualna radoznalost.

U uslovima rastućeg značaja višestrukih izvora informacija na mreži, važno je razumeti širi kontekst ključnih pitanja, imati odgovarajuće sagovornika i demonstrirati znanje. U okruženju brzine inputa informacija, delotvornost izveštavanja postaje zavisna od upravljanja izveštajima, projektima, procesima, vremenom i opterećenjem. Sposobnost upravljanja procesom prikupljanja informacija zahteva više veština: rad na strukturiran način, izbor ciljeva i racionalno

angažovanje, otpornost na simboličku komunikaciju, odgovornost, praktičnost i posvećenost. Uz to je, čini se, neophodno imati razvijen vrednosni sistem i apstraktno mišljenje.

U uslovima intenzivne međupovezanosti na mreži, preduslov delotvornosti postaje i saradnja sa okruženjem. Uloga profesionalaca u informacionom prostoru postaje i da prevazilazi posledice obilja činjenica i mišljenja. Komuniciranje zahteva niz veština u odnosu sa ljudima: kako se stvaraju, održavaju i razvijaju relevantni odnosi i veze, kako se stiče poverenje drugih učesnika, uključujući korisnika (neprofesionalnih izvora), a posebno kako da se spoznaju i razumeju interesi u pozadini.

CITIRANA DELA

Alford, M.; Secker, T. (2017). National Security Cinema: The Shocking New Evidence of Government Control in Hollywood. CreateSpace Independent Publishing Platform.

Ali, S.S., Associated Press (2017). Accounts in France Ahead of Presidential Election. NBC News, April 15.2017. Preuzeto Jul 31, 2018 sa. <https://www.facebook.com/notes/facebook-security/improvements-in-protecting-the-integrity-of-activity-on-facebook/10154323366590766/>

Boisot, M. H. (1995). Information Space: A Framework for Learning in Organizations, Institutions and Culture. Routledge, London.

Boutilier, A. (2018). Trudeau to Facebook: Fix your fake news problem or face stricter regulations. The Star, Feb. 8, 2018. Preuzeto Jul 31, 2018 sa: <https://www.thestar.com/news/canada/2018/02/08/trudeau-to-facebook-fix-your-fake-news-problem-or-else.html>

Chalmers, M. (2003). Informatics, Architecture and Language. Höök, U: K., Benyon D., Munro A. J. (eds.), Social Navigation of Information Space. London: Springer Verlag, pp. 315-343.

Đurđević, D., Stevanović, M. (2017). Internet as a Method od Trolling Offensive Intelligence Operations in Cyberspace. *NBP Journal of Criminalistics and Law*, 22(2), 13-32.

Karatas, M., Zihni T. M. (2010). Sustainable Economic Development and the Influence of Information Technologies: Dynamics of Knowledge Society Transformation. IGI Global, Hershey/New York.

Miltiadis, L., Novo-Corti, I. (2012). Trends and Effects of Technology Advancement in the Knowledge Society. Information Science Reference, Hershey.

MIT Artificial Intelligence Laboratory (1998). The JAIR Information Space. Preuzeto Jul 31, 2018 sa: <http://www.ai.mit.edu/projects/infoarch/jair/jair-help.html>.

Newby G. (2001). Cognitive Space and Information Space. *Journal of the American Society for Information Science and Technology*, 52(12), 1026-1048.

Reddick, C. (2012). Public Administration and Information Technology“. Jones & Bartlett Learning, Burlington/Ontario/London.

- Stevanović, M., Đurđević, D. (2015). The Capacity of Perception: The Need for an Educational System in Support of the National Security. In: Grozdanić R., Jovančević, D. (eds.), Creative Education for Employment Growth: Proceedings Fourth International Conference „Employment, Education and Entrepreneurship“, 14-16 October 2015, Belgrade. Belgrade: Faculty of Business Economics and Entrepreneurship/ Chicago: Bar Code Graphics, 47-56.
- Stevanović, M., Đurđević, D. (2018). The Challenges of Shaping Narratives in Cyberspace for National Security. Proceedings of the 10th Scientific Conference "Freedom and security in real and syber space", Belgrade, 08.06.2018.

Datum prve prijave: 15.08.2018.
Datum prijema korigovanog članka: 22.03.2019.
Datum prihvatanja članka: 27.03.2019.

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

Style – **APA Sixth Edition:**

Stevanović, M. D., & Đurđević, D. Ž. (2019, 04 15). Izazov zloupotrebe informacionih tehnologija za javno informisanje. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 159-169.
doi:10.12709/fbim.07.07.01.18

Style – **Chicago Sixteenth Edition:**

Stevanović, Miroslav D, i Dragan Ž Đurđević. 2019. „Izazov zloupotrebe informacionih tehnologija za javno informisanje.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 159-169.
doi:10.12709/fbim.07.07.01.18.

Style – **GOST Name Sort:**

Stevanović Miroslav D i Đurđević Dragan Ž Izazov zloupotrebe informacionih tehnologija za javno informisanje [Časopis] // *FBIM Transactions* / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 159-169.

Style – **Harvard Anglia:**

Stevanović, M. D. & Đurđević, D. Ž., 2019. Izazov zloupotrebe informacionih tehnologija za javno informisanje. *FBIM Transactions*, 15 04, 7(1), pp. 159-169.

Style – **ISO 690 Numerical Reference:**

Izazov zloupotrebe informacionih tehnologija za javno informisanje. **Stevanović, Miroslav D i Đurđević, Dragan Ž.** [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, *FBIM Transactions*, T. 7, str. 159-169.



UTICAJ TRANSFORMACIONOG LIDERSTVA I LIDERSTVA PROMENE NA SPREMNOST ZA PROMENU I PREDANOST PROMENI

THE IMPACT OF TRANSFORMATIONAL AND CHANGE LEADERSHIP ON CHANGE READINESS AND COMMITMENT TO CHANGE

Salih Šutković

Cost und Effect, Frankfurt am Main, Germany

Nebojša Zakić

Univerzitet „Union – Nikola Tesla“, Beograd, Srbija

Aleksandra Tornjanski

Visoka turistička škola strukovnih studija, Beograd, Srbija

©MESTE

JEL kategorija: **L16, O33**

Apstrakt

Negativni stavovi o promeni su jedan od glavnih uzroka neuspeha organizacione promene. Istraživači su se isprva najviše fokusirali na otpor promeni a kasnije je razvijeno više konstrukta sa istraživačkim instrumentima koji reprezentuju pozitivne stavove članova organizacije o promenama među kojima se izdvajaju spremnost za promenu i predanosti promeni. Spremnost za promenu stvara pozitivnu energiju neophodnu za uspeh napora promene i važna je karika za dostizanje željenih ishoda promene. Spremnost za promenu je složen i multidimenzionalan konstrukt. Predanost promeni je konstrukt sa snažnim pozitivnim fokusom. Visoko predani članovi organizacije ulažu napore, pokazuju inicijativu i kooperativno se ponašaju što doprinosi efektivnoj implementaciji promene. U kontekstu organizacione promene se generalno koriste dva pristupa za razumevanje uloge liderstva u oblikovanju odgovora sledbenika na promenu: transformaciono liderstvo i liderstvo promene. Transformaciono liderstvo je dugo razvijan konstrukt i jedna je od najinteresantnijih tema savremenih istraživanja o liderstvu iznedrivši veliki broj studija. S druge strane mnogo je manje istraživačkih radova o liderstvu promene i tek u novije vreme je uspostavljen konstrukt i istraživački instrument. U radu se istražuje uticaj transformacionog liderstva i liderstva promene na spremnost za promenu i predanost promeni uključujući i međusobne relacije između spremnosti za promenu i predanosti promeni i predlaže

Adresa autora zaduženog za korespondenciju:

Nebojša Zakić

nebojsa.z@fpb.edu.rs



model u kojem spremnost za promenu ima medijatorsku ulogu između liderskih ponašanja i predanosti promeni.

Ključne reči: organizacione promene, spremnost za promenu, predanost promeni, transformaciono liderstvo, liderstvo promene

Abstract

Negative attitudes towards change are one of the main reasons why an organizational change fails. Initially, researchers focused on resistance to change, subsequently developing several constructs with research instruments, which represent positive attitudes of organizational members to change, among which a readiness for change and a commitment to change stands out. Readiness for change creates positive energy necessary for the success of a change effort and it is an important link for achieving the desired outcome of a change. Readiness for change is a complex and multidimensional construct. A commitment to change is a construct with a strong positive focus. Highly committed organizational members make efforts, show initiative and act cooperatively, which contributes to the effective change implementation. Within the context of organizational change, two approaches are generally used to understanding the role of leadership in shaping a follower's response to change: transformational leadership and change leadership. Transformational leadership is a construct which took a long time to develop, and it is one of the most interesting topics in modern leadership research. On the other hand, there are infinitely fewer research papers on change leadership, the construct and research instrument having been established only recently. This paper examines the influence of transformational leadership and change leadership on a readiness for change and a commitment to change, including relationship between a readiness for change and a commitment to change, and suggests a model in which a readiness for change has a mediating role between leadership behaviors and a commitment to change.

Keywords: organizational change, readiness for change, commitment to change, transformational leadership, change leadership

1 UVOD

Organizacije moraju da se menjaju kako bi opstale i prosperirale. Organizacije implementiraju programe promene u pokušaju da anticipiraju, ili se adaptiraju, snagama okruženja kao što su globalizacija, porast kompeticije, promene potreba i očekivanja kupaca, tehnološke promene i promene regulative ili internim snagama kao što su novi menadžment, promene strategije, pad organizacionih performansi, slabosti postojećeg sistema ili kriza. Sposobnost da se upravlja eksterno i interno generisanim promenama postaje jedna od ključnih sposobnosti savremenih organizacija. Međutim mnoge organizacije ne uspevaju da uspešno implementiraju promenu. Iako mnogi faktori nesumnjivo doprinose uspehu ili neuspehu napora organizacione promene u literaturi postoji konsenzus da je za uspešno uvođenje promene potrebna podrška od strane zaposlenih (Georgiades, 2015). Posebno pozitivni stavovi zaposlenih ka organizacionoj promeni se vide kao neophodni za uspeh planirane promene (Chou, 2013), s druge strane negativni stavovi ka promeni imaju suprotan efekat, povećavajući

verovatnoću neuspeha (Neiva, Ros, & Torres de Paz, 2005).

Tokom poslednjih decenija razvijani su različiti konstrukti koji se odnose na stavove o organizacionoj promeni rangirajući od negativnih kao što su otpor promeni, cinizam u vezi promene i suočavanje sa promenom do pozitivnih među kojima su spremnost za promenu, otvorenost promeni, predanost promeni i usklađivanje sa promenom (Bouckenooghe, 2010). Dva najviše istražena konstrukta koji reprezentuju pozitivne stavove o promeni su spremnost za promenu i predanost promeni. U radu uspostavljamo relacije ova dva konstrukta međusobno kao i sa liderstvom koje saglasno istraživačkoj evidenciji ima značajan uticaj na stavove i ponašanje članova organizacije (Tanner, et al., 2010; Wang, Tsui, & Xin, 2011). Među različitim paradigmama i konstruktima koji se odnose na liderstvo i stilove liderstva konstrukti transformacionog i transakcionog liderstva privukli su najveću pažnju istraživača i praktičara. U radu se usmeravamo na transformaciono liderstvo koje je posebno kritično u situacijama kada se izaziva postojeći status quo i organizacija menja (Boga & Ensari, 2009).

Liderstvo promene je takođe predmet ovog rada, ovaj konstrukt je kreiran relativno skoro (Liu, 2010) i istraživačka evidencija je još nedovoljna. Uticaj ova dva liderska stila, posebno liderstva promene, na spremnost za promenu i predanost promeni nije dovoljno zastupljen u literaturi. Takođe veoma je mali broj radova o relacijama između spremnosti za promenu i predanosti promeni.

Naš rad pokušava da popuni jaz u literaturi povezujući transformaciono liderstvo, liderstvo promene, spremnost za promenu i predanost promeni. Rad je organizovan u pet sekcija. Posle prve sekcije (uvod) u drugoj sekciji razmatramo konstrukte spremnosti za promenu i predanosti promeni. U sledećoj sekciji prezentujemo konstrukte transformacionog liderstva i liderstva promene. Centralni deo rada je četvrta sekcija u kojoj povezujemo transformaciono liderstvo, liderstvo promene, spremnost za promenu i predanost promeni, predlažemo hipoteze i teorijski model. Poslednje sekcija je zaključak.

2 SPREMNOST ZA PROMENU I PREDANOST PROMENI

Stavovi o organizacionoj promeni su, saglasno brojnim istraživačima (Eby et al., 2000; Yousef, 2000; Elias, 2009; Choi & Ruona, 2011 i dr.), esencijalni za uspeh ili neuspeh organizacione promene. Stoga se u literaturi pridaje značajna pažnja istraživanju stavova o organizacionoj promeni, varijablama koje deluju na pozitivan ili negativan način na ove stavove i njihovom uticaju na ishod organizacione promene. Vremenom je razvijeno više konstrukta koji reprezentuju pozitivne i negativne stavove o organizacionim promenama. Među onima koji su pobudili najveću pažnju su otpor promeni i cinizam u vezi sa promenom, na negativnoj strani, i spremnost za promenu i predanost promeni, na pozitivnoj strani. Negativni stavovi o promeni uzrokuju neuspeh promene i isprva su bili više u fokusu istraživača, što se uglavnom odnosi na otpor promeni. Kako je organizacijama sve više bilo potrebno da poboljšaju njihove sposobnosti za podršku i prihvatanje inicijativa promene, konstrukti koji reprezentuju pozitivne stavove o promeni su zadobijali sve veću pažnju istraživača.

Spremnost za promenu je, uz otpor promeni, konstrukt koji je iznedrio najviše studija. Spremnost za promenu je preduslov za uspeh

inicijativa promene (Armenakis, Harris, & Mosholder 1993; Eby et al., 2000; Bernerth, 2004). Za razliku od otpora spremnost za promenu je proaktivan i dinamičan pogled na promenu, stvara pozitivnu energiju neophodnu za uspeh napora promene i važna je karika za dostizanje željenih ishoda promene. Spremnost za promenu je složen i multidimenzionalan konstrukt. Od uvođenja u organizacionu teoriju i praksu nastale su različite definicije, pristupi i modeli. Choi & Ruona (2011) argumentuju da se većina definicija slaže u vezi opšteg razumevanja pojma koji povezuje individualnu spremnost za organizacione promene koja uključuje individualnu procenu individualnog i organizacionog kapaciteta za uspešnu realizaciju promene, potrebu za promenom i benefite koje organizacija i njeni članovi mogu postići od promene. Sa praktične strane istraživači su nastojali da kreiraju odgovarajući istraživački instrument kako bi se mogla izvršiti pouzdana i validna ocena spremnosti za promenu po organizacijama.

Jedan od reprezentativnih modela i istraživačkih instrumenata spremnosti za promenu, često korišćen u istraživanjima, daju Holt et al. (2007). Autori u gradnji modela polaze od više perspektiva (ustanovljenih od Armenakis & Bedeian, 1999):

1. sadržaj promene - šta se menja;
2. proces promene - kako se promena inicira i implementira;
3. kontekst promene - okruženje u kojem se promena dešava; i
4. individualni atributi - sklonosti i karakteristike ljudi uključenih u proces promene.

Multidimenzionalni konstrukt sastoji se iz četiri dimenzije (Holt et al., 2007):

1. prikladnost,
2. podrška menadžmenta,
3. efikasnost i
4. personalna valenca.

Dimenzija prikladnosti je izvedena iz dve ranije dimenzije: nesaglasnosti – percepcije učesnika u pogledu opravdanosti promene i organizacione valence – percepcije učesnika u kojem stepenu bi promena bila korisna za organizaciju. Podrška menadžmenta se odnosi na stepen do kojeg pojedinci opažaju da li menadžment i liderstvo organizacije podržavaju ili ne organizacionu

promenu. Efikasnost (samo-efikasnost) se odnosi na stepen do kojeg se pojedinci osećaju sigurnim da su sposobni da izvrše sve zadatke i aktivnosti vezane za promenu. Personalna valenca je stepen do kojeg učesnici u promeni opažaju da li će ili ne imati benefite od promene (Holt et al., 2007).

U osamdesetim i devedesetim više istraživača je ustanovilo važnost predanosti promeni kao jednog od ključnih faktora za uspeh inicijative promene (Conner & Patterson, 1982; Klein & Sorra, 1996). Primarna studija o predanosti promeni je rad Herscovitch & Meyer (2002) u kojoj se predanost promeni razvija na osnovu organizacione predanosti kao multidimenzionog konstrukta. Autori transformišu tri dimenzije organizacione predanosti i povezuju svaku dimenziju sa organizacionom promenom. Saglasno Bouckennooghe (2010), u poređenju sa ranijim studijama, model koji daju Herscovitch, & Meyer (2002) nudi robustan i više teorijski utemeljen pristup predanosti promeni. Prema Herscovitch & Meyer (2002) tri dimenzije predanosti promeni su:

1. afektivna predanost promeni – želja da se podrži specifična promena;
2. kontinuirana predanost promeni - prepoznavanje da postoje troškovi asocirani sa neuspehom da se obezbedi podrška za promenu; i
3. normativna predanost promeni - reflektuje osećaj obaveze da se obezbedi podrška za promenu.

Drugim rečima, pojedinci mogu podržati napor promene zato što oni to žele, moraju ili trebaju (Herscovitch & Meyer, 2002). Herscovitch & Meyer (2002) razvijaju istraživački instrument koji se zasniva na tri dimenzije predanosti promeni.

Predanost promeni kao trodimenzionalni konstrukt primio je značajnu pažnju istraživača ali saglasno Bouckennooghe, Schwaz, & Amirali (2015) ukupan broj studija van severnoameričkog područja je još mali. Istraživači demonstriraju da predanost promeni je konceptualno i empirijski različit konstrukt od organizacione predanosti i bolji je prediktor podrške za promenu (Herold et al. 2008). Prema meta analizi koju su sprovedi Bouckennooghe, Schwaz, & Amirali (2015) utvrđena je visoka korelacija između afektivne i normativne predanosti promeni, umerena korelacija između normativne i kontinuirane

predanosti promeni i visoka ali negativna korelacija između afektivne i kontinuirane predanosti promeni. Meta analiza pokazuje da su afektivna i normativna predanost promeni pozitivno asocirane sa ponašanjima koja podržavaju promenu dok je kontinuirana predanost promeni umereno negativno povezana sa tim ponašanjima (Bouckennooghe, Schwaz, & Amirali, 2015).

3 TRANSFORMACIONO LIDERSTVO I LIDERSTVO PROMENE

Transformaciono liderstvo je jedna od najinteresantnijih tema među istraživačima liderstva iznedrivši veliki broj studija. Pojam transformacionog liderstva uveo je Burns (1978) čineći distinkciju između transformacionog i transakcionog liderstva. Bass (1985) je dalje proširio i razvio teoriju definišući ponašanja transformacionih i transakcionih lidera. Prema Bass (1985) transakcioni lideri fokusiraju se na razjašnjavanje zadataka koji treba da se izvrše, očekivanja koja imaju, odgovornosti sledbenika i benefite za sledbenike ako je zadatak ispunjen. Transformacioni lideri svojom ličnom vizijom i energijom motivišu sledbenike da se angažuju izvan granica očekivanog, uveravajući sledbenike u značaj i vrednost njihovih zadataka, podstičući klimu poverenja, aktivirajući njihove potrebe višeg reda (kao što je samoostvarivanje), i navodeći ih da pređu granicu sopstvenih interesa radi dobrobiti organizacije.

Saglasno Bass & Avolio (1994) dimenzije transformacionog liderstva uključuju:

1. idealizovani uticaj - lideri predstavljaju jak model uloga za sledbenike, lideri su poželjni, poštovani i zaslužuju poverenje;
2. inspiraciona motivacija – lideri motivišu i inspirišu sledbenike projektujući entuzijazam i optimizam i artikulišu viziju budućeg stanja;
3. intelektualna stimulacija – lideri izražavaju nove ideje, podstiču sledbenike da budu uključeni u proces adresiranja problema i pronalaženja rešenja i promovišu kreativnost i inovacije; i
4. individualizovano razmatranje – lideri izražavaju brigu za individualne potrebe sledbenika i deluju kao učitelji i mentori dok nastoje da pomognu sledbenicima. Bass & Avolio (1994) razvijaju model potpunog

liderstva koji se sastoji iz četiri dimenzije transformacionog liderstva, i tri dimenzije transakcionog liderstva kao i istraživački instrument - Multifaktorski liderski upitnik. Istraživači širom sveta koriste ovaj instrument i njegova validnost je podržana u meta analizama (Lowe, Creck, & Sivasubramaniam, 1996; Judge & Piccolo, 2004).

U literaturi se generalno ističe značajna uloga transformacionog liderstva u organizacionim promenama (Gibbons, 1992; Eisenbach et al., 1999; Bass & Riggio, 2006). Prema Bass & Riggio (2006) transformaciono liderstvo je u svojoj srži vezano za proces transformacije i promene. Eisenbach et al. (1999) argumentuju da transformacioni lideri mogu uspešno menjati status quo u njihovim organizacijama ispoljavajući odgovarajuća ponašanja u različitim stadijumima transformacionog procesa. Saglasno Herold et al. (2008) opšte mišljenje je da je transformaciono liderstvo posebno važno u toku promene zbog sposobnosti transformacionih lidera da angažuju sledbenike i motivišu ih da podrže izabrani pravac. Efektivnost transformacionog liderstva u organizacionim promenama je potvrđena u više studija (Bommer, Rich, & Roubin, 2005; Nemanich & Keller, 2007; Herold et al., 2008; Oreg & Berson, 2011).

Liderstvo promene je u osamdesetim i devedesetim godinama prošlog veka primilo pažnju mnogih autora. Kreirano je više modela procesa vođenja organizacione promene koji uključuju faze od iniciranja do zamrzavanja promene (Judson, 1991; Kotter, 1995; Galpin, 1996 i dr.). Najpopularniji pristup je Kotter-ov model u 8 koraka (Kotter, 1995) koji čine sledeće faze: (1) razvijanja svesti o neophodnosti promene, (2) stvaranja vodeće koalicije; (3) razvoj vizije i strategije; (4) komuniciranje vizije i strategije; (5) osnaživanje zaposlenih za široku akciju; (6) ostvarivanje kratkoročnih uspeha; (7) konsolidovanje ostvarenih prednosti i stvaranje daljih promena; i (8) usađivanje novih pristupa u kulturu. Određene studije su podržale Kotter-ov model (Cegielski, Hal, & Rebman, 2006; Ansari & Bell, 2009). Kritike su išle u pravcu da Kotter-ov model ne reprezentuje realnosti organizacionog života (Hay et al., 2001) i da daje malo detalja kako promena treba da se ostvari (Pfeifer, Schnitt, & Voight, 2005). Međutim, istraživačka evidencija

je još nedovoljna, saglasno Pollack (2015) čak i Kotter-ov pristup koji je najistaknutiji pristup vođenja organizacione promene je ostao uglavnom neistražen i nepodvrgnut rigoroznoj naučnoj analizi.

Iako se pojavilo više modela i preporuka kako da se inicira i vodi promena, saglasno Higgs & Roland (2000) vrlo malo je bilo specifičnih istraživanja u odnosu na deskriptivne i preskriptivne perspektive. Praktično sve do rada Herold et al. (2008) koji su istraživali transformaciono liderstvo, liderstvo promene i afektivnu predanost promeni, efekti liderskog ponašanja nisu bili testirani sa kvantitativnim metodama. Za razliku od transformacionog liderstva koje se odnosi na dugoročne relacije između lidera i sledbenika i koje ima više organizacionu ili stratešku orijentaciju liderstvo promene se odnosi na specifičnu promenu i kako lider vodi tu promenu i više je taktičku usmereno. Liu (2010) čini dalji progres razvijajući istraživački instrument za liderstvo promene koji uključuje: (1) ponašanje koje se odnosi na prodaju promene – naponi lidera da „proda“ promenu sledbenicima u toku stadijuma odmrzavanja i (2) ponašanje koje se odnosi na implementaciju promene – obuhvata sva ponašanja lidera u toku implementacije i konsolidacije promene.

4 RELACIJE IZMEĐU TRANSFORMACIONOG LIDERSTVA, LIDERSTVA PROMENE, SPREMNOSTI ZA PROMENU I PREDANOSTI PROMENI

U poslednjih deset godina bilo je nekoliko istraživanja o uticaju transformacionog liderstva na spremnost za promenu i predanost promeni. Istraživači nalaze da transformaciono liderstvo značajno i pozitivno utiče na spremnost za promenu (Allen, 2007; Griffith, 2010; Abbasi, 2017). Po pitanju predanosti promeni istraživači su se usmeravali uglavnom na afektivnu predanost promeni (Herold et al., 2008; Chou, 2013) i afektivnu i normativnu predanost promeni (Shrestha & Mishra, 2011; Seo et al., 2012). Herold et al. (2008) i Chou (2013) nalaze značajne i pozitivne relacije između transformacionog liderstva i afektivne predanosti promeni. Seo et al. (2012) utvrđuju da je transformaciono liderstvo u inicijalnoj fazi značajno i pozitivno povezano sa afektivnom i sa normativnom predanošću

promeni. Shrestha & Mishra (2011) prikazuju da je transformaciono liderstvo jak prediktor afektivne i normative predanosti promeni. Mnogo je manje istraživanja koja uključuju i kontinuiranu predanost promeni pošto istraživači ne pretpostavljaju da postoje značajan pozitivan uticaj transformacionog liderstva na ovu dimenziju. U jednom istraživanju u Maleziji, Gelaidan, & Ahmed (2013) nalaze da je transformaciono liderstvo pozitivno i značajno povezano i sa kontinuiranom predanošću promeni što ukazuje, i pored toga što je jedno istraživanje nedovoljno za šire zaključke, da kontinuiranu predanost promeni ne treba a priori izostavljati iz istraživanja.

Na osnovu prethodne diskusije prve dve hipoteze su sledeće:

H1: Transformaciono liderstvo ima pozitivan uticaj na spremnost za promenu

H2: Transformaciono liderstvo ima pozitivan uticaj na predanost promeni

Liderstvo promene je manje istraživani subjekt u odnosu na transformaciono liderstvo. U jednom istraživanju uticaja liderstva promene na spremnost za promenu u američkoj vojsci Lyons i saradnici (2009) nalaze da je liderstvo promene prediktor spremnosti za promenu. U studiji Herold et al. (2008) pretpostavljene pozitivne relacije između liderstva promene i predanosti promeni (istraživana je samo dimenzija afektivne predanosti promeni) nisu podržane što je suprotno očekivanjima u literaturi o organizacionim promenama. Liu (2010) nalazi drugačije ishode, u zavisnosti od dve dimenzije liderstva promene. Jedna od dve dimenzije liderstva promene – ponašanje koje se odnosi na prodaju promene ima pozitivne relacije sa afektivnom predanošću promeni, međutim druga dimenzija liderstva promene – ponašanje koje se odnosi na implementaciju promene nije imalo značajne relacije sa afektivnom predanošću promeni (ni pozitivne ni negativne). Objašnjenje za ovakve rezultate su da liderski naponi „prodaje“ promene stvaraju intrističke potrebe i valencu promene koji su onda motivatori za promenu i vode do pozitivnih ishoda kao što je veća predanost promeni. S druge strane liderska ponašanja implementacije promene po svojoj prirodi su transakcioni i eksterni pokretači koji se mogu shvatiti kao higijenski faktori u toku promene (higijenski faktori

saglasno Herzberg-ovoj motivacionoj teoriji dva faktora). Iako nedostatak higijenskih faktora dovodi do nezadovoljstva njihovo prisustvo ne generiše motivaciju da podrži promenu (Liu, 2010). Svakako dalja istraživanja u različitim kontekstima su neophodna.

Na osnovu prethodne diskusije za očekivati je da postoje pozitivne relacije između liderstva promene i spremnosti za promenu, i može se pretpostaviti da se mogu ustanoviti pozitivne relacije i između liderstva promene (uključujući obe dimenzije) i predanosti promeni, stoga treća i četvrta hipoteza su:

H3: Liderstvo promene ima pozitivan uticaj na spremnost za promenu

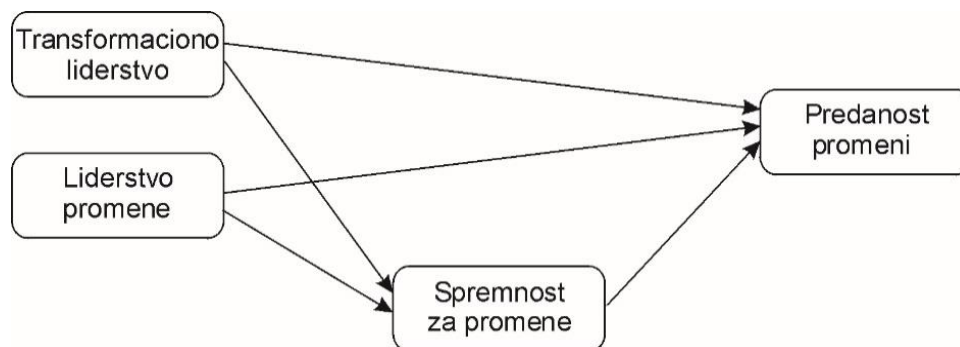
H4: Liderstvo promene ima pozitivan uticaj na predanost promeni

Iako su relacije između spremnosti za promenu i predanosti promeni važne za efektivnu realizaciju promene empirijska evidencija je mala. Rezultati studije čiji su autori Bakari, Hunza, & Niaz (2017) pokazuju da za uspešnu implementaciju planirane promene lideri treba da kreiraju spremnost za promenu koja će razviti njihovu predanost promeni. Ovo je u skladu sa teorijom da se spremnost za promenu kreira u toku inicijalnih koraka napora organizacione promene (Armenakis, Harris, & Mosholder, 1993) i održava se kroz proces promene pošto spremnost osnažuje ponašanja podrške promeni. Stvaranje spremnosti za promenu uključuje proaktivna nastojanja agenta promene da utiče na verovanja i namere članova organizacije, što je saglasno studiji Walker et al. (2007) pozitivno povezano sa afektivnom predanošću promeni. Adil (2014) nalazi pozitivne relacije između dimenzija spremnosti za promenu i afektivne predanosti promeni i negativne relacije sa kontinuiranom predanošću promeni. Iz ove diskusije se može uočiti da transformaciono liderstvo i liderstvo promene imaju i indirektan uticaj na predanost promeni tako što utiču na spremnost za promenu, što je neophodno za pripremu članova organizacije na koje utiče promena, a spremnost za promenu dalje utiče na predanost promeni što nas vodi petoj i šestoj hipotezi.

H5: Spremnost za promenu ima medijatorsku ulogu između transformacionog liderstva i predanosti promeni.

H6: Spremnost za promenu ima medijatorsku ulogu između liderstva promene i predanosti promeni.

Na slici 1 je prikazan rezultujući model sa medijatorskom ulogom spremnosti za promenu.



Slika 1. Strukturalne relacije između transformacionog liderstva, liderstva promene, spremnosti za promenu i predanosti promeni

Empirijska potvrda ovog teorijskog modela je jedna od oblasti budućih istraživanja. Ovaj teorijski model treba da bude empirijski testiran tako da se potvrdi njegova validnost. Dalja istraživanja zasnovana na ovom modelu mogu uključiti njegovo proširenje. Osim liderstva promene i transformacionog liderstva mogu biti uključeni i drugi liderski stilovi kao što je transakciono liderstvo. Pored spremnosti za promenu i predanosti promeni mogu biti uvedeni i drugi konstrukti unutar modela kao što je otvorenost za promenu i usklađivanje sa promenom (Bouckenooghe, 2010). Medijatorsku ulogu pored spremnosti za promenu može imati još varijabli. Takođe ovaj model može biti deo robusnijih modela koji uključuju više antecedenata, varijabli sa medijatorskom i kontrolnom ulogom i ishoda, već prema tome šta je tema istraživačkog poduhvata.

5 ZAKLJUČAK

U literaturi o organizacionim promenama spremnost za promenu i predanost promeni, kao konstrukti koji reprezentuju pozitivne stavove o promeni, ističu se kao ključni za uspeh organizacione promene. Iako se spremnost za promenu i predanost promeni koriste kao termini u literaturi o organizacionim promenama više decenija konstrukti u osamdesetim i devedesetim nisu bili dovoljno razvijeni niti su postojali odgovarajući istraživački instrument prihvaćeni od strane istraživačke zajednice. Armenakis, Harris, & Mossholder (1993) su uspostavili temelje za proučavanje spremnosti za promenu, a Holt et al. (2007) nakon prečišćavanja ranijih modela i istraživačkih instrumenata ustanovljuju model i

istraživački instrument koji se uz određene varijacije uspostavio kao reprezentativan. Kao odgovor na nedostatak konsenzusa devedesetih u definiciji konstrukta predanosti promeni, Herscovitch & Meyer uvode trokomponentni model koji se sastoji iz afektivne, kontinuirane i normativne predanosti promeni i istraživački instrument koji meri ove tri komponente. Pregledom istraživačkih studija može se ustanoviti da su istraživači prihvatili model Herscovitch & Meyer (2002), često se usmeravajući na jednu ili dve komponente modela (samo afektivnu ili afektivnu i normativnu predanost promeni).

Istraživanja liderstva van konteksta organizacione promene imaju mnogo dugu tradiciju. Transformaciono liderstvo je široko zastupljeno u istraživačkim studijama o liderstvu, i istraživački instrument u okviru šireg modela, potpunog ranga liderstva (Bass & Avolio, 1994), već dugo se koristi kao vodeći u istraživačkoj zajednici. Međutim liderstvo promene, i pored obimne literature, ali većinom deskriptivne, je mlad konstrukt, uobličen u radovima Herold et al. (2008) i Liu (2010). Model i istraživački instrument liderstva promene (Liu, 2010), sastoji se iz dve dimenzije: ponašanje koje se odnosi na prodaju promene i ponašanje koje se odnosi na implementaciju promene.

Pretpostavke u radu su izvođene na osnovu postojeće teorijske i istraživačke literature imajući u vidu nedovoljnu zastupljenosti istraživanja koja se odnose na uticaj liderstva promene na spremnost za promenu i predanosti promeni, kao i oskudnih empirijskih izvora o relacijama između spremnosti za promenu i predanosti promeni.

Teorijski model dat u radu doprinosi telu znanja o organizacionim promenama ali zahteva empirijsku potvrdu. Ukoliko istraživanja potvrde date pretpostavke model se može dalje širiti ili umetati u robusnije modele u zavisnosti od teme istraživačkog poduhvata.

CITIRANA DELA

- Abbasi, B. (2017). Transformational leadership and change readiness and a moderating role of perceived bureaucratic structure: An empirical investigation. *Problems and Perspectives in Management*, 15(1), 35-44.
- Adil, M. S. (2016). Impact of change readiness commitment on to technological change, focal, and discretionary behaviors: Evidence from manufacturing sector of Karachi. *Journal of Organizational Change Management*, 29(2), 222-241.
- Allen, S. L. (2007). *Transformational leadership change readiness, and creativity*. San Jose: San Jose State University.
- Ansari, S., & Bell, J. (2009). Five easy pieces: a case study of cost management as organizational change. *Journal of Accounting and Organizational Change*, 5, 139–167.
- Armenakis, A. A. & Bedeian A. G. (1999). Organizational change: A review of theory and research in the 1990s. *Journal of Management*, 25(3), 293-315.
- Armenakis, A. A., Harris S. G., & Mossholder, K. W. (1993). Creating readiness for organizational change. *Human Relations*, 46(6), 681-783.
- Bakari, H., Hunjra A. I. & Niazi, G. S. K. (2017). How Does Authentic Leadership Influence Planned Organizational Change? The Role of Employees' Perceptions: Integration of Theory of Planned Behavior and Lewin's Three Step Model. *Journal of Change Management*, 17(2), 155-187.
- Bass, B. M. & Avolio B. J. (1994). *Improving organizational effectiveness through transformational leadership*. Thousand Oaks: Sage.
- Bass, B. M. (1985). *Leadership and performance beyond expectations*. New York: Free Press.
- Bass, B. M., & Riggio, R. E. (2006). *Transformational leadership*, 2nd ed. Mahwah: Lawrence Erlbaum Associates.
- Bernerth, J. (2004). Expanding our understanding of the change message. *Human Resource Development Review*, 3(1), 36-52.
- Boga, I., & Ensari, N. (2009). The role of transformational leadership and organizational change on perceived organizational success. *The Psychologist-Manager Journal*, 12(4), 235-251.
- Bommer, W. H., Rich G. A., & Rubin R. (2005). Changing attitudes about change: Longitudinal effects of transformational leader behavior on employee cynicism about orghizational change. *Journal of Organizational Behavior*, 26, 733-753.
- Bouckenooghe, D. (2010). Positioning Change Recipients' Attitudes Toward Change in the Organizational Change Literature. *The Journal of Applied Behavioral*, 46(4), 500-531.
- Bouckenooghe, D., Schwaz G. M., & Amirali M. (2015). Herscovitch and Meyer's three-component model of commitment to change: Meta-analytic findings. *European Journal of Work and Organizational Psychology*, 24(4), 578-595.
- Burns, J. 1978. *Leadership*. New York: Harper & Row.
- Cegielski C, Hall D, & Rebman C (2006) Enterprise resource planning systems implementation success. *International Journal Information System Change Management*, 1, 301–317.
- Choi, M. (2011). Employees' attitudes toward organizational change: A literature review. *Human Resource Management*, 50(4), 479-500.

- Choi, M., & Ruona, W. E. A. (2011). Individual readiness for organizational change and its implications for human resource and organization development. *Human Resource Development Review*, 10(1), 46–73.
- Chou, P. (2013). The effect of transformational leadership on follower's affective commitment to change. *World Journal of Social Sciences*, 3(1), 38-52.
- Clegg, C., & Walsh, S. (2004). Change management: Time for a change. *European Journal of Work and Organizational Psychology*, 13, 217-239.
- Conner, D. R., & Patterson, R. B. (1982). Building commitment to organizational change. *Training and Development Journal*, 36(4), 18-30.
- Eby, L. T., Adams, D. M., Russell J. E. A., & Stephen, G. H. (2000). Perceptions of Organizational Readiness for Change: Factors Related to Employees' Reactions to the Implementation of Team-Based Selling. *Human Relations*, 53(3), 419-442.
- Eisenbach, R., Watson, K., & Pillai, R. (1999). Transformational leadership in the context of organizational change. *Journal of Organizational Change Management*, 12(2), 80-89.
- Elias, S. M. (2009). Employee Commitment in Times of Change: Assessing the Importance of Attitudes Toward Organizational Change. *Journal of Management*, 35(1), 37-55.
- Galpin, T. (1996). *The human side of change: A practical guide to organizational redesign*. Oxford: Oxford University Press.
- Gelaidan, H. M., & Ahmed, H. (2013). Using partial least squares approach to predict the impact of transformational leadership on employee commitment to organizational change. *International Business Management*, 7(4), 306-316.
- Gelaidan, H. M., & Ahmed, H. (2013). Using partial least squares approach to predict the impact of transformational leadership on employee commitment to organizational change. *International Business Management*, 7(4), 306-316.
- Georgiades, S. (2015). *Employee engagement in Media Management: Creativeness and Organizational Development*. Cham: Springer International Publishing.
- Gibbons, P. T. (1992). Impact of organizational evolution on leadership roles and behaviors. *Human Relations*, 45, 1-18
- Griffith, S. D. (2010). *Transformational leadership and change readiness using assessments for near-term prescriptive organizational intervention*. Marion: Indiana Wesleyan University.
- Hay G, Beattie R, Livingstone R, & Munro P (2001). Change, HRM and the voluntary sector. *Employee Relations*. 23(3), 240–255.
- Herold, D. M., Fedor, D. B., Caldwell S. D., & Liu Y. (2008). The effects of transformational and change leadership on employees' commitment to a change: A multilevel study. *Journal of Applied Psychology*, 93(2), 346-357.
- Herscovitch, L., & Meyer J. P. (2002). Commitment to organizational change: Extension of a three-component model. *Journal of Applied Psychology*, 87(3), 474-487.
- Higgs, M. J. & Rowland, D. (2000). Building change leadership capability: "the quest for change competence". *Journal of Change Management*, 1(2), 116–131.
- Holt, D. T., Armenakis, A. A., Field, H. S., & Harris, S. G. (2007). Readiness for organizational change: The systematic development of scale. *The Journal of Applied Behavioral Science*, 43(2), 232-255.
- Judge, T. A., & Piccolo. R. F. (2004). Transformational and transactional leadership: A meta-analytic test of their relative validity. *Journal of Applied Psychology*, 89(5), 755-768.

- Judson, A. (1991). *Changing Behavior in Organizations: Minimizing Resistance to Change*. Cambridge: Basil Blackwell.
- Klein K., J., & Sorra, J. S. (1996). The challenge of innovation implementation. *Academy of Management Journal*, 21(4), 1055-1080.
- Kotter, J. P. (1996). *Leading change*. Boston: Harvard Business School Press.
- Liu, Y. (2010). *When change leadership impacts commitment to change and when it doesn't: A multi-level multidimensional investigation*. Atlanta: Georgia Institute of Technology.
- Lowe, K. B., Kroeck, K. G., & Sivasubramaniam, N. (1996). Effectiveness correlates of transformation and transactional leadership: A meta-analytic review of the MLQ literature. *Leadership Quarterly*, 7, 385–425.
- Lowe, K. B., Kroeck, K. G., & Sivasubramaniam, N. (1996). Effectiveness correlates of transformation and transactional leadership: A meta-analytic review of the MLQ literature. *Leadership Quarterly*, 7, 385–425.
- Neiva, E. R., Ros M., Torres de Paz M. G. (2005). Attitudes towards organizational change: Validation of a scale. *Psychology in Spain*, 9(1): 81-90.
- Nemanich, L. A. & Keller R. (2007). Transformational leadership in an acquisition: A field study of employees. *The Leadership Quarterly*, 18(1): 49-68.
- Oreg, S, & Berson Y. (2011). Leadership and employees' reactions to change: The role of leaders' personal attributes and transformational leadership style. *Personell Psychology*, 64(3), 627-659.
- Pfeifer T, Schnitt R, & Voigt T (2005). Managing change: quality-oriented design of strategic change processes. *The TQM Management*, 17, 297–308.
- Pollack, J. (2015). *Understanding the divide between the theory and practice of organisational change*. Sydney: University of Technology.
- Shretsha, A. K., & Mishra, A. K. (2011). Leadership styles, employees' commitment to organizational change, and organizational performance: A study in a Nepali technology based organization. 11th South Asian Management Forum (SAMF) organized by Association of Management Development Institutions in South Asia (AMDISA).
- Tanner, C., Brugger, A., van Schie, S., & Lebherz, C., (2010). Action speak louder than words: The benefits of ethical behaviors of leaders. *Zeitschrift für Psychologie/Journal of Psychology*, 218(4), 225-233.
- Wang, H., Tsui, A. A., & Xin, R. (2011). CEO leadership behaviors, organizational performance, and employees' attitudes. *The Leadership Quarterly* 22(1):92-105.
- Yousef, D.A. (2000). Organizational commitment and job satisfaction as predictors of attitudes toward organizational change in a non-western setting. *Personnel Review*, (29), 567–592.

Datum prve prijave: 15.08.2018.
Datum prijema korigovanog članka: 22.03.2019.
Datum prihvatanja članka: 27.03.2019.

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

Style – APA Sixth Edition:

Šutković, S., Zakić, N., & Tornjanski, A. (2019, 04 15). Uticaj transformacionog liderstva i liderstva promene na spremnost za promenu i predanost promeni. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 170-180. doi:10.12709/fbim.07.07.01.19

Style – Chicago Sixteenth Edition:

Šutković, Salih, Nebojša Zakić, i Aleksandra Tornjanski. 2019. „Uticaj transformacionog liderstva i liderstva promene na spremnost za promenu i predanost promeni.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 170-180. doi:10.12709/fbim.07.07.01.19.

Style – GOST Name Sort:

Šutković Salih, Zakić Nebojša i Tornjanski Aleksandra Uticaj transformacionog liderstva i liderstva promene na spremnost za promenu i predanost promeni [Časopis] // *FBIM Transactions* / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 170-180.

Style – Harvard Anglia:

Šutković, S., Zakić, N. & Tornjanski, A., 2019. Uticaj transformacionog liderstva i liderstva promene na spremnost za promenu i predanost promeni. *FBIM Transactions*, 15 04, 7(1), pp. 170-180.

Style – ISO 690 Numerical Reference:

Uticaj transformacionog liderstva i liderstva promene na spremnost za promenu i predanost promeni.
Šutković, Salih, Zakić, Nebojša i Tornjanski, Aleksandra. [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, *FBIM Transactions*, T. 7, str. 170-180.



MENADŽMENT U NASTAVNOM PROCESU - ULOGA NASTAVNIKA

MANAGEMENT IN THE TEACHING PROCESS - THE ROLE OF TEACHERS

Slobodan Vuksanović

Poslovni i pravni fakultet „Union-Nikola Tesla“ Univerziteta, Beograd, Srbija

©MESTE
JEL Category: I21

Apstrakt

Cilj ovog teksta jeste u tome da pokaže ulogu nastavnika u organizovanju nastavnog procesa. Polovinu nastavnog procesa predstavlja nastavnik, a drugu polovinu predstavljaju njegovi studenti. U njihovom međusobnom odnosu, koji podrazumeva predavanja, diskusije, pitanja, predloge, nove ideje, ostvaruje se celokupni proces nastave. U tom procesu nastavnik predstavlja samo jedan deo koji ne može da funkcioniše bez saradnje studenata. Ovaj tekst obrađuje obaveze nastavnika koje su neophodne da bi studenti bili motivisani i inspirisani da učestvuju u zajedničkom radu. Nastavnik, kao pojedinac, ne može da ostvari svoj cilj ukoliko nema zainteresovane i ravnopravne sagovornike među studentima.

Ključne reči: Menadžment, nastavni proces, nastavnik, student

Abstract

The aim of this paper is that it shows teachers role in organizing the teaching process. Half of the teaching process represents the teacher, and the other half presents his students. In their mutual relations, which includes lectures, discussions, questions, suggestions, new ideas, makes the whole process of teaching. In the process, the teacher is only one part that cannot function without the cooperation of students. This text deals with the obligations of teachers that are necessary to make the students were motivated and inspired to also take part in joint work. The teacher, as an individual, cannot achieve its objective if there are interested and equal interlocutors among students.

Keywords: management, teaching process, teacher, student

1 UVOD

Uloga nastavnika može se posmatrati kroz dve krajnosti – ulogu kontrolora i ulogu pomagača. Nastavnik – kontrolor stoji pred učenicima i strogo

nadgleda i komentariše svako učeničko izlaganje, dok nastavnik – pomagač ne postavlja sebe u centar zbivanja na času već samo podstiče učenike na samostalan rad. Od kreativnosti nastavnika zavisi kakav će pristup času izabrati koje će postupke koristiti u realizaciji nastave. „Kreativni nastavnik je pre svega u poziciji organizatora, čoveka koji motiviše, modelira, pomaže, istražuje, inicira, podstiče, prati,

Adresa autora:

Slobodan Vuksanović

 slobodanmef@gmail.com



usmerava i stalno traga za novim vidovima organizacije, nalazeći i sam zadovoljstvo u svojoj kreativnosti i kreativnosti svojih učenika.

A. Majls ističe pet osobina kreativnog nastavnika (Vuksanović, 2012):

- to je osoba koja poseduje primarnu sliku (model) koji vodi njegovo mišljenje i delovanje,
- osoba koja prihvata samog sebe čvrsto, tačno i realistički, pa iskoristi svoj puni potencijal,
- osoba koja je svesna drugih ljudi, osetljiva prema njima i reaguje na ljude, ideje i događaje,
- osoba koja poseduje osećaj sigurnosti, koja toleriše dvosmislenost,
- osoba koja je učenik.

Pod ovim se, naročito, razume da nastavnik treba da ima opšti koncept cilja koji treba da ostvari, svest o važnosti i veličini svog zadatka, da ima poverenja u svoje ja i da stalno traga za novim, tj. da uči. Bitna osobina kreativnog nastavnika je vedrina, dobro raspoloženje, humor, entuzijazam i kreativni stav prema životu, tj. odstupanje od stereotipa i šablona i težnja ka novom, originalnom, duhovitom, progresivnom. To znači da kreativan nastavnik treba da je lično opredeljen za kreativnu nastavu, da dobro poznaje ne samo jezik i književnost, nego i prirodu kreativnog procesa i strategiju kreativne nastave. "Određeni delovi predavanja zahtevaju veće angažovanje nastavnika – tada on više govori, trudi se da pažnja učenika u potpunosti bude usmerena na njegovo izlaganje. Logično je da ovakvu ulogu nastavnik mora da preuzima na početku časa (u njegovom uvodnom delu), kao i u svakom drugom trenutku kada daje nove informacije učenicima. U zavisnosti od vlastitog karaktera, pojedini nastavnici teško prihvataju poziciju u kojoj nisu u centru pažnje i ne mogu da se oslobode potrebe da sve vreme časa zadrže ulogu kontrolora. Međutim, inspirativni nastavnici ne postižu atraktivnost predavanja tako što će po svaku cenu i neprekidno „držati“ poziciju kontrolora. Upravo obrnuto, nastavnik će više inspirisati učenike ukoliko im pruži više slobode i samostalnog rada; ukoliko su mu izlaganja kraća ali zanimljivija; ukoliko je opušten, raspoložen i tolerantan. To ne znači da se nastavnik u potpunosti odrekao uloge kontrolora, već je on obavlja diskretno, nenametljivo – ponekad gotovo neprimetno. Takav pristup nastavi predstavlja jedan od bazičnih elemenata kreativne nastave.

2 ANALIZA

Među odlikama kreativnosti i kreativne nastave ističemo sledeće:

- *Intenzivan rad*, tj. obuzetost problemima, predanost poslu. O tome je Čajkovski rekao: „nadahnuto se rađa samo iz rada i za vreme rada“. A Nikola Tesla je napisao: „Stalno duševno naprezanje razvilo je moju moć opažanja i omogućilo mi da otkrijem veoma značajnu istinu“ (Novaković, 2012).
- *Radoznalost*, tj. nastojanje da se i u običnim stvarima traži neobičnost, da se začuđeno zagleda i da se svetu pristupi kao još neotkrivenoj tajni. „Razviti trajnu naučnu radoznalost učenika, vrhunska je umetnost i umetnost nastavnika“ - kaže Ajnštajn (Randelović, 2018).
- *Sloboda* u iznošenju vlastitih ocena i uverenja, bez zazora i straha od podsmeha, pogrde i kazne, ili suprotnog stava autoriteta. To znači i razvijeno osećanje da se znanja stiču slobodno, bez prinude.
- *Otvorenost*, o kojoj A. Majls kaže: „Prvi zahtev kreativnosti jeste da čovek promišljeno otvori podatke – sve podatke... da nauči da gleda otvoreno, nestrukturizano...“ (Đorđević Boljanović & Pavić, 2011) To znači i otvorenost za nove ideje i estetsku osetljivost duha. *Stvaralačko posmatranje*, tj. uočavanje udaljenih veza i odnosa, koji se na prvi pogled ne mogu otkriti, a onda i odvajanje bitnog od nebitnog.
- *Nekonformizam*, o kome Borislav Stevanović (1984) kaže da je „jedan od najvažnijih subjektivnih uslova stvaralaštva“, a to znači „nepriklanjavanje onome što je već ustaljeno u društvu, odstupanje od utvrđenih navika, stereotipija i šablona, od onoga što predstavlja stagnaciju i mrtvilo“. To znači i težnju ka drugačijem, originalnom gledanju na stvari i pojave.
- *Kreativna usmerenost mišljenja*, koja podrazumeva usmerenost ka traganju za novim, neobičnim, neočekivanim i duhovnim rešenjima.
- *Divergentno mišljenje*, koje teži raznovrsnim pristupima, putevima rešavanja i rešenjima (za razliku od konvergentnog, koje je usmereno ka jednoj mogućnosti, jednom rešenju).
- *Tolerancija* prema dvosmislenosti, neodređenosti, prema nedovoljno

strukturisanim i nedovoljno jasnim situacijama, tolerancija prema stranputicama u razmišljanju.

Pokretljivost mišljenja, fleksibilnost, težnja ka elastičnom razumevanju pojava, sumnja u ono što izgleda samo po sebi jasno, kombinovanje karakteristika, unošenje mnogoznačnosti i nepreciznosti, okretanje naglavačke elemenata i odnosa, težnja ka višeznačnoj direkciji. (Marinković, 2007)

Pored svih navedenih odlika kreativne nastave ne treba zaboraviti da nastavnikovo poznavanje osobina i sposobnosti svojih učenika predstavlja preduslov uspešne nastave. Bez toga se ne može ostvariti kreativnost u nastavnom procesu, što znači da će i uspeh izostati. Iz toga ponovo proističe zaključak da nastavnik mora znati kako da motiviše učenike, odnosno, da treba da zna da razlikuje različite vrste motivacija koje se uočavaju kod učenika različitih nivoa sposobnosti i interesovanja.

Tokom procesa učenja učenici će ispoljavati različite vrste ponašanja u skladu sa svojim afinitetima, konkretnom nastavnom jedinicom, nastavnikovim postupcima i drugim faktorima od kojih mnogi ne mogu biti predvidivi. Zbog toga nastavnik treba da prepozna najmanje tri vrste motivacije kod učenika. Verovatno jedan od najvažnijih i najtežih nastavnikovih zadataka predstavlja planiranje nastavnog procesa. Uspeh učenja zavisi od organizacije nastave u kojoj učenici treba tačno da znaju šta uče i zbog čega uče. Mnogo vremena može biti izgubljeno tokom časa ukoliko nastavnik propusti da saopšti učenicima najvažnije podatke o ciljevima nastave.

Osnovni zadatak nastavnika jeste u tome da saopšti učenicima o čemu će razgovarati, zatim da im pruži jasna uputstva (radne naloge), da započne razgovor i predvidi vreme na kraju časa za pružanje povratnih informacija i izvođenje zaključaka. Naravno, ovakav redosled aktivnosti zvuči jednostavno, ali ukoliko se pažljivo ne sprovede – izazvaće konfuziju među učenicima i onemogućiti uspešan rad na času. Najvažniji preduslov dobre organizacije časa predstavljaju jasne instrukcije koje nastavnik upućuje učenicima. Nastavnik nikada ne treba da pretpostavlja da su ga učenici odmah razumeli, već treba to i da proveriti. To je posebno važno u radu sa učenicima najmlađih uzrasta. Na primer, ukoliko je nastavnik planirao da učenicima podeli

tekstove (ili neki drugi pisani materijal), on to nikako ne treba da uradi pre nego što im saopšti jasna uputstva i objašnjenja o tome šta učenici treba da rade. Ukoliko učini obrnuto – učenici će usmeriti pažnju na podeljene tekstove i neće slušati nastavnikove instrukcije. Najčešće se organizacija časa sastoji iz četiri dela:

1. Uvodna objašnjenja
2. Davanje instrukcija
3. Pokretanje diskusije
4. Sumiranje zaključaka

Uvodna objašnjenja treba da budu sasvim kratka i jednostavna. Nastavnik treba samo da obavesti učenike o temi rada na času.

Davanje instrukcija jeste sledeća faza časa u kojoj nastavnik konkretno i detaljno saopštava učenicima na koji način će vežbati, odnosno, na koji način će voditi razgovor (na primer, u parovima, grupama ili zajedno).

Kada je završio davanje instrukcija – nastavnik započinje razgovor (ili vežbanje) što predstavlja glavni deo časa. Obično pokretanju diskusije prethodi završno nastavnikovo pitanje uvodnog dela časa koje glasi – Da li ima još nekih pitanja?

Ukoliko učenici nemaju pitanja – tada počinje *diskusija* (ili pisane vežbe). U ovoj fazi časa nastavnik treba da smanji svoju kontrolnu ulogu, odnosno, da što manje interveniše svojim govorom, već da pruži mogućnost učenicima da što slobodnije iskažu svoj utiske i stavove.

Sumiranje zaključaka obavlja se u nekoliko poslednjih minuta časa kada nastavnik, kao dobar organizator, saopštava glavne zaključke i piše ih na tabli. Međutim, da bi mogao uspešno da organizuje jedan čas, nastavnik treba na istim principima da pripremi godišnji i operativni plan koji predstavljaju okvir za organizovanje svakog pojedinačnog časa.

3 ZAKLJUČAK

Ovaj tekst jeste pokušaj da se objasni uloga nastavnika u organizaciji nastavnog procesa. Njegove obaveze, improvizacije i kreativnost u odnosu na zadatu situaciju jesu tema ovog teksta. Nije moguće da nastavnik obavi svoj zadatak bez saradnje studenata. Utoliko je njegov zadatak težji i zavisi od interakcije sa aktivnostima studenata. Ovaj rad posvećen je upravo zadacima nastavnika kojima on treba da motiviše studente na saradnju.

Uloga nastavnika može se posmatrati kroz dve krajnosti – ulogu kontrolora i ulogu pomagača. Nastavnik – kontrolor stoji pred učenicima i strogo nadgleda i komentariše svako učeničko izlaganje, dok nastavnik – pomagač ne postavlja sebe u centar zbivanja na času već samo podstiče učenike na samostalan rad. Od kreativnosti nastavnika zavisi kakav će pristup času izabrati koje će postupke koristiti u realizaciji nastave. „Kreativni nastavnik je pre svega u poziciji organizatora, čoveka koji motiviše, modelira, pomaže, istražuje, inicira, podstiče, prati, usmerava i stalno traga za novim vidovima organizacije, nalazeći i sam zadovoljstvo u svojoj kreativnosti i kreativnosti svojih učenika.

Osnovni zadatak nastavnika jeste u tome da saopšti učenicima o čemu će razgovarati, zatim da im pruži jasna uputstva (radne naloge), da započne razgovor i predvidi vreme na kraju časa za pružanje povratnih informacija i izvođenje zaključaka. Naravno, ovakav redosled aktivnosti zvuči jednostavno, ali ukoliko se pažljivo ne sprovede – izazvaće konfuziju među učenicima i onemogućiti uspešan rad na času. Najvažniji preduslov dobre organizacije časa predstavljaju jasne instrukcije koje nastavnik upućuje učenicima. Nastavnik nikada ne treba da pretpostavlja da su ga učenici odmah razumeli, već treba to i da proveri.

CITIRANA DELA

- Đorđević Boljanović, J., & Pavić, Ž. (2011). *Osnove menadžmenta ljudskih resursa*. Beograd: Univerzitet Singidunum.
- Marinković, S. (2007). *Metodika*. Beograd: Kreativni centar.
- Nikolić, M. (2006). *Metodika nastave*. Beograd: Zavod za udžbenike.
- Novaković, M. (2012, 07 09). *Umetnost filma u Teslinom kodu*. Preuzeto sa Novi Filmograf.
- Randelović, D. (2018, 07 09). *Nastava kao umetnost*. Preuzeto sa LINK Educational Alliance: <http://www.institut.edu.rs/nastava-kao-umetnost/>
- Stevanović, B. (1984). *Pedagoška psihologija*. Beograd: Zavod za udžbenike i nastavna sredstva.
- Vuksanović, S. (2012). *Metodička praksa*. Beograd: Šprint.

Datum prve prijave: 15.08.2018.
Datum prijema korigovanog članka: 22.03.2019.
Datum prihvatanja članka: 27.03.2019.

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

Style – APA Sixth Edition:

Vuksanović, S. (2019, 04 15). Menadžment u nastavnom procesu -uloga nastavnika. (Z. Čekerevac, Ur.) *FBIM Transactions*, 7(1), 181-184. doi:10.12709/fbim.07.07.01.20

Style – Chicago Sixteenth Edition:

Vuksanović, Slobodan. 2019. „Menadžment u nastavnom procesu -uloga nastavnika.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 181-184. doi:10.12709/fbim.07.07.01.20.

Style – GOST Name Sort:

Vuksanović Slobodan Menadžment u nastavnom procesu -uloga nastavnika [Časopis] // *FBIM Transactions* / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 181-184.

Style – Harvard Anglia:

Vuksanović, S., 2019. Menadžment u nastavnom procesu -uloga nastavnika. *FBIM Transactions*, 15 04, 7(1), pp. 181-184.

Style – ISO 690 Numerical Reference:

Menadžment u nastavnom procesu -uloga nastavnika. **Vuksanović, Slobodan**. [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, *FBIM Transactions*, T. 7, str. 181-184.



Reviewers of the FBIM Transactions – alphabetically

1. Dr. **Svetlana Andelić**, 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, Adiyaman Merkez/Adiyaman, 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**, "Ukrasbank", 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 Ćucić**, 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 Damjanović**, 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 Kableshev" 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 Kableshev" 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 Kableshev" 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-Lypovyyk**, 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 Kableshev" 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**, "Mediterranean" 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 Kableshev" 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., Wrocław University of Environmental and Life Sciences, Wrocław, 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_1_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, Adiyaman, 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**, "Ukrasbank", 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 Ćučić**, 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 Damjanović**, 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, Černivci, 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 **Dobrovoje Mihailović**, Univerzitet u Beogradu, Fakultet organizacionih nauka, Beograd, Srbija
56. prof. dr **Božidar Mihajlović**, Visoka škola za poslovnu ekonomiju 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 Vykyuk**, Bukovinski Univerzitet, Černivci, Ukrajina
101. dr hab. ing. **Zenon Zamiar**, v. prof., Univerzitet prirodnih nauka i ekologije u Wroclavu, 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_1_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 no 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 JOURNAL may 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 koautor 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 priložima, 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 priložima, 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 pružiti na web adresi:

http://fbim.meste.org/FBIM_1_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.docx (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 objavljene 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 korespondenciju obrađeni članak, kako bi autor mogao da prekontroliše da li je pri obradi članka došlo do nekih nepravilnosti. Takođe, autor zadužen za korespondenciju treba da proveriti 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.

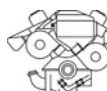
http://fbim.meste.org/FBIM_1_2019/Submit_a_manuscript_srb.html

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_1_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 adresa i broj telefona autora zaduženog za korespondenciju sa FBIM Transactions
 - Kratak naziv rada (sažet i informativan naslov, ne duži od 50 karaktera sa razmacima)
 - Rezime i Abstract
 - Ključne reči i KeywordsNa veb stranici http://fbim.meste.org/FBIM_1_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	Yes ☐	No ☐
	Citation is in accordance with the requirements	Yes ☐	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	

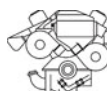
SECTION IV – Recommendations for publication:

(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)

Prihvati 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_1_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_1_2019/Submit_a_manuscript_srb.html





Intentionally left blank – Namerno ostavljeno prazno

Intentionally left blank – Namerno ostavljeno prazno

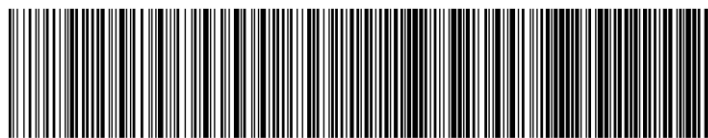
4D414E4147454D454E54

454455434154494F4E

534349454E4345

544543484E4F4C4F47

45434F4E4F4D494353



FBI Transactions DOI 10.12709/issn.2334-704X