IT Veštak
IT Expert Witness
&
Univerzitet „Union – Nikola Tesla" Beograd
"Union – Nikola Tesla" University Belgrade
Poslovni i pravni fakultet
Faculty of Business and Law

Međunarodna naučno-stručna konferencija
International scientific-professional conference

# ZITEH 2019

ZBORNIK REZIMEA
ABSTRACT PROCEEDINGS

| | | |
|---|---|---|
| Beograd | Srbija | 25. oktobar 2019 |
| Belgrade | Serbia | 25 October 2019 |

***IT VEŠTAK***
***and***
***FACULTY OF BUSINESS AND LAW***
***"Union - Nikola Tesla" University in Belgrade***
***supported by***
***MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGICAL DEVELOPMENT OF REPUBLIC OF SERBIA***
***and***
***MINISTRY OF JUSTICE OF THE REPUBLIC OF SERBIA***
*in cooperation with*
*"Todor Kableshkov" University of Transport, Sofia, BG*
*Bukovina University, Chernivtsi, UA*
*High School of Economics and Management in Public Administration, Bratislava, SK*
*Faculty of Security Engineering, University of Zilina, SK*
*Maikop State Technological University, Maikop, RF*
*Ningbo University of Technology, Ningbo, CN*
*Russian State University for the Humanities, branch in Domodedovo city Domodedovo, RU*
*Jan Długosz University, Czestochowa, PL*
*North-Caucasian Institute of Business, Engineering and Information Technology, Armavir, RU*
*Chernivtsi Institute of Trade and Economics of Kyiv National University of Trade and Economics, Chernivtsi, Ukraine*
*Lviv Polytechnic National University,*
*Lviv, Ukraine*
*and*
*MESTE, Belgrade*

***International Scientific Conference***
***"ZITEH 2019"***
*Belgrade*
*25th of October 2019*

# ABSTRACT PROCEEDINGS

ICIM+

Izdavački centar za INDUSTRIJSKI MENADŽMENT plus
Beograd-Mladenovac, 2019

**Međunarodna naučna konferencija**
**ZITEH 2019**
**Zbornik rezimea**

*Izdavač:*
IT Veštak
Poslovni i pravni fakultet
MESTE
ICIM plus
Beograd, Knez Mihailova 33
tel/faks + 381 11 823-24-27

*Za izdavača:*
Prof. dr Milija Bogavac
Prof. dr Zoran Čekerevac

*Dizajn korica:*
Mladen Stojanović

*Kompjuterska priprema:*
Zoran Čekerevac

*Štampa:*
Planeta print, Beograd

*Tiraž:*
100

**International Scientific Conference**
**ZITEH 2019**
**Abstract Proceedings**

*Publisher:*
IT Expert Witness
Faculty of Business and Law
MESTE
ICIM plus,
Belgrade, Knez Mihailova 33
tel./fax + 381 11 823-24-27

*For publisher:*
Prof. Dr. Milija Bogavac
Prof. Dr. Zoran Cekerevac

*Cover design:*
Mladen Stojanovic

*Technical editing:*
Zoran Cekerevac

*Printed by:*
Planeta print, Belgrade

*Circulation:*
100

ISBN 978-86-6375-119-4

Izdavanje Zbornika rezimea, organizaciju i održavanje Međunarodne naučne konferencije ZITEH 2019 pomoglo je
**Ministarstvo prosvete, nauke i tehnološkog razvoja Republike Srbije**

Publishing of the Abstract Proceedings, organization and realization of the International Scientific Conference ZITEH 2019 was sponsored by
**Ministry of Education, Science, and Technological Development of the Republic of Serbia**

*IT VEŠTAK*
*i*
*POSLOVNI I PRAVNI FAKULTET*
*„Union – Nikola Tesla“ univerziteta u Beogradu*
*podržani od*
*MINISTARSTVA PROSVETE, NAUKE I TEHNOLOŠKOG RAZVOJA REPUBLIKE SRBIJE*
*i*
*MINISTARSTVA PRAVDE REPUBLIKE SRBIJE*
*u saradnji sa*
*"Todor Kableshkov" University of Transport, Sofia, BG*
*Bukovina University, Chernivtsi, UA*
*High School of Economics and Management in Public Administration, Bratislava, SK*
*Faculty of Security Engineering, University of Žilina, SK*
*Maikop State Technological University, Maikop, RU*
*Ningbo University of Technology, Ningbo, CN*
*Russian State University for the Humanities, branch in Domodedovo city Domodedovo, RU*
*Jan Długosz University, Czestochowa, PL*
*North-Caucasian Institute of Business, Engineering and Information Technology, Armavir, RU*
*Chernivtsi Institute of Trade and Economics of Kyiv National University of Trade and Economics, Chernivtsi, Ukraine*
*Lviv Polytechnic National University,*
*Lviv, Ukraine*
*i*
*MESTE, Beograd*

***Međunarodna naučna konferencija***
***„ZITEH 2019“***
*Beograd, Srbija*
*25. oktobar 2019*

# ZBORNIK REZIMEA

ICIM+

Izdavački centar za INDUSTRIJSKI MENADŽMENT plus
Beograd-Mladenovac, 2019

# NAUČNI ODBOR / SCIENTIFIC BOARD

prof. dr Zoran Čekerevac, PPF i IT Veštak, Beograd - Predsednik
dr Srđan Blagojević, IT Veštak - Kopredsednik
prof. dr Milija Bogavac, PPF, Beograd – Kopredsednik
prof. dr Boško Rodić, IT Veštak, Beograd
prof. Ing. Viera Cibakova,PhD, VŠEMvs, Bratislava, SK
prof. Kuiževa Saida Kazbekovna, CSc, MGTU, Majkop, RU
prof. Mikhail Manylich, PhD, BU, Černivci, UA
prof. Daniela Todorova, PhD, VTU „Todor Kableškov“, Sofija, BG
prof. dr. Lyu Zhongda, NUT, Ningbo, CN
dr Wang Bo, docent, Ninbo TU, Ninbo, CN
prof. dr Petar Kolev, VTU „Todor Kableškov“, Sofija, BG
prof. dr Evgenij Safonov, RGGU, Domadedovo, RU
prof. dr Yaroslav Vyklyuk, Bukovinski Univerzitet, Černivci, UA
prof. dr Vasyl Luchyk, ČTEI KNTEU, Černivci, UA
prof. Maria Hristova, PhD, VTU „Todor Kableškov“, Sofija, BG
prof. ing. Zdenek Dvorak, PhD, FBI, Žilina, SK
prof. dr Lyudmila Prigoda, MGTU, Majkop, RU
prof. dr Natalija Šakovska, LPNU, Ljvov, UA
docent Stanislav Filip, PhD, VŠEMvs, Bratislava, SK
prof. dr Sergei Kirsanov, IMD, Sankt Peterburg, RU
prof. dr Yurii Koroliuk, ČTEI KNTEU, Černivci, UA
prof. dr Dragan Đurđević, Akademija za nacionalnu bezbednost, Beograd
dr Oksana Koshulko, PhD, PAS, Varšava, PL
prof. dr Savo Radonjić, VŠSS "Čačak", Beograd
doc. dr Vladica Babić, Pravni fakultet, Univerzitet Vitez, Vitez, BA

# ORGANIZACIONI ODBOR / ORGANIZING BOARD

Prof. Dr. Srdjan Blagojevic – co-president
Prof. Dr. Milija Bogavac – co-president
Prof. Dr. Zoran Cekerevac
mr Momir Ostojic
Milanka Bogavac, PhD
Aleksandar Matic, LL.M.

**Proofreading:**

Dr. Ljiljana Jovković
Sanja Manojlović, MA

# TEMATSKE OBLASTI

**NOVE TEHNOLOGIJE**
Blokčejn tehnologija
Internet stvari
Kriptovalute
...
**IT ZLOUPOTREBE**
Kriminogeni faktori
Potencijalni ciljevi zloupotrebe
Kategorije zloupotrebe, kompjuterski kriminal, kiber-terorizam, obaveštajno delovanje, informaciono ratovanje
Nove forme zloupotreba IT
Metode i tehnike zloupotrebe
Motivi i profili izvršilaca
Otkrivanje i dokazivanje
Mesto i uloga državnih organa, obrazovnih ustanova i medija
Sudsko veštačenje u oblasti IT
Sankcionisanje
Informatička etika
Međunarodna saradnja u oblasti kompjuterskog kriminala
Digitalna forenzika
Forenzički alati, verifikacija i validacija alata
...
**ZAŠTITA**
Informaciona bezbednost
Politike zaštite
Arhitektura sistema zaštite
Aspekti zaštite: normativni, fizičko-tehnički i logički aspekt
Kripto zaštita
Steganografija i digitalni vodeni pečat
Zaštita: na Internetu, baza podataka, PC
Zakonska regulativa u svetu i kod nas
Modeli obuke...

# TOPICS

**NEW TECHNOLOGIES**
Blockchain Technology
Internet of Things
Cryptocurrency
...
**MISUSE OF INFORMATION TECHNOLOGY**
Criminogenic factors
Potential goals of abuse
Categories of abuse, computer crime, cyber-terrorism, intelligence, information warfare
New forms of IT abuse
Methods and techniques of abuse
Motives and profiles of the perpetrators
Detection and proof
Place and role of state authorities, educational institutions, and the media
Judicial expertise in IT
Sanctioning
Informatics ethics
International cooperation in the field of computer crime
Digital forensics
Forensic tools, tool verification, and validation
...
**PROTECTION**
Information security
Protection policies
The architecture of the protection system
Aspects of protection: normative, physical-technical and logical aspect
Crypto protection
Steganography and digital watermark
Protection: on the Internet, database, PC
Legislation in the world and in Serbia
Training Models ...

# PREDGOVOR

Ekspanzija informacionih tehnologija i automatizacija poslovnih procesa u svim sferama društvenog života predstavljaju istinski fenomen današnjice. On je savremenom društvu doneo bezbroj pogodnosti, ali je takođe stvorio niz problema i rizika, kako za pojedince, grupe i organizacije, tako i za društvo u celini. Ove probleme i rizike, od kojih mnogi ranije nikada nisu postojali, ponekad je teško i razumeti, a još teže im se suprotstaviti.

Društvo je već postalo veoma zavisno od različitih formi informacione tehnologije, a ta zavisnost će se, bez sumnje, još više širiti i pojačavati. Kako digitalni prostor sve više postaje opšte mesto odvijanja svih ljudskih aktivnosti, pa i najsloženijih oblika kriminala, špijunaže i terorizma, jedan od najvećih izazova postaje pronalaženje načina kako, pri transformaciji iz industrijskog u informaciono društvo, najviše i najbolje iskoristiti moć informacione tehnologije, a istovremeno sprečiti njenu zloupotrebu.

Udruženje sudskih veštaka za informacione tehnologije IT VEŠTAK, koje okuplja vrhunske eksperte iz oblasti informacionih tehnologija, sada već davne 2004. godine organizovalo je prvu konferenciju na ovu temu. U saradnji sa različitim organizacijama, Udruženje je održalo kontinuitet skupa, čiji su sadržaji sigurno doprineli podizanju svesti i znanja u pomenutoj oblasti kod državnih organa, privrednih subjekata, grupa i pojedinaca, kao i u preventivnom delovanju da do neželjenih događaja ne dođe.

Pod sloganom Upotreba – Zloupotreba – Zaštita održava se ovogodišnja, 8. po redu konferencija ZITEH, sa ciljem organizovanog objedinjavanja, uvećavanja i širenja raspoloživih znanja i iskustava o načinima i mogućnostima zaštite od zloupotrebe informacionih tehnologija. I ove godine ključni suorganizator konferencije je Poslovni i pravni fakultet Univerziteta „Union – Nikola Tesla", koji je obezbedio da ZITEH sa regionalne izađe na međunarodnu scenu.

Verujemo da će ova međunarodna konferencija doprineti generisanju kritične mase svesti i znanja radi dugoročnog i celovitog stavljanja pod kontrolu ovog izuzetno složenog i, sa društvenog aspekta, veoma opasnog problema digitalne sigurnosti.

Naučni i Organizacioni odbor zahvaljuju svim partnerskim organizacijama, suorganizatorima, naučnicima, istraživačima i svim učesnicima koji su dali doprinos uspešnoj pripremi i realizaciji ove konferencije.

U Beogradu,
oktobar 2019. godine

Naučni i Organizacioni odbor

# PREFACE

The expansion of information technologies and business process automation covering all spheres of social life are a true phenomenon of today. This phenomenon has brought countless benefits to modern society, but it has also created a number of problems and risks, both for individuals, groups, and organizations and society as a whole. These problems and risks, many of which have never existed before, can sometimes be difficult to understand and it can be even more difficult to confront them.

Society has already become highly dependent on various forms of information technology and this dependence will undoubtedly grow and expand even further. As the digital space is increasingly becoming the general place of all human activities, including the most complex forms of crime, espionage, and terrorism, one of the biggest challenges during the transformation from an industrial to an information society is to discover how to make good use of information technology power and how to prevent its abuse at the same time.

As early as 2004, Association of Forensic Testimony Experts for Information – IT VEŠTAK, which brings together IT top-quality experts in the field of information technology, organized the first conference on this topic. The Association has maintained the meeting continuity in cooperation with various organizations. The contents of the meeting have certainly contributed to raising awareness and expanding knowledge in the aforementioned field among state authorities, business entities, groups, and individuals, but they have also contributed to preventing undesired events from occurring.

This year's 8$^{th}$ ZITEH conference is held under the slogan Use-Misuse–Protection. Its aim is organized unification, expansion, and spreading of available knowledge and experiences on the ways and possibilities of protection against information technology abuse. This year, also, the key partner is the Faculty of Business and Law of the University "Union - Nikola Tesla", which has enabled ZITEH to move from regional to the international scene.

We believe that this international conference will contribute to generating a critical mass of awareness and knowledge for this extremely complex and, from the social point of view, a very dangerous problem of digital security to be brought under control completely and over the long term.

The Scientific and Organizational Board express their gratitude to all partner organizations, co-organizers, scientists, researchers, and all participants who have contributed to the successful preparation and realization of this conference.

Belgrade, October 2019 Scientific and Organizational Board

# SADRŽAJ – TABLE OF CONTENTS

# MJERE PREVENCIJE I SIGURNOSNE POLITIKE PROTIV CYBER TERORIZMA

## PREVENTION MEASURES AND SECURITY POLICIES AGAINST CYBER TERRORISM

**Vladica Babić**
Visoka škola Logos, Mostar, Bosna i Hercegovina

JEL kategorija rada: **L86**

***Apstrakt***

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

*Adresa autora:*
***Vladica Babić***
*vladica_babic@net.hr*

***Ključne reči:*** *Terorizam, cyber kriminal, prevencija, sigurnosna politika*

***Abstract***

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

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

# DIGITALIZACIJA MALIH I SREDNJIH PRIVREDNIH DRUŠTAVA – POTENCIJALI I RIZICI

## DIGITALIZATION OF SMALL AND MEDIUM-SIZED ENTERPRISES - POTENTIALS AND RISKS

**Milanka Bogavac**
Poslovni i pravni fakultet „Union – Nikola Tesla“ Univerziteta, Beograd, Srbija

**Lyudmila Prigoda**
Maikop State Technological University, Maikop, Russian Federation

**Zoran Čekerevac**
Poslovni i pravni fakultet „Union – Nikola Tesla“ Univerziteta, Beograd, Srbija

JEL kategorija rada: **G32, J53, M15, O32**

*Adresa autora zaduženog za korespodenciju:*
***Milanka Bogavac***
*bogavac.milanka@gmail.com*

***Apstrakt***

*Razvoj i širenje digitalnih tehnologija imao je nesumnjiv uticaj na poslovanje svih privrednih*

*društava na globalnom nivou i na čovečanstvo uopšte. Iako nezaobilazan fenomen, digitalizacija i njeni efekti su tek odnedavno ušli u fokus istraživača, ali i država i njihovih vlada. Digitalizacija nije dočekana u svim zemljama i u svim oblastima na isti način. Oni koji su bili spremniji da se prilagode promenama ostvarili su bolje, pa čak i ekstremno dobre rezultate, a oni koji nisu bili spremni na promene, iz bilo kog razloga, suočili su se sa nepremostivim problemima i rizikom od propasti. Analize Svetske trgovinske organizacije su 2016. godine pokazale da mala i srednja privredna društva, iako predstavljaju ogromnu većinu svih privrednih društava, nisu dovoljno izučena. S obzirom na to da se situacija ni do danas nije značajno promenila, mnogi MSP i njihove potrebe i mogućnosti ne shvataju, nedovoljno cene, pa i ignorišu. Cilj ovog rada je da ukaže na mogućnosti i rizike kojima su MSP izložena u vreme digitalizacije poslovnih procesa i digitalizacije uopšte. U radu su razmatrani (1) digitalizacija kao savremeni svetski proces poboljšanja performansi i konkurentnosti, (2) digitalizacija poslovnih procesa, (3) Uticaji Interneta i društvenih mreža na MSP, (5) uticaji IoT i IIoT na MSP i (6) potencijal i rizici u slučaju MSP. Za analiziranje trenutne situacije autori su izvršili i eksperimentalno istraživanje koje omogućava da se sagleda nivo koji su MSP iz Ruske Federacije, Slovačke i Srbije ostvarila u 2019. godini. Na kraju rada su izloženi zaključci istraživanja i date su preporuke za buduća istraživanja. Rad može da posluži korisno svima koji se bave poslovanjem MSP i aktivnostima u vezi sa digitalizacijom privrede i društva.*

***Ključne reči:*** *digitalizacija, digitalna transformacija, IoT, IIoT, IDSME, mala i srednja privredna društva, MSP*

***Abstract***

*The development and diffusion of digital technologies have undoubtedly affected the business of all businesses globally and humanity in general. Although an unavoidable phenomenon, digitalization and its effects have only recently become the focus of researchers, as well as states and their governments. Digitization has not been welcomed in all countries and areas in the same way. Those who were more willing to adapt to change achieved better and even extremely good results, and those who were not ready for change, for whatever reason, faced insurmountable problems and the risk of failure. Analyzes of the World Trade Organization in 2016 showed that SMEs, although representing the vast majority of all companies, are not sufficiently trained. Given that the situation has not changed significantly to date, many SMEs and*

*their needs and opportunities are not understood, under-appreciated and even ignored. The aim of this paper is to highlight the opportunities and risks that SMEs are exposed to at the time of digitalization of business processes and digitization in general. The paper discusses (1) digitization as a contemporary global process for improving performance and competitiveness, (2) digitizing business processes, (3) the impacts of the Internet and social networks on SMEs, (5) the impacts of IoT and IIoT on SMEs, and (6) the potential and risks in the case of SMEs. To analyze the current situation, the authors also carried out an experimental study that allows one to look at the level achieved by SMEs from the Russian Federation, Slovakia, and Serbia in 2019. The conclusions of the research are presented at the end of the paper and recommendations for future research are given. The work can be of benefit to anyone involved in SME business and activities related to the digitization of the economy and society.*

***Keywords:*** *digitalization, digital transformation, IoT, IIoT, IDSME, SMEs*

# RAZVOJ TRŽIŠTA DIGITALNIH VALUTA

## DIGITAL CURRENCY MARKET DEVELOPMENT

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

JEL kategorija rada: **D85**

***Apstrakt***

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

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

*ravnopravnih kompanija. Bitkoin je krajem prošle godine bio valuta sa najviše vrednosti u celom svetu. Da je tržište kriptovaluta u ekspanziji potvrđuju i primeri Južne Amerike, koja je imala ogroman porast transakcija s bitkoinima nakon 2014. godine kao i Argentine koja je središte za povećanu upotrebu kriptovalute.*

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

***Abstract***

*After steady growth over the last few years, the cryptocurrency market has been on the rise since 2017. Cryptocurrencies, like Bitcoin, consist of a network of peer-to-peer nodes that together maintain a common record of historical transactions resistant to tampering. It uses encryption techniques to control the creation of monetary units and to verify the transfer of funds. Cryptocurrency is a concept that is an alternative to the fiat currency used in the current monetary system. Entrepreneurs, start-ups and large as well as small and medium-sized enterprises (SMEs) are interested in cryptocurrencies and consider it a revolutionary concept for counteraction to transactions. Technology is advancing at high speed, and the success of the technology is almost exclusively dictated by the market in which it wants to improve. Cryptocurrencies can revolutionize digital commerce markets by creating a royalty-free system of free circulation and has a great advantage over traditional value and since it presents great flexibility in making fast peer-to-peer transactions, especially in international scenarios. By its nature, it can fill gaps in current financial technologies and be able to help solve traditional banking problems by being a peer-to-peer system. Bitcoin was the highest valued currency in the world at the end of last year. The cryptocurrency market is in expansion what is also confirmed by the examples of South America, which saw a huge increase in transactions with bitcoins after 2014, as well as Argentina, which is the hub for increased use of cryptocurrency.*

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

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

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

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

**Predrag Radovanović**
Visoka poslovna škola strukovnih studija, Leskovac, Srbija

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

***Apstrakt***

*Prvi platni sistemi bazirani na elektronskom/digitalnom novcu pojavili su se početkom i sredinom devedesetih godina prošloga veka. U svom razvoju, elektronski/digitalni novac prošao je kroz nekoliko generacija. Mada prva generacija platnih sistema baziranih na digitalnom novcu nije doživela veći komercijalni uspeh, jedna forma digitalne valute tiho je evoluirala tokom vremena u ono što danas poznajemo kao kriptovalute. Kriptovalute su generalno bazirane na decentralizovanim, direktnim P2P plaćanjima. U radu će biti predstavljen nastanak, razvoj i izvesni tehnički aspekti kriptovaluta. Biće*

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

*sumirani preduslovi koje su brojni analitičari isticali kao najbitnije koje jedan platni sistem baziran na digitalnoj (kripto)valuti mora da ispuni kako bi bio uspešan. Spisku preduslova biće dodati i oni kojima u teoriji i praksi digitalnih (kripto)valuta do sada nije posvećena dovoljna pažnja. Zaključujemo da je cilj uspešnog platnog sistema baziranog na digitalnoj (kripto)valuti da što vernije preslika karakteristike realnog novca, zbog čega je, međutim, nužno pratiti slične modalitete kreiranja, opticaja i valuacije.*

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

***Abstract***

*The first electronic/digital money-based payment systems emerged in the early and mid-1990s. In its development, electronic/digital money has passed through several generations. Although the first generation of digital money-based payment systems failed to achieve commercial success, one form of digital currency has quietly evolved over time into what we now know as cryptocurrencies. Cryptocurrencies are generally based on decentralized, direct P2P payments. The origin, development and certain technical aspects of cryptocurrency will be presented in the paper. The paper will also summarize the prerequisites that many analysts have highlighted as the most important that a digital (crypto)currency-based payment system must meet in order to be successful. The list of prerequisites will be extended with those who have not received enough attention in the theory and practice of digital (crypto)currencies so far. We conclude that the goal of a successful digital (crypto)currency-based payment system is to accurately capture the characteristics of real money; therefore, it is necessary to follow similar modalities creation, circulation, and valuation.*

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

# PROCJENA UČINKA NA ZAŠTITU LIČNIH PODATAKA

## PRIVACY IMPACT ASSESSMENT

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

JEL kategorija rada: **K22, M15**

***Apstrakt***

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

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

*temeljem preporuka francuske agencije za zaštitu privatnosti podataka i preporuka međunarodnih standarda ISO/IEC 29134 i ISO/IEC 27005.*

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

***Abstract***

*Integrating the privacy requirement in the information system design is not an easy task. First of all, privacy is a complex, multiple, and contextual concept in itself. In addition, the issue of privacy is not a primary requirement of the system, and sometimes even this requirement can come into conflict with other (functional or non-functional) requirements of the information system. Therefore, it is of utmost importance to precisely define the objectives of privacy in the process of realizing privacy by design. One way to define the objectives of the information system in terms of the privacy requirement is to conduct a privacy impact assessment or a privacy risk analysis. Conducting a privacy impact assessment is in line with the principles of technical and integrated data protection under Article 25 of the General Data Protection Regulation – GDPR. In accordance with the principles of technical and integrated data protection, a privacy impact assessment should be carried out before the processing itself with the aim of using it as a tool for decision-making, in particular for the selection of appropriate technical protection measures. Although the General Data Protection Regulation does not prescribe any specific methodology or standard for privacy impact assessment in the guidelines of the Article 29 Working Group on Data Protection, there are recommendations for the use of international standards. This paper presents the method of privacy impact assessment based on the recommendations of the French Data Protection Agency and the recommendations of international standards ISO/IEC 29134 and ISO/IEC 27005.*

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

# DIGITALIZACIJA U RUSKOJ EKONOMIJI: PREDNOSTI I PRETNJE

## DIGITALIZATION IN THE RUSSIAN ECONOMY: ADVANTAGES AND THREATS

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

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

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

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

***Apstrakt***

*Značaj digitalne transformacije kako u poslovanju tako i u čitavim sektorima ekonomije budi sve veće interesovanje za izazove i pretnje, rizike i koristi koji mogu nastati u digitalnoj ekonomiji. U narednim godinama, sva područja vladine aktivnosti i tržišta će se preorijentisati u skladu sa zahtevima novih digitalnih ekonomskih modela. Nemoguće je zaustaviti tranziciju velikih razmera na „digital", jer je korisna za potrošača, korisna za poslovanje, a značajna za vlasti. Vrednost digitalnih*

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

*rešenja raste, a cena njihovog dobijanja opada. Digitalizacija počinje da prevazilazi promene same tehnologije - postaje makroekonomski i politički faktor. U članku se govori o trenutnom stanju digitalne ekonomije Rusije, o programima finansiranja digitalizacije ekonomije. Rejting zemlje se analizira u skladu sa u međunarodnoj zajednici usvojenim indeksima, koji mere koliko dobro ruska ekonomija koristi digitalne tehnologije za povećanje konkurentnosti i blagostanja. Istovremeno, indeksima se i procenjuju faktori koji utiču na razvoj digitalne ekonomije. Značajno zaostajanje u razvoju digitalne ekonomije Rusije od svetskih lidera objašnjava se nedostatkom regulatornog okvira za digitalizaciju i nedovoljno povoljnim okruženjem za poslovanje i inovacijama i, kao rezultat toga, niskim nivoom primene digitalnih tehnologija u biznisu i vladinim strukturama.*

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

***Abstract***

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

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

# CRIME INDEX AS ONE OF THE MAIN INDICATORS OF SAFETY

**Roman Kmet**
University of Zilina, Faculty of Security Engineering, Zilina, Slovakia

**Zdenek Dvorak**
University of Zilina, Faculty of Security Engineering, Zilina, Slovakia

JEL Category: **C88, L86**

***Abstract***

*The evolution of crime and its constant changes bring with it several new types of crime, which have many different crimes. By collecting and analyzing data in the form of these offenses, crime statistics are often generated for different periods of time or territorial units. The aim of these statistics is to divide the territory into smaller territorial units in which the level of crime is mutually assessed. For this purpose, a crime index has been created and is currently used to determine the level of crime in a territory. As crime is constantly developing and globalizing, it is necessary to modify this index to optimize and apply it in the European Union. Recently, security research has focused on crime index research. In the currently solved projects at the University of Zilina, creating a set of security indexes is one of the important challenges.*

***Keywords:*** *safety, crime, the crime index*

*Address of the corresponding author:*
***Roman Kmet***
*roman.kmet@fbi.uniza.sk*

# UPRAVLJANJE RIZIKOM – CYBER SIGURNOST

## RISK MANAGEMENT - CYBER SECURITY

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

JEL kategorija rada: **G32**

***Apstrakt***

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

*Adresa autora:*
***Branka Mijić***
*brankica_mijic@net.hr*

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

***Abstract***

*We are witnessing the great impact of the Internet and information technology on human life. Today, we can say with certainty that business entities and individuals are becoming more and more exposed to various forms of cyber-attacks and crime. The information and technology carry certain challenges and risks. Cyber-attacks can have devastating consequences and a huge impact on government, business subjects, their employees, customers, but also third parties. Such attacks and threats are among the biggest risks facing the corporate sector in the world today, and different modes of Internet and information technology security are used to cover risks. Risk management is a moral and legal obligation of every organization and society. Risk management gives the organization a clear view of the risks and the ability to act proactively to protect the resources and operations of the organization. Cybersecurity has been something that has finally started to be talked about and paid more attention in recent years, as we are witnessing an increasing number of hacking attacks, which represent one of the biggest challenges for managements of most prominent global companies.*

***Keywords**: Cybersecurity; cybercrime; cyber risk; risk management*

# KRIVIČNA DELA PROTIV BEZBEDNOSTI RAČUNARSKIH PODATAKA

**Živanka Miladinović Bogavac**
Poslovni I pravni fakultet, Univerzitet Union Nikola Tesla, Beograd

JEL kategorija rada: **K11, K14, K22**

***Apstrakt***

*Krivični zakonik Republike Srbije u glavi dvadeset i sedmoj propisuje krivična dela koja za svoj zaštitni objekat imaju računarske podatke. Shodno navedenom u ovoj glavi regulisana su sledeća krivična dela : oštećenje računarskih podataka i programa, računarska sabotaža, pravljenje i unošenje računarskih virusa, računarska prevara, neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka, sprečavanje i ograničavanje pristupa javnoj računarskoj mreži, neovlašćeno korišćenje računara ili računarske mreže, I pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka. Ova krivična dela su uvedena u krivično zakonodavstvo Republike Srbije 2003 godine, izmenama I dopunama KZS, izmenama i dopunama KZS, tako što su prihvaćena rešenja iz Nacrta KZ SR Jugoslavije iz februara 2000.godine. Republika Srbija je 2005 godine potpisala Konvenciju o sajber kriminalu Saveta Evrope. U skladu sa preuzetim obavezama, u cilju suzbijanje kompjuterskog kriminaliteta, pored odredbi u Krivičnom Zakoniku Republike Srbije, od značaja su odredbe Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala kojim se, između ostalog predviđa i formiranje specijalizovanih odeljenja u tužilaštvu i MUP-u. U radu će biti analizirana krivična dela protiv bezbednosti računarskih podataka, međusobno razlikovanje I specifičnosti istih, čime će se skrenuti pažnja da li*

*Adresa autora:*
***Živanka Miladinović Bogavac***
*zivankamiladinovic@gmail.com*

*je Republika Srbija u svom zakonodavstvu svoje odredbe prilagodila potpisanoj Konvenciji o sajber kriminalu.*

***Ključne reči**: krivična dela, bezbednost računarskih podataka, Krivični zakonik Republike Srbije, pravna regulative*

***Abstract :***

*The Criminal Code of the Republic of Serbia, in part twenty-seven, prescribes criminal offenses that have computer data for their protective object. Pursuant to this chapter, the following offenses are regulated: damage to computer data and programs, computer sabotage, creation and introduction of computer viruses, computer fraud, unauthorized access to a secure computer, computer network and electronic data processing, preventing and organizing access to a public computer network, unauthorized use of a computer or computer network, and making, procuring and providing other means of committing criminal offenses against computer data security. These criminal offenses were introduced into the criminal legislation of the Republic of Serbia in 2003, as amended by the CCS, as amended by the CCS, by adopting the decisions of the Draft CC of the Federal Republic of Yugoslavia of February 2000. In 2005, the Republic of Serbia signed the Council of Europe Convention on Cybercrime. In accordance with the undertaken obligations, in order to combat computer crime, in addition to the provisions of the Criminal Code of the Republic of Serbia, the provisions of the Law on Organization and Competence of State Bodies for Combating High-Tech Crime, which, among other things, provide for the establishment of specialized departments in the prosecution and Police. The paper will analyze criminal offenses against the security of computer data, their differentiation and their specificities, which will draw attention to whether the Republic of Serbia has in its legislation adapted its provisions to the signed Convention on Cybercrime.*

***Keywords:** criminal offenses, computer data security, Criminal Code of the Republic of Serbia, legal regulation*

# ZLOUPOTREBA NOVIH TEHNOLOGIJA I DIGITALNO NASILJE

## NEW TECHNOLOGY ABUSE AND DIGITAL VIOLENCE

**Zoran Milanović**
Kriminalističko-policijski Univerzitet, Beograd, Srbija

JEL kategorija rada: **L86**

***Apstrakt***

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

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

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

***Abstract***

*The rapid development of new technologies has also led to their unlawful application to the extent*

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

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

# RADIKALIZACIJA VISOKOTEHNOLOŠKOG TERORIZMA

## THE RADICALIZATION OF HIGH-TECH TERRORISM

**Ivica Petrović**
Akademija za nacionalnu bezbednost, Beograd, Srbija

**Dragana Trnavac**
Poslovni i pravni fakultet, Univerzitet UNION-Nikola Tesla, Beograd, Srbija

JEL kategorija rada: **L86**

***Apstrakt***

*Visokotehnološki terorizam je rizik još od pojave Interneta. Tehnologija se razvijala brzim tempom samim tim i rizik i uticaj visokotehnološkog terorizma. Važno je da postoje sigurni i ažurirani mehanizmi za ublažavanje rizika visokotehnološkog terorizma, uz međunarodnu saradnju radi daljeg unapređenja istrage i informacija. Ovaj rad govori o mehanizmima kao što su bezbednost aplikacije, bezbednosne politike, razumevanje obrazovanja programi, međunarodna saradnja, nadgledanje i veštačka inteligencija (VI), praćenje, korišćenje i ometanje pristupa. Implementacija svih mehanizama omogućava računarske mreže i sisteme koji su manje ranjivi zato što svaki mehanizam poseduje odvojene funkcije za borbu protiv visokotehnološkog terorizma. Kao rezultat toga, ovo istraživanje dokazuje pozitivnu povezanost između*

*Adresa autora zaduženog za korespodenciju:*
***Dragana Trnavac***
*draganatrnavac@gmail.com*

*prepoznatih mehanizama i percipiranog rizika od visokotehnološkog terorizma. Bilo je različitih inicijativa, koje su pokrenuli nadležni organi iz celog sveta, kako bi se osiguralo da je pretnja od visokotehnološkog terorizma pod kontrolom. Međutim, pretnja od visokotehnološkog terorizma neprestano raste zbog stalnog razvoja platformi zasnovanih na Internetu. Tako, sprovođenje zakona, politike, prakse i neophodnih mera trebalo bi da se nastavi sa savremenim razvojem kompjuterskih tehnologija.*

***Ključne reči:*** *visokotehnološki terorizam, veštačka inteligencija (VI), nadgledanje, korišćenje i ometanje*

***Abstract***

*High-tech terrorism has been a risk since the advent of the Internet. Technology has evolved at a rapid pace, thus the risk and impact of high-tech terrorism. Importantly, there are secure and up-to-date mechanisms to mitigate the risks of high-tech terrorism, with international cooperation to further advance investigations and information. This paper discusses mechanisms such as application security, security policies, education understanding of programs, international collaboration, monitoring and artificial intelligence (VI), monitoring, use and disruption of access. The implementation of all mechanisms is facilitated by computer networks and systems that are less vulnerable because each mechanism has separate functions to counter high-tech terrorism. As a result, the goals for this research prove a positive correlation between the mechanisms identified and the perceived risk of high-tech terrorism. There have been various initiatives, introduced by authorities around the world, to ensure that the threat of high-tech terrorism is under control. However, the threat of high-tech terrorism is steadily rising due to the constant development of Internet-based platforms. Thus, the implementation of the law, policies, practices and necessary measures should continue with the modern development of computer technologies.*

***Keywords****: high-tech terrorism, artificial intelligence, surveillance, utilization, interference.*

# SELECTED SAFETY FEATURES FOR MEDICINES SOLD IN TRADITIONAL PHARMACIES

**Marek Stych**
Pedagogical University, Faculty of Political Science, Institute of Law, Administration and Economics, Crakow, Poland

JEL Category: **I18, K33, K38**

***Abstract***

*Nowadays, every EU resident can easily find advertisements of non-prescription medicinal products (over-the-counter drugs) on the Internet. They get to mailboxes as the so-called commercial information or can be seen on websites devoted to health in general or a specific disease. Certain drugs can also be found on various websites or via search engines. It is thus possible for patients to buy medicines through legal websites run by traditional pharmacies, but also through websites run by shady entities that cannot be considered pharmacies or any other entities. That is why additional safety features for batches and individual packagings of medicines introduced on 9 February 2019 are so important.*

***Keywords:*** *falsification of medicines, medicine serialization, EAN code*

*Address of the author:*
***Marek Stych***
*stycma@interia.pl*

# NEVIDLJIVE TRANSAKCIJE U DARK WEB-U

## STEALTH TRANSACTIONS IN THE DARK WEB

**Sergej Uljanov**
Fakultet za poslovne studije i pravo Univerztiteta „UNION – Nikola Tesla“, Beograd, Republika Srbija

**Đorđe Milošević**
Centar za pravnu pomoć, Beograd, Republika Srbija

JEL Kategorija rada: **E49, F38, L86**

***Apstrakt***

*Autori u ovom radu razmatraju mogućnosti vršenja novčanih transakcija skrivenih u okruženju dark web-a. Kao ključne komponente ovakve aktivnosti autori ističu fenomenološki tripod, koji čine pojmovi kripto valute, blokčejn tehnologije i virtuelnog novčanika (web wallet). S tim u vezi, autori će prikazati u radu, u posebnim poglavljima, pojmove i vrste virtuelnog novca, web wallet-a i način funkcionisanja blokčejn razmene podataka odnosno jedinica kripto valute. Poseban osvrt biće napravljen u odnosu na pitanja anonimnosti i skrivanja tragova novčanih tokova u Darknetu. Autori teže da objasne razloge zbog kojih nosioci transakcija virtuelnog novca insistiraju na svojoj anonimnosti i nemogućnosti praćenja njihove aktivnosti od strane drugih subjekata prisutnih u tamnom vebu, bez obzira na to da li je reč o hakerima ili organima za primenu zakona. Takođe, autori smatraju značajnim obuhvatno posmatranje želje za anonimnim delovanjem, koja ne podrazumeva uvek i isključivo kriminalnu intenciju. U radu su otvorena pitanja stvarne anonimnosti virtuelnih novčanika, kao i ranjivosti blockchain modusa u odnosu na sajber napade i zloupotrebu radi skrivanja*

*Adresa autora zaduženog za korespodenciju:*
***Đorđe Milošević***
*djodjolos@gmail.com*

*novčanih transakcija u kriminalne svrhe, te „pranje“ kripto valuta. Autori u radu nastoje da iznesu najnovije podatke koji se odnose na navedenu problematiku, kako bi istraživani fenomen mogao biti sagledan u svojoj aktuelnosti. Namera autora je da svoje zaključke temelje na punoj voluminoznosti ključnih pojmova, čiji značaj predstavlja okosnicu ovog rada.*

***Ključne reči:*** *dark web, kripto valuta, blockchain, web wallet, kripto novčanik, „pranje“ virtuelnog novca, transakcija kripto valute*

***Abstract***

*The authors of this article deem possibilities of doing money transactions covered by the network of the dark web. As key components of such activity, the authors highlight phenomenological tripod made of terms related to cryptocurrency, blockchain technology and virtual wallet (known as web wallet). Thereby, the authors are about to present in this article, as chaptered, terms and kinds of virtual money, web wallets and the way of running, both, blockchain exchanging of data and of cryptocurrencies units. The special overview is to be done considering questions of anonymity and hiding traces of money transactions in the Darknet. The authors tend to explain the reasons why subjects of cryptocurrency transactions insist to remain stealth and anonymized having their activities untraceable to other subjects presented in the dark web, no matter if it is up to hackers or law enforcement. Also, the authors consider it as important to make a broader view of the phenomenon of having a need for an anonymized way of doing transactions, which is not always to be solely connected to criminal intent. There are issues of virtual wallets anonymity and blockchain modus vulnerability relate to cyber-attacks and misuse of stealth money transactions, both, for illegal purposes and for cryptocurrencies money laundering, to be mattered in this article. The authors strive to express the most recent data on the above-mentioned challenges, to make researched phenomena to be perceived as an actual one. The intention of the authors is to base their conclusions on the full-scale volume of essential terms whose importance represents a framework for this article.*

***Keywords****: the dark web, cryptocurrency, blockchain, web wallet, dark wallet, cryptocurrency money laundering, cryptocurrency transaction*

# PREVARE PUTEM INTERNETA: SAJBER ZABAVA KOJA „PRAZNI" RAČUNE ŠIROM SVETA

## INTERNET FRAUD: CYBER ENTERTAINMENT THAT "CLEANS" BANK ACCOUNTS WORLDWIDE

**Vida M. Vilić**
Klinika za stomatologiju Niš, Niš, Srbija

JEL Kategorija rada: **L86**

***Apstrakt***

*Postoje različiti oblici prevara putem Interneta, a kako najveći broj izvršilaca ovog dela pripada mlađoj populaciji, stiče se utisak da je ova vrsta kriminalne aktivnosti postala sve češća zabava mlađih ljudi koji su vešti u poznavanju informaciono-komunikacionih tehnologija. Pojavni oblici prevara su mnogobrojni i zbog različitih načina njihovog izvršenja nemoguće ih je u potpunosti sagledati. U praksi se javljaju kako primitivne i grube prevare tako i one prevare kod kojih učinioci ispoljavaju visok stepen veštine. Kao česti oblici Internet prevara javljaju se „Valentino" prevare, „lančana pisma", piramidalne šeme, „lutajući" trgovci, transfer novca u dobrotvorne svrhe i lutrijske prevare, dok je svakako jedan od najčešće viđenih oblika sa kojim se svako od nas susreo u svom poštanskom sandučetu tzv. "Nigerijska prevara". Prevare putem Interneta u Republici Srbiji još uvek nisu pravno regulisane. U toku 2008. i 2009. godine na teritoriji Republike Srbije prijavljeno je devet krivičnih dela prevare sa elementima „nigerijskih" prevara protiv nepoznatih učinilaca, dok je na svetskom nivou procena da su Internet*

*Adresa autora:*
***Vida M. Vilić***
*: vila979@gmail.com*

*prevare dostigle svoj vrhunac 2009. godine. Pored definisanja i klasifikacije najčešćih pojavnih oblika prevara putem Interneta, u radu su dati i neki praktični saveti kako sprečiti viktimizaciju od prevarnog ponašanja na Internetu.*

***Ključne reči:*** *Prevare putem Interneta, računarske prevare, nigerijska prevara, krivično delo prevare*

***Abstract***

*There are various forms of Internet fraud, and since most of the perpetrators belong to the younger population, it seems that this type of criminal activity has become even more and more fun for younger people with great knowledge and practical skills in the field of information and communication technologies. There are many forms of this act, because of the many different modus operandi, so it is almost impossible to fully understand and to explain them, or even harder to prevent them. Common forms of Internet scams include so-called "Valentine" scams, "chain letters", pyramidal schemes, "wandering" merchants, charity transfers and lottery scams, while certainly one of the most commonly seen forms we've encountered are so-called "Nigerian scams". In the Republic of Serbia, Internet fraud is not yet legally regulated as criminal acts. During 2008 and 2009, nine criminal offenses with elements of "Nigerian scam" were reported in the territory of the Republic of Serbia against unknown perpetrators, while at the global level, it is estimated that this particular kind of Internet fraud reached its top in 2009. In addition to defining and classifying the most common forms of Internet frauds, this paper also provides some practical tips on how to prevent victimization from fraudulent behavior on the Internet.*

***Keywords****: Internet scams, computer fraud, Nigerian scam, fraud*

# DIGITALIZATION OR ICT IN TOURISM

**Slavoljub M. Vujovic**
Institute of Economics, Belgrade, Serbia

JEL Category: **O3, O31, O32, O33, Z3, Z32.**

***Abstract***

*The research presented in the paper is theoretical, focused on analyzing and clarifying the role and importance of using information technology for tourism development as an economic activity. It also seeks to point out that the use of the term "digitalization of tourism" (or digitization of business in the tourism economy) is unnecessary. Research is not focused on information technology as a new discipline, but on the practical use of technologies to process and transfer data and information, technologies for communications, to enable faster flow of capital and services, and so on. The special purpose of the research is the analysis of the benefits of the use of information and communication technologies from the aspect of the providers of tourism supply, carriers of tourist demand and intermediary factors. The work is part of the research on the project "Development and application of new and traditional technologies in the production of competitive food products with added value for the domestic and world markets - Let's create wealth from the wealth of Serbia" (MPNTR RS, No. 046001).*

***Keywords:*** *tourism development, information technology, tourism digitalization.*

*Address of the author*
***Slavoljub Vujović***
*kelovic1967@yahoo.com*

# DA LI SU PROBLEMI U IT VEŠTINAMA REŠIVI ILI OSTAJU DA BUDU UVEK PRISUTNI?

## ARE THE PROBLEMS IN INFORMATION TECHNOLOGY SKILLS SOLVABLE, OR WILL STAY FOREVER?

**Hana Rizqallah Qananah**
Univerzitet ''UNION – Nikola Tesla'', Beograd, Fakultet za informacione tehnologije i inženjerstvo, Beograd, Srbija

**Khalefa Altaher Mohamed Alnagasa**
Univerzitet ''UNION – Nikola Tesla'' Beograd, Fakultet za informacione tehnologije i inženjerstvo, Beograd, Srbija

**Mohamed Salem Almabrouk**
Univerzitet ''UNION – Nikola Tesla'', Beograd, Fakultet za poslovne studije i pravo, Beograd, Srbija

**Nada Živanović**
Univerzitet ''UNION – Nikola Tesla'' Beograd, Poslovni i pravni fakultet, Beograd, Srbija

JEL kategorija rada: **A29, I21, J24**

*Adresa autora zaduženog za korespodenciju:*
***Hana Rizqallah Qananah***
*hana.gananah@gmail.com*

***Apstrakt***

*Četvrta svetska revolucija nauke i prakse pripada primeni novih IT informacionih tehnologija i*

*njihovoj velikoj mogućnosti primene u svim sferama poslovanja. Polazeći od najrazvijenije društvene mreže – Interneta, gde je otvorena javna upotreba ove mreže, ali kako podaci pokazuju, postoje primeri u svetu koji dokazuju suprotno, odnosno da priroda Interneta kroz njegovu upotrebu ugrožava zatvorene informativne mreže, npr. koje je razvila finansijska industrija krajem 20. veka. Problemi koji su rezultirali ovom konfliktu, u prvom redu najbolje se objašnjavaju u bankama. To govori, da su te tehnologije dominirale u formi, kao tehnologije za razmenu informacija i za sigurnost informacija. Prema podacima, evolutivni razvoj on-line komercijalne transakcije počeo je još 1995. godine, a do 1998. godine preko Internet mreže je obrađeno više od 50 milijardi dolara transakcija. U 21-om veku, godišnja vrednost internet transakcija je značajno porasla što se shodno tome, zahteva više mreža, više računara i više programa sigurnosti. Tako su uglavnom finansijske institucije usmerene na razvoj i sticanje više veština u korišćenju IT tehnologija da bi se mogle takmičiti. Jasna koncepcija primene IT preferira preciznost odnosno, ne mogu se finansijske institucije takmičiti bez široke i sigurne informacione mreže što govori, da su informacione tehnologije od suštinskog značaja za poslovne procese i dugoročni uspeh. Šta podrazumeva, termin ''Globalno finansiranje''? To se u modernom finansijskom svetu praktično objašnjava na sledeći način: da informacione tehnologije omogućavaju, posmatrano na globalnom nivou, da finansiranje funkcioniše na osnovu poslovne sintagme koja strukturira koncepciju u IT sektoru za finansije na sledeći način: "da se finansijska tržišta mogu smatrati prvim organizovanim globalnim informacionim tržištima koja rade preko umreženih računara". (n.d., Investment planning, 2019) Suština je, da se spozna u informacionom svetu, da većina ljudi ne planira neuspeh. (Beckley, 2009) Iako su nekada troškovi visoki, veštine u IT okruženju treba da napreduju, jer ne treba čekati da se zaradi novac pa da se snize troškovi. Kako podaci govore, to zvuči dobro, ali nikada se realno tako ne događa. Finansijski plan koji se temelji na ciljevima pomaže, da se učini ono što je najbolje za uspešno poslovanje. Cilj je, da se proces finansijskog planiranja pojednostavi, i da se eliminišu sve pretpostavke ili nagađanja, šta može da bude. U suštini, u pogledu usredsređivanja pažnje na korišćenje sopstvenih veština prilikom primene IT tehnika i tehnologija, treba uraditi sledeće: 1. Upoznati planove i odrediti prioritete. 2. Minimizirati razlike u ostvarivanju uspeha. 3. Definisati strategiju primene veština. 4. Razvijati i primenjivati fleksibilnost primene tih veština. 5. Spremno odgovoriti na potrebe i fluktuacije na tržištu.*

***Ključne reči:*** *Problemi u nedostatku veština, IT tehnologije, rizici, komunikacije, promene, liderstvo, poslovanje*

***Abstract***

*The fourth world revolution of science and practice belongs to the application of new IT information technologies and their great application in all spheres of business. Starting from the most developed social network - the Internet, where the public use of this network is open, but as the data show, there are examples in the world that prove otherwise, that is, the nature of the Internet through its use threatens closed information networks, e.g. developed by the financial industry in the late 20th century. The problems that have resulted in this conflict are primarily explained by banks. That said, these technologies have dominated form, as information-sharing and information-security technologies. According to the data, the evolutionary development of online commercial transactions began back in 1995, and by 1998, more than $ 50 billion in transactions had been processed through the Internet. In the 21st century, the annual value of Internet transactions has increased significantly, which consequently requires more networks, more computers, and more security programs. Thus, it is mainly financial institutions that are focused on developing and acquiring more skills in using IT technologies to compete. A clear conception of implementing IT prefers precision, that is, financial institutions cannot compete without a broad and secure information network, which is to say that information technologies are essential for business processes and long-term success. What is meant by the term ''Global Financing''? In the modern financial world, this is practically explained as follows: that information technologies enable, globally, financing to operate on the basis of a business syntax that structures the conception in the IT sector for finance as follows: "that financial markets can be considered as the first organized global information markets to operate over networked computers." The bottom line is to realize in the information world that most people do not plan to fail. Although sometimes costs are high, skills in the IT environment need to thrive because you don't have to wait for money to be made and costs reduced. As the data say, it sounds good, but it never really happens. A goal-based financial plan helps to do what is best for a successful business. The goal is to streamline the financial planning process and to eliminate all assumptions or speculations, which may be. Basically, in order to focus on using your own skills when applying IT techniques and technologies, the following should be done: 1. Know the plans and prioritize. 2. Minimize the chances of*

*success. 3. Define a strategy for applying skills. 4. Develop and apply the flexibility of applying these skills. 5. Ready to respond to market needs and fluctuations.*

***Keywords:*** *Skills problems, IT technologies, risks, communications, change, leadership, business.*

# IZAZOVI PRIMENE INFORMACIONE TEHNOLOGIJE U ZDRAVSTVENIM SISTEMIMA

## CHALLENGES OF APPLICATION OF INFORMATION TECHNOLOGY IN HEALTH SYSTEMS

**Nataša Mazić**
Klinički centar Srbije, Beograd, Srbija

**Srđan Blagojević**
Visoka poslovna škola strukovnih studija u Beogradu, Zemun, Srbija

JEL kategorija rada: **C55, L86**

***Apstrakt***

*Razvoj informacionih tehnologija je u velikoj meri doprineo unapređenju zdravlja i pružanja zdravstvenih usluga. Vođenje elektronske medicinske dokumentacije, zakazivanje pregleda, primena elektronskih recepata i praćenje ishoda lečenja su postali svakodnevna praksa. Sa sve većim obimom prikupljenih i obrađenih podataka, raste i značaj njihovog pravilnog prikupljanja, obrade, skladištenja i prenošenja. Poseban problem predstavlja primena dela informacionih tehnologija koje omogućavanju pružanje medicinskih usluga kada su korisnici i pružaoci usluge na različitim lokacijama, tj. telemedicina koja se može koristiti za nadzor, konsultacije, dijagnostiku, negu i edukaciju. Napredak u ovoj oblasti doneo je rizik od neovlašćene primene medicinskih sredstava kojima se mogu*

*Adresa autora zaduženog za korespodenciju:*
***Srđan Blagojević***
*srdjan@hotmail.ca*

*izazvati oštećenja zdravlja, pa čak i smrtni ishod. Razvoj i primena informacionih tehnologija u našoj zemlji evidentna je i u oblasti zakonske regulative. Prema Zakonu o zdravstvenoj dokumentaciji i evidencijama u oblasti zdravstva do 1. januara 2020. zdravstvene ustanove u našoj zemlji u obavezi su da vode medicinsku dokumentaciju u elektronskoj formi. Iz tog razloga neophodno je da budu uvedene adekvatne mere zaštite od neovlašćenog pristupa, uvida, kopiranja i zloupotrebe podataka kako bi se obezbedilo da uvođenje novih tehnologija ostvari svoj cilj, a to je da bude u interesu očuvanja i unapređenja zdravlja. U radu je poseban akcenat stavljen na upravljanje podacima o pacijentima u rasutom zdravstvenom sistemu.*

***Ključne reči:*** *elektronska medicinska dokumentacija, pacijent, podaci, medicina, zakon, zdravstvena zaštita.*

***Abstract***

*Development of information technology greatly contributed to the improvement of health and health services. Conducting electronic medical documentation, scheduling of examination, application of electronic recipes and monitoring of the outcome of the treatment became daily practice. With increasing volume of collected and processed data, the importance of their proper collection, processing, storage and transfer is also increased. A specific problem is the application of a portion of the information technology that enables medical services when users and service providers in different locations, for example Telemedicine that can be used for supervision, consultation, diagnostics, care and education. Progress in this area has brought the risk of unauthorized implementation of medical devices that can cause health damage and even a death outcome. The development and implementation of information technologies in our country is evident in the field of legal regulations. According to the Law on Health, documentation and records in the field of healthcare, by January 1st, 2020, health institutions in Serbia will be obliged to conduct medical documents in electronic form. For this reason, it is necessary to impose adequate safeguards against unauthorized access, insight, copying and misuse of data to ensure that the introduction of new technologies achieves its goal, which is to be in the interest of preserving and improving health. The paper focuses on the management of patient data in the bulk health system.*

***Keywords****: Electronic medical documentation, patient, data, medicine, law, health care.*

# RECENZENTI – REVIEWERS

1. Prof. Dr. **Zoran Čekerevac**, Faculty of Business and Law of the "Union - Nikola Tesla" University Belgrade, Belgrade, Serbia
2. Prof. Ing. **Zdenek Dvorak**, Ph.D., Faculty of Special Engineering University of Žilina, Žilina, Slovakia
3. Ing. **Stanislav Filip**, Ph.D., Assoc. Prof., School of Economics and Management in Public Administration in Bratislava, Slovakia
4. **Mariya P. Hristova**, Ph.D., Assoc. Prof., "Todor Kableshkov" University of Transport, Sofia, Bulgaria
5. Prof. **Petar Kolev**, Dr, "Todor Kableshkov" University of Transport, Sofia, Bulgaria
6. Prof. Dr. **Lyudmila Prigoda**, Maikop State Technological University, Maikop, Russia
7. Prof. Dr. **Dušan Regodić**, Faculty of Business and Law, "Union - Nikola Tesla" University, Belgrade, Serbia
8. Prof. Dr. **Dubravka Škunca**, Faculty of Business and Law, "Union - Nikola Tesla" University, Belgrade, Serbia
9. Prof. **Daniela Todorova**, Ph.D., "Todor Kableshkov" University of Transport, Sofia, Bulgaria
10. Prof. Dr. **Miomir Todorović**, Faculty of Business and Law, "Union - Nikola Tesla" University, Belgrade, Serbia
11. Prof. **Yaroslav Vyklyuk**, DSc, Bukovinian University, Chernivtsi, Ukraine
12. Prof. Dr. **Nada Živanović**, Faculty of Business and Law, "Union - Nikola Tesla" University, Belgrade, Serbia

**IT Veštak**
**Hadži Melentijeva 33**
**11000 Beograd**
**Republika Srbija**

**Poslovni i pravni fakultet**
**Knez Mihailova 33**
**11000 Beograd**
**Republika Srbija**