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 2018

ZBORNIK REZIMEA
ABSTRACT PROCEEDINGS

Beograd	Srbija	26. septembar 2018
Belgrade	Serbia	26 September 2018

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
Bukovinian University, Chernivtsi, UA
High School of Economics and Management in Public Administration, Bratislava, SK
Faculty of Security Engineering, University of Zilina, SK
Maykop State Technological University, Maykop, 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
and
MESTE, Belgrade

International Scientific Conference
"ZITEH 2018"
Belgrade
26th of September 2018

ABSTRACT PROCEEDINGS

ICIM+

Izdavački centar za INDUSTRIJSKI MENADŽMENT plus
Beograd-Mladenovac, 2018

IT VEŠTAK
and
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
Bukovinian University, Chernivtsi, UA
High School of Economics and Management in Public Administration, Bratislava, SK
Faculty of Security Engineering, University of Žilina, SK
Maykop State Technological University, Maykop, 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
i
MESTE, Beograd

Međunarodna naučna konferencija
„ZITEH 2018“
Beograd, Srbija
26. septembar 2018

ZBORNIK REZIMEA

ICIM+

Izdavački centar za INDUSTRIJSKI MENADŽMENT plus
Beograd-Mladenovac, 2018

Međunarodna naučna konferencija
MENADŽMENT 2018
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 Srđan Blagojević

Dizajn korica:
Mladen Stojanović

Kompjuterska priprema:
Zoran Čekerevac

Štampa:
Planeta print, Beograd

Tiraž:
100

International Scientific Conference
MANAGEMENT 2018
Abstract Proceedings

Publisher:
IT Veštak
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. Srdjan Blagojevic

Cover design:
Mladen Stojanovic

Technical editing:
Zoran Cekerevac

Printed by:
Planeta print, Belgrade

Circulation:
100

ISBN 978-86-6375-104-0

Izdavanje Zbornika rezimea, organizaciju i održavanje Međunarodne naučne konferencije ZITEH 2018 pomoglo je
Ministarstvo prosvete, nauke i tehnološkog razvoja Republike Srbije

Financing of the Abstract Proceedings, organization and realization of the International Scientific Conference ZITEH 2018 was sponsored by
Ministry of Education, Science and Technological Development of the Republic of Serbia

NAUČNI ODBOR / SCIENTIFIC BOARD

Prof. Dr. Zoran Cekerevac, FBL, Belgrade - President

Prof. Dr. Srdjan Blagojevic, VPSSS, Belgrade

Prof. Dr. Milija Bogavac, FBL, Belgrade

prof. dr Dragana Becejski Vujaklija, IT Vestak, Beograd

prof. dr Dragan Đurđević, Akademija za nacionalnu bezbednost, Beograd

prof. Daniela Todorova, PhD, VTU „Todor Kableshkov“, Sofija

prof. Mikhail Manylich, PhD, BU, Cernivci

prof. Kuizheva Saida Kazbekovna, CSc, MGTU, Majkop

Prof. Dr. Lyu Zhongda, NUT, Ningbo

prof. Ing. Viera Cibakova,PhD, VSEMvs, Bratislava

prof. dr Evgenij Safonov, RGGU, Domadedovo

prof. dr Petar Kolev, VTU „Todor Kableshkov“, Sofija

prof. dr Yaroslav Vyklyuk, Bukovinski Univerzitet, Cernivci

prof. ing. Zdenek Dvorak, PhD, FBI, Zilina

prof. dr Ludmila Prigoda, MGTU, Maykop

prof. dr Sergei Kirsanov, IMD, Sankt Peterburg

dr Wang Bo, docent, Ninbo TU, Ninbo

doc. Stanislav Filip, PhD, VSEMvs Bratislava

doc. dr Vladica Babic, Univerzitet Vitez

Dr. Oksana Koshulko, PhD, PAS, Warsaw

ORGANIZACIONI ODBOR / ORGANIZING BOARD

Prof. Dr. Srdjan Blagojevic – co-president

Prof. Dr. Milija Bogavac – co-president

Prof. Dr. Zoran Cekerevac

mr Aleksandar Mirkovic

mr Momir Ostojic

Milanka Bogavac, MBA

Aleksandar Matic, LL.M.

Proofreading:

Dr. Ljiljana Jovkovic

Sanja Cukic, 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
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, 7. po redu konferencija ZITEH, sa ciljem organizovanog objedinjavanja, uvećavanja i širenja raspoloživih znanja i iskustava o načinima i mogućnostima zaštite od zloupotrebe informacionih tehnologija. 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,
septembar 2018. 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 for 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 7th 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, 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, 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, September2018 Scientific and Organizational Board

SADRŽAJ – TABLE OF CONTENTS

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

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

Adresa autora zaduženog za korespodenciju:
Hatidža Beriša
berisa.hatidza@gmail.com

„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 razmatraju 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. 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*

NEDOZVOLJENOST OBRADE 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

JEL Category: **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 smilsu, 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

Adresa autora:
Nenad Bingulac
nbingulac@pravni-fakultet.info

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*

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*

SOCIJALNI INŽENJERING I LIČNI PODACI

SOCIAL ENGINEERING AND PERSONAL DATA

Srđan Blagojević
Visoka poslovna škola strukovnih studija „Čačak“, Beograd i „IT veštak“, Beograd, Srbija

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

Adresa autora:
Srđan Blagojević
srdjan@hotmail.ca

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 huge amount of information published and often publicly shared on user's 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 personal data from internet users that is easy to trade with or to cash in. 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.*

SECURITY OF INFORMATION AND COMMUNICATION TECHNOLOGIES

BEZBEDNOST INFORMACIONIH I KOMUNIKACIONIH TEHNOLOGIJA

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

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

Zoran Čekerevac
Faculty of Business and Law, "Union – Nikola Tesla" University, Belgrade, Serbia

JEL Category: **C88, L86**

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,

Adresa autora zaduženog za korespodenciju:
Kamil Boc
kamil.boc@fbi.uniza.sk

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.*

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 the Republic 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.*

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 Techological University, Maykop, Russian Federation

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

Adresa autora zaduženog za korespodenciju:
Zoran Čekerevac
zoran@cekerevac.eu

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.

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.*

DIGITAL COALITION OF THE SLOVAK REPUBLIC - OPPORTUNITY FOR THE INTERNATIONALIZATION OF HIGHER EDUCATION IN IT AREA

Ľuboš Cibák
School of Economics and Management in Public Administration in Bratislava, Bratislava, Slovak Republic

Stanislav Filip
School of Economics and Management in Public Administration in Bratislava, Bratislava, Slovak Republic

Olena Rayevneva
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine

Abstract

Authors in the article state the reasons for giving rise and existence of the Digital Coalition of the Slovak Republic. They analyze its position in society, specify its objectives, priorities, and commitments. In the following part, they discuss the possibilities of using the coalition to improve the internationalization of higher education. On the example of the School of Economics and Management in Public Administration in Bratislava, they identify and consider the advantages and disadvantages of membership in the coalition. They analyze the process of

Adresa autora zaduženog za korespodenciju:
Stanislav Filip
stanislav.filip@vsemvs.sk

preparing and implementing their commitment to membership in the coalition by creating a joint master's study program with the partner Simon Kuznets Kharkiv National University of Economics in Ukraine. In conclusion, benefits of membership of a higher education school in the Digital Coalition are evaluated as one of the most important tools for improving the internationalization of higher education. The aim of the contribution is to provide a wide professional and general public in the Central European space with guidance for solving the personnel problems of the IT sector on the example of the Slovak Republic. The contribution is based on the theoretical and practical knowledge and experience of the authors acquired through long-term pedagogical and scientific research activities, international cooperation and cooperation with the IT sector of the Slovak Republic.

***Keywords**: IT sector, digital coalition, human resources management, internationalization of education, joint study program*

DIGITÁLNA KOALÍCIA SLOVENSKEJ REPUBLIKY – PRÍLEŽITOSŤ NA INTERNACIONALIZÁCIU VYSOKOŠKOLSKÉHO VZDELÁVANIA V IT OBLASTI

Abstrakt

Autori v článku uvádzajú príčiny vzniku a existencie Digitálnej koalície Slovenskej republiky. Analyzujú jej postavenie v spoločnosti, špecifikujú jej ciele, priority a záväzky. V ďalšej časti sa zaoberajú možnosťami využitia koalície na skvalitnenie internacionalizácie vysokoškolského vzdelávania. Na príklade Vysokej školy ekonómie a manažmentu verejnej správy v Bratislave identifikujú a posudzujú výhody a nevýhody členstva v koalícii. Analyzujú proces prípravy a realizácie svojho záväzku členstva v koalícii vytvorením spoločného magisterského študijného programu s partnerskou Národnou ekonomickou univerzitou Simona Kuzneca v Charkove na Ukrajine. V závere hodnotia prínosy členstva vysokej školy v Digitálnej koalícii ako jeden z najvýznamnejších nástrojov na skvalitňovanie internacionalizácie vysokoškolského vzdelávania. Cieľom príspevku je poskytnúť širokej odbornej aj laickej verejnosti v Stredoeurópskom priestore návod na riešenie personálnej problematiky IT sektoru na príklade Slovenskej republiky.V príspevku sú uplatnené teoretické aj praktické poznatky a skúsenosti autorov nadobudnuté dlhoročnou pedagogickou a vedecko-výskumnou činnosťou, medzinárodnou spoluprácou a spoluprácou s IT sektorom Slovenskej republiky.

***Kľúčové slová:** IT sektor, digitálna koalícia, manažmentu ľudských zdrojov, internacionalizácia vzdelávania, spoločný študijný program*

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

JEL Category: **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

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

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, author presents 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*

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, Srbija

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

Radovan Radovanović
Kriminalističko policijska akademija, Beograd, Srbija

Apstrakt

U procesnoj industriji menadžment rizika je tradicionalno fokusiran na razmatranje verovatnoće specifičnih događaja ili havarijskih situacija. U energetskim postrojenjima koja predstavljaju najznačajnije polje primene, od 70-ih godina

Adresa autora zaduženog za korespodenciju:
Goran Jovanov
goran.jovanov@kpa.edu.rs

prošlog veka u SAD je uveden struktuirani 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 odnosno snimanje situacije poslovnog sistema.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 vrši se rangiranje numeričko procenjivanje rizika, odnosno Rizik (R) se rangira od prihvatljivog (zanemarljivo malog rizka) 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 the 1970's of the last century, in the USA the structural approach for identification of failure scenario was introduced. Risk assessment 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 assessment is the possibility for risk management, its decrease or elimination. Risk assessment 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 assessment will be accomplished. The methodological course of risk assessment procedure represents the ground for proper estimation, i.e. for monitoring the situation of the business system. The result of system's condition at the application of certain models for risk assessment, depends exclusively on properly made results within the methodological course of risk assessment. Based on further results, the ranking of numerical risk assessment 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 an action 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 assessment is accomplished by showing the matrix model. There are matrices with a different number of levels, but the simplest model of the 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*

MODEL UPRAVLJANJA BEZBEDNOSNIM RIZIKOM

SECURITY RISK MANAGEMENT MODEL

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

Nikola Glođović
Kriminalističko policijska akademija, Beograd, Srbija

Goran Jovanov
Kriminalističko policijska akademija, Beograd, Srbija

JEL Category: **G32**

Apstrakt

Danas u svetu imamo više razvijenih modela za upravljanje bezbednosnim rizikom, a u ovom radu će se predstaviti razvijeni model sa osam faza. Faza „Identifikacija poslovnog sistema treba da identifikuje sve objekte poslovnog sistema, aktivnosti koje se u njemu realizuju i zaposlene radnike, jer oni potencijalno mogu biti ugroženi nekom opasnošću. Znači, neophodno je izvršiti procenu zašto i kako bi potencijalni nepredviđeni događaj uticao na poslovni sistem i sve njegove resurse, a takođe treba da se utvrdi da li potencijalni nepredviđeni događaj koji bi mogao prouzrokovati određenu opasnost predstavlja događaj koji bi ostvario štetu koju poslovni sistem ne sme sebi da dozvoli, ili je za njega konkretni potencijalni događaj zanemarljiv. U fazi „Procena opasnosti“ vrši se predviđanje potencijalnih specifičnih opasnosti i situacija u kojima bi

Adresa autora zaduženog za korespodenciju:
Nemanja Jovanov
nemanjjajovanov@gmail.com

one mogle da se dese. U ovoj fazi se znači ne realizuje procena bezbednosnog rizika, ali se dolazi do potrebnih informacija i smernica koje će se koristiti za procenu. „Procena ranjivosti“ je faza modela upravljanja bezbednosnim rizikom u kojoj se trebaju prepoznati snaga i slabosti poslovnog sistema po pitanju bezbednosnih mera koje štite isti od uticaja iz okruženja. U narednoj fazi se realizuje procena bezbednosnog rizika. Vrši se kombinovanje svih raspoloživih relevantnih (direktnih i indirektnih) informacija po pitanju bezbednosti, kako bi se uspeo identifikovati potencijalni uticaj i verovatnoća pojave potencijalne opasnosti po poslovni sistem, tj. dobili trenutni nivo bezbednosnog rizika. U fazi „Bezbednosne mere i strategije“ realizuje se razvoj i stvaranje istih, kako bi se njihovom primenom ostvarilo smanjenje verovatnoće pojave bezbednosnog rizika i njegovog štetnog (opasnog) uticaja. U fazi „Donošenje odluke“ neophodno je da se donesu odluke po pitanju prioriteta, logističke podrške, vremenskih rokova, finansija, itd. Ova faza se realizuje u tri koraka, i to: procedure za smanjenje bezbednosnog rizika na prihvatljiv nivo; utvrđivanje prioriteta; i, odobravanje finansija i potrebnih resursa. Posle ove faze realizuje se po ovom modelu priprema i implementacija razvijenih bezbednosnih mera. Na kraju se vrši ocena svega što je urađeno, realizuju se potencijalno potrebne korekcije i vrše se pripreme za buduću modernizaciju bezbednosnih mera i strategija.

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

Abstract

Today, worldwide, there are many developed models for managing security risks, and within these theses, the developed model with eight phases will be represented. The phase “Business System Identification” should identify all objects of a business system, the activities realized within it and the employees, because these potentially can be jeopardized by some threat. Therefore, it is necessary to make an estimate why and how a potential unpredictable event could influence a business system and all its resources, as well as it should be determined whether potential unpredictable event, which could cause certain threat, represents the event which would cause damage which business system must not allow, or a specific potential event is irrelevant for it. In the phase “Threat Estimate” potential specific threats and situations in which these may occur are predicted. In this phase, security risk estimate is not made, but the necessary information and instructions which will be used for the estimate are gathered. “Vulnerability Estimate“ is the phase of a security risk management model in which the strength and weakness of a business system should be

recognized, related to security measures which protect the system from the surrounding influences. In the next phase, the security risk estimate is realized. All available, relevant (direct and indirect) security-related information are combined, to identify potential influence and probability of the occurrence of a potential threat on a business system, i.e. to get current level of security risk. In the phase „Security Measures and Strategies“ their development and creation are realized, in order to accomplish the reduction of probable occurrence of security risk and its harmful (dangerous) influence by their application. In the phase „Decision Making“ it is necessary to bring the decisions related to priorities, logistics support, timelines, financials, etc. This phase is realized in three steps, as follows: the procedure for reducing the security risk to an acceptable level; setting the priorities; and approving financials and necessary resources. After this phase, the preparation and implementation of developed security measures are released, by this model. In the end, the estimate of everything done is made, potential, necessary corrections are realized, as well as the preparation for future modernization of security measures and strategies is made.

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

KRIPTOVALUTE, BLOKČEJN I BITKOIN

CRYPTOCURRENCY, BLOCKCHAIN, AND BITCOIN

Mario Lukinović
Pravni fakultet Univerziteta Union, Beograd, Srbija

JEL Category: **D84**

Apstrakt

Kriptovalute (eng."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

Adresa autora:
Mario Lukinović
lukinovicmario@gmail.com

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.

Ključne reči: *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 (digikesh, Heshesh, 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 the bitcoin functioned is based on blockchain technology, whose potential reaches far beyond the cryptocurrencies. Although there is still a controversy over the pseudonyms of Satoshi Nagano, 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*

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

JEL Category: **D82, 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 svrsi zaštite, odnosno, sigurnosti informacije i informacionog sustava, a za sve to je potrebna primjena standarda iz serije ISO27001.

Adresa autora:
Branka Mijić
brankica_mijic@net.hr

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, the clear majority 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 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.*

PRAVNA REGULATIVA DEČIJE PORNOGRAFIJE NA INTERNETU

LEGISATIVE REGULATIONS OF CHILD PORNOGRAPHY ON INTERNET

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

Vesna Stojanović
Slobodni istraživač, Beograd, Srbija

JEL Category: **K14, L86**

Apstrakt

Dečija pornografija, tj. zloupotreba dece u pornografske svrhe, prema samom svom nazivu aludira na nešto loše i nesporno je da je ona veliki problem društva današnjice 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

Adresa autora zaduženog za korespodenciju:
Živanka Miladinović Bogavac
zivankamiladinovic@gmail.com

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, by its very name, alludes to something bad, and it is undisputed that 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 in 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 is an attempt to reach an "ideal" solution. With the development of technology, modern age facilitates the expansion of child pornography. The world's most famous social network that has a wide range of functions and possibilities – the internet – has developed with the 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 the 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*

RAČUNARSKA SABOTAŽA

COMPUTER SABOTAGE

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

JEL Category: **L86**

Apstrakt

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

Adresa autora:
Živanka Miladinović Bogavac
zivankamiladinovic@gmail.com

obzirom na to da je danas nemoguće funkcionisati ni za pojedinca ni za državu bez upotrebe računara i savremenih tehnologija, važna je činjenica da je sve više razvijena svest o opasnosti istih, te je stoga neophodno da države preduzmu značajne korake ka regulisanju računarske sabotaže i ostalih opasnih radnji koje se vrše putem računarske tehnologije.

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

Abstract

There is a growing interest among lawyers in computer crime, otherwise known as cyber-crime. Since it is increasingly developing together with the development of innovations in the field of information technologies, legislative measures are necessary to regulate and sanction this type of crime. Nowadays, a computer sabotage appears as a frequent criminal offense, which is incriminated by the Criminal Legislation of the Republic of Serbia. Since it is very generally defined by the Criminal Code, it is necessary to determine the very notion of computer sabotage as well as its types, i.e. it is necessary to present some of the many possibilities for the execution of this crime. International legal regulation is of great importance because the criminal offense in question is the one where the perpetrators may be from different countries and thus work together. The International Convention on Cyber Crime defined terms that are important for determining the concept of computer sabotage. Certainly, computer sabotage and other criminal acts of cybercrime are mutually intertwined, and it is necessary to connect them, compare the similarities and differences and analyze in what relation they stand to each other. It is of particular importance to distinguish computer sabotage from cyberterrorism, which is one of the biggest dangers in the world of computers, computer networks, the internet, and social networks. Given that nowadays it is impossible for an individual or a country to function without the use of computers and modern technologies, it is important that the awareness about the danger of those above-mentioned spreads, and it is, therefore, necessary that countries take significant steps towards regulating computer sabotage and other dangerous activities that are carried out through computer technology.

***Keywords**: computer sabotage, cybercrime, computer misuse, computer protection, computer network defense*

INFORMACIONO-BEZBEDNOSNA KULTURA MLADIH U SRBIJI

INFORMATION-SECURITY CULTURE OF YOUTH IN SERBIA

Zoran Milanović
Kriminalističko-policijska akademija, Beograd

JEL Kategorija rada: **L86**

Apstrakt

Mlađe populacije su najčešći korisnici interneta, a posebno društvenih mreža i kao takve su najugroženija ciljna grupa većine pojavnih 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 istraživanje 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 (primenjivačkih) 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*

Adresa autora:
Zoran Milanović
zoran.milanovic@yahoo.com

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 cause of these inconsistencies is a lack of the 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.*

KRIPTOVALUTE – NOVI MODEL POSLOVANJA

CRYPTOCURRENCIES - A NEW BUSINESS MODEL

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

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

JEL Category: **E27, M21**

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 kontroverze, 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

Adresa autora zaduženog za korespodenciju:
Miljković Ljubomir
ljubomir.miljkovic@ppf.edu.rs

sredstvo plaćanja sa stvarnim posledicama. Bitkoin 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 bitkoin obezbedila je svoje mesto u svetu finansija uprkos brojnim osporavanjima. Rast vrednosti bitkoina, 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, bitkoin, digitalna valuta, internet, međunarodno poslovanje*

Abstract

The development of technology has led to the creation of new phenomena in the financial world. One of these phenomena is a crypt, digitally decentralized currencies created for the "world of the future - which is global and virtual, based on highly sophisticated technologies and mathematical algorithms. Crypt represents 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-calendars 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*: crypt, bitcoin, digital currency, internet, international business*

KRIVIČNOPRAVNI ZNAČAJ VAŽNIJIH REŠENJA IZ ZAKONA O NACIONALNOM DNK REGISTRU

CRIMINAL LAW SIGNIFICANCE OF IMPORTANT SOLUTIONS FROM THE LAW ON NATIONAL DNA REGISTRY

Željko Nikač
Kriminalističko-policijska akademija, Beograd, Srbija

Vanda Božić
Pravni fakultet, Katedra za kazneno pravo, Zagreb, Hrvatska vanda.bozic@pravo.hr

JEL Category: **K14**

Apstrakt

U referatu autori daju analizu najvažnijih odredaba Zakona o nacionalnom registru DNK, koji je usvojila Narodna skupština RS u proleće 2018.godine. Posebno se ukazuje na krivičnopravni značaj uspostavljanja i upotrebe DNK registra i tehnologije u forenzičkom postupku otkrivanja izvršilaca krivičnih dela, s ciljem njihovog procesuiranja i izricanja adekvatne sudske sankcije. Smisao ovih odredaba je da nevine osobe ne budu osuđene, već da ruka pravde stigne stvarne izvršioce krivičnih dela. Registar se koristi i za potrebe utvrđivanja identiteta nestalih i nepoznatih lica, kao i za utvrđivanje identiteta leševa i delova tela. Centralno mesto u

Adresa autora zaduženog za korespodenciju:
Željko Nikač
zeljko.nikac@kpa.edu.rs

Registru ima baza podataka DNK profila nespornih i spornih bioloških uzoraka, kao i profila utvrđenih u krivičnim postupcima koji su dostavljeni centralnoj laboratoriji. U radu se posebno ukazuje na osetljivost ovih podataka i potrebu njihovog zakonitog korišćenja i obrade, prema svrsi koja je određena Zakonom. U zaključnim razmatranjima autori predlažu da se u dogledno vreme uspostavi trajna baza DNK podataka i unapredi postupak veštačenja u praksi, saglasno normama nacionalnog krivičnog zakonodavstva i propisima EU.

***Ključne reči**: krivični postupak, DNK baza podataka, identitet nestalih i nepoznatih lica, Srbija i EU.*

Abstract

In the paper, the authors give an analysis of the most important provisions of the Law on National DNA Registry, adopted by the RS National Assembly in the spring of 2018. It specifically points to the criminal law importance of the establishment and use of DNA registers and technologies in the forensic process of detecting perpetrators of criminal offenses with the aim of prosecuting and imposing adequate judicial sanctions. The point of these provisions is that innocent persons are not sentenced, but that the hand of justice reaches the actual perpetrators of criminal offenses. The register is also used to identify the identity of missing and unknown persons, as well as to identify the identity of bodies and parts of the body. The central location in the Registry has DNA profiles of undisputable and controversial biological samples, as well as profiles established in criminal proceedings delivered to the Central Laboratory. In particular, this paper addresses the sensitivity of these data and the need for their legitimate use and processing, for the purpose defined by the Law. In concluding considerations, the authors propose to establish a permanent database of DNA data in a timely manner and to improve the practice of expertise, in accordance with national criminal law norms and EU regulations.

***Keywords**: criminal procedure, DNA database, identity of missing and unknown persons, Serbia and the EU.*

PREKRŠAJNA ODGOVORNOST KAO MODALITET ZAŠTITE POSLOVANJA ZASNOVANIH NA NOVIM INFORMACIONIM TEHNOLOGIJAMA

MISCELLANEOUS RESPONSIBILITY AS A MODALITY OF PROTECTION OF BUSINESS OPERATIONS BASED ON NEW INFORMATION TECHNOLOGIES

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

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

JEL Category: **K19**

Apstrakt

Poslovni ambijent ili poslovno okruženje, bez obzira da li ga posmatramo kao globalno tržište ili kao pojedinačni poslovni segment na organizacionom nivou,

Adresa autora zaduženog za korespodenciju:
Nenad Bingulac
nbingulac@pravni-fakultet.info

obavezno u nekoj formi podrazumeva primenu informacionih tehnologija iz čega proizilazi nužnost obezbeđivanja uspešnih modela poslovanja zasnovanih na novim tehnologijama. Najznačajniji rast u okviru globalnog poslovnog ambijenta dostiže već skoro dve decenije upravo oblast elektronskog poslovanja. Kompleksnost sistema e-poslovanja i značaj koji ima za organizaciju, podrazumevaju da je neophodno posvetiti značajnu pažnju aspektima koji direktno utiču na uspešnu implementaciju e-poslovanja. Sinergijski efekti zaštite, bezbednosti i privatnosti, kontinuirano upravljanje kvalitetom usluga, obezbeđuju realizaciju snažnog potencijala e-poslovanja i Interneta. Uspešnost e-psolovanja podrazumeva primenu čitavog seta metoda i tehnika, kako bi se dostigla odgovarajuća bezbednost. Između ostalog, Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju, predstavlja još jedan korak napred u planiranom i aktuelnom procesu digitalizacije i uopšteno modernizacije javne uprave, koji za cilj ima omogućavanje građanima i privrednim subjektima jednostavnijeg pristupa uslugama koje pružaju nadležni organi javne vlasti, odnosno brže, jeftinije i efikasnije poslovanje. Zakonom se uvodi elektronski pečat, te na taj način proširuje mogućnosti pravnih lica u pogledu korišćenja pogodnosti koje pruža elektronsko poslovanje. Shodno navedenom, cilj ovog rada je da se razmotre pomenuta pitanja koja se odnose na poslovanja zasnovana na novim tehnologijama i da se ukaže na njihovu zakonodavnu zaštitu koja proizilazi iz Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju.

Ključne reči: *prekršajna odgovornost, e poslovanje, savremene tehnologije u funkciji poslovana, zakonodavna zaštita*

Abstract

The business environment, regardless of whether it is viewed as a global market or as an individual business segment at the organizational level, is mandatory in some form implies the application of information technologies, resulting in the necessity of securing successful business models based on new technologies. The most significant growth in the global business environment has reached almost two decades in the field of electronic business. The complexity of the e-business system and the importance it has for the organization means that it is necessary to pay considerable attention to the aspects that directly affect the successful implementation of e-business. Synergic effects of protection, security and privacy, continuous quality management of services, provide realization of

strong potential of e-business and the Internet. The effectiveness of e-learning involves the application of a whole set of methods and techniques in order to achieve appropriate security. Among other things, the Law on electronic document, electronic identification and trust services in electronic commerce is another step forward in the planned and actual process of digitization and general modernization of the public administration, which aims to provide citizens and businesses with easier access to the services provided by the competent public authorities, or faster, cheaper and more efficient operations. The law introduces an electronic seal, thus extending the possibilities of legal entities regarding the use of e-commerce benefits. In accordance with the above, the aim of this paper is to consider issues related to business based on new technologies and to point to their legislative protection arising from the Law on the electronic document, electronic identification, and trust services in electronic commerce

Keywords: *misdemeanor responsibility, e-business, modern technologies in the function of business, legislative protection*

PRIMENA RFID TEHNOLOGIJE – NEKI PROBLEMI I PRAVCI RAZVOJA

APPLICATION OF RFID TECHNOLOGY – SOME PROBLEMS AND DEVELOPMENT DIRECTIONS

Lyudmila Prigoda
Maykop State Technological University, Maykop, Russian Federation

Jelena Maletić
Technical School GSB, Belgrade, Serbia

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

JEL Category: **R41**

Apstrakt

U uslovima savremenog poslovanja i sve veće primene kompjuterskih tehnologija, postavljaju se sve stroža vremenska ograničenja, sve veći zahtevi u pogledu efikasnosti upotrebe mehanizacije, automatizacija tehnoloških procesa, veća

Adresa autora zaduženog za korespodenciju:
Lyudmila Prigoda
lv_prigoda@mail.ru

pouzdanost i niži troškovi i bolji ekonomski pokazatelji. Kao jedno od pogodnih rešenja, pojavljuje se upotreba RFID tehnologije. RFID sistemi poslednjih desetak godina imaju sve značajnu ulogu u povećanju efikasnosti i smanjenju troškova poslovanja i pored toga što još uvek nisu otkriveni ni iskorišćeni svi potencijali ove tehnologije. RFID tehnologija pruža praktične koristi svakome ko ima potrebe da prati fizičko prisustvo objekata u nekoj sredini. Mnogi unapređuju lance snabdevanja i procese proizvodnje uvođenjem ove tehnologije. Razlozi za korišćenje RFID tehnologije u velikim sistemima su mogućnost potpune automatizacije rada primenom kompjuterskog upravljanja i nadzora, kao i bolja kontrola izdavanja i praćenja stanja u magacinima, uz smanjenje mogućnosti greške kao i krađe i prevare, povećanje profita i kvaliteta, dobijanje izveštaja o izdavanju delova ili goriva (u koje vreme je preuzeto, u kojoj količini...) i dr. U ovom radu je detaljnije prikazano jedno rešenje za kontrolu točenja goriva na stanicama za snabdevanje gorivom na bazi RFID tehnologije. Razmotrene su prednosti i nedostaci ove tehnologije, ekonomski aspekti primene, kao i mogućnosti potpune zaštite od krađe i raznih drugih prevara. Analiza je pokazala da efekti mogu biti: smanjenje ukupnih troškova, optimizacija postojećeg sistema snabdevanja, optimizacija postojećeg sistema praćenja kvantitativnog stanja zaliha goriva na stanicama za snabdevanje gorivom, potrošnja goriva po vozilima i dr. Na kraju rada je analizirana budućnost primene RFID tehnologije, putevi daljeg razvoja i potencijalni rizici primene ove tehnologije.

***Ključne reči**: Informacione tehnologije, RFID, kontrola, gorivo, nedostaci, napadi*

Abstract

In the conditions of modern business and the increasing use of computer technologies, more time constraints are being imposed to businesses, increasing demands in terms of efficiency of the use of machinery, automation of technological processes, higher reliability, lower costs and better economic indicators. As one of the convenient solutions, the use of RFID technology appears. RFID systems are playing a significant role in increasing efficiency and reducing operating costs in the last dozen years, even though all the potentials of this technology have not yet been discovered or exploited. RFID technology provides practical benefits to anyone who needs to monitor the physical presence of objects in a certain environment. Many improve supply chains and production processes by introducing this technology. The reasons for the use of

RFID technology in large systems are the ability to fully automate the work with the use of computer management and control, better control of issuing and monitoring the stock situation, while reducing the possibility of error as well as theft and fraud, increasing profits and quality, obtaining reports on the issue of parts or fuel (at what time it was taken, in what quantity ...) etc. In this paper, one RFID solution for controlling fuel refueling at fuel supply stations is shown in more detail. The advantages and disadvantages of this technology, the economic aspects of the application, as well as the possibilities of complete protection against theft and various other frauds are considered. The analysis has shown that the positive effects can be: reduction of total costs, optimization of the existing supply system, optimization of the existing system for monitoring the quantitative state of the fuel stock at fuel stations, fuel consumption by vehicles, etc. At the end of the paper, the future of RFID technology, the paths for further development, and the potential risks of applying this technology are analyzed.

Keywords: *Information Technologies, RFID, control, fuel, disadvantages, attacks*

IT VEŠTAK IZMEĐU SCILE I HARIBDE

IT COURT EXPERT BETWEEN SCILA AND HARIBDA

Boško S. Rodić
Visoka škola akademskih studija „Dositej“, Beograd

JEL Category: **Y20**

Apstrakt

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. Prihvatajući se veštačenja u IT sudski veštak se susreće sa brojnim: moralnim, stručnim, i, razume se objektivnim problemima. U ovom radu pokušaćemo da dodirnemo 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

Adresa autora:
Boško Rodić
bosko.rodic@gmail.com

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 [Int18a] 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, to do the job, and the third -to charge for 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 suggested by someone past them. In order for this work to be successfully realized, already mentioned at the beginning of this text, the expert has to master numerous Scile and Haribde. Still, a typical problem for the Serbian judiciary in relation to experts is payment, or rather - non-payment. According to [Int18a] experts are owed 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 a 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.*

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

JEL Category: **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 relnom

Adresa autora zaduženog za korespodenciju:
Miroslav D. Stevanović
mstvnv297@gmail.com

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 na nametanje mnjenja umesto informisanja. Rezultati analize ukazuju na postojanje niza 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" 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 instrumentalized to relativize 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 analyzed from the perspective of the potential structural and functional impact of systematic instrumentalization 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 organization 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*

ZNAČAJ JEDINSTVENOG INFORMACIONOG SISTEMA ZA PLAĆANJE POREZA U SRBIJI

THE IMPORTANCE OF A UNIQUE INFORMATION SYSTEM FOR PAYING TAXES IN SERBIA

Vesna Aleksić
Pravni fakultet Univerziteta Union u Beogradu, Beograd

Apstrakt

Cilj rada je da prikaže kako primena integrisanog informacionog sistema povećava efikasnost i bezbednost sistema, unapređuje poslovanje unutar Poreske uprave, ali i poslovanje Poreske uprave sa drugim državnim institucijama i korisnicima njenih usluga. Informacione i komunikacione tehnologije koriste se za poslove planiranja i upravljanja projektima informacionih tehnologija na nivou Poreske uprave. Modernizaciju i razvoj IT administracije je prioritetni zadatak ove državne institucije, a da bi u tome uspela, Poreska uprava sarađuje sa organima i organizacijama kao i sa stranim tehničkim misijama koji su uključeni u projekat uvođenja E uprave u organe državne uprave.

***Ključne reči**: porezi, poreska uprava, informacione tehnologije, e-uprava, državna uprava*

Abstract

The aim of the paper is to demonstrate that the implementation of an integrated information system increases the efficiency and security of the system, improves the operations within the Tax Administration, as well as the operations of the Tax

Administration with other state institutions and users of its services. Information and communication technologies are used for the planning and management of information technology projects at the Tax Administration level. Modernization and development of IT administration is a priority task of this state institution, and to succeed, the Tax Administration cooperates with authorities and organizations as well as with foreign technical missions involved in the project of introducing E administration into state administration bodies.

***Keywords**: taxes, tax administration, information technology, e-government, state administration*