SOUDNÍ INŽENÝRSTVÍ

Prof. Ing. Jiří Dvořák, DrSc.
Ing. et Ing. Jiří Konečný, Ph.D.
Ing. Martina Janková, BA (Hons)

Kybernetická bezpečnost jako součást kyberprostoru moderní znalostní společnosti

Cyber Serurity as a Part of Cyberspace of Modern Knowledge Society

ABSTRAKT: V příspěvku jsou stručně uvedeny některé vybrané možnosti kybernetické bezpečnosti z pohledu systémové integrace útoků a obrany. Vše především z nového pohledu aktuálního kyberprostoru uvedeného v Kybernetickém zákonu a aplikacích Agentury pro kybernetickou bezpečnost a také spolupracujících podniků v této oblasti. Cílem příspěvku je především upozornit odborníky na nepochopení veřejnosti v oblasti modelování moderního řízení systémů a sdělování informace v živých a neživých organismech. Dále na možné a nové užití kybernetického prostoru při modelování kybernetických útoků a vytváření modelových variant obrany objektů. Moderním přístupem je vyjádření prostorů systémově vymezených aktivit. V tomto příspěvku je to možnost další identifikace kybernetických útoků v sektoru daném kyberprostorem. Dále tvorby odolných a později inteligentních prostředků aplikované bezpečnostní kybernetiky.

KLÍČOVÁ SLOVA: aplikovaná kybernetika, modelování systémů, kybernetické útoky, kyberprostor, rizikové řízení, soudní inženýrství

ABSTRACT: The paper briefly mentions some selected options of cyber security from the perspective of system integration of attacks and defence. Everything primarily from a new perspective of current cyberspace mentioned in Cyber law and applications of Agency for cyber security and also cooperating companies in this field. This paper aims primarily to draw experts' attention to the public misunderstanding in field of modelling modern management systems of information communicating in living and non-living organisms. Furthermore, to possible and new use of cyberspace for modelling cyber attacks and creating model variants of objects' defence. Modern approach is the expression of space systemically defined activities. In this paper, it is possibility of further identification of cyber attacks in a sector given by cyberspace. Also, the creation of durable and later on intelligent means of applied safety cybernetics.

KEYWORDS: applied cybernetics, systems modeling, cyber attacks, cyberspace, risk management, forensic engineering

1. ÚVOD

Na prahu 21. století je světová ekonomika konfrontována s řadou výzev v prostředí charakterizovaném procesy informatiky (informačních a komunikačních technologií – ICT), kybernetiky (teoretické, technické a aplikační), robotiky (robototechnikou, mechatronikou a umělou inteligencí učících se robotických systémů), globalizací a novými technologiemi (pramenícími z pochopení a rozvoje fyziky, matematiky, teoretické a prakticky aplikované kybernetiky – například také simulace). Je také významně ovlivňována dynamikou zavádění nových vědeckých poznatků do praxe a rozvíjením progresivních technologických postupů, nových systémových poznatků a vybraných možnosti kybernetické bezpečnosti z pohledu systémové integrace útoků a obrany a to především z nového pohledu aktuálního kyberprostoru moderní společnosti.

Smyslem je především moderní užití kybernetického prostoru při modelování kybernetických útoků a vytváření modelových variant zejména kybernetické obrany objektů. Moderním přístupem je vyjádření prostorů systémově vymezených aktivit – je to možnost další identifikace kybernetických útoků vedenými inteligentními například robotickými bezpilotními prostředky v sektoru daném kyberprostorem moderní společnosti, dále pak tvorby odolných a později také inteligentních prostředků aplikované bezpečnostní kybernetiky.

2. MOŽNOSTI SYSTÉMOVÉHO PŘÍSTUPU KE KYBERNETICKÉ BEZPEČNOSTI

Vznik znalostně založené ekonomiky [1], [6], [8] je charakterizován širokým záběrem procesu intenzifikace inovační aktivity. Tento

Dodáno autory do redakce 14. 9. 2017. • Recenzní řízení od 20. 9. do 9. 10. 2017.

Prof. Ing. Jiří Dvořák Jiří, DrSc., Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení, Ústav krizového řízení, Studentské nám. 1532, 686 01 Uherské Hradiště, e-mail: dvorakji@centrum.cz
Ing. et Ing. Jiří Konečný, Ph.D., Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení, Ústav krizového řízení, Studentské nám. 1532, 686 01 Uherské Hradiště, e-mail: konecny@flkr.utb.cz
Ing. Martina Janková, BA (Hons), Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky, Kolejní 2906/4, 612 00 Brno, e-mail: martina.jankova@email.cz

proces probíhá napříč ekonomickými a dalšími sektory a odvětvími v podobě technologických změn.

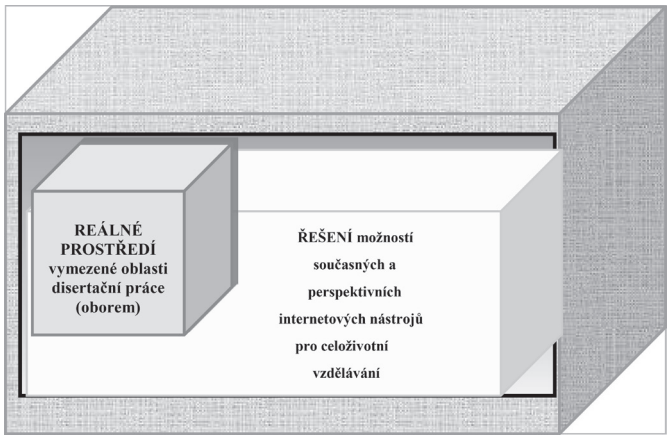
Management znalostí s bezpečnosti systémů se stává klíčovou složkou strategického managementu, mění způsob fungování podniků včetně samotného dynamického rozvoje inteligentních roboto-technických prostředků kybernetické bezpečnosti v moderní společnosti; bude se podílet na předpokládaném novém pojetí „*elektronické osoby*“ pro řešení soudním znalcem, zejména při posuzování odpovědnosti za vznik a řešení krizových stavů v uvedených kybernetických systémech a začleňování uvedeného prostředí do soudního inženýrství.

Přechod ke znalostně založené ekonomice je rovněž spojen s významnými celospolečenskými dopady. Jde tedy o proces velmi komplexní, systémově vymezený. Vyžaduje nové znalosti, mění pracovní a životní podmínky a ovlivňuje i nerovnost mezi skupinami obyvatelstva.

V ekonomice tažené znalostmi sehrává klíčovou úlohu [1] dostupnost kvalitního lidského kapitálu. Vybavenost bezpečnými informačními a komunikačními technologiemi tedy přestavuje významnou příležitost pro získání znalostí jako zdrojů konkurenceschopnosti. Nové technologie umožňují přechod na novou růstovou trajektorii pouze za předpokladu, že jsou provázeny dlouhodobou dostupností vysoce kvalifikované pracovní síly a dochází ke vzniku tzv. znalostních pracovníků (Knowledge Workers). Nedostatečné investice do lidských zdrojů se často stávají omezujícím faktorem inovačního a ekonomického úspěchu.

Konkurenceschopnost podniků [1], [9] je pak systémově charakterizována jako schopnost soustavně vykazovat růst produktivity, tj. dosahovat s omezenými vstupy práce a kapitálu vyšších výstupů. Konkurenceschopnost se projevuje získáním, udržením a zvyšováním podílu na trhu. Tato schopnost závisí na vývoji, technologickém pokroku a zlepšování kvalifikace pracovních sil.

Konkurenční prostředí je hlavní hnací silou inovací a také prostředím pro nové pojetí „*Kybernetické bezpečnosti jako součásti kyberprostoru moderní společnosti*“. Kybernetika (jako „*oblast řízení a sdělování v živých a neživých organismech*“ – Norbert Wiener, 1946) a v moderním systémově vymezeném prostředí jsou



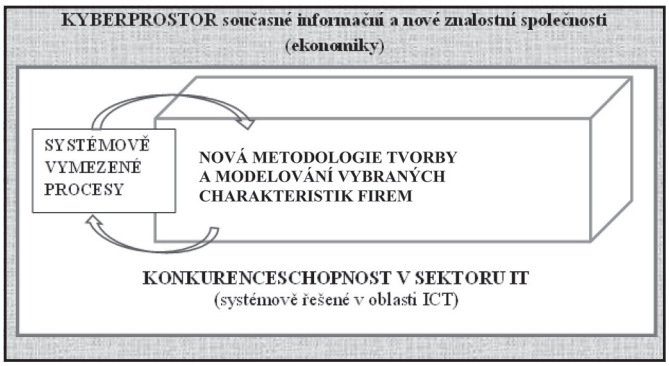
Obr. 1 Systémové vymezení vybraných oblastí pro řešenou problematiku v kyberprostoru informační a znalostní ekonomiky. Zdroj: [3].
Figure 1 System definition of selected areas to tackle in cyberspace information and knowledge economy. Source: [3].

to především nové informační (například Internetové) technologie, umožňující ve virtuálním prostředí informačních zdrojů světa nalézat potřebné znalosti v nově zavedeném kybernetickém prostoru (kyberprostoru) definovaném v zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (*zákon o kybernetické bezpečnosti*)[1)]. Dále souvisejícími oblastmi zkoumání jsou řízení lidských zdrojů (Human Resource) a řízení znalostí (Knowledge Management).

3. MODELOVÁNÍ BEZPEČNOSTI V KYBERPROSTORU SPOLEČNOSTI

Ověřované modelování pro uvedenou oblast kyberprostoru má tyto charakteristiky [2], [4]:

- vyjádření metodologie tvorby systémově pojaté a podložené moderním kybernetickým přístupem k řízení možného modelu,
- vyjádření jako sociální a technické rozhraní se zpětnovazebními aktivitami v systémovém pojetí pro zvolenou oblast řízení a ekonomiku konkurenceschopného podniku (v kyberprostoru moderní společnosti),
- vyjádření metodologie pro využití vybraných nástrojů a orientování se na dynamické vysoce hierarchicky členěné kybernetické systémy vzdělávání manažerů a znalostních pracovníků vybrané firmy,
- průběžné vytvoření a zdokonalování metodologie nového pojetí kybernetických modelů a postupně vytvářeném modelu na PC s novou konkurenceschopností.



Obr. 2 Metodologie modelování útoků a obrany v kyberprostoru. Zdroj: [3].
Figure 2 Methodology modeling of attacks and defense in cyberspace. Source: [3].

4. SYSTÉMOVÉ POJETÍ MODELOVÁNÍ PODLE METODOLOGIE

Cílem moderního přístupu k vymezení současné aktuální problematiky [5], [7] vyjádřené názvem příspěvku „*Kybernetická bezpečnost jako součást kyberprostoru moderní společnosti*“

[1)] § 2: V tomto zákoně se rozumí a) kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.

bude především ve výchově odborníků na vysokoškolské úrovni poskytnout čtenářům požadovaný integrující profil aplikované kybernetiky v rozsáhlém kyberprostoru bezpečnosti a to především cílevědomým rozvojem jejich znalostí teoretických disciplín jako *Teorie systémů* (v oblasti nejen informačních a komunikačních technologií – ICT, ale především chápání abstraktních systémů), *Teorii modelů a modelování* (v oblasti možnosti tvorby nejenom algoritmů a modelů počítačů a počítačových sítí na základě znalostí vysokoškolské matematiky a fyziky), *Kybernetiky* (v oblasti řízení, ale také v chápání obecnějších a aplikovatelných systémově vymezených modelů v technických a sociálně-technických prostředích), *Aplikované kybernetiky* (v oblasti moderní konstrukce modulárních PC a bezpečných počítačových sítí), *teorii Simulace a simulátorů* (s ohledem na efektivní vzdělávání profesionálů pro informační a znalostní společnost), *Kybernetické bezpečnosti* (v oblasti systémově vymezené kyberprostoru určeném pro tvorbu a užití datových a stavových prostorů a jejich odolnosti proti kybernetickým útokům a všem dalším formám kybernetické války), *Systémů utajování citlivých informací a dat a užití moderní kryptografie* (v oblasti bezpečné komunikace mezi systémy a zálohování struktur a chování rozsáhlých hierarchicky členěných dynamických systémů), *Vědy, výzkumu*, *inovací*, *vzdělávání a nových technologií a techniky* (v oblasti vývoje nových a perspektivních technologií v oblasti ICT a širším okolí systémů v informační a znalostní společnosti a samozřejmě užití prostředků Umělé inteligence).

Společným prostředím bude integrující směr daný teoretickou kybernetikou jako oborem pro řízení a sdělování informací v živých a technických objektech sjednocující uvedené oblasti a na základě systémového vnímání kybernetické bezpečnosti vycházející ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

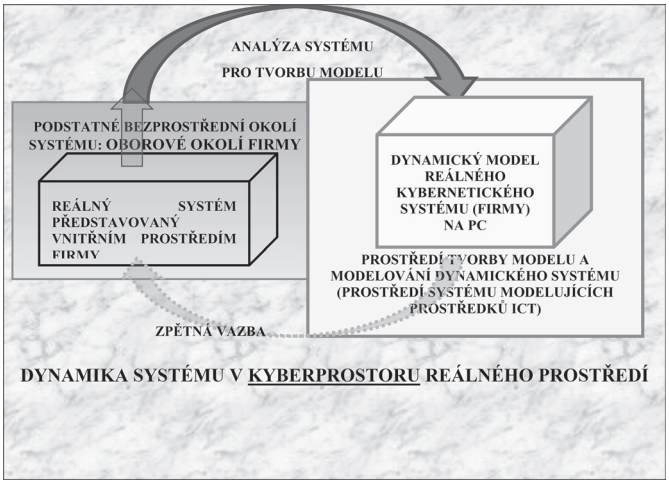
Základním cílem tohoto zákona je zvýšit systémově pojatou mezioborovou bezpečnost v kybernetickém prostoru a ochránit tu část infrastruktury, která je pro fungování státu důležitá a jejíž narušení by vedlo k poškození nebo ohrožení zájmu České republiky. Zákon stanovuje, jakým způsobem má být kybernetická bezpečnost zajištěna a určuje způsob reakce na kybernetické hrozby nebo řešení nastalého incidentu.

Profilující oblasti vzdělávání musejí mít minimální obsahové standardy v krizovém řízení, v analýze rizik, bezpečnostní politice a prevenci kriminality, ochraně obyvatelstva, ekonomice krizových situací, aplikované informatice; cílem vzdělávání odborníků je poskytnout základní teoretické zázemí v oblasti informačních a komunikačních technologií, umožnit jim pochopit role informačních technologií v řídící a rozhodovací činnosti a orientovat je v produktech a technologiích. Poskytnout komplexní pohled na charakter, obsah, možnosti i nároky současných a budoucích informačních systémů, zajistit pochopení širších souvislostí rozvoje a provozu informačních a komunikačních technologií. Poskytnout jim potřebné vstupní praktické zkušenosti s vybranými typy informačních a komunikačních technologií i na úrovni odpovídajících aplikací. Efektivně kooperovat a komunikovat se specialisty z oblastí: zpracování dat, bezpečnosti počítačových sítí a obecně všech současných i perspektivních informačních systémů, dále také z oblastí bezpečnostní politiky a prevence kriminality (právních norem a opatření ve věcech vnitřního pořádku a bezpečnosti, mezinárodní dimenze bezpečnosti), z oblasti analýzy rizik (řízení rizik a řízení bezpečnosti území), z oblasti krizového managementu (bezpečnosti a bezpečí systémů, bezpečnostní systém a krizové řízení ČR, řízení bezpečnosti a rozvoje území) a další oblasti.

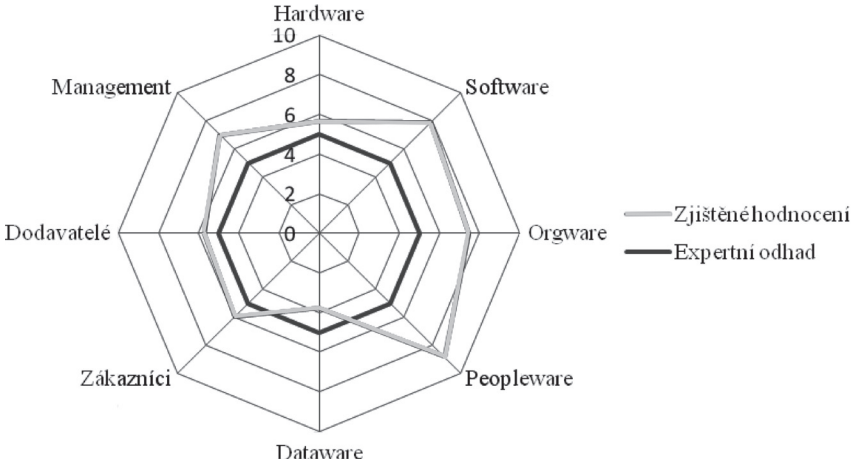
Cílem je pochopit a rozvíjet na základě znalostí teoretických přístupů nové možnosti aplikované kybernetické bezpečnosti a tak mohou současní a budoucí doktorandi, vědeckopedagogičtí pracovníci různých oborů a specializací a také řešitelé vědeckých úkolů vycházet z aktuálního a tedy moderního pojetí prostředí informační a rozvíjející znalostní společnosti, která bude stále více preferovat systémová a teoretická vymezení prostředí výzkumu a vzdělávání s cílem zachycení podstatného vlivu na existenci reálně definovaných systémů.

Nová uskupení znalostního přístupu k celoživotnímu vzdělávání budou vymezována prostředím časoprostorových a hraničních kybernetických prostorů daných zde dynamikou logistiky a krizovým řízením a také riziky odvíjejícími se od optimálních a stabilních systémů světa se svým reálným časem a v sociálně-technickém prostředí nazývaným kybernetickým prostorem (kyberprostorem) naplňujícím přijatý a realizovaný „*Kybernetický zákon*“.

V zájmovém kyberprostoru musí být postupně definovány nové technické a technologické úlohy transformací informací především v oblasti dnešních aplikací informačních a komunikačních systémů. Cílem musí být hluboké osvojení základních a vhodných prostředků komunikace mezi systémy a pochopení moderních principů systémového a kybernetického přístupu k tvorbě modelů a modelování bezpečných reálných systémů, jejich diagnostikování a obnovy zejména při aplikacích logistiky a krizového řízení na pozadí elektroniky, optoelektroniky a v budoucnosti bioniky a také v budoucích projektech s umělou inteligencí spojených s rozvojem inženýrských přístupů pro zajímavou a potřebnou systémovou integraci na pozadí aktivní kybernetické bezpečnosti (inteligentních roboto-technických prostředků).



Obr. 3 Systémové vyjádření analýzy pro tvorbu modelu reálného prostředí. Zdroj: [3].
Figure 3 System expression analysis to create models of real environments. Source: [3].

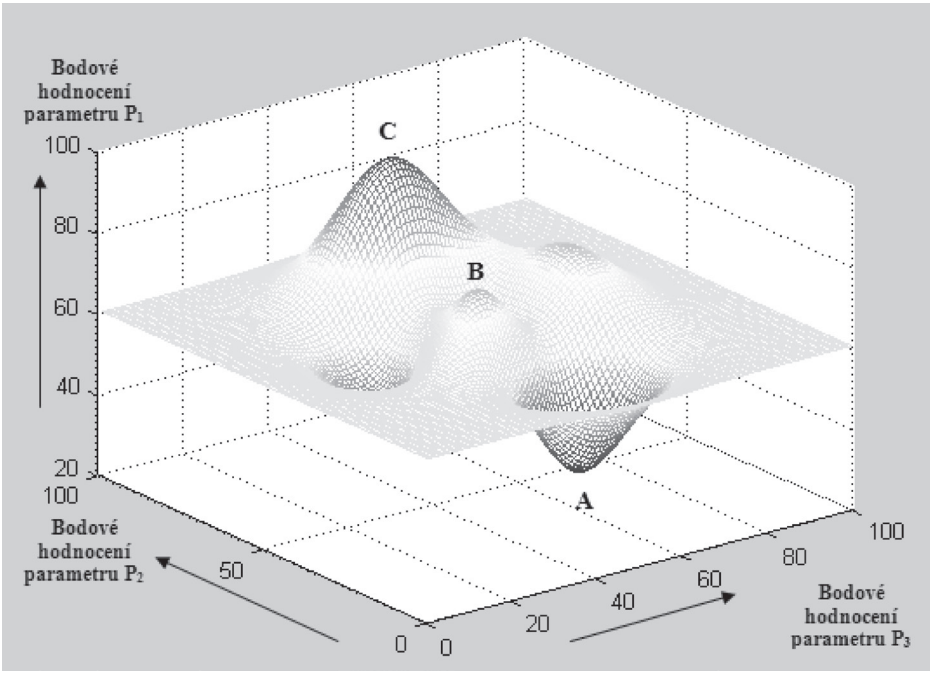


Obr. 4 Měření konkurenceschopnosti vybraného podniku 2 – informační kritérium. Zdroj: [3].
Figure 4 Measurement of competitiveness chosen company 2 – information criterion. Source: [3].

5. DÍLČÍ VÝSLEDKY MODELOVÁNÍ

Podle modelu Harryho Pollaka [3] užité v praktickém modelování kritérií konkurence-schopnosti podniků. Dalším významným úhlem pohledu na řešení praktického modelu a případně krizových situací. Nezbytnou součástí vědeckovýzkumné práce jsou také dílčí poznámky vyplývající z pohledu na moderní prostředí konkurenceschopnosti a doporučení vnímat také prostředí modelování bezpečnosti a to jak informační, tak obecně pojatou bezpečnosti podle zákona č. 181/2014 Sb. Prostřednictvím [3] dotazníkového šetření (obr. 4) byla zjištěna hodnota informačního kritéria podniku 2, která činí 52,28 bodů tj. vitalita podniku je nalomena, musí dojít ke změně. Odchylka mezi očekávanou a zjištěnou hodnotou je 12,28. Pro porovnání konkurenceschopnosti [3] mezi podnikem 1 (etalonem) a podnikem 2 (zákazníkem – vhodně vybranými zákazníky podniku 1) byla použita metoda benchmarking jako nástroj řízení kvality formou zlepšování učením se od druhých. Tento porovnávací ukazatel obsahuje ekonomické, informační, inovační a vzdělávací kritérium.

Na základě uvedeného řešení [3] byly hodnoty spolehlivost dodavatelů, dataware, náklady na rozvoj vědy a výzkumu a dosažené vzdělání označeny jako rizikové (mezní, hraniční) hodnoty, které je nutné stále sledovat. Jedná se o *„slabá“* místa podniku 2 (zákazníků). Management typického podniku 2 musí přijmout nezbytná opatření k eliminaci těchto faktorů, která negativně ovlivňují úroveň konkurenceschopnosti. Podnik 1 (etalon) je o 44,55 bodů lepší než podnik 2 (současný zákazník). Podnik 1 byl tedy správně vybrán jako etalon (školící podnik). Úspěch procesu inovace podniku 2 vychází z předpokladu, že podnik 1 může poskytnout kvalitnější nabídku svých prostředků



Obr. 5 Možný pouze ilustrativní výsledný proces konkurenceschopnosti podniku. Zdroj: [3].
Figure 5 A possible illustrative process resulting competitiveness. Source: [3].

a metod při výstavbě a užívání internetového i intranetového prostředí a celoživotního vzdělávání podniku 2 (zákazníkovi).

6. ZÁVĚR

V příspěvku jsou stručně uvedeny některé vybrané možnosti posouzení konkurenceschopnosti dvou podniků v podmínkách rozvíjejících se principů kybernetické bezpečnosti. Cílem příspěvku je především upozornit odborníky na možné systémové vymezení reálného prostředí v nově pojatém kyberprostoru moderní společnosti. Moderním přístupem je právě modelování konkurenceschopnosti v kyberprostoru dvou podniků s cílem možného nalezení kybernetických možných útoků v sektoru daném kyberprostorem a námětem v jakých oblastech vytvářet kybernetickou obranu a to podle kritérií konkurenceschopnosti podniků 1 a 2 a tím dát podklady pro zdůvodnitelné vytváření kybernetické bezpečnosti v sektoru působnosti analyzovaných firem. Tím také přispět k vytváření nových odolných a později inteligentních prostředků aplikované bezpečnosti a podílet se také na novém pojetí předpokládaných a dalších možných vymezení právních norem soudního inženýrství a zejména s ohledem na systémové hodnocení konkurenceschopnosti podniků a jejich posuzování soudními znalci v oblastech právní a zejména ekonomické a kybernetické stability prostředí ve znalostní společnosti.

7. Poděkování

Příspěvek je výstupem projektu specifického výzkumu „*Efektivní využití ICT a kvantitativních metod pro optimalizaci podnikových procesů*“ Interní grantové agentury Vysokého učení technického v Brně s registračním číslem FP-S-15-2787 a Specifického výzkumu na FLKŘ grantové agentury UTB ve Zlíně.

Příspěvek byl publikován ve Sborníku příspěvků z konference Krizové řízení a řešení krizových situací 2016, ISBN 978-80-7454-632-7, zde doplněn a aktualizován.

Příspěvek spadá podle vyhlášky č. 123/2015 Sb. pod obor kybernetika a dále do nové oblasti možné výpočetní techniky pro informační a kybernetickou bezpečnost soudního inženýrství.

7. LITERATURA

[1] BAREŠOVÁ, A.: *E-learning ve vzdělávání dospělých*. 1. vyd. Nakladatelství VOX, Praha, 2003. 174 s. ISBN 80-86324-27-2

[2] JANÍČEK, P., MAREK, J.: *Expertní inženýrství v systémovém pojetí*. Professional Publishing, Praha, 2013. ISBN 978-80-247-4127-7

[3] JANKOVÁ, M.: *Internetové nástroje pro celoživotní vzdělávání v sektoru IT*. Vysoké učení technické v Brně, Fakulta podnikatelská, Brno, 2016. 234 s.

[4] JANKOVÁ, M., DVOŘÁK, J.: Options of Electronic Commerce Modelling in a Cyberspace of New Economy. In: *EBES Conference.* EBES, Rusko, Ekaterinburg, s. 43–51. ISBN 978-605-64002-3-0

[5] JANKOVÁ, M., DVOŘÁK, J.: The ICT possibilities in the virtual universities cyberspace. In: *Mathematics, Information Technologies and Applied Sciences 2014 (post-conference proceedings of selected papers extended versions)*. MITAV, Brno, 2014, s. 59–65. ISBN 978-80-7231-978- 7

[6] KADEŘÁBKOVÁ, A.: *Výzvy pro podnikání – inovace a vzdělání*. 1. vyd. Linde, Praha, 2004. 199 s. ISBN 80-86141-50-5

[7] KŘUPKA, J.: *Základy technickej kybernetiky*. Akadémia ozbrojených síl gen. M.R. Štefánika, Liptovský Mikuláš, 2008. ISBN 978-80-8040-357-7

[8] PETŘÍKOVÁ, R.: *Moderní management znalostí*. Professional Publishing, Praha, 2010. ISBN 978-80-7431-011-9

[9] SMEJKAL, V., RAIS, K.: *Řízení rizik ve firmách a jiných organizacích.* Expert. Grada Publishing, a.s., Praha, 2013, 466 s. ISBN 978-80-247-4644-9