CONFERENCE

CRISCON

WWW.KRIZOVERIZENI-UH.CZ

KRIZOVÉ ŘÍZENÍ A ŘEŠENÍ KRIZOVÝCH SITUACÍ

13. - 14. 9. 2018

FLKŘ UHERSKÉ HRADIŠTĚ

CRISIS MANAGEMENT AND CRISIS SITUATIONS SOLUTIONS

ISBN 978-80-7454-821-5

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

Zlínský kraj

Uherské Hradiště
Srdce Slovácka

Název: Krizové řízení a řešení krizových situací

Konference Krizové řízení a řešení krizových situací se konala ve dnech 13. a 14. září 2018 v Uherském Hradišti pod záštitou rektora UTB ve Zlíně prof. Ing. Petra Sáhy, CSc., rektora VUT v Brně prof. RNDr. Ing. Petra Štěpánka, CSc., hejtmana Zlínského kraje Jiřího Čunka a starosty Uherského Hradiště Ing. Stanislava Blahy.

Title: Crisis Management and Crisis Situation Solutions

The Conference Crisis Management and Crisis Situation Solutions took place on the 13th and 14th September 2018 in Uherské Hradiště under the auspices of the TBU Rector Petr Sáha, Rector of BUT Petr Štěpánek, Governor of the Zlín Region Jiří Čunek and Mayor of Uherské Hradiště Stanislav Blaha.

Editor / Edit by:
Ing. et Ing. Jiří Konečný, Ph.D.

Recenzenti / Reviewers:

doc. Ing. Vladimír Adamec, CSc., prof. Ing. Jiří Dvořák, DrSc., Ing. et Ing. Jiří Konečný, Ph.D., Ing. Mgr. Jindřich Kučera, prof. Ing. Vieroslav Molnár, PhD., Ing. Robert Pekaj, doc. Ing. Radim Roudný, CSc., Mgr. Marek Tomaštík, Ph.D., doc. Ing. Zuzana Tučková, Ph.D., Ing. Jan Valouch, Ph.D., Ing. Pavel Viskup, Ph.D.

Garant / Guarantor:

Ing. et Ing. Jiří Konečný, Ph.D. – UTB ve Zlíně, Fakulta logistiky a krizového řízení

Vydavatel / Publisher:
Univerzita Tomáše Bati ve Zlíně / Tomas Bata University in Zlín
ISBN: 978-80-7454-821-5

Uherské Hradiště 2018

OBSAH

ŘÍZENÍ RIZIK LOGISTICKÝCH PROJEKTŮ V PODMÍNKÁCH PODNIKÁNÍ FIREM V ČESKÉ REPUBLICE

RISK MANAGEMENT OF LOGISTICS PROJECTS IN BUSINESS OF CONDITIONS OF COMPANIES IN THE CZECH REPUBLIC

Ing. Tereza Belantová
Univerzita Tomáše Bati ve Zlíně, Fakulta managementu a ekonomiky
Mostní 5139, Zlín, 760 01
belantova@utb.cz

ABSTRAKT

Logistika se stává rychle se rozvíjejícím odvětvím s nepřeberným množstvím logistických projektů, které s sebou přináší nová neidentifikovaná rizika, která bez jakéhokoliv ošetření můžou dosáhnout takových rozměrů, až budou pro společnost likvidační. Cílem článku je prezentace záměru disertační práce, která se zabývá řízením rizik logistických projektů v podmínkách podnikání firem v České republice. Práce dále poukazuje na reálná rizika vyskytující se v logistických projektech u firem podnikajících na českém trhu a taky poukazuje na důležitost procesu řízení rizik projektů.

KLÍČOVÁ SLOVA

logistika, projekt, riziko

ABSTRACT

Logistics is becoming a fast growing industry with endless amount of logistics projects, which brings new unidentified risks that can achieve of such dimensions without treatment that they will cause destruction of the company. The purpose of article is presentation of intention of dissertation which deals with risk management of logistics projects in business conditions of companies in the Czech Republic. In the thesis I would like to point out the real risks which occur in logistics projects of companies who are doing business on the Czech market and I would like to point out the importance of the process of project risk management too.

KEY WORDS

logistics, project, risk

ÚVOD

Jak jednoduché je vstoupit na trh s novým výrobkem či službou, o to složitější je se na trhu udržet a prosperovat. Výrobci potřebují neustále vyrábět, obchodníci neustále prodávat a zákazník chce své zboží v co nejvyšší kvalitě a v co nejkratším čase mít u sebe. Splnění všech požadavků vyžaduje komplexní řešení. Řešením se stala logistika, která s rostoucími požadavky všech subjektů získává na významu. Jedná se o rychle se rozvíjející odvětví, jehož rozvoj s sebou přináší nová neidentifikovaná rizika. Pokud nedojde k včasné identifikaci a následnému ošetření těchto rizik, může se stát, že jejich projev nabyde takových rozměrů, až bude pro společnost likvidační.

Logistický projekt si můžeme představit jako jedinečnou sadu úkolů, jejichž účelem je provedení opatření, která mají dopad na změnu logistického systému. Takové a podobné definice najdeme především u polských autorů. Tuzemští a ostatní autoři však nepoužívají

pojem logistické projekty, nýbrž v odborné literatuře najdeme spíše pojmy zaměřující se na logistiku ve městech než na celkové pojetí logistických projektů.

1. ZAMĚŘENÍ OBLASTI ZÁJMU A OBSAHU PRÁCE

V poslední době je logistika považována za relativně rychle se rozvíjející odvětví se vznikem nových neidentifikovaných a tudíž neošetřených rizik. Vetší společnosti mají pro analyzování potenciálních rizik odborníky, nebo dokonce celá oddělení odborníků, kdežto pro menší společnosti a drobné podnikatele nemusí být otázka řízení rizik zcela jasná.

Oblast zájmu mé práce se bude věnovat řízením rizik logistických projektů v podmínkách podnikání firem v České republice. Budou vytipovány společnosti podnikající v oblasti logistiky, na jejichž projektech bude aplikován postup řízení rizik podle ISO 31000. Na základě využití moderních metod posouzení rizik budou identifikována, analyzována a ohodnocena významná rizika nacházející se v logistických projektech a na základě praktických zkušeností s aplikací vybraných metod projektového managementu, budou navrhnuty doporučení v uvedených rizikových oblastech, respektující specifika logistických projektů realizovaných ve firmách podnikající v České republice.

Tímto bych chtěla poukázat na reálná rizika vyskytující se v logistických projektech realizovaných firmami v České republice, dále poukázat na proces řízení rizik projektů a implementací navržených opatření, eliminovat rizika, případně snížit negativní dopad těchto rizik na minimum. Řízení rizik projektů považuji za důležitou oblast v podnikání, které by se mělo věnovat větší pozornosti, aby se předcházelo vzniku rizik s negativním dopadem případně, aby tento dopad byl zmírněn. Pokud společnosti podnikající v podmínkách podnikání v České republice budou více obeznámeny s postupy řízení rizik projektů, které v sobě zahrnují identifikaci rizik až po samotné ošetření rizik, můžou odvrátit či zmírnit nemalé finanční ztráty, které jsou důsledkem vzniklých a neošetřených rizik jejich projektů. Dále bych chtěla definovat pojem logistický projekt, protože definice tohoto pojmu můžeme nalézt ve velké míře u polských autorů, nikoliv však u českých autorů. Možnou příčinou proč není pojem logistický projekt v českých podmínkách definován, je malý zájem o tuto problematiku, kterou bych se chtěla zabývat a více dostat do podvědomí nejenom logistických firem, ale i veřejnosti.

2. CHARAKTERISTIKA SOUČASNÉHO STAVU ŘEŠENÉ PROBLEMATIKY

Vývoj logistiky je nyní ve stadiu, kdy se stává nedílnou a významnou součástí řízení dodavatelských systémů typických nejen horizontálním a vertikálním rozšířením původních logistických systémů a zapojením reverzních toků, ale zejména integrací manažerských funkcí v podniku a spolupracujících subjektů s cílem dosažení kvality dodávaných služeb zákazníkům [1]. Logistika je velmi široký pojem, ke kterému se vztahuje řada definic. Zahraniční společnosti formulují logistiku následovně. Podle Chartered Institute of Logistics and Transport [2] je britská logistika definována jako *"postup navrhování a řízení dodavatelských řetězců včetně nákupu, výroby, skladování a přepravy"* oproti tomu německý Bundesvereinigung Logistik [3] ji vymezuje jako *„celkové plánování, řízení a uskutečňování všech informačních a zbožových toků podniků a hodnototvorných řetězců (supply chains) se zásadním vlivem na podnikový úspěch“*. Švýcarský International Institute for the Management of Logistics [4] definuje logistiku jako *„operační a strategický nástroj“, „výtečný nástroj pro soukromé nebo veřejné společnosti k systematickému zkvalitňování souladu s přáním zákazníků, zlepšování flexibility výroby, vytváření celistvé organizace s partnery, poskytovateli služeb, spolupracujícími firmami, distributory a zákazníky.“* European

Committee for Standardization [5] ji definují jako *„plánování, provádění a kontrolu pohybu a rozmístění lidí a/nebo zboží a podpůrných aktivit, spojených s takovýmto pohybem a rozmístěním, v systému organizovaném k dosažení určitých cílů.“* Z výše uvedených definic je patrné, že odvětví logistiky je široce obsáhlé a zahrnuje činnosti od výroby, přes skladování, dopravu, dále plánování všech procesů v podniku včetně toku informací a rozmístění osob, s využitím jak v soukromém, tak veřejném sektoru.

Čeští autoři, zabývající se problematikou logistiky, logistiku definují následovně: *„Logistika je postup, jak řídit proces plánování, rozmisťování a kontroly materiálových a lidských zdrojů vázaných ve fyzické distribuci výrobků odběratelům, podpoře výrobní činnosti a nákupních operací“* [1]. Pernica [6] shledává logistiku jako proces plánování, realizace a řízení toků a skladování zboží, služeb a souvisejících informací z místa vzniku do místa spotřeby s cílem uspokojit požadavky zákazníků. Autoři Stehlík a Kapoun konstatují: *„Logistika znamená systematické plánování, organizování, řízení a kontrolu všech toků fyzických objektů a s nimi spojených informací do podniku a logistického systému, skrze něj až k zákazníkům, tj. partnerům a až k finálním uživatelům a spotřebitelům.“* A dodávají: *„K logistice patří všechny činnosti, které plánují, řídí, provádějí nebo kontrolují prostorově časovou transformaci zboží a s ní související transformace týkající se množství a druhu zboží, vlastností manipulace se zbožím a logistických determinantů zboží. Jejich vzájemnou souhrou se má uvést do chodu tok objektů tak, aby bylo místo odeslání a místo příjmu spojeno co nejefektivněji“* [7]. Obecně tedy můžeme říci, že se logistika zabývá pohybem zboží a materiálu z místa svého vzniku na místo spotřeby i se souvisejícím informačním tokem.

Ze států střední Evropy má Česká republika jedinečné postavení hned z několika hledisek. Jedná se o dobrou geografickou polohu, je zde dobrá dopravní infrastruktura a velké logistické firmy lákají především nízké mzdy a kvalifikovaní zaměstnanci. V dnešní době můžeme v regionu najít prakticky všechny velké globální i evropské logistické firmy a odborníci se domnívají, že příznivý rozvoj logistiky bude i nadále pokračovat. Česká republika podporuje logistiku zejména v oblasti budování dopravní infrastruktury pro nákladní dopravu. V rámci středoevropských zemí je výhodou logistiky v České republice vysoká úroveň pro provádění logistických procesů avšak problémem je nedostatečný počet veřejných logistických center, umožňující převážet zboží pomocí několika druhů dopravy. Do budoucna bude logistiku ovlivňovat rozvoj nových informačních technologií a pokračující digitalizace. [8]

3. LOGISTICKÉ PROJEKTY

Po provedené literární rešerši byl pojem logistický projekt nalezen především u polských autorů. Jedním z autorů definujících pojem logistický projekt je autorka Pisz, která pojem definuje následovně: *Logistický projekt lze definovat jako komplexní, zvláštní a jedinečné soubory činností, které lze popsat technickými a ekonomickými parametry a které jsou určeny náklady, časem a rozsahem, aby pomohly logistickému řízení v podnikovém / dodavatelském řetězci* [9]. Druhá její definice zní takto: *Logistický projekt je mimořádný soubor úkolů lišící se od ostatních projektů časem a náklady, jejichž účelem je provádět jednotlivá a jedinečná opatření, která ovlivňují změnu logistického systému jednoho podniku nebo dodavatelského řetězce, v rámci něhož tento podnik funguje* [10], [11], [12]. Další z mnoha autorů jsou Kisperska-Morón a Krzyżaniak jejichž definice pojmu logistický projekt je následující: *Projekt logistiky může být definován jako plánovaný soubor vzájemně propojených úkolů, které mají být provedeny v pevně stanoveném období, s omezeným rozpočtem a časem, který se provádí za účelem zvýšení efektivnosti a účinnosti toků výrobků a souvisejících informací ve společnostech, dodavatelských řetězcích nebo prostorových systémech* [13].

Ostatní autoři zabývající se projekty v oblasti logistiky, je však nedefinují jako Logistics Project. V odborné literatuře se používají pojmy jako: city logistics project, urban logistics project, reverse logistics project. Nicméně tyto pojmy charakterizují spíše projekty zaměřující se na logistiku ve městech, než na celkové pojetí logistických projektů. Už u samotné definice tohoto pojmu můžeme vidět tzv. research gap. Proto i jedním z mých cílů dizertační práce je definování logistických projektů.

4. ŘÍZENÍ RIZIK

Aby podnik mohl fungovat z dlouhodobého hlediska, měl by fungovat systém řízení rizik. Právě jednou ze základních podmínek konkurenceschopnosti společnosti je zavedení řízení rizik do rozhodovacího procesu [14]. Burke [15] konstatuje, že s rostoucí konkurencí na trhu, s rostoucími technologiemi a s rostoucí mírou změn, získává řízení rizik význam a důležitost. Řízení rizik na projektech je tedy vysvětlováno jako proaktivní přístup, kdy se vědomě pracuje s nejistotami tak, aby nejistoty s negativním důsledkem byly včas rozpoznány a ošetřeny [16]. Jedná se o takovou oblast řízení, která se zaměřuje na analýzu a snižování rizik různými metodami a postupy prevence rizik. Tyto metody a postupy odstraňují současné a budoucí faktory, které by mohly zapříčinit zvýšení rizika. Řízení rizik je systematická a opakující se řada vzájemně propojených činností, s cílem zvládnout potenciální rizika, a tím snížit pravděpodobnost jejich výskytu, nebo snížit jejich dopad. Smyslem řízení rizik je vyvarovat se jakýmkoliv problémům nebo negativním jevům [17] a spočívá v nepřetržitém procesu, odehrávající se ve všech fázích životního cyklu projektu, tzn. od počátečního nápadu až po jeho ukončení a zahrnuje následující procesy:

- Stanovení kontextu
- Identifikaci rizik
- Analýzu rizik
- Hodnocení rizik
- Ošetření rizik
- Monitorování a přezkoumávání
- Komunikace a konzultace [18]

Stanovení kontextu

Cílem kroku stanovení kontextu je zachytit cíle organizace, prostředí, ve kterém usiluje o své cíle, její zainteresované strany a různorodost kritérií rizik – to všechno pomůže odkrýt a vyhodnotit povahu a komplexnost jejích rizik. [19]

Identifikace rizik

Identifikace rizik je prvním a nejdůležitějším krokem řízení rizik. Rizika musí být idenfitikována ve všech fázích projektu. Začíná se ve fázi zahájení projektu, kde jsou identifikována první rizika. Jakmile jsou nalezena první rizika, začíná proces řízení rizik, který probíhá, dokud nebude proces uzavřen nebo ukončen. Fázi identifikace rizik si můžeme představit jako transformační proces, ve kterém přeměňujeme vstupy na výstupy. Jako vstupy slouží vnější a vnitřní faktory projektového prostředí. Dále můžeme použít informace z předchozích projektů, kde jsou zaznamenány zkušenosti, vývoj, selhání a rizika. Tyto informace pomáhají identifikovat rizika v novém projektu. [20]

Analýza rizik

Aby bylo možné rizika snížit, musí se nejprve analyzovat. Fáze analýza rizik následuje po fázi identifikace a má stanovit, v jakém rozsahu mohou tato rizika ovlivnit cíle projektu a dále určit priority jejich dalšího ošetření. Důležitým faktorem, který ovlivňuje postup v této fázi je počet identifikovaných rizik. Zde platí, že počet rizik se zvětšuje s růstem rizikovosti projektu a s růstem důležitosti projektu. Cílem této fáze je blíže analyzovat rizika a jejich vzájemné vazby, ohodnotit rizika kvantitativně nebo kvalitativně, ohodnotit celkové riziko projektu a stanovit tak priority k ošetření rizik. [21], [22]

Metody analýzy rizik

Podle způsobu vyjádření veličin, s nimiž se v analýze rizik pracuje, dělíme metody používané v analýze rizik do dvou kategorií – kvantitativní metody a kvalitativní metody. [21]

Použitím metody spadající do kategorie kvalitativních metod, se rizika projektu uspořádají podle jejich důležitosti z hlediska jejich dopadu na projekt a pravděpodobnosti jejich výskytu. Toto uspořádání pomáhá k rozhodování o tom, jaká strategie bude pro zvládnutí každého rizika použita. [18]

Kvantitativní posouzení rizik přináší číselné hodnoty, které měří dopad těchto rizik. [18]

Hodnocení rizik

Hodnocení rizik je nejobtížnější částí analýzy rizik. Od této části celé analýzy se očekává, že analytik shrne rozdělení pravděpodobnosti do jednoho případně několika čísel. V moderní společnosti existuje mnoho různých typů rizik, a tak jedním z hlavních způsobů, jak zobrazit a sdělit míru rizika, je pomocí indexů. Rizikové indexy se stále častěji stávají důležitým prostředkem, který shrnuje riziko pomocí čísel nebo kategorií, jako jsou písmena, slova či barvy. Tyto indexy se používají ke sdělení závažnosti rizik veřejnosti, ukazují, jak se riziko mění v průběhu času, srovnávají s jinými riziky a podporují rozhodování. [23]

Ošetření rizik

Jakmile posoudíme hodnotu rizika a rozhodneme se toto riziko nějak ošetřit, měli bychom se zamyslet, jak budeme na riziko reagovat. Existuje pět hlavních možností jak riziko ošetřit: snížit riziko, vyhnout se riziku, přenést riziko, sdílet riziko nebo udržet riziko. [18], [20]

- **Snížit riziko –** Jedná se o první možnost, která projektové manažery napadne. Využívají se zde techniky, které mají za cíl snížit pravděpodobnost rizika projektu a negativně ovlivnit techniky zmírnění dopadů rizik. Většinou se používají techniky pro snižování pravděpodobnosti. [14]
- **Vyhnout se riziku –** Jde o relativně drastický přístup, kdy se změní celý plán projektu, jen aby se předešlo riziku. [20]
- **Přenést riziko –** Při přenosu rizika je riziko přesunuto nikoliv eliminováno. Dobře známým přístupem k přenosu rizika je uzavírání pojistných smluv. Avšak je třeba poznamenat, že pro řízení projektů to není správný přístup a pojištění podnikatelských rizik je příliš drahé. [20]
- **Sdílet riziko** – Jedná se o přístup, kdy různé strany sdílejí rizika stejného projektu. Tento přístup najdeme často v oblasti logistiky. [20]

- **Udržet riziko** – Pokud je pravděpodobnost rizika malá nebo není možné riziko eliminovat jinými prostředky. V tomto případě je nutné, aby podnik měl dostatečné finanční i časové rezervy a důkladnou přípravu pohotovostních plánů. [14]

Cox [24] poukazuje na to, že výběr mezi různými možnostmi ošetření rizik, by se měl opírat jak o náklady podniku, tak o účinnost každé zvolené možnosti.

Monitorování a přezkoumání

V celém průběhu procesu je nutné rizika neustále sledovat, protože může dojít k nenadálým událostem, jako například, že se změní podmínky, které ovlivní hodnotu pravděpodobnosti, nebo hodnotu škody, případně obojího. Dále může vzniknout nová hrozba či nějaké hrozby můžou pominout a podobně. Sledování rizik bývá často pravidelným bodem při poradách projektových týmů. Dokument, který obsahuje listinu sledovaných rizik, se nazývá registr rizik. [18]

Komunikace a konzultace

Průběžná komunikace a konzultace probíhá od první do poslední fáze procesu řízení rizik a je nutné ji zajistit všemi zainteresovanými stranami, které se na procesu řízení rizik podílejí. Všechny zainteresované strany by mezi sebou měli komunikovat ve všech fázích managementu rizika z důvodů zachycení rozdílného vnímání rizik, které může mít významný vliv na přijímaná rozhodnutí v projektu. [22], [18]

Zatímco většina organizací řídí rizika jen do určité úrovně, mezinárodní norma ISO 31000 stanovuje řadu principů, které je třeba naplnit, aby byl management rizik efektivní. Tato mezinárodní norma doporučuje organizacím rozvíjet, implementovat a kontinuálně zlepšovat rámec, jehož účelem je integrovat proces pro řízení rizik do svého celkového vedení, strategie a plánování, managementu, procesů podávání hlášení, politik, hodnot a kultury. [19]

ZÁVĚR

Výše napsaný článek pojednává o předmětu zkoumání budoucí disertační práce, jejíž obsah se zaměřuje na řízení rizik logistických projektů v podmínkách podnikání firem v České republice. Budou představené základní východiska s důrazem na oblast projektových rizik v logistických projektech. U logistických projektů bude aplikován podrobný postup řízení rizik podle normy ISO 31000, na jehož závěru budou pomocí vybraných metod identifikována rizika vyskytující se v projektech logistických firem a dále budou tyto rizika analyzována. Po vypracované analýze zjištěných rizik budou rizika následně ohodnocena a zařazena do vytyčených oblastí závažnosti podle zjištěných hodnot. V rámci postupu řízení rizik budou vybrány možnosti jak identifikované, analyzované a ohodnocené rizika ošetřit. Při výběru vhodné metody k ošetření rizik budou brány v úvahu finanční možnosti společností a účinnost zvolené varianty. K úspěšnému dokončení dizertační práce budou použity metody spadající do oblasti řízení rizik a metody projektového managementu, na jejichž základě budou navrhnuty doporučení týkající se rizikových oblastí realizovaných logistických projektů, při čemž všechny kroky budou konzultovány s odborníky z praxe a lidmi působící v oblasti logistiky. Metody z oblasti řízení rizik, které mohou být využity v dizertační práci pro identifikaci rizik, jsou například brainstorming, technika Pre-Mortem, dotazníky nebo strukturované rozhovory. K analýze rizik mohou být použity metody jako například PNH, RIPRAN nebo FMEA. Z metod projektového managementu můžeme použít Logical Framework Approach, Ganttův diagram, Work Breakdown Structure, Statement of work, Histogram lidských zdrojů a jiné. Neméně důležitým výsledkem disertační práce bude

i definice pojmu logistický projekt, protože definice tohoto pojmu nemá u tuzemských autorů velké zastoupení.

Literatura

[1] GROS, Ivan. *Velká kniha logistiky*. Praha: Vysoká škola chemicko-technologická v Praze, 2016. ISBN 978-80-7080-952-5.

[2] CHARTERED INSTITUTE OF LOGISTICS AND TRANSPORT. *Chartered Institute of Logistics and Transport* [online]. 2006. Dostupné z: http://www.ciltinternational.org/

[3] BUNDESVEREINIGUNG LOGISTIK. *Bundesvereinigung Logistik* [online]. 2018. Dostupné z: https://www.bvl.de/

[4] INTERNATIONAL INSTITUTE FOR THE MANAGEMENT OF LOGISTICS. *International Institute for the Management of Logistics* [online]. 2018. Dostupné z: https://iml.epfl.ch/

[5] EUROPEAN COMMITTEE FOR STANDARDIZATION. *European Committee for Standardization* [online]. 2018. Dostupné z: https://www.cen.eu/Pages/default.aspx

[6] PERNICA, Petr. *Logistika (supply chain management) pro 21. století*. Praha: Radix, 2005. ISBN 80-86031-59-4.

[7] STEHLÍK, Antonín a Josef KAPOUN. *Logistika pro manažery*. B.m.: Ekopress, 2008. ISBN 978-80-86929-37-8.

[8] BARTÍK, Petr. *Význam české logistiky ve středoevropském regionu roste* [online]. 2016. Dostupné z: https://www.elogistika.info/vyznam-ceske-logistiky-ve-stredoevropskem-regionu-roste/

[9] PISZ, Iwona. *Applying fuzzy logic and soft logic to logistics projects modelling*. Poznan: House of Poznan University of Technology, 2009.

[10] PISZ, Iwona. Controlling of logistics project. *Total Logistics Management*. 2011, 107–125.

[11] PISZ, Iwona. *Identification and risk assessment of logistics project*. Poznan: Poznan House of Poznan University of Technology, 2011.

[12] PISZ, Iwona. Multi-criteria evaluation of the efficiency of logistics projects based on the Balanced Scorecard and fuzzy set theory. 2013, 64–169.

[13] KISPERSKA-MOROŃ, Danuta a Stanisław KRZYŻANIAK. *Logistyka*. 2009. ISBN 978-83-87344-09-2.

[14] TARABA, Pavel, Martin HART a Kateřina PITROVÁ. Risk Management Of Projects In The Czech Republic. *Polish Journal of Management Studies* [online]. 2016. Dostupné z: doi:10.17512/pjms.2016.13.1.17

[15] BURKE, Rory. *Project management: planning and control techniques*. 5. United Kingdom: John Wiley & Sons, 2013. ISBN 978-1-118-66076-8.

[16] SPOLEČNOST PRO PROJEKTOVÉ ŘÍZENÍ. *Doporučená praxe Společnosti pro projektové řízení - oblast Řízení rizik*. 2013.

[17] BARTOŠÍKOVÁ, Romana, Jana BILÍKOVÁ a Pavel TARABA. Risk Management in the Business Sector in the Czech Republic. *Vision 2020: Sustainable Growth, Economic Development, and Global Competitiveness - Proceedings of the 23rd*

International Business Information Management Association Conference. 2014.

[18] DOLEŽAL, Jan, Pavel MÁCHAL a Branislav LACKO. *Projektový management podle IPMA*. Praha: Grada, 2012. ISBN 978-80-247-4275-5.

[19] ČSN ISO 31000. *Management rizik - Principy a směrnice*. 2009.

[20] PASSENHEIM, Olaf. *Project Management* [online]. 2009. ISBN 978-87-7681-487-8. Dostupné z: http://bookboon.com/cs/projectmanagement-ebook

[21] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích* [online]. 3. Praha: Grada, 2010. ISBN 978-80-247-3051-6. Dostupné z: http://toc.nkp.cz/NKC/200912/contents/nkc20092012359_1.pdf

[22] KORECKÝ, Michal a Václav TRKOVSKÝ. *Management rizik projektů*. Praha: Grada, 2011. ISBN 978-80-247-3221-3.

[23] MACKENZIE, Cameron A. Summarizing Risk Using Risk Measures and Risk Indices. *Risk Analysis* [online]. 2014. Dostupné z: doi:10.1111/risa.12220

[24] COX, Louis Anthony Jr. Evaluating and Improving Risk Formulas for Allocating Limited Budgets to Expensive Risk-Reduction Opportunities. *Risk Analysis* [online]. 2012. Dostupné z: doi:10.1111/j.1539-6924.2011.01735.x

INCORPORATING TIME INTO RISK MANAGEMENT – A DIFFERENT APPROACH AND VIEW ON RELEVANT FACTORS IN EVALUATING RISK: THE RISK CUBE

Prof. Dr. rer. pol. Dr. h.c. mult. H.-Christian Brauweiler
Faculty of Business Administration and Economics, WHZ Westsächsische Hochschule Zwickau (Univ. of Applied Sciences), D-08066 Zwickau
christian.brauweiler@fh-zwickau.de

ABSTRACT

The importance of risk management is ever increasing, visible at its incorporation in integrated management systems, legal regulations concerning the requirement of an internal audit with a dedicated risk management part and so on. Risk is necessary, as there is no risk-free business. However, the amount of risk that a company is able or willing to bear may vary. Usually risk is categorized regarding two aspects: the probability of occurrence and the size of the negative impact. After a thorough description of the risk management process and its integration in an integrated management system, the traditional risk map is enhanced to a risk cube, taking the new dimension of the proximity and speed of the risk into consideration.

KEY WORDS:

Risk Management, Integrated Management System, Risk Detection, Risk Identification, Risk Classification, Risk Assessment, Risk Treatment, Risk Documentation, Risk Communication, COSO, Risk Map, Proximity and Speed of Risk, Risk Cube

1. THOUGHTS ABOUT RISK IN INDUSTRY

The importance of risk management has evolved and grown over the past few decades. It is seen as a vital and crucial part of an Integrated Management System. Setting up a company and running a business is associated with taking risks. However, the risk should be as small as possible. However, risk usually correlates with return, thus wishing a certain profit during the life of the company means to be aware of a certain amount and size of risk. Companies of all kinds of industry as well as individuals are exposed to different kinds and sorts of risks. These risks vary in visibility, source, probability, strength, speed, damage and other factors. The influencing factors of the industry are – due to a more and more volatile business environment – becoming more and more risky. Additionally, many companies have enlarged their international activities in a globalized world considerately. The management has to take this into consideration. Controlling, reporting, external as well as internal auditing face certain new challenges. Whereas the aforementioned points of visibility, source, probability, strength, damage and some other factors have been discussed widely in literature and are usually depicted in the risk map, the speed and proximity, which are to be seen mutually as one more threatening aspect in business environment, are not well defined. The author enhanced the risk map to a risk cube in taking speed and/or proximity of risks additionally into account.

Management has to decide on a daily basis on how to deal with and how to manage and control risks. This is necessary to counteract the steadily increasing threats, especially in a more and more globalized economy with growing impediments by political and other factors. After defining a company strategy, philosophy and especially risk culture and risk appetite, which has to be done with regard to the different requirements of shareholders and stakeholders a proper organizational as well as procedural system of risk management has

to be set up. Empirical studies deliver evidence that especially SME take risks in order to introduce new processes and products. Additionally it can be stated that strategy, competence or even guidelines about the question of identifying, evaluating and treating risks are lacking. This leads regularly to an uncoordinated and inefficient handling of risks, which can put the whole company in danger.

In the focus of this article is the presentation of the risk cube, which incorporates the speed of an approaching risk as well as the distance on a timeline until arrival of the risk. First, this article gives a short and theoretical overview about relevant topics in terms of risk management and risk controlling. It starts with a presentation of different terms such as risk, risk types, risk management and risk controlling. [1]

1.1 Terminology and Classification of Risk

Sometimes “risk” is defined as a neutral term in scientific articles. I.e. this term can have negative or positive impact (threats and opportunities) on business. But mostly risk is associated with something negative, e.g. in the Oxford dictionary risk is described as a situation in which one is exposed to Langer

1.2 Conceptual Alignment of the Risk Management System

Risk management can be a central part of an integrated management system. Furthermore, it has to be set up, introduced and run in a very systematic way, in order to sufficiently and efficiently reduce and/or eliminate risks. The overall goal is to create sustainable benefits for the company by employing opportunities and avoiding threats or at least the impact of threats. In addition, the efficient and synergetic combination of the various mentioned part of an integrated management system together with risk management can save resources. [2]

Risk management is a process that involves the earliest possible identification of potential risk, evaluate and assess risk and its possible impact, development of risk culture and risk strategy as well as risk minimisation. Risk management is intended to increase the probability and size of success and eliminate – in the best case – or at least reduce uncertainty and failure to achieve the overall goals of the organization and minimize (financial) losses. Risk management has to be a steady and continuous as well as an evolving process that has to be integrated into an integrated management system. All potential risks that can be estimated or identified have to be fully observed and included in the risk management. Risk management hast to be integrated into the corporate culture, included in target planning and known to all employees. As these tasks can be – in the long run – crucial for the survival of the company, a responsible person has to be in charge, the so called Chief Risk Officer, who is part of the upper or top management team. [2, 3]

1.3 Preconditions and Principles of Risk Management Systems

A company should have a high interest to monitor and control risk. However, especially in SME, but also – but for very different reasons – in larger companies up to MNC, management does not solely have risk management in focus, sometimes not at all in focus. Incorporating risk management into an overall established integrated management system and using synergies could support fighting risk. As other stakeholders might suffer from a not or inefficiently established control and risk management system, various institutions from industry up to parliaments enacted norms, standards, regulations and laws in order to

implement. E.g. in Germany the parliament enacted the "Law on Control and Transparency in Companies" and made several alterations to specialized laws (e.g. the "Law on Stock Exchange Companies") in order to incorporate European guidelines from the EU into national law. Additionally international and national professional institutions and associations emitted standards, guidelines, recommendations and interpretations in order to harmonize and systematize risk management. These institutions comprise for example the "Committee of Sponsoring Organizations of the Treadway Commission (COSO)", which was founded in 1985 in the USA and published various papers on how to best set up and implement a standardized and efficiently functioning system of internal control and risk management. One major paperwork "Enterprise Risk Management Integrated Framework" was first published in 2004, the current version dates from 2017. This publication is an internationally recognized standard for risk management. It concludes that the value of a company can only be increased if the strategies form an optimal balance between growth, return goals and risks as well as employing all resources in a best way. This means that an internal monitoring system must be set up, as going concern risks must be identified at an early stage. [4]

Another international requirement is the "ISO 31000 – Risk Management" standard. This was published by the International Organization for Standardization (ISO) in 2009 as "ISO 31000: 2009 Risk management - Principles and guidelines". This document shows principles and processes for risk management in companies, and it defines risk management as a management task. This standard is valid for any industry or branch. It is helpful to identify opportunities and risks, so that resources can be used in an optimal way for the treatment of risk. In line with other ISO - standards the integrated management system can be well developed. [5]

1.4 Risk Management as part of an Integrated Management System

Companies have – independently from their line of business – various systematic approaches to manage certain tasks in order to comply with laws and norms or to avoid risk for themselves, employees or customers. Examples for these systems are a quality management system, an occupational health and safety system, environmental management, internal control system, energy management system or information security management system etc. As some or a lot of processes are similar or identical, it makes perfect sense for a business in order to work efficiently and safe resources to combine and integrate these various system. An integrated management system thus combines all processes and systems within a company into one unified system with uniform aims. Thus a Risk Management System can be and should be integrated as well. [6]

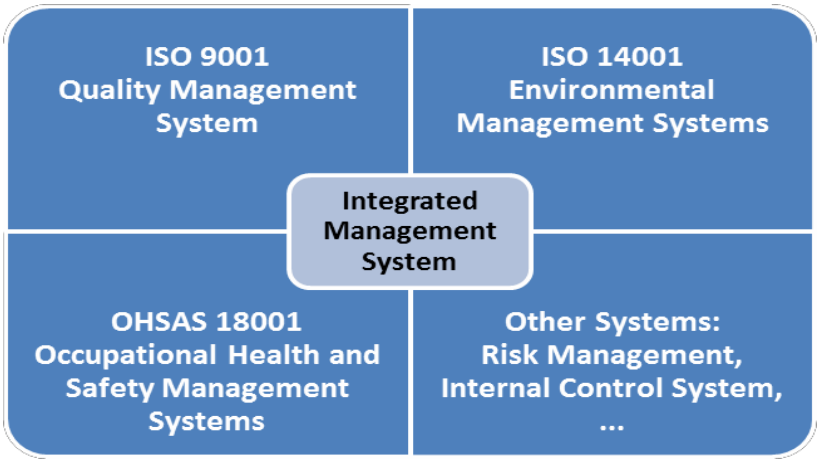


Figure 1 Example for Subsystems in an Integrated Management System

(Source: own depiction)

2. THE RISK MANAGEMENT PROCESS

Risk management starts with detecting risks. Then the risks have to be analysed, categorized and evaluated. On this basis, the systematic treatment and controlling of corporate risks can take place. Risk management is geared to recognize critical situations early in the business activities. It should in the best case avoid, but in any case minimize or reduce effects of possible risks. The activities of risk management are summarized in Figure 2.

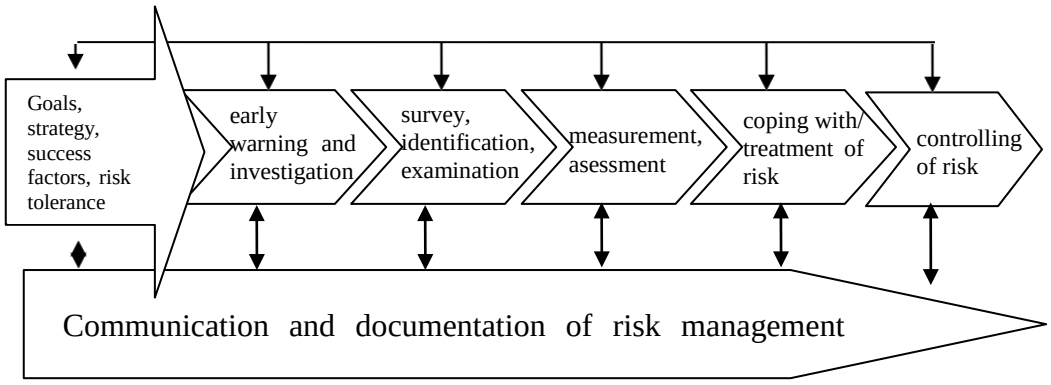


Figure 2 Elements of the Risk Management Process [7]

2.1 Recognition and Assessment of Risks

As mentioned, every single risk or other threat to the company´s strategy, market, position etc. must be identified at the earliest possible moment in order to achieve a viable and efficient risk treatment. Uncertainties and risks are to be identified systematically, consistently and continuously. Management should be aware of the uncertainties both in scope as well as in probability and timeline. This last point needs to be addressed intensively, which will be done below.

All personnel involved has to be sensitized and if needed trained. A certain organizational and procedural structure is needed for the proper identification of all risks in a business environment. Within this structured approach to detecting risk within the organizational setup systematic action should be taken to identify as many risks as possible from different sources and activities. Identifying risks requires knowledge of the actual, potential and future traits of the organisation, the market and its environment (suppliers, customers, actual and potential competition etc.), the legal, social, political and cultural environment, the shareholders as well as the stakeholders. This knowledge can be used to derive threats and opportunities that influence corporate strategy and ultimately the fulfilment of strategic and operational goals. It is also important to systemize and record the identified risks, e. g. in a risk-matrix as depicted in the following figure. Compre- hensive checklists help identify risks. [3, 8, 9, 10]

To derive a systematic and comprehensive overview, the risk map is used. Within this a company can cluster all risks according to their probability and impact. Thus very strong risks that have to be addressed immediately, can be recognized and controlled, whereas lower risks, either in likelihood or size of possible loss or damage, can be merely monitored. The following Figure 3 shows the layout of a risk map.

Expected value and normstrategy		Probability		
		low, e.g. <30%	medium, e.g. 30-85%	high, e.g. >85%
Damage or loss in EUR size depending on company	low (negligible)	Accept	Accept and monitor	Monitor and Control
	medium (requires treatment)	Accept and monitor	Monitor and Control	Monitor, Control, and Manage
	high (threat to survival of company)	Monitor and Control	Monitor, Control, and Manage	Extended risk management

Figure 3 Risk Map [11]

Recognizing, identifying, assessing and classifying the various forms and strengths of risk are crucial for the planning and implementation of countermeasures. First of all it is important to analyse the intensity of the uncertainty, or to put it the other way, the likelihood. The intensity, the probability of occurrence as well as the size or amount of consequences can either be precisely determined, subjectively estimated or not at all determined. If relatively objective values for the uncertainty are available, then there are different models to determine the loss, e.g. via the value at risk calculation. This method is in use when trading equity securities. However, the effects can often only be estimated in a very subjective way. Then the portfolio method helps to classify risks into categories and estimate the occurrence probability and impact, whether high, medium or low. The possible consequences that influence the strategy and operations must be determined. [8, 9]

Finally the risk evaluation compares the identified risks with the risk criteria established by the company. These are dependent on the overall risk strategy, the risk culture and the amount of bearable risk without posing a serious threat to the company. Further risk criteria could be costs and benefits in the short and in the long run, social and environmental factors as well as shareholders´ and stakeholders´ interests. Risk assessment assists in deciding whether to take action or accept the risks. This determines the significance of the risks. [2]

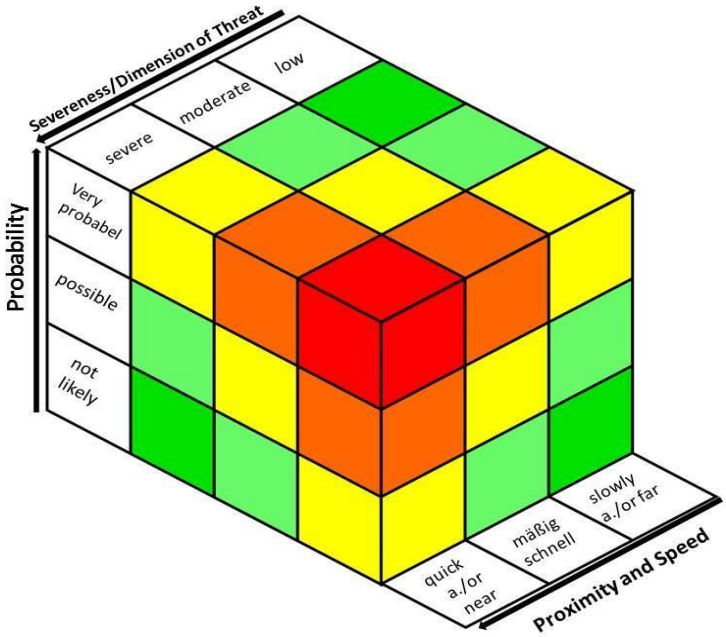


Figure 4 Risk Cube [10]

Traditionally, literature picks out scope and probability, to cluster risks according to the volume of impact they possibly can have, as mentioned. This is depicted in the two-dimensional risk map. However, treatment of risk needs a certain time to be thoroughly thought off, set up and implemented. Furthermore, measures and actions taken into account and started for counteracting and treating risks, might need a definite or indefinite time until they come to full effect. Thirdly, the speed of the approaching risk is a relevant factor in the detection and treating of risk[1]. Thus the author suggests including the important third dimension of time, i.e. proximity and/or speed of risks, to derive by the risk cube as it is shown in

Figure 4. This graphical depiction clusters risks even more clearly into important and threatening risks that need urgent, immediate and efficient treatment, risks, that need attention as second in line and risks, that need only be monitored on a regular bases.

[1] This can be exemplified at the "Brexit" where the economies and industry have or had more than two years to prepare for the threat of not being in the unified European Union´s market vs. the short and quicker decrees by the current President of the US with excises and customs on goods especially coming from China, but as well coming the EU.

2.2 Surveillance and Handling of Risks

In defining a strategy and philosophy on risk, a company has to take into consideration, which specific amount of risk it is able or willing to accept. This is known as risk appetite and has to be defined before risks can be addressed. Risk appetite is the level or amount of risk which will be accepted by an organization, because it is prepared to bear this risk in order to achieve its goals under the given circumstances (strategy, philosophy, market, political, juridical environment etc). In setting up a definition of an appropriate risk appetite, a company can balance between

innovative (i.e. inherently risky) activities and sensitive (i.e. not exaggerated) caution. If an identified risk is viewed to be a serious threat, it must be considered whether the risk is justifiable and reasonable. Secondly, the company has to appraise the risk, if it is avoidable or not and if in this case can possibly be reduced to an acceptable level, if not eliminated at all.

In the literature four classes of addressing risk are given:

1. Transfer - The risk is transferred to a third party. This can be either an insurance company or the regular contract partner, i.e. the supplier or customer. The transfer is arranged by agreement in contracts. It can be associated with payment (insurance premium, reduction or increase in price of the traded good or service etc.).
2. Treat - The risk should be limited to an acceptable level by appropriate measures (e.g. training of personnel, installation of technical safety measures etc.).
3. Tolerate - The effects are tolerable, even if there are no further measures. Or you cannot do anything about risk because the costs of transfer or treatment are higher than the benefits.
4. Terminate - A risk can be treated when the triggering activity is terminated (e.g. retraction from a geographical market etc.). [9]

Risks can be addressed passively or actively. Passive risk management introduces control systems to ensure compliance with laws and/or internal regulations or to protect the interests of stakeholders. The more proactive approach also includes the assessment of controls in terms of benefits. There are a huge number of further options for treating and handling individual risks on a more active basis which will be discussed later. One can name several options: First, preventive controls are used to prevent the occurrence of a risk. The prevention of the occurrence of risks is in itself a possible way to terminate risks. Preventive measures aim at limiting negative impact of the risk, i.e. (financial) loss or other undesirable results. A company has to pay attention to the importance of results for the overall wellbeing and benefit of the company, if those results are under threat. The more important a result is, the more important it is to introduce proactively preventive measures. Measures could be the separation of functions. Then action may only be taken with the consent of another person (two-person-rule). Or – as another example – only authorized persons may perform certain actions, e.g. only the company's press spokesperson is allowed to speak to the media. [12]

If a risk occurs with a high probability and low magnitude, it is possible to treat a risk. Corrective controls are intended to reduce the likelihood of occurrence and support the treatment of risks. The aim is to reduce the likelihood of the undesirable event and limit losses. Measures in companies include the use of passwords or access controls, occupational safety and health measures. The advantages of the measures are often simple and outweigh the costs of introduction, as those measures are usually inexpensive.

Directive controls can be seen as another point in reducing risk. These are certain behaviours or instructions by the upper management, regulation on how to behave when a risk occurs. These regulations aim at achieving a particular positive result and are used to transfer risks. One example is the wearing of protective clothing during hazardous activities. Other controls and assessments ("detective controls") are used to detect undesirable events that have occurred in the past and can only be used if the risks can be tolerated and the damage is acceptable. Detective controls are, for example, stock or inventory taking to show whether something has been removed without permission. The disadvantage of this method is that the risk has already occurred. It should always be borne in mind when carrying out controls that binding commitments have to be implemented, too. [9]

Risk monitoring requires the introduction of processes that show whether identified risks still exist, whether new risks have arisen or whether any alterations happened. The controls should be carried out on the bases of an adjusted and adequate frequency. This frequency should be based on the probability, size and likelihood of risks on the one hand and risk appetite on the other hand. Frequency can vary for risk, thus having a monitoring on a weekly or monthly base, others only on a biannual or even a biennial basis.

SUMMARY AND CONCLUSIONS

This article aimed at the repetition of some theoretical approaches to the topic of risk, including risk management and risk treatment. Furthermore, the conceptual change to traditional depictions in adding the timeline to the assessment of risk formed the risk cube. In respect to the company organization and processes, risks are mostly defined as events with uncertain (negative) outcomes or events with (negative) impact on the organization. It must be accepted that there are risks in every industry or business activity. Risk management is to be seen as the process that involves the development of a risk strategy, defining the risk appetite, the identification of risks, risk assessment, risk management and minimization. Risk management should be a continuous and evolving process which supports the achievement of corporate goals and strategies. Risks from the past, present and above all the future are to be included. Risks must also be considered mutually, as they often are interactive or have a cumulative effect on the company.

Risk management should be a vital and integrated aspect of all activities in business life: It supports controlling (and is supported by controlling activities itself), it interacts with internal and external auditing, support their work and goals. It supports several aspects of corporate governance and compliance. And it can be an integrative part of an integrated management system, which combines environmental, health- and security, quality and possibly other management systems.

Risk management has to be set up in an efficient way, done on an educated, regular basis and in line with company philosophy, strategy and aims. Employees must be involved at all phases of the risk management and sensitized to risks and risk management. The effects on the market, finances and value chain of the analysed events must be assessed. The identified risks are compared with the risk appetite of the company. After that, the management has to decide if the specific risks are treated, transferred, terminated or tolerated. The aim of the treatment is to limit the sum of all risks to an acceptable level, so that the company´s existence is not endangered. However, the effects may be tolerable and the risk may persist, which makes it necessary to keep an ongoing monitoring of all risks.

Literature and References:

[1] Henschel, Thomas: Risk Management Practices of SMEs: Evaluating and Implementing Effective Risk Management Systems, Berlin 2008

[2] The Institute of Risk Management (IRM): A Risk Management Standard, London, 2002

[3] Agrawal, R.C.: Risk Management, Jaipur 2009

[4] Committee of Sponsoring Organizations of the Treadway Commission (COSO): Enterprise Risk Management, Integrating with Strategy and Performance, Executive Summary, United States of America 2017

[5] International Organization for Standardization: ISO 31000 – Risk management, downloaded 8th October 2017, https://www.iso.org/iso-31000-risk-management.html

[6] Mourougan, Sendil: Planning Integrated Management System audit to ensure Conformance, Consistency and Continual Improvement, in OSR Journal of Business and Management (IOSR -JBM), Volume 17, Issue 10, 2015, PP 41-53

[7] Brauweiler, Hans-Christian; Brauweiler, Jana: Risk- und Claimmanagement, 2. Edition, AKAD, Stuttgart, 2014

[8] Weber, Jürgen; Liekweg, Arnim: Statutory Regulation of the Risk Management Function in Germany: Implementation Issues for the Non-Financial Sector, in: Frenkel, Michael, Hommel, Ulrich, Rudolf Markus (Ed.): Risk Management, Challenge and Opportunities, 2nd Edition, Heidelberg 2005, PP 495 – 512

[9] Hopkin, Paul: Risk management, London, Philadelphia, New Delhi 2013

[10] Brauweiler, Hans-Christian: Risikomanagement in Unternehmen, 2. Edition, Springer Essentials, Springer, 2018 (forthcoming)

[11] Brauweiler, Hans-Christian: Risikomanagement in Unternehmen, Springer Essentials, Springer, 2015

[12] Her Majesty's Treasury on behalf of the Controller of Her Majesty's Stationery Office (HM Treasury): The Orange Book, Management of Risk – Principles and Concepts, London 2004

[13] Brauweiler, Hans-Christian: Risikomanagement in Banken und Kreditinstituten, Springer Essentials, Springer, 2015

[14] Brauweiler, Hans-Christian; Zirkler, Bernd: Risk Management – Theoretical Basis, Comparison and Impact in a Globalized Economy, KAFU Kazakh American Free University, Ust Kamenogorsk, Conference Proceedings, September 2018

[15] Drucker, Peter: Managing For Results, New York 1955 (first published by Butterworth-Heinemann), 2011

[16] Oxford dictionary (2017): risk, downloaded 28th July 2018, https://en.oxforddictionaries.com/definition/risk

[17] Volkswagen Group: Annual Report 2016, Report on risks and opportunities: Risk management and internal control system, downloaded 19th October 2017, http://annualreport2016.volkswagenag.com/group-management-report/report-on-risks-and- opportunities/risk-management-and-control-system.html

MĚKKÉ CÍLE

SOFT TARGETS

Veronika Ďurčíková, Ing. Jan Kyselák, Ph.D.
Fakulta logistiky a krizového řízení
Studentské náměstí 1532, 686 01 Uherské Hradiště
v_durcikova@utb.cz, kyselak@utb.cz

ABSTRAKT

Příspěvek se kriticky zamýšlí nad úrovní zabezpečení budov (coby měkkého cíle), ve kterých je dislokována Fakulta logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně, a tím současně i nad zajištěním bezpečnosti studentů a personálu této fakulty. Na základě vyvozených závěrů, příspěvek navrhuje řešení na zlepšení aktuálního stavu.

KLÍČOVÁ SLOVA

Měkké cíle, objekty s větším počtem osob, terorismus, školská zařízení.

ABSTRACT

The work in its content critically deals with the level of security of building (as soft targets) in which the Faculty of Logistics and Crisis Management of Tomas Bata University in Zlín is located. The work also deals with assurance of safety students and staff of this faculty. Based on our conclusions the work suggests solutions to improving of actual situation.

KEY WORDS

Soft targets, objects with a larger number of people, terrorism, schools facilities.

ÚVOD

S problematikou obsaženou v příspěvku se poslední době setkáváme čím dál častěji. V posledních letech můžeme pozorovat postupné zhoršování bezpečnostní situace nejen v zahraničí, ale dle našeho názoru i u nás, s čímž úzce souvisí nárůst teroristických útoků, extrémismu, národnostních a etnických konfliktů. Dochází také ke zvyšování četnosti migrace, agresivity, ale i k útokům tzv. „osamělých vlků“. V důsledku toho narůstá i počet nejen ideologicky motivovaných, násilných útoků, které jsou vedeny i na měkké cíle. V České republice nefunguje žádná domácí teroristická organizace, ani zde nejsou podstatné části zahraničních organizací. To ovšem neznamená, že náš stát se danou problematikou nezaobírá, ba naopak.

Již 30. března 2009 vzniká ve struktuře České policie nový útvar – Národní kontaktní bod pro terorismus [1]. Oblastí spojenou s bojem proti terorismu a také s ochranou měkkých cílů se Česká republika se intenzivně zabývá „Strategie České republiky pro boj proti terorismu od roku 2013“ [2]. Dalším důležitým přijatým dokumentem je metodika z roku 2016 „Základy ochrany měkkých cílů“ [3]. Ve stejném roce je přijata i norma „Prevence kriminality – řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení řeší“ [4]. Problematiku ochrany měkkých cílů konkrétně potom řeší „Koncepce ochrany měkkých cílů pro roky 2017–2020“ [5].

Za tzv. „soft targets“, čili měkké cíle, jsou bezpečnostní komunitou označována místa s vysokou koncentrací osob a zároveň s nízkou úrovní zabezpečení proti násilným útokům.

Právě tato místa jsou kvůli své charakteristice často vybírána jako cíl teroristických útoků. K těmto cílům lze zařadit zejména nákupní centra, náměstí, kulturní, sportovní a další akce, ale také školská zařízení vč. jejich ubytovacích prostorů. Vzhledem k přítomnosti dětí a jejich zranitelnosti a současně vzhledem k hodnotě, jakou představují pro společnost, jsou útoky ve školách vnímány jako jedny z nejhorších. Proběhnuvší incidenty ukázaly, že hlavními aktéry útoků mohou být teroristé, psychicky nemocní lidé i samotní studenti. Útoky na školská zařízení v České republice jsou na rozdíl od jiných zemí světa velmi ojedinělé. Za jeden z nejtragičtějších útoků poslední doby lze označit útok, který se odehrál v únoru 2018 na Floridě, na střední škole v Parklandu, při kterém přišlo při střelbě o život 17 osob. Útočníkem byl někdejší student, který byl ze školy vyloučen. V České republice se stal dosud nejtragičtější incident ve Žďáru nad Sázavou, který se odehrál v říjnu 2014, kdy po útoku psychicky narušené ženy zemřel žák střední školy.

Univerzitu Tomáše Bati ve Zlíně (dále jen „UTB“) lze v podstatě pokládat také za jeden z měkkých cílů. Část budovy, ve které sídlí rektorát univerzity, je možno považovat za důkladně zabezpečený. „Jak je zabezpečena Fakulta logistiky a krizového řízení?“. „Je možné aktuální úroveň zabezpečení této fakulty kvalitativně zvýšit?“ Na tyto otázky podává odpověď právě tento příspěvek.

1. FAKULTA LOGISTIKY A KRIZOVÉHO ŘÍZENÍ, CHARAKTERISTIKA

Areál Fakulty logistiky a krizového řízení (dále jen „FLKŘ“) v sobě zahrnuje jak všechny výukové prostory, tak i knihovnu, děkanát a administrativní oddělení. Součástí je i ubytovací zařízení (vysokoškolské koleje) a stravovací zařízení. Vlastníkem budov, ve kterých fakulta působí, je společnost EDUHA, s.r.o., na které má významný podíl město Uherského Hradiště. Společnost své prostory fakultě pronajímá. Město Uherské Hradiště zároveň vlastní pozemky, ve kterých je fakulta dislokována.

Fakulta má k dispozici tyto budovy:

UH1 – výukové prostory, knihovna, kanceláře
UH2 – přednáškové sály, kanceláře
UH3 – část prostoru pro ubytování pedagogů
UH4 – ubytovací zařízení
UH5 – ubytovací a stravovací zařízení.

Ke dni 28. března 2018 byl celkový počet všech studentů prezenční a zároveň kombinované formy studia na fakultě 651. Dále je zde zaměstnáno přibližně 70 pracovníků z řad pedagogických pracovníků, zaměstnanců na součástech děkanátu, zaměstnanců vykonávající úklid, dohled na vrátnici apod. Ubytovací zařízení (budovy UH4 + UH5), mají celkovou kapacitu ubytovaných 300 osob. Ke stejnému datu zde bylo ubytováno 103 osob ze strany veřejnosti, další část ubytovaných tvořili studenti fakulty. Zbytek volné kapacity je využíván pro tranzitní ubytování (studenti kombinované formy studia či zájemci z řad veřejnosti).

Obr. 1 Mapa areálu Fakulty logistiky a krizového řízení [6]

2. SLABÁ MÍSTA Z POHLEDU BEZPEČNOSTI

Při identifikaci slabých míst (za slabá místa jsou v tomto příspěvku označovány nedostatky v rámci zabezpečení FLKŘ) byla použita metoda pozorování a dotazníkové šetření. Dotazníkové šetření bylo realizováno v prvním pololetí roku 2018 mezi studenty fakulty (respondenti – 40 studentů všech ročníku prezenčního i dálkového bakalářského studia) a to pouze s jednou otevřenou otázkou, kdy studenti odpovídali na otázku: „Vnímáte nějaká negativa v zajištění bezpečnosti objektů, ve kterých je dislokována FLKŘ UTB?“ Výsledek průzkumu je vždy uveden v rámci jednotlivých podkapitol.

2.1 Obvodová ochrana areálu

Cílem obvodové ochrany je zajistit obvodovou ochranu areálu. V tomto případě se jedná o areál, ve kterém se nachází budovy UH1, UH2, UH4, UH5 a rozsáhlé parkoviště s příjezdovými cestami a chodníky, popř. budova UH3, kterou ovšem fakulta využívá pouze omezeně – jen pro ubytování některých pedagogických pracovníků. Umožněn vstup do tohoto areálu a na parkoviště má kdokoliv – studenti, zaměstnanci, ubytované osoby, strávníci i osoby z veřejné frekvence.

Závěry z pozorování a šetření (slabá místa), a návrhy na zlepšení situace v relaci k obvodové ochraně areálu FLKŘ jsou uvedeny v tab. 1.

Slabé místo	Aktuální stav	Navrhované řešení
Oplocení	Bez oplocení.	Není možné oplotit areál – veřejný prostor.
Kamerový systém	Bez archivace záznamu.	A. Pověřit osobu online sledování kamer. B. Zavést kamerový systém s archivací záznamu.
Kontrola vjezdu automobilů do areálu, popř. kontrola vstupu osob	Bez vrátnice, kontroly.	Není možné zavést kontrolu vjezdu automobilů ani vstupu osob – veřejný prostor.

Tab. 1 Slabá místa a návrhy na zlepšení v obvodové ochraně areálu

V případě chybějícího oplocení a neomezeného vjezdu automobilů či vstupu osob do areálu je velmi složité hledat možná zkvalitnění aktuálního stavu zabezpečení. Celý areál včetně budov a parkoviště se nachází v katastru města Uherské Hradiště – změnu by tedy musel provést vlastník areálu – město Uherské Hradiště.

Vnější okolí fakultních budov není nijak personálně hlídáno, je zde ale umístěn kamerový systém. Areál snímá celkem 5 kamerových zařízení bez archivace pořízených záběrů (budovy viz např. Obr. 2 UH4 – 2x, viz Obr. 3 UH2 – 1x, UH3 – 2x). Jedná se tedy pouze o systém fungující na bázi on-line monitoringu, tedy bez záznamu. Takový kamerový systém je zde zcela neefektivní a bezvýznamný. Například v případě vloupání do objektu by nebyl pořízen žádný záznam, na který by se dalo po činu zpětně odkázat.

Je zde tedy dvojí řešení k návrhu na zlepšení stavu bezpečnosti v rámci kamerového systému:

A. Online monitoring

Jedním z řešení je pověřit zodpovědnou osobu, která by online monitoring zajišťovala v rámci výkonu své pracovní doby, tudíž by se výstup z kamerového systému nemusel archivovat. Jako nejpraktičtější návrh osoby se jeví zaměstnanci, kteří vykonávají svou práci na vrátnici UH1, popř. UH4 nebo UH5 (na těchto dvou budovách je nepřetržitá služba). Je však třeba mít na paměti, že i online monitoring musí respektovat určitá práva sledovaných osob. Z toho důvodu by bylo potřeba umístit na viditelné místo např. informační ceduli ve znění „Prostor je monitorován kamerovým systémem“. Nevýhoda – občasné absence vrátného na stanovišti.

B. Kamerový systém s možností archivaci záznamu

Tato možná varianta je náročnější na realizaci, ale za to mnohem efektivnější. Jedná se o variantu kamerového monitoringu s archivací pořízených záběrů. Pořizování záběrů s využitím identifikace fyzických osob je považováno za zpracování osobních údajů podléhajících režimu zákona č. 100/2000 Sb., o ochraně osobních údajů. Zde je nutné dbát na určitá pravidla dle tohoto zákona.

V obou případech se zde nabízí možnost využití stávajícího kamerového systému např. i městskou policií.

Obr. 2 Vnější kamerový systém na budově UH4

Obr. 3 Vnější kamerový systém na budově UH2

2.2 Plášťová ochrana budov a režimová opatření

Plášťová ochrana má zamezit narušení pláště objektu či aspoň zpomalit vstup neoprávněné osoby a prodloužit dobu vniknutí do objektu. Mezi hlavní problém v plášťové ochraně je možno jednoznačně zařadit zabezpečení hlavních vchodových dveří na budovách UH1 a UH2.

Závěry z pozorování a šetření (slabá místa), a návrhy na zlepšení situace v relaci k plášťové ochraně budov užívaných FLKŘ a režimových opatření, jsou uvedeny v tab. 2.

Slabé místo	Aktuální stav	Navrhované řešení
Hlavní vchody (UH1, UH2)	Dveře bývají otevřené.	A. Poučit zaměstnance fakulty. B. Zavést turnikety na čipové karty.
	Čipové karty nejsou účelné – cizí osoba vyčká otevření od osoby s kartou.	Zavést turnikety na čipové karty.
	Otevření dveří od zaměstnanců na vrátnici bez prokázání karty.	Poučit zaměstnance na vrátnici.

Tab. 2 Slabá místa a návrhy na zlepšení v plášťové ochraně a režimových opatřeních

Vchodové dveře do obou budov bývají často otevřené, tudíž není ani potřeba využít čipové karty. Do budov se tak teoreticky může dostat kdokoliv. V tomto případě je potřeba poučit zaměstnance fakulty (také uklízečky a vrátné) aby dávaly pozor a dveře zavíraly nebo požádat vedení společnosti EDUHA, s.r.o., o zavedení vstupních turniketů.

Další slabé místo u vchodových dveří spočívá při vstupu na kartu (ISIC, studentská karta, karta zaměstnance). Při vstupu do objektu se na jedno otevření přes kartu dostane i více osob, které si dveře vzájemně podrží. Ve skupince může být i osoba, která do objektu nemá přístup. Za nejefektivnější řešení ke zlepšení lze považovat zavedení turniketů na čipovou kartu (viz Obr. 4 – Tripod, Obr. 5 – Speedgate) ve směru vchodu i východu z objektu.

Obr. 4 Tripod TRISTAR – kapacita průchodu: 40 osob/min [7]

Obr. 5 Speedgate DNG460 – kapacita průchodu: 40 osob/min [8]

Za negativum v rámci bezpečnosti na FLKŘ je považováno i nekontrolovatelný vstup cizích osob bez čipové karty. U neoprávněné osoby stačí, aby zazvonila na zvonek či před dveřmi „hledala kartu“ a dveře se otevřou od zaměstnanců z vrátnice. Vrátné by si v tomto případě měly osobu zkontrolovat a zjistit za jakým účelem se chce do objektu dostat. Dále zavolat osobu, kterou jde dotyčný navštívit. Mělo by být standardem, aby se návštěvy pohybovaly pouze v doprovodu.

2.3 Prostorová ochrana budov a režimová opatření

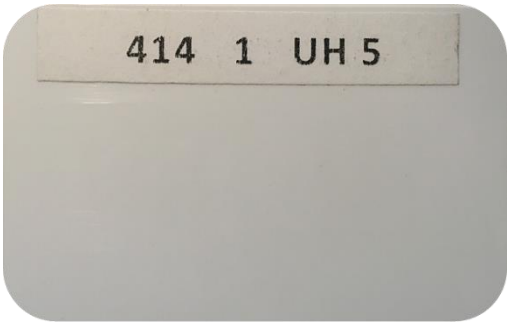
Prostorová ochrana slouží především k detekci pohybu uvnitř střeženého objektu. Místnosti fakulty (učebny, přednáškové sály, některé kanceláře) jsou vybaveny pasivními infračervenými čidly (PIR). Tato skutečnost odpovídá standartnímu zabezpečení těchto prostor v době mimo výuku. Dále je objekt doplněn kamerovým systémem na chodbě při vstupu do budov UH1, UH2 dále v přednáškovém sále P2 a na každém patře jednotlivého ústavu. Jak už ale bylo výše uvedeno, kamerový systém je bez možné archivace záznamu, proto návrh na zlepšení aktuálního stavu bude stejný jako při plášťové ochraně.

Závěry z pozorování a šetření (slabá místa), a návrhy na zlepšení situace v relaci k prostorové ochraně budov užívaných FLKŘ a režimových opatření jsou uvedeny v tab. 3.

Slabé místo	Aktuální stav	Navrhované řešení
Vrátnice (UH4, UH5)	Vrátnice je v nočních hodinách mnohdy bez dozoru (např. v době konání obchůzky vrátným, ale i v jiných případech).	Upozornit zaměstnance na dodržování své pracovní náplně a doby.
Vrátnice (UH1)	A. Vydání klíčů osobě, u níž není prokázané, že je student nebo zaměstnanec fakulty (popř. jinou oprávněnou osobou). B. Nezájem o dění kolem sebe.	Poučit zaměstnance, poukázat na chyby, kterých se dopouští.
Kamerový systém (UH1, UH2)	Bez archivace záznamu.	A. Pověřit osobu za online sledování kamer. B. Zavést kamerový systém s archivací záznamu.
Čipová karta od ubytovacího zařízení	Na čipové kartě je označení budovy a čísla pokoje – v případě odcizení dojde ke snadnému zjištění příslušnosti karty k pokoji a následnému možnému vloupání do pokoje.	Odstranit označení budovy a čísla pokoje z čipové karty.

Tab. 3 Slabá místa a návrhy na zlepšení v prostorové ochraně a režimových opatřeních

Ubytovací zařízení preferuje místo klasických dveřních zámků s klíči raději čipové karty, které při přiložení na určené místo ve dveřích zajistí jejich otevření. Karty jsou ze zadní strany označeny nápisem s budovou UH4 nebo UH5 a číslem pokoje (viz Obr. 6). Při ztrátě či odcizení může dojít ke snadnému zjištění, k jakému konkrétnímu pokoji náleží a v konečném důsledku může dojít ke vloupání. Pachatelé, v tomto případě, by mohli být z větší pravděpodobností osoby ubytované na budově UH4 a UH5, jelikož mají povědomí o označení čipové karty a umístění pokojů.



Obr. 4 Zadní strana čipové karty s označenímbudovy a číslem pokoje

2.4 Požární zabezpečení

Požární zabezpečení se velkou mírou podílí na ochraně lidského zdraví či majetku. Univerzita by proto měla zajistit co nejefektivnější ochranu zdraví a životů všech osob, které se nacházejí ve školních objektech nebo provádějí činnosti pod jejím vedením i z tohoto pohledu.

Závěry z pozorování a šetření (slabá místa), a návrhy na zlepšení situace v relaci k požárnímu zabezpečení budov užívaných FLKŘ jsou uvedeny v tab. 4.

Slabé místo	Aktuální stav	Navrhované řešení
Hlásič požáru (UH5)	Samovolně se spouští.	Opravit popřípadě pořídit nový funkční hlásič.
Hlásič požáru (UH2 – S1,S2)	Chybí hlásič požáru.	Nainstalovat hlásič.
Únikové východy (UH1,UH2)	Budovy UH1 – 4. podlaží a UH2 jsou bez únikového východu (vnějšího požární schodiště).	Zajistit dostavění požárního schodiště do horního podlaží.
Přehled o počtu osob	Bez přehledu počtu osob v budovách fakulty.	Zavedení turniketu na čipové karty (evidence osob v budově).
Poučení o požární ochraně	Ne všichni studenti byli poučení o požární ochraně.	Řádně poučit všechny studenty.

Tab. 4 Slabá místa a návrhy zlepšení v požárním zabezpečení

Hlásiče požáru obsahují v sobě všechny komponenty potřebné pro detekci kouře a vyhlášení poplachu (zvukovým signálem). Hlásiče jsou umístěny téměř ve všech místnostech fakulty kromě místnosti S1 a S2 na budově UH2. Zde by bylo vhodné hlásiče doinstalovat. V prostorech ubytovacího zařízení, na chodbách a pokojích se ovšem tyto hlásiče často samovolně spouští a nikdo z ubytovaných na ně už nereaguje (ubytovaní předpokládají, že jde opět o planý poplach).

V rámci imatrikulace v prvním ročníku byli žáci poučeni o tom jak se zachovat v případě požáru. Tato slavnostní událost ale nebyla povinná (ne všichni se zúčastnili) a značná část studentů nastoupila na fakultu až v rámci druhého kola přijímacího řízení. Z toho lze jednoznačně odvodit, že studenti nejsou dostatečně o požární ochraně poučeni. Chybí zde i praktický nácvik jak postupovat v případě požáru (nácvik objektové evakuace). Poučení o požární ochraně má zajistit pověřená osoba na fakultě, která zodpovídá, aby byli všichni studenti a zaměstnanci řádně poučeni o těchto interních předpisech.

Při realizaci požárního zabezpečení byla vystavěna požární schodiště pro evakuaci osob. Schodiště nalezneme na budově UH1, UH4, UH5. Budova UH2 požární schodiště nemá. Budovy UH4, UH5 mají zajištěné všechny podlaží požárním schodištěm (viz Obr. 2 a Obr. 7). U budovy UH1 schodiště končí u třetího podlaží, únik po požárním schodišti z nejvyššího podlaží (prostory půdní vestavby) tak není možný (viz Obr. 8). Bylo by vhodné schodiště dostavět do posledního podlaží, v kterém se nachází dva velké přednáškové sály, dále dvě učebny, studentská místnost, kancelář a sociální zařízení.

Obr. 5 Požární schodiště na budově UH5

Obr. 6 Požární schodiště na budově UH1

ZÁVĚR

Příspěvek se zaměřuje na problematiku spojenou se zabezpečením budov, které využívá v Uherském Hradišti pro potřeby vzdělávacího procesu FLKŘ UTB. V rámci realizovaného kritického posouzení reálného stavu tohoto zabezpečení lze konstatovat jak negativa (tak ale i pozitiva), na která by bylo vhodné odpovídajícím způsobem reagovat. Za hlavní nedostatek je možno považovat nainstalovaný kamerový systém, který je takřka neefektivní. V dalších případech se jedná o problematiku požárního schodiště u budovy UH1, čipové karty, hlásiče požáru, neoplocení areálu apod. Za kladnou stránku v zabezpečení lze považovat přítomnost pasivních infračervených čidel (PIR), které jsou umístěny ve vybraných místnostech objektů.

Přínosem příspěvku je identifikace slabých míst v rámci zabezpečení budov užívaných FLKŘ a zároveň vytvoření možných návrhů na zkvalitnění současného stavu tak, aby byla docílena nejideálnější účinná ochrana. Doporučení se dotýkají systému elektronické kontroly vstupů, kamerových záznamů, mechanického zábranného systému, elektronické požární signalizace a zlepšení pracovní činnosti z řad zaměstnanců – vrátných. Pokud by byly naše uvedené návrhy realizovány ze strany společnosti EDUHA s. r. o, jednoznačně by bylo dosaženo kvalitativně vyššího stupně v zabezpečení uvedených budov a tím i zvýšení úrovně bezpečnosti studentů a ostatních zaměstnanců této součástí UTB.

Literatura

[1] Ministerstvo vnitra České republiky. Národní kontaktní bod pro terorismus. [online]. [cit. 2018-11-10]. Dostupné z: http://www.policie.cz/clanek/kopie-terorismus.aspx?q=Y2hudW09Mw%3D%3D.

[2] Strategie České republiky pro boj proti terorismu od roku 2013. Praha: Ministerstvo vnitra, Odbor bezpečnostní politiky, 2013.

[3] Ministerstvo vnitra České republiky. Základy ochrany měkkých cílů. [Metodika] [online]. [cit. 2018-11-10]. Dostupné z: http://www.stpi.cz/soubor-doc907/.

[4] Ministerstvo vnitra České republiky. Zveřejnění české technické normy ČSN 73 4400 „Prevence kriminality – řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení“. [online]. [cit. 2018-11-10]. Dostupné z: http://www.mvcr.cz/clanek/zverejneni-ceske-technicke-normy-csn-73-4400-prevence-kriminality-rizeni-bezpecnosti-pri-planovani-realizaci-a-uzivani-skol-a-skolskych-zarizeni.aspx

[5] Ministerstvo vnitra České republiky. Vláda schválila Koncepci ochrany měkkých cílů pro roky 2017–2020. [online]. [cit. 2018-11-10]. Dostupné z: http://www.mvcr.cz/clanek/vlada-schvalila-koncepci-ochrany-mekkych-cilu-pro-roky-2017-2020.aspx.

[6] Mapy.cz [online]. [cit. 2018-11-10]. Dostupné z: https://mapy.cz/zakladni?x=17.4729726&y=49.0705011&z=18&q=fakulta%20logistiky%20a%20krizov%C3%A9ho%20%C5%99%C3%ADzen%C3%AD.

[7] ASParking [online]. [cit. 2018-11-10]. Dostupné z: http://www.asparking.cz/_media/asparking-fb91247f6951a7ff17da887adc993e9d/TRISTAR.pdf

[8] ASParking [online]. [cit. 2018-11-10]. Dostupné z: http://www.asparking.cz/_media/asparking-c0ccb6bc943f5cb09752d05929ef9b47/DNG460.pdf

HODNOCENÍ RANIVÉHO POTENCIÁLU EXPANZNÍ ZBRANĚ

EVALUATING THE POTENTIAL OF THE EXPANSIVE WEAPON

Ing. Martin Ficek[1], doc. Ing. Ludvík Juříček, Ph.D. [2], JUDr. Ing. Olga Vojtěchovská, Ph.D. [3]

[1]Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství
Nad Stráněmi 4511, 760 05 Zlín, Česká republika
Email: ficek@utb.cz
Telefon: +420 731 829 550

[2]Vysoká škola Karla Engliše, a.s.
Ústav bezpečnosti
Mezírka 775/1, 602 00 Brno, Česká republika
Email: ludvik.juricek@vske.cz
Telefon: +420 728 232 698

[3]Vysoká škola regionálního rozvoje a Bankovní institut – AMBIS, a.s. Praha
Katedra bezpečnosti a práva
Lindnerova 575/1, 180 00 Praha 8, Česká republika
Email: o.vojtechovska@atlas.cz
Telefon: +420 603 300 064

ABSTRAKT

Narůstá počet použití expanzních zbraní. Mezi lidmi zbraně známé jako „plynovky“ jsou palné zbraně relativně snadno dostupné v České republice každému občanu staršímu 18 let. Tyto zbraně jsou poměrně rozšířeny a stéle častěji používány v rámci obrany, ale také v rámci „řešení“ nejrůznějších konfliktů. Na tento fakt je nutné reagovat. Příspěvek se zabývá ranivým potenciálem expanzní zbraně. Ranivý potenciál je hodnocen prostřednictvím balistického experimentu, kdy je z relativní blízkosti postřelován zkušební blok nehomogenního náhradního materiálu. Průběh je zaznamenán a analyzován pomocí rychloběžné kamery, kdy je zjišťován tvar a objem trvalé dutiny v zasažené substituci. Dutina je následně zobrazena pomocí metody „profilu zranění“. Závěry jsou vyvozeny na základě provedeného kvantitativního i kvalitativního hodnocení. Poznatky mohou být použity v oblasti soudního lékařství, válečné chirurgie, traumatologie a experimentální ranivé balistiky.

KLÍČOVÁ SLOVA

Balistika, ranivá balistika, expanzní zbraň, plynová nábojka, akustická nábojka, balistický gel, střelecký (balistický) experiment, profil zranění, biologická tkáň, substituční fyzikální model.

ABSTRACT

The number of using of expansive weapons is increasing. Among the weapons known as "gas gun" firearms are relatively easely available in the Czech Republic to every citizen over the age of 18. These weapons are relatively widespread and more often used in defense, but also in the "solution" of various conflicts. This fact needs to be addressed. The paper deals with the wounding potential of the expansion weapon. The wounding potential is evaluated through a ballistic experiment where a non-homogeneous replacement material block is shot from a relative proximity. The process is recorded and analyzed by a high-speed camera, where the shape and volume of the permanent cavity is detected in the affected substitution.

The cavity is then displayed using the "injury profile" method. Conclusions are based on quantitative and qualitative assessments. Knowledge can be used in the field of forensic medicine, war surgery, traumatology and experimental ballistic balancing.

KEY WORDS

Ballistics, wounding ballistics, expansion weapon, gas cartridge, acoustic cartridge, ballistic gel, shooting (ballistic) experiment, injury profile, biological tissue, substitution physical model.

ÚVOD

Zbraně, které jsou v České republice zařazeny do kategorie D, mají prokazatelně výrazně nižší ranivý potenciál než zbraně kategorií A, B, či C. To je jeden z důvodů proč se jim v ranivé balistice nevěnuje taková pozornost jako zbraním dalších kategorií. Přesto jistá pozornost jim věnována je, dokladem tohoto tvrzení jsou například:

Zajímavých výsledků bylo dosaženo C. M. Milroy a kolektivem, v článku Air weapon fatalities.[1] Zde se autoři zaměřili na expanzní zbraň.

M. Gracla, A. Chocholatý, a Z. Maláník se ve svém článku Analysis of the Wounding Effect of Elementary Weapons of Category D Analysis of the Wounding Effect of Elementary Weapons of Category D.[2] analyzovali ranivý efekt vybraných zbaní katgorie D. Poznatky jsou ceněné zvláště pro policejní složky.

Ranivým potenciálem se zabývali i články autorů Carr, D. J., T. Stevenson, and P. F. Mahoney ve své publikaci The use of Gelatine in Wound Ballistics [3], nebo Mahoney, P., D. Carr, R. Arm, I. Gibb, N. Hunt, and R. J. Delaney v článku Ballistic Impacts on an Anatomically Correct Synthetic Skull with a Surrogate Skin/Soft Tissue Layer.[4]. Oba články přináší významné poznatky.

Autoři Mac Phee, N., A. Savage, N. Noton, E. Beattie, L. Milne, and J. Fraser ve svém článku A Comparison of Penetration and Damage Caused by Different Types of Arrow heads on Loose and Tight Fit Clothing.[5] Zkoumaly ranivý potenciál luků. Tento článek je zajímavý, neboť luky jsou řazeny taktéž do zbraní kategorie D a článek tak přináší cenné poznatky do této oblasti.

Relativně nová publikace Ranivá balistika. Technické, soudnělékařské a kriminalistické aspekty od Ludvíka Juřička a kolektivu [6] je z hlediska ranivé balistiky natolik významná, že ji lze označit za balistickou bibli.

Mikuličova, M., M. Gracla, M. Ficek a A. Kunčar v článku Comparison of Depth of Incomplete Penetration for Different Types of Pellets for Shooting Weapon of Category D.[7] zkoumají vliv munice na ranivý potenciál u vybrané zbraně kategorie D a přináší tak zajímavé poznatky, neboť se zaměřují na munici a její vlil na výsledný ranivý potenciál.

Jak je vidět jistá pozornost z hlediska ranivé balistiky je zbraním kategorie D věnována, ale i v této oblasti lze nalézt určité části, které jsou relativně málo zmapovány. A to především zbraně expanzní, které jsou schopny způsobit zranění jen z relativní blízkosti. To je patrně důvod, proč jim není věnována taková pozornost, jako jiným zbraním kategorie D.

Náš společný příspěvek se zabývá ranivým potenciálem expanzní zbraně a metodami jeho kvantitativního hodnocení.

1. HODNOTÍCÍ METODY

Ke zjištění úrovně ranivého potenciálu (RP) vybraných druhů expanzních zbraní byla použita metoda nepřímé identifikace ve spojení s balistickým experimentem. Ten spočíval v postřelování bloku nehomogenního substitučního modelu vyrobeného z náhradních materiálů biologické tkáně z absolutní blízkosti, kdy hlaveň expanzní pistole byla přiložena ke stěně tohoto bloku. Následná dynamika pohybu byla zaznamenána pomocí rychloběžné kamery. Vzniklá dutina byla poté vylita vodou a změřena její velikost (objem) a doplněna o profil zranění postihující její geometrický tvar.

K měření vzdáleností bylo použito digitální posuvné měřidlo Powerfix Z11155 s přesností ± 0,02 mm. Expanzní zbraň byla zvolena erxpanzní pistole Umarex Walther P22 se startovacími náboji Walther ráže 9 mm.

Blok substitučního materiálu byl snímán z pravého boku ve směru střelby ze vzdálenosti 3 metrů rychloběžnou kamerou Olympus I-SPEED FS s rozlišením 1 280x1 024, Clona je volitelná od 200 nanosekund ~~a~~ s maximální rychlostí 1,000,000 fps. Pro experiment byla zvolena frekvence snímání 20 000 fps.

Substituční materiál se skládal z balistické želatiny o dvou koncentracích, 20 % (odpovídá kosternímu svalstvu) a 10 % (ta odpovídá parametrům poněkud křehčím parenchymatózním tkáním, jako jsou např. ledviny, játra nebo plíce). Zkušební blok z balistické želatiny byl vytvořen podle následujícího pracovního postupu:

Želatina byla vmíchána do vody o pokojové teplotě za stálého míchání (bez tvorby bublin). Poté se nechala 2 hodiny odstát v ledničce o teplotě 10°C, následně se nádoba s želatinou usadila do vodní lázně o teplotě 40°C, kde byla ponechána do úplného rozpuštění želatiny. Poté se želatina přelila do předem připravené formy (vymazané transparentní vazelínou) a umístěna do lednice za účelem ztuhnutí při teplotě 10°C. Po ztuhnutí a kontrole byl želatinový blok vyjmut z formy a zabalen do připravené polyetylénové folie a umístěna do chladícího zařízení s nastavenou teplotou 4°C na dobu 36 hodin (dle M. L. Fackler) k jeho temperaci. Takto připravený želatinový blok byl použit k experimentálnímu postřelování.

Látka	t	ρ	K	η	ν	c
	[°C]	[kg.m^{-3}]	[Pa^{-1}]	[Pa.s]	[m^2.s^{-1}]	[m.s^{-1}]
Želatina 10 %	20	1 022	$4{,}05.10^{-10}$	35.0	0,03	1 514
Želatina 20 %	20	1 054	$3{,}68.10^{-10}$	$0{,}9.10^{2}$	0,09	1 535

Tab. 1 Fyzikální parametry balistických želatin

t – teplota, ρ – hustota, K – stlačitelnost, η – dynamická viskozita, ν – kinetická viskozita, c – rychlost zvuku

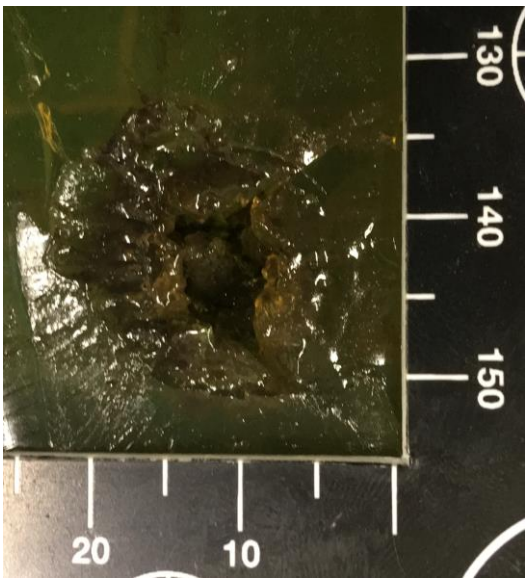
Želatina byla rozměrově upravena: želatina o koncentraci 20 % na rozměry 10x10 cm a tloušťce 2,5 cm což odpovídá průměrné tloušťce vrstvy zádového svalstva (musculus latissimus dorsi) dospělého muže v oblasti beder. A želatina o koncentraci 10 % na rozměry 10 x 10 cm a tloušťce 5 cm, což odpovídá šířce tloušťce průměrné ledviny dospělého muže.

Metoda profilu zranění podle *M. L. Facklera* a *A. Malinowskeho* je grafickým popisem účinku střely v bloku balistické želatiny. Profil zranění popisuje maximální porušení živé tkáně, které může být od dané střely očekáváno.

Při tvorbě tohoto profilu se sledují čtyři složky účinku střely na želatinový blok - hloubku vniku střely do zkušebního bloku, - velikost (objem) dočasné dutiny, - velikost trvalé dutiny a - přítomnost fragmentů (dojde-li k rozpadu těla střely).

2. VÝSLEDKY

Po ukončení postřelování zkušebního bloku bylo zjištěno, že trvalé poškození utrpěla pouze první vrstva tvořená balistickou želatinou o koncentraci 20 %. Vzniklá dutina byla vylita vodou a změřeno její množství, které bylo 0,71 ml, což představuje objem dutiny 0,71 cm^3.

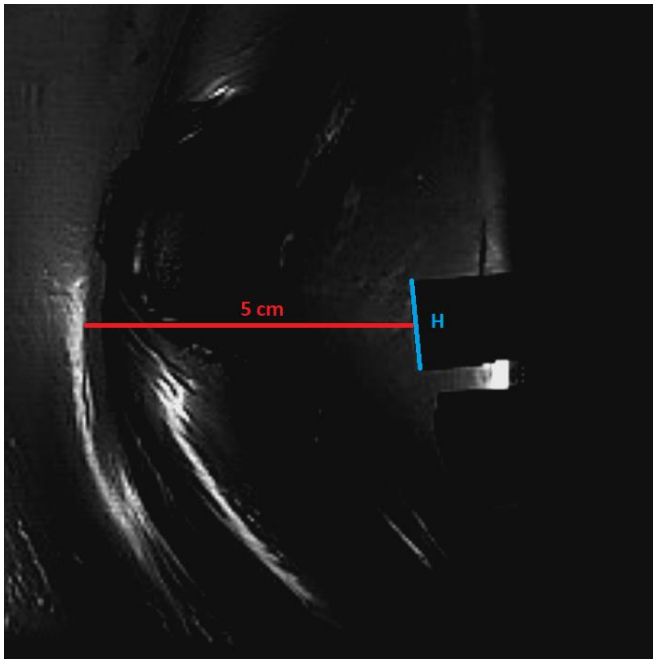


Obr. 1 Fotografie balistické želatiny po jejím postřelování – trvalá dutina v želatinovém bloku o koncentraci 20 % postřelovaného expanzní zbraní ráže 9 mm

Na obrázku je vidět trhlina oválného tvaru. Dosahuje hloubky až cca 2 cm a průměru 0,6 až 0,9 cm. Tvar vzniklé dutiny je těžko popsatelný, je nepravidelný a mění se s její hloubkou. Svým geometrickým uspořádáním se snad nejvíce blíží rotačnímu tělesu.

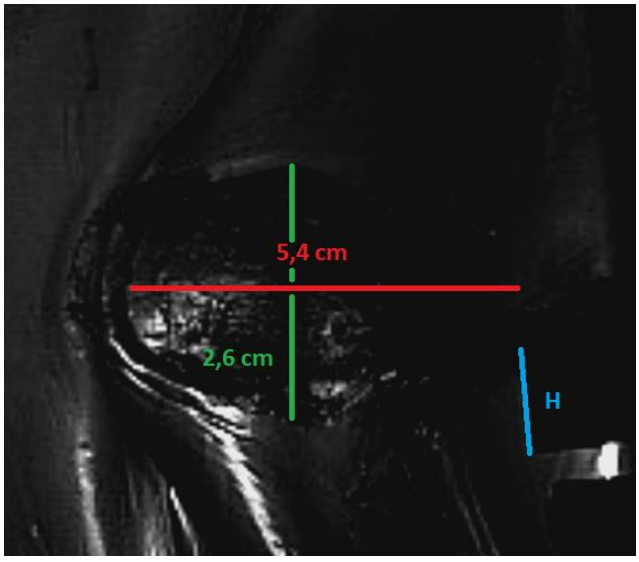
Obr. 2 Fotografie transparentní balistické želatiny po postřelování – trvalá dutina v želatinovém bloku – hloubka zástřelu

K měření byl použit princip velikosti pixelu. Byl změřen velikost výsledného kanálu, spočten počet pixelů a na základě toho vypočtena velikost jednoho pixelu. Jelikož snímky byly ve stejné kvalitě, mohl být tento údaj použit pro všechny fotografie pořízené rychloběžnou kamerou.



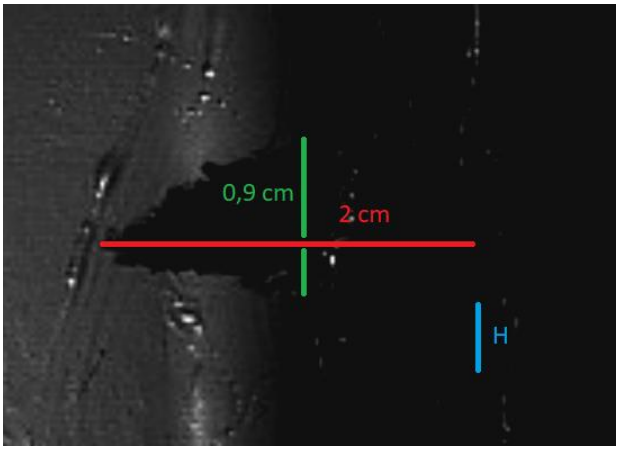
Obr. 3 Rázová vlna v želatinovém bloku o koncentraci 20 %

Na obrázku č. 3 lze vidět rázovou vlnu v bloku balistické želatiny. Vzdálenost maxima vlny od hlavně je znázorněna červenou úsečkou o délce 5 cm. Modrou čárou a písmenem H je znázorněno ústí hlavně expanzní pistole.



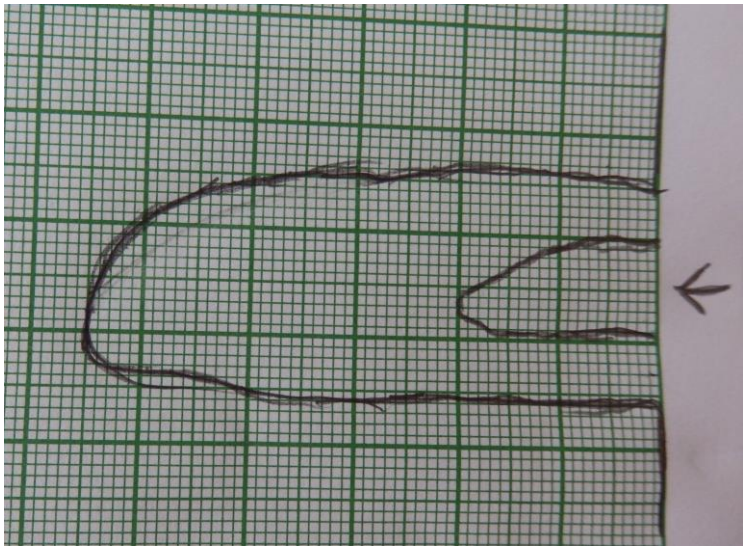
Obr. 4 Snímek dočasné dutiny v želatinovém zkušebním bloku

Dočasná dutina je zobrazena na obrázku č. 4. Zde je opět modrou barvou a písmenem H zobrazeno ústí hlavně expanzní pistole. Také zde je znázorněna maximální hloubka, které je znázorněna úsečkou červené barvy délky 5,4 cm a maximum průměru znázorněné zelenou úsečkou velikosti 2,6 cm. Dutina je dočasná a po dosažení svého maxima ~~a~~ následuje fáze smrštění do podoby trvalé dutiny.



Obr. 5 Trvalá dutina

Na obr. 5 lze vidět absolutní maxima trvalé dutiny. I zde je hlaveň znázorněna písmenem H a modrou barvu. Hloubka zástřelu je znázorněna červenou barvou o velikosti 2 cm a výškou zelené barvy o velikosti 0,9 cm. Zde již je zobrazena trvalá dutina. Fáze smršťování a rozpínání již skončili a výsledný kanál by odpovídal zranění ve svalové tkáni.



Obr. 6 Schematické zobrazení (nákres) profilu zranění

Obr. 6 zobrazuje grafické znázornění trvalého kanálu a současně dočasné trhliny (profil zranění). Ten je zobrazen na milimetrovém papíře. Je na něm velmi dobře vidět rozdíl tvaru a velikosti mezi trvalou a dočasnou dutinou.

ZÁVĚR

Tento příspěvek se zabýval ranivým potenciálem expanzní zbraně a jeho ranivě balistickým hodnocením. Expanzní zbraň způsobí zranění pouze na blízkou vzdálenost a klinická závažnost střelného poranění je závislá na této vzdálenosti. Z tohoto důvodu byly zvoleny podmínky střeleckého experimentu, kdy je hlaveň expanzní pistole přiložena ke stěně substitučního materiálu a zkušební střelba je vedena z absolutní blízkosti.

Trvalá dutina způsobila relativně vážnější zranění. To lze spatřit na obrázcích číslo 1, 2 a 5. Hloubka trvalé dutiny dosahuje až 2 cm. a průměr až 0,9 cm. Průměrná svalová tkáň u dospělého muže v oblasti beder dosahuje tloušťku přibližně 2,5 cm. Tato oblast je zmíněna záměrně, neboť za ní se nacházejí ledviny, které jsou životně důležitým párovým orgánem člověka uloženým v hloubce. Takto byl koncipován i substituční fyzikální model tedy 2,5 cm tlustý blok balistické želatiny o koncentraci 20 % nahrazující zádové svalstvo a 5 cm tlustý blok balistické želatiny o koncentraci 10 % nahrazující vitální orgán ledvinu.

Přestože, jak již bylo řečeno, trvalá dutina je pouze v první části substituce (tedy v oblasti svalstva) dočasná dutina dosahuje více než dvounásobné délky. Rozdíl mezi oběma dutinami je patrný na obr. 6, který znázorňuje grafický profil zranění. To je velmi nebezpečné neboť šok, který utrpí tkáně, především parenchymatózní (ledviny), je značný a může vést až ke kolapsu daného orgánu. Tedy akutnímu selhání ledviny což může vést až ke smrti daného jedince. Je třeba brát na zřetel, že v provedeném experimentu nebyl zohledněn kožní kryt, který daný efekt zbraně relativně výrazně snižuje. Již v těchto dnech připravujeme balistický experiment, kde tato skutečnost (přítomnost kůže) bude zohledněna. Bude velmi zajímavé a současně přínosné sledovat rozdíly v ranivém potenciálu expanzní zbraně u substitučního materiálu s kůží a bez ní.

Expanzní zbraně jsou v podmínkách ČR volně dostupné od 18 let. Tyto zbraně jsou relativně bezpečné. Nebezpečnými se stávají teprve po té, co jsou použity skutečně na velmi krátkou vzdálenost. Obecně se jedná dle použitého střeliva od několika desítek centimetrů (maximálně

50 cm) až do absolutní blízkosti (přiložení zbraně). Dle vzdálenosti způsobí od lehkých popálenin (termická poranění) až po výrazné poškození tkání (devastační poranění). V tomto příspěvku byla zvolena varianta s maximálně dosažitelným ranivým potenciálem. Výsledky získané tímto experimentem mohou být přínosné pro oblasti soudního lékařství, válečné chirurgie, traumatologie, ale také experimentální ranivé balistiky.

PODĚKOVÁNÍ

Tato práce byla, podpořena Interní grantovou agenturou Univerzity Tomáše Bati pod číslem projeku IGA/FAI/2018/014.

Literatura

[1] C. M. Milroy, J. C. Clark, N. Carter, G. Rutty, and N. Rooney, *Air weapon fatalities*, JOURNAL OF CLINICAL PATHOLOGY, pp. 525-529

[2] M. Gracla, A. Chocholatý, and Z. Maláník, *Analýza ranivého účinku základních zbraní kategorie D*, ve Sborníku příspěvků konference Expert Forensic Science Brno 2017 (ExFoS 2017): XXVI. mezinárodní vědecká konference soudního inženýrství, 2017, pp. 327-336.

[3] Carr, D. J., T. Stevenson, and P. F. Mahoney. 2018. *The use ofGelatine in WoundBallistics Research.* V International Journal of Legal Medicine: 1-6. 2018 doi:10.1007/s00414-018-1831-7. Dostupné na WWW: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046414181&doi=10.1007%2fs00414-018-1831-7&partnerID=40&md5=0f19ce6504f6a8d89aa68c6985db5390

[4] Mahoney, P., D. Carr, R. Arm, I. Gibb, N. Hunt, a R. J. Delaney. *BallisticImpacts on an Anatomically Correct Synthetic Skull with a Surrogate Skin/Soft Tissue Layer.* V International Journal of Legal Medicine 132 (2): 519-530. 2018. doi:10.1007/s00414-017-1737-9. Dostupné na WWW: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046841930&doi=10.1007%2fs00414-017-1737-9&partnerID=40&md5=792c144fc7af41d5e2e0ac186e19579d

[5] MacPhee, N., A. Savage, N. Noton, E. Beattie, L. Milne, and J. Fraser. *A Comparison of Penetration and Damage Caused by Different Types of Arrow heads on Loose and Tight Fit Clothing.* V Science and Justice 58 (2): 109-120. 2018. doi:10.1016/j.scijus.2017.11.005. Dostupné na WWW: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85035351282&doi=10.1016%2fj.scijus.2017.11.005&partnerID=40&md5=b99b5ed7f31f38963c0ace1d6b7363b5

[6] JUŘÍČEK, Ludvík, *Ranivá balistika. Technické, soudnělékařské a kriminalistické aspekty*. Ostrava: Key Publishing, 2017, 614 s. ISBN 978-80-7418-274-7.

[7] Mikulicova, M., M. Gracla, M. Ficek, and A. Kuncar. *Comparison of Depth of Incomplete Penetration for Different Types of Pellets for Shooting Weapon of Category D.* 2017. doi:10.1109/MILTECHS.2017.7988732. Dostupné na WWW: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85029374209&doi=10.1109%2fMILTECHS.2017.7988732&partnerID=40&md5=4dc468ee0e12e181fcfe61daf3fa2d41

KRIZOVÉ ŘÍZENÍ V KONTEXTU KYBERNETICKÉ BEZPEČNOSTI

CRISIS MANAGEMENT IN THE CONTEXT OF CYBER SECURITY

Ing. Radek Fujdiak, Ph.D., doc. Ing. Petr Mlýnek, Ph.D., prof. Ing. Jiří Mišurec, CSc.
Vysoké učení technické v Brně
Technická 12, Brno 61600, Česká Republika
fujdiak, mlynek, misurec@feec.vutbr.cz

ABSTRAKT

Technologický rozvoj společnosti vyústil ve vytvoření kybernetického prostoru, který napomáhá v každodenní činnosti veřejných i privátních institucí a stal se součástí běžného života lidské společnosti. Tato čím dál větší závislost na kybernetických systémech však nepřináší jen ulehčení každodenních úloh a procesů, nicméně s sebou nese také mnohé společensko-vědecké výzvy, kde jednou z nejvýznamnějších je právě kybernetická bezpečnost. Složitá definice kybernetického prostoru pak bohužel ještě více znesnadňuje úlohu kybernetické bezpečnosti, jelikož díky samotné abstrakci a nejednotnosti jsou vytvářena pouze polovičatá řešení, která neobsáhnou či nebrání kybernetický prostor komplexně. Tento článek se zabývá nejen samotnou definicí kybernetického prostoru a shrnuje tak dosavadní současný stav, ale představuje zjednodušenou formu definice kybernetického prostoru, společně s ustálením terminologie v podobě kybernetického bezpečnostního incidentu či kybernetické krize. Nad rámec terminologie jsou pak představen průběh takových událostí, možné mitigační opatření i metodiku pro kybernetickou bezpečnost.

KLÍČOVÁ SLOVA

Kybernetický prostor; kybernetická bezpečnost; kybernetický bezpečnostní incident; kybernetická krizová situace; kritická infrastruktura; krizové řízení; řízení rizik; terminologie.

ABSTRACT

The technological development resulted in the creation of cyberspace, which helps with activities of public and private institutions and becomes a part of the every-day life. However, the increasing dependency on cyber systems does not only come with the simplification of everyday tasks and processes, but it also brings many socio-scientific challenges with cybersecurity being one of the most important. Unfortunately, the complex definition of cyberspace makes the role of cybersecurity even more difficult, thanks to the level of abstraction and inconsistency. Therefore, the solutions are often insufficient and do not obstruct or defend whole cyberspace. This paper deals with simplification for the definition of cyberspace, cyber security, cyber security incident or cyber crisis, all based on state of the art and best practices. Above the terminology, we explain the life-cycle of cybersecurity incidents, introduces possible mitigation measures, and highlight the common mistakes in cybersecurity.

KEYWORDS

Cyberspace; cybersecurity; cybersecurity incident, cyber crisis; critical infrastructure; crisis management; risk management; terminology.

ÚVOD

Rozvoj kybernetiky a kybernetických systémů, který pohání společně i vývoj informačních technologií či mnohých dalších, přinesl mnoho nových možností i výzev. Kybernetický prostor je jedením z fenoménů dnešního světa, který stále není zcela definován a je vnímán mnohými způsoby [1]. I přesto, že kybernetický prostor není zcela přesně definován, pohybujeme se v něm téměř každý den, obklopuje nás a využíváme výhody jeho existence. Samotné propojení systémů, sítí, zařízení a moderní způsob přenosu informací dává za vznik trendům v podobě internetu věcí, chytrých měst, chytrých továren, inteligentních budov a spousty dalších odvětví, které využívají přenos, analýzu i zpracování dat či informací [4]-[6].

Rostoucí závislost na kybernetickém prostoru však s sebou přináší i mnohé nové výzvy, kde jednou z největších se bezesporu stává kybernetická bezpečnost, která se stává globálním problémem [2]. Každoročně se stávají národní agentury i privátní sektor cílem pro tisíce až milióny úspěšných kybernetických útoků, společně s pokusy o kybernetickou infiltraci a další způsoby hackingu či škodlivého kriminálního chování [3]. Kybernetická bezpečnost je také častou otázkou krizového řízení, krizové politiky a krizových situací [7]-[12]. Nepřesná, neúplná i nejednotná definice kybernetického prostoru pak již jen přispívá k samotné složitosti zabezpečení kybernetického prostoru.

Můžeme si představit jednoduchý příklad, kdy se snažíme fyzicky zabezpečit klasický rodinný dům. Pokud definujeme možný vstup do domu (systému) pouze jako hlavní vstupní dveře, bude naše obrana proti zloději (kriminálnímu chování – kybernetickému útoku) nedostatečná. I v takto jednoduchém případě lze uvažovat vstupy jako zadní dveře (úmyslné či neúmyslné tzv. backdoors systému), okna (nezamýšlený vstup do systému) a spousty dalších. Tedy i na takto jednoduchém příkladu lze vidět, že pokud nejsme schopni definovat veškeré vstupy a systém jako celek, není možné jej efektivně a dostatečně chránit či navrhnout bezpečnostní opatření pro jeho ochranu. V kybernetickém prostoru se pak jedná o chápání prostoru např. pouze jako virtualizované prostředí, pouze jako softwarová řešení bez hardwarových prvků, či pouze jako hardwarové prvky zpracovávající informace a dalších [13]-[15]. Nicméně dnešní definice se již od sebe takto přímým způsobem od sebe neliší, čímž je mnohem těžší rozeznat přené hranice kybernetického prostoru a vytvářet tak efektivní bezpečnostní mechanismy. Tento článek je zaměřen na srovnání jednotlivých hlavních definic kybernetického prostoru a terminologii spojenou s tímto termínem, společně s definicí kybernetické bezpečnosti i minimalizaci případných incidentů uvnitř kybernetického prostoru, v základů tak článek odpovídá na tyto identifikované otázky:

(1) Co je to kybernetický prostor?

(2) Jak se tedy bránit v něčem tak abstraktním jako je kybernetický prostor a proč je tento pojem definován různorodě?

(3) Jakým způsobem vznikají kybernetické bezpečnostní incidenty?

(4) Kdy se stává z incidentu - krize? Jaký je vlastně rozdíl mezi těmito událostmi?

(5) Jak se efektivně připravit a reagovat na kybernetické bezpečnostní incidenty?

(6) Je možné kybernetickým incidentům či dokonce krizovým situacím předcházet?

(7) Jak minimalizovat dopady kybernetických krizových incidentů?

Článek je dále rozdělen následujícím způsobem. První kapitola se zabývá analýzou současného stavu a základní terminologií, tedy zodpovězení otázek, co je to kybernetický prostor, kybernetický incident, kybernetická krizová situace, vztah k dnešnímu chápání

krizového řízení či kritické infrastruktuře a další. Druhá kapitola se již zabývá celým cyklem kybernetického bezpečnostního incidentu. Kapitola třetí pak již řeší obecně kybernetickou bezpečnost, minimalizaci dopadů i samotnou metodiku pro kybernetickou bezpečnost. Poslední kapitola pak již závěrem shrnuje nalezené poznatky.

1. ANALÝZA A STATNOVENI ZÁKLADNÍ TERMINOLOGIE

Dříve než bude možné přistoupit k diskuzi o krizovém řízení v rámci kybernetického prostoru je nutno prvně definovat základní pojmy: kybernetický prostor, kybernetická bezpečnost a kybernetický incident. Z pohledu kybernetického prostoru a kybernetické bezpečnosti je situace poněkud složitější. Velmi dlouhou dobu v podstatě neexistovala přesná definice pojmu „kybernetický prostor“, ale ani pojmu „kybernetický bezpečnostní incident“. Průzkum [22] z roku 2012 ukazuje jistou podobnost mnoha definic, kterou lze sumarizovat do následujících bodů:

- Většina definic se shoduje, že kybernetický prostor obsahuje hmatatelné prvky (hardware) a nemůže tedy bez nich existovat.
- Většina definic se shoduje, že kybernetický prostor obsahuje informace, které jsou jeho základní prvkem. Informace mohou být uložená data, signalizace mezi procesy a/nebo zařízeními či přenášena.

Internet nemusí být nutně součástí, naopak se spíše tyto definice soustředí na samotnou podstatu a tedy propojenost jednotlivých struktur.

Nicméně i samotný průzkum sumarizuje fakt, že většina organizací neměla v dané době striktně definován pojem kybernetický prostor mj. jmenována i Evropská Unie. V roce 2016 vnikl dokument [23] publikovaný Evropskou agenturou pro bezpečnost sítí a informací (ENISA). Dokument vychází mj. z definic uváděných ve standardech ETSI, ISO/IEC, ITU, NIST, NATO a CNSS. V neposlední řadě pak definuje pojmy kybernetická bezpečnost a kybernetický prostor jako:

- Kybernetická bezpečnost odpovídá bezpečnosti v kybernetickém prostoru, kde kybernetický prostor odpovídá vazbám a vztahům mezi objekty, které jsou přístupné zobecněným modelem telekomunikační sítě, ale také samotným objektům, které reprezentují rozhraní umožňující jejich vzdálenou kontrolu, vzdálený přístup k datům, či jejich participaci na kontrolních procesech v rámci kybernetického prostoru.

Tato definice v podstatě shrnuje obecné mínění o kybernetickém prostoru a je v soulad i s výsledky předchozího průzkumu z roku 2012. ENISA také v tomto dokumentu zmiňuje velmi zajímavý fakt o napojení fyzických objektů (fyzických aktiv) jako jsou např. průmyslových systémů (ICS, SCADA, aj.), produkčních linek, elektráren, a dalších objektů, které původně nebyly zamýšleny ani vyvíjeny proto být napojeny na kybernetický prostor. Tento fakt je velmi důležitý v uvědomění si možných nových hrozeb a rizik spojených právě s napojením takových systémy do kybernetického prostoru. Samotná definice kybernetického prostoru a kybernetické bezpečnosti je však velice rozsáhlá, a pokud vezmeme v potaz nové paradigma internetu věcí, chytrých měst, továren a dalších, zahrnuje tato definice kompletně celé propojené město, stát i svět. Z pohledu autorů se dá v rámci definice kybernetického prostoru použít představené definice i již velmi známé a zažité pojmy pro vytvoření jednoduché a uchopitelné definice.

Úvaha: Pokud rozložíme kybernetický prostor na jednotlivé části, můžeme velice jednoduše definovat pojmy „kyber“ (vztahováno k či charakterizující moderní kulturu počítačů, informačních systémů, informačních technologií a virtuální reality; pojem „kybernetika“ pak

značí vědu zabývající se obecnými principy řízení a přenosu informací ve strojích a živých organismech. Prostor nejspíše vytváří právě onen prvek, který vytváří v různorodých definicích jiné chápaní kybernetické bezpečnosti, jelikož samotný pojem, používán napříč téměř všemi vědeckými obory, znamená vždy něco jiného. Z tohoto důvodu věříme, že lze s nadsázkou vytvořit zjednodušený pojem kybernetického prostoru jako „prostor, kde dochází ke vzniku, zpracování, zachování a zániku informací“. Jeho konec i začátek můžeme zanechat relativní a může být určen vždy až samotným omezením díky aplikaci, použití, vlastnímu citu a dalším. Nicméně abychom stanovili jisté hranice, omezíme pojem „informace“ dle definice Norberta Wienera jako sdělení, komunikovatelný poznatek, které má význam pro příjemce nebo údaj usnadňující volbu mezi alternativními rozhodovacími možnostmi vztažený pro oblast kybernetiky a informační vědy [30], [31].

Dle českého kybernetického zákona je pozornost pak spíše směřována na tématiku kybernetických bezpečnostních událostí, které se rozdělují na dva základní typy: (i) bezpečnostní událost a (ii) bezpečnostní incident [16]:

- Kybernetická bezpečnostní událost může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
- Kybernetický bezpečnostní incident je na druhé straně narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.

Z tohoto pohledu, když vezmeme v potaz definici kybernetického prostoru, pak bezpečnostní událost a incident může být v podstatě cokoliv, což opět velmi znesnadňuje případné krizové řízení a řízení rizik.

Z pohledu krizové situace jsou tyto definice nedostatečné, nicméně termín krizová situace je definován v [18] jako „škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací, narušení kritické infrastruktury nebo jiné nebezpečí, při nichž je vyhlášen stav nebezpečí“. Z pohledu krizové situace jsou pak zmíněny čtyři druhy krizové situace: stav nebezpečí, nouzový stav, stav ohrožení státu a válečný stav. Tyto stavy nejsou pouze informativní, ale navazují na celou řadu postupů a nařízení spojených se zvládáním i řízením nastalé situace. V rámci krizového řízení však chybí navázání na kybernetickou bezpečnost a identifikace kybernetické krizové situace. Nepřímé navázání můžeme vidět v rámci krizového zákona v definici kritické infrastruktury, jejíchž narušení by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu [24]. V rámci mezinárodních definic existuje několik pohledů, viz Tab. 1.

	Evropská Unie	**Akademické prostředí**	**Praxe**
Kybernetický incident	Kybernetický incident nastane přerušením informačních služeb, tedy narušením dostupnosti (částečně či úplně). Dále sem patří i mj. nezákonné zveřejnění, získávání a/nebo změna informací uložených v informačních systémech.	Narušení či bezprostřední hrozba pro bezpečnostní politiku.	Škodlivý čin či událost, která kompromituje (či se pokouší kompromitovat) elektronickou či fyzickou bezpečnost či narušuje (pokouší se narušovat) provoz kybernetického systému.

Kybernetická krizová situace	Abnormální či nestabilní situace, která ohrožuje strategické cíle organizace, její pověst či životaschopnost. V podstatě událost zasahující nitro organizace.	Vážná hrozba pro základní struktury nebo základní hodnoty a normy systému (v kybernetickém prostoru) vyvolávající nutnost v časovém tlaku a nejisté situaci učinit rozhodnutí.	Situace, kdy je narušena rovnováha mezi základními komponenty systému a samotným prostředím systému.

Tab. 1 Přehled definic pro pojmy kybernetický incident a kybernetická krizová situace [25], [26], [27], [28], [29]

Tedy rozdíl mezi kybernetickým incidentem a kybernetickou krizovou situací je v rozsahu, kdy kybernetickým incidentem je pouhé narušení či pokus o narušení např. dostupnosti jedné z poskytovaných služeb (v rámci chytrého města si můžeme představit např. DDoS útok na chytré osvětlení poskytující lokálně konektivitu k Internetu). Nicméně krizová situace zde má mnohem větší rozsah a dopad – opět velmi teoreticky řečeno. Důvod však pro obecnou definici je velmi prostý, každá organizace, město, stát či organizační složka zodpovídá za jiné aktivum, disponuje jinými zdroji a definuje různou důležitost jednotlivých aktiv. Z tohoto pohledu tedy není prakticky možné, vytvořit specifičtější popis než byl v tomto ohledu představen výše. Z našeho pohledu je tedy kybernetická krizová situace jen speciální typ kybernetického bezpečnostního incidentu se specifickými vlastnostmi. Kybernetickou krizovou situaci nicméně doprovází také většinou i další vlastnost oproti klasickému kybernetickému bezpečnostnímu incidentu – kybernetická krizová situace je většinou méně předvídatelná (mnohdy uvažována jako situace s minimální pravděpodobností).

Pokud bychom měli být více specifičtí, můžeme vztáhnout kybernetický bezpečnostní incident a kybernetickou krizovou situaci např. na kritickou infrastrukturu (KI, definovanou dle nařízení vlády 432/2010 Sb. [32]), kde máme ochranu prvků kritické infrastruktury rozdělenou na bezpečnostní kategorie I. až V. (či nezabezpečeno) [33]. Nejvyšší Kategorie I odpovídá převážně objektům jaderné povahy (dle vyhlášky č. 361/2016 b. [34]), kde narušení bezpečnosti by mělo v tomto případě národní až nadnárodní charakter. Kategorie II navazuje na prvky KI ČR tzv. nenahraditelné či obtížně nahraditelné objekty, které mají kritický význam pro fungování a řízení dodávek elektrické energie a při výpadku by došlo ke kritickému dopadu na systém dodávek elektrické energie i pro navazující objekty (např. technický dispečink provozovatele, energetické stanice přenosové soustavy s napětím nejméně 110 kV aj.). Následně pak Kategorie III představuje prvky se zásadním významem pro KI, tedy obtížně nahraditelné prvky, kdy vliv je převážně většího lokálního charakteru (např. kraj). Kategorie IV jsou objekty s důležitým významem pro zabezpečení funkčnosti prvků KI (podpůrné prvky pro Kategorie II a III), kdy jejich vyřazením by došlo ke komplikacím dodávek elektrické energie. V neposlední řadě pak Kategorie V představuje objekty podprůměrného charakteru s malým významem pro zabezpečení funkčnosti prvků KI (příkladem může být distribuční stanice vysokého a nízkého napětí DTS VN/NN), kdy vyřazení má pouze místní charakter (např. vesnice). Následně poslední kategorie tzv. objekty nezařazeny do bezpečnostní kategorie jako např. sklady aj., které nemají žádný vliv na dodávky elektrické energie.

Na tomto příkladu můžeme nejen vidět, že je definována bezpečnost vůči nějakému aktivu (dodávka elektrické energie), ale také rozdělena dle závažnosti. Jsou vyjmuty prvky, které nemají žádný vliv na dané aktivum, které není z toho pohledu tedy nutné chránit (ale z jiného pohledu následně např. ano – logistika aj.), a na bezpečnostní Kategorie dle vlivu na dané aktivum. Kategorie I, II a nejspíše i III se dají považovat za odstupňování závažnosti krizové situace, díky jejich velkému vlivu na dané aktivum. Následně pak již máme pouze

bezpečnostní incidenty závažného (IV) a méně závažného (V) charakteru. Je však nutné si také uvědomit, že pokud by výpadek Kategorie V měl větší rozsah, tedy nedošlo by k narušení prvků vyšší kategorie, ale pouze k většímu množství prvků Kategorie V, může i tato událost přejít v krizovou situaci.

Z tohoto pohledu je tedy nutno vždy stanovit pro bezpečnostní (kybernetických) incident jeho rozsah i dopad, aby bylo možné správně zvolit následně odpovídající protiopatření, které bude mít za následek postupné zotavení se a obnovení standardního chodu systému. Z pohledu řízení rizik pak přibývá samozřejmě ještě pravděpodobnost, která nám dává pak celý obraz pro rozhodovací procesy.

2. CYKLUS KYBERNETICKÉHO BEZPEČNOSTNÍHO INCIDENTU

Vznik bezpečnostního incidentu je zpravidla zapříčiněn aktivním či pasivním působení na daný systém či aktivum. Za pasivní můžeme považovat např. chyby systému, nezamýšlené narušení bezpečnosti systému chybnou manipulací a další. Aktivní příčiny jsou způsobeny škodlivým chování s cílem uškodit danému systému či vidinou vlastního zisku (informačního, finančního a jiného). Vznik kybernetických bezpečnostních incidentů viz Tab. 2.

Tradiční (informační) bezpečnostní incidenty	Kybernetické bezpečnostní útoky
Škodlivé kriminální činy malého rozsahu, jedincové či skupiny se „baví“ na účet uživatele, lokální či komunitní „hacktivismus“, incidenty způsobené zevnitř.	Závažné škodlivé kriminální (organizované) činy, útoky sponzorované státy či podobnými vlivnými skupinami, incidenty způsobené extrémistickými skupinami.

Tab. 2 Vznik kybernetických bezpečnostních incidentů [35]

Existují různé názory a definice pro cyklus bezpečnostních incidentů. CREST vidí cyklus bezpečnostního incidentu jako tří fázový [35]: (i) příprava, (ii) odpověď, a (iii) ponaučení. Deloitte následně popisuje cyklus také jako třífázový [36]: (i) příprava, (ii) odpověď, a (iii) zotavení. Odborníci z belgického centra pro kybernetickou bezpečnost vidí opět celý cyklus jako třífázový [37]: (i) příprava, (ii) detekce, a (iii) zadržení, mitigace a zotavení. Nicméně např. národní agentura NIST vidí čtyři fáze [38]: (i) detekce a analýza, (ii) zadržení a zotavení, (iii) po-incidentní stav, a (iv) příprava. Stejně tak akademici z australské univerzity Newcastle rozlišují čtyři fáze [39]: (i) příprava, (ii) detekce/analýza, (iii) zadržení, mitigace, zotavení, a (iv) po-incidentní stav. Experti z kanadské JUNO však vidí cyklus jako pěti fázový [40]: (i) plánování a příprava, (ii) detekce a report, (iii) vyhodnocení a rozhodování, (iv) odpověď, a (v) po-incidentní stav. Akademici z Carnegie Mellon dokonce rozlišují až šest fází [41]: (i) příprava, (ii) detekce, (iii) zadržení, (iv) vyšetřování (analýza), (v) náprava, (vi) zotavení. Pokud vezmeme v potaz časovou osu incidentu a tedy dobu před, během a po incidentu, můžeme jednotlivé fáze následně rozprostřít v čase, viz Tab. 3.

Plánování	Příprava	Protekce	Detekce	Vyhodnocení	Report	Odpověď	Zotavení	Ponaučení
Před			**Během**				**Po**	
Hodnocení bezpečnosti. Risk analýza. Hazard analýza. Edukace. ... Vytvoření vhodné obrany. Vytvoření vhodného plánu.			Identifikace kybernetického bezpečnostního incidentu. Odpověď a reakce na základě vytvořeného plánu. Volba vhodné odpovědi (akce). ... Obnova systému, dat, konektivity a zotavení se.				Analýza incidentu, jeho průběhu, dopadu i zvolené reakce. Vyhodnocení a informovaní o zjištěných chybách. ... Optimalizace, zapracování, aktualizace. Analýza nových trendů.	

Tab. 3 Činnosti v rámci průběhu bezpečnostního incidentu [35],[36], [37], [38], [39], [40], [41]

Po skončení incidentu, zotavením a následně ponaučením ze získaných zkušeností nastává vždy opět fáze před incidentem, kdy daný cyklus opět pokračovat. Tedy jedná se o zacyklenou smyčku, protože je vždy pouze otázka času, než se vyskytne další bezpečnostní incident.

3. BEZPEČNOSTNÍ INCIDENTY V KYBER-PROSTORU

Je nutno si uvědomit, že není možné identifikovat zcela všechny možné zranitelnosti v rámci vybraného systému či kybernetického prostoru obecně. Z tohoto pohledu pak je jasné, že také není možné následné eliminovat pravděpodobnost vzniku těchto neidentifikovaných bezpečnostních incidentů. Obecně se jedná o zdravý balanc mezi zdroji (finance, materiál, personál) a kybernetickou bezpečností uvažovaného systému. Znamená to tedy najít akceptovatelnou úroveň zabezpečení, založenou na akceptovatelné úrovni pravděpodobnosti vzniku či dopadu rizika bezpečnostního incidentu. Z naší praxe lze odvodit následující metodiku pro definovanou fázi před bezpečnostním incidentem:

(i) **Definice vstupů** (Aplikace a Aktiva). Jeden z nejdůležitějších prvků, pomocí kterého jsou řízeny všechny následující akce. Stanovení aktiv, které je nutno chránit i modelu (vnitřní a vnější vazby i navazující hrozby),

(ii) **Teoretická evaluace** (Chyby, Zranitelnosti, Rizika a Hrozby). Teoretické ověření pomocí tzv. white/grey/black boxingu (pomocí kompletní, částečné či žádné dokumentace), spadají sem i různé rizikové analýzy, hazard analýzy, „co-když“ analýzy (What-If? či Hazop) a další.

(iii) **Praktická evaluace** (Modelování). Praktická evaluace zaměřená převážně na ověřování pomocí modelovacích nástrojů, příkladem může být i např. pokročilá virtualizace.

(iv) **Fyzická evaluace** (Funkční a penetrační testy). Funkční testování pomocí pasivních metod, ověřování správnosti implementace atd. Penetrační testování tedy pomocí aktivních metod (mj. i sociální inženýrství aj.).

(v) **Vyhodnocení** (Optimalizace, Mitigace, Rozhodování). Mitigační opatření, optimalizace a implementace v podobě vytvoření akčních plánů, metodik, krizových postupů, a dalších.

(vi) **Monitoring** (Pasivní, Aktivní). Nástroje sloužící pro detekci hrozeb a to aktivním (vyhledávání v systému, periodické ověřování zabezpečení) či pasivním způsobem (naslouchání a notifikace).

Fázi (i) musí být věnována nejvyšší možná pozornost, jelikož na ni navazují všechny následující fáze. Fáze (ii) až (iv) slouží k identifikaci rizik, hrozeb, chyb a obecně nedostatků systému. Volba jednotlivých metod i jejich hloubka je volena na základě nastavených dostupných zdrojů, aby bylo možné identifikovat, co největší část z množiny rizik a hrozeb. Fáze (v) obsahuje převážně manažérská rozhodnutí, která vedou k mitigaci či přijetí identifikovaných rizik. Fáze (vi) by měla být nastavena dle (ii) až (v), společně s mechanismy, které dovolí detekci i neidentifikovaných hrozeb, což pomůže následně nejen ve fázi během případného bezpečnostního incidentu, ale také ve fázi po něm, kdy nastává fáze zotavení a hlavně ponaučení. Tedy jak již bylo řečenou, není možné identifikovat a mitigovat veškerá rizika, nicméně je možné se metodickým postupem dostat až na přijatelnou hodnotu rizikovosti.

ZÁVĚR

V rámci tohoto článku jsme přiblížili problematiku terminologie kybernetického prostoru a kybernetické bezpečnosti a dále zodpověděli na otázky:

(1) Co je to kybernetický prostor?

Jedná se o prostor, kde dochází ke vzniku, zpracování, zachování a zániku informace, která je definována oborem kybernetika.

(2) Jak se tedy bránit v něčem tak abstraktním jako je kybernetický prostor a proč je tento pojem definován různorodě?

Různorodost pochází z podstaty chápání „prostoru“ různými způsoby. Efektivně se lze bránit pouze v případě, pokud naše definice obsáhne komplexně celý kybernetický prostor i se všemi jeho vstupy a výstupy.

(3) Jakým způsobem vznikají kybernetické bezpečnostní incidenty?

Kybernetický bezpečnostní incident vzniká porušení bezpečnostní politiky či zásahem do kybernetického prostoru jiným než zamýšleným způsobem.

(4) Kdy se stává z incidentu - krize? Jaký je vlastně rozdíl mezi těmito událostmi?

Rozdíl mezi pojmem „incident“ a „krize“ je převážně v rozsahu škod a dopadu. Kybernetická krizová situace je doprovázena většinou destruktivním až likvidačním dopadem. Další vlastností kybernetické krizové situace je oproti běžným kybernetickým bezpečnostním incidentům mnohem menší (minimální) pravděpodobnost vzniku.

(5) Jak efektivně reagovat na kybernetické bezpečnostní incidenty?

Hlavním bodem je identifikace kybernetického bezpečnostního incidentu, bez které není možné reagovat. Tedy musí existovat nástroje pro odhalení a správnou identifikaci kybernetického bezpečnostního incidentu s minimalizací tzv. falešných zpráv. Reakce samotná by pak následně měla navazovat na vytvořenou bezpečnostní politiku instituce a vést k minimalizaci škod i doby trvání.

(6) Je možné kybernetickým incidentům či dokonce krizovým situacím předcházet?

Ano i ne, neexistuje zde zcela jednoznačná odpověď. Je totiž možné nalézt zranitelnosti či rizika systému (vnější i vnitřní) a následně se snažit o jejich eliminaci (mitigaci). Nicméně není již možné nalézt zcela všechny a to i díky metodám používaných v tzv. zero-day útocích.

Nicméně v rámci dnešní strategie již není otázkou mitigace všech rizik, nicméně mitigace a identifikace podstatných rizik. Dále se také na rizika pohlíží z pohledu ekonomického a tedy zda díky riziku firma přijde o zisk *x*/rok a mitigace takového rizika by stála *y*, tak pokud $x << y$ je v tomto z ekonomického hlediska vhodné uvažovat o přijmutí daného rizika (velice podobným principem se pak řídí i pravděpodobnost rizik). Velmi důležitým faktem však při přijímání rizika je věnovat pozornost kybernetickým krizovým situacím, které by mohli mít likvidační následky, a kterým se dá rozumným způsobem zabránit.

(7) Jak minimalizovat dopady kybernetických krizových incidentů?

Minimalizace výskytu kybernetických krizových incidentů je zdravé balancování představené již v rámci (6). Mitigaci si můžeme pak představit jako jeden z bodů představený v rámci metodiky, viz Kapitola 3. Samotné dopady jsou pak minimalizovány pomocí včasné identifikace a efektivního řešení za pomocí vhodně nastavené bezpečnostní politiky (bezpečnostních i rozhodovacích procesů) a krizového plánu.

Literatura

[1] MAHAPATRA, N. *Introduction to Cyberspace and Its Architecture*. 2017.

[2] ASHIBANI, Y., MAHMOUD, Q. H. *Cyber physical systems security: Analysis, challenges and solutions*. Computer & Security, č. 68, s. 81-97, 2017.

[3] JU, Ch. *Creating Safe Cyberspace: Strategies for Deterring Cyberattacks*. Chicago Policy Review, 2017.

[4] ZHUKOVSKIY, Y., MALOV, D. *Concept of Smart Cyberspace for Smart Grid Implementation*. Journal of Physics: Conference Series. IOP Publishing, č. 1015/4, 2018.

[5] KHATOUN, R. ZEADALLY, S. *Cybersecurity and privacy solutions in smart cities*. IEEE Communication Magazine, č. 55/3, s. 51-59, 2017.

[6] LIU, H. et al. *A review of the smart world. Future Generation Computer Systems*, 2017.

[7] DVOŘÁK, J., KONEČNÝ, J., JANKOVÁ, M. *Options of Identifying Attacks in Cyberspace of Crisis Management*. In: Crisis Management and Solution of the Crisis Situations. Uherske Hradiste, 2015. ISBN 978-80-7454-573-3.

[8] DVORAK, J., KONECNY, J., JANKOVA, M. *Cyber Security as a part of Cyberspace of Modern Society*. In: Crisis Management and Solution of the Crisis Situations. Uherske Hradiste, 2016. ISBN 978-80-7454-632-7.

[9] SULC, V. *Cyberwar and its Implications in the World*. In: Crisis Management and Solution of the Crisis Situations. Uherske Hradiste, 2016. ISBN 978-80-7454-632-7.

[10] TROJAN, J., SVOBODA, P. *Cyber Security in the Context of E-Government of the Czech Republic – Polemic Discussion on „Case Silverlight"*. In: Crisis Management and Solution of the Crisis Situations. Uherske Hradiste, 2016. ISBN 978-80-7454-632-7.

[11] DVOŘÁK, J., KONEČNÝ, J., SULC, V., JANKOVÁ, M. *Systemic Conception of Artificial Intelligence for Modeling of Modern Cybernetic Safety*. In: Crisis Management and Solution of the Crisis Situations. Uherske Hradiste, 2016. Uherske Hradiste, 2017. ISBN 978-80-7454-717-1.

[12] VAVRA, J., HROMADA, M. *Anomaly as a Symptom of Cyber-Attack in ICS*. In: Crisis Management and Solution of the Crisis Situations. Uherske Hradiste, 2016. Uherske Hradiste, 2017. ISBN 978-80-7454-717-1.

[13] ANDERS, P. Envisioning cyberspace: Designing 3D electronic spaces. McGraw-Hill Professional, 1998.

[14] ADAMS, P. Cyberspace and virtual places. Geographical Review, č. 87/2, s. 155-171, 1997.

[15] RHEINGOLD, H. Virtual Reality: Exploring the Brave New Technologies of Artificial Experience and Interactive Worlds From Cyberspace to Teledildonics. Secker & Warburg, 1991.

[16] Česká Republika. *Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. In: Sbírka zákonů. ISSN 1211-1244.

[17] Česká Republika. *Zákon č. 240/2000 Sb., Zákon o krizovém řízení a o změně některých zákonů (krizový zákon)*. In: Sbírka zákonů. ISSN 1211-1244.

[18] Česká Republika. *Zákon č. 239/2000 Sb., Zákon o integrovaném záchranném systému*. In: Sbírka zákonů. ISSN 1211-1244.

[19] Česká Republika. *Zákon č. 1/1993 Sb., Zákon o integrovaném záchranném systému*. In: Ústava České Republiky. ISSN 1211-1244.

[20] Česká Republika. *Zákon č. 241/2000 Sb., Zákon o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů*. In: Sbírka zákonů. ISSN 1211-1244.

[21] Česká Republika. *Zákon č. 110/1998 Sb., Zákon o bezpečnostní České republiky*. In: Ústava České Republiky. ISSN 1211-1244.

[22] RAJNOVIC, R. *Cyberspace – What is it?* Cisco Blogs (Security). 2012.

[23] ENISA. *Definition of Cybersecurity – Gaps and overlaps in standardisation*. 2016.

[24] SMEJKLA, *V. Jaké povinnosti vyplývají pro orgány veřejné moci ze zákona o kybernetické bezpečnosti?* Právní prostor. 2015.

[25] ENISA. *Report on Cyber Crisis Cooperation and Management*, 2014

[26] WILSHUSEN, P.R. *Capitalizing Conservation/Development: Dissimulation, Misrecognition, and the Erasure of Power*. Nature™ Inc: Environmental Conservation in the Neoliberal Age, Chapter: Pre-publication version. 127-157, 2014.

[27] Snowdon, C., *Managing a Cyber Crisis: What is the most effective way to prepare leadership teams for a high tech threat?* Regester Larkin, 2014.

[28] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. Výkladový slovník kybernetické bezpečnosti. Policejní akademie ČR v Praze (Česká pobočka AFCEA), 2013.

[29] HANSON, F., UREN, T. Policy Brief: Australia's offensive cyber capability. International Cyber Policy Centre – Australian Strategic Policy Institute (ASPI), 2018.

[30] SOUČEK, Martin. *UK UISK modul č. 3 - Informační věda, v rámci projektu Studium informační vědy a komunikačního managementu v evropském kontextu*.

[31] WIENER, Norbert. *Kybernetika neboli řízení a sdělování v živých organismech a strojích*. Praha: Státní nakladatelství technické literatury, 1960.

[32] Česká Republika. Nařízení vlády č. 432/2010 Sb., Nařízení vlády o kritériích pro určení prvku kritické infrastruktury. In: Sbírka zákonů. ISSN 1211-1244.

[33] *Fyzická ochrana prvků kritické infrastruktury a ostatních objektů odvětví energetika – elektřina – Přenosová a distribuční soustava*. ČEZ Distribuce, E.ON Česká Republika, PRE Distribuce, ČEPT. Podniková norma PNE 73 4450-2-1 (první vydání). 2017.

[34] Česká Republika. Vyhláška č. 361/2016 Sb., *Vyhláška o zabezpečení jaderného zařízení a jaderného materiálu*. In: Sbírka zákonů. ISSN 1211-1244.

[35] CEASEY, J., GLOVER, I. *Cyber Security Incident Response Guide*. CREST (ver. 1), 2013.

[36] *Cyber crisis management: Readiness, reponse, and recovery*. Deloitte. Strtegic & Reputation Risk. 2016.

[37] *Cyber security incident management guide*. Centre for cyber security Belgium (Cyber Security Coalition). 2016.

[38] CICHONSKI, P., MILLAR, T., GRANCE, T., SCARFONE, K. *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*. NIST SP 800-61 (rev. 2), 2012.

[39] *Information Security Incident Management Guidelines*. The university of Newcastle Australia. 2017.

[40] *Cyber Incident Management Planning Guide: For IIROC Dealer Members*. IIRON a JUNO. 2016.

[41] *Computer Security Incident Response Plan*. Carnegia Mellon (Information Security Office). 2015.

SROVNÁNÍ VÝZNAMNÝCH MARKANTŮ VYBRANÝCH STŘELNÝCH ZBRANÍ PODLÉHAJÍCÍCH REGISTRACI A JEJICH VOLNĚ DOSTUPNÝCH KOPIÍ

COMPARISON OF SIGNIFICANT MARKERS OF THE SELECTED SHOOTING WEAPONS SUBJECT TO REGISTRATION AND THEIR FREELY AVAILABLE COPIES

Ing. Michal Gracla, Ing. David Hamřík, Ing. Zdeněk Maláník, DCv.
Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky
Nad Stráněmi 4511, 760 05 Zlín
gracla@utb.cz, malanik@utb.cz

ABSTRAKT

Střelné zbraně mají dlouhou historii a jsou známy po celém světě a ve všech věkových kategoriích. Někteří lidé znají střelné zbraně jako smrtící prostředky, jiní zase jako možnost obrany a poslední skupina lidí jako „hračky“. V dnešní době existuje mnoho různých výrobců, kteří vyrábějí vlastní modely s designem střelných zbraní podléhajících registraci dle zákona o zbraních. Článek je zaměřen hlavně na ty výrobce, kteří napodobují tyto střelné zbraně. Byly vybrány tři základní střelné zbraně, ze kterých vychází zbylé střelné zbraně. Dále byly vybrány jejich volně dostupné kopie, které jsou na českém trhu k dostání. Jedná se především o expanzní a airsoftové střelné zbraně. U nich byly hledány významné markanty, kterými se odlišují především střelné zbraně podléhající registraci od jejich volně dostupných kopií. Na závěr byly všechny zjištěné markanty zaznamenány do přehledné tabulky a vyznačeny na obrázcích.

KLÍČOVÁ SLOVA

Střelné zbraně, obrana, kopie, expanzní zbraň, airsoftová zbraň, markanty

ABSTRACT

Shooting weapons have a long history and are known all over the world and in all ages. Some people know shooting weapons as lethal means, others as the possibility of defence, and the last group of people as "toys". Nowadays, there are many different manufacturers who make their own models with the design of shooting weapon subjected to registration under the Weapons Act. The paper focuses mainly on those manufacturers who imitates these shooting weapons. Three basic shooting weapons, on which the remaining shooting weapons are based, were selected. Furthermore, their freely available copies, which are available on the Czech market, were selected. These are mainly expansion and airsoft shooting weapons. Significant markers have been sought for them. These markers differentiate them above all mainly shooting weapons subjected to registration from their freely available copies. Finally, all of the observed markers were recorded to an organized table and marked in the figures.

KEY WORDS

Shooting weapons, defence, copy, expansion weapon, airsoft weapon, markers

ÚVOD

V dnešní době se více lidí zabývá vlastní bezpečností, protože si začínají uvědomovat, že policisté nemohou být vždy a všude s nimi. Není to jen z důvodu nedostatku policistů, ale hlavně z toho, že i policisté jsou také pouze lidé a žádní superhrdinové, kteří by nebezpečné situace předvídat či byli u nich do pár sekund, jak mnozí mohou znát např. ze seriálu Superman. Tomuto trendu napomáhá i bezpečnostní situace převážně v Evropě. Díky tomu se obyvatelé České republiky začali více zajímat o vlastní bezpečnost a bezpečnost svých blízkých. Někteří začali navštěvovat různé bojové systémy (Krav Maga, Systema) nebo si pořídili obranný prostředek (obranný sprej, teleskopický obušek) či dokonce střelnou zbraň. K popsání jednotlivých oblastí by bylo potřeba mnoho stran, proto následující řádky se budou zabývat pouze poslední zmíněnou oblastí, kterou jsou střelné zbraně.

Střelné zbraně mohou být v nesprávných rukou velmi nebezpečné, v jiných naopak mohou pomáhat či dokonce efektivně napomoci k odvrácení útoku. Střelné zbraně můžeme rozdělit podle zákona o střelných zbraních a střelivu do čtyř kategorií. Nejzajímavější k obraně jsou zbraně kategorie B a D. Zásadním rozdílem mezi těmito kategorie je to, že na první jmenovanou je potřeba zbrojní průkaz a střelné zbraně převážně teda palné zbraně podléhají registraci. Naopak ke zbraním kategorie D není potřeba vlastnit zbojní průkaz a nepodléhají registraci.

Občané, kteří začali dbát o svoji bezpečnost sami, si většinou udělají zkoušky na zbrojní průkaz a pořídí si na svou obranu zbraň kategorie B. Ti, kteří si z nějakého důvodu nechtějí udělat zkoušky na získání zbrojního průkazu nebo nemohou, volí právě druhou variantu. Tou jsou zbraně kategorie D, které nepodléhají registraci, jsou levnější a často svým vzhledem jsou nerozeznatelné od zbraně kategorie B.

Při držení a nošení střelné zbraně je potřeba mít na zřeteli jistá pravidla zacházení se střelnými zbraněmi, ale také následky, které mohou nastat. Tím je ranivý účinek střelné zbraně, který je testován a ověřován na náhradních materiálech, kde se určuje ranivý potenciál. Na tyto témata vzniklo mnoho publikací, které jsou zaměřeny spíše jen na zbraně kategorie B (1-5).

Zbraněmi kategorie D se mnoho výzkumníků nezabývá, protože si myslí, že postačuje se zabývat předchozí oblastí. Opak je pravdou, nýbrž zbraně kategorie D jsou dosti rozšířené nejen proto, že na ně není potřeba zbrojní průkaz, ale i proto, že jsou levnější a mají vzhled připomínající zbraň kategorie B. Na určení ranivého potenciálu zbraní kategorie D vznikly a vznikají nové a nové výzkumy (6-10). To nebude tedy předmětem následujících řádků. Ty se budou zaměřovat právě na vizuální rozdíl střelných zbraní zařazených do zbraní kategorie B a jejich volně dostupných kopií, které jsou zařazeny do zbraní kategorie D.

1. VYBRANÉ STŘELNÉ ZBRANĚ PODLÉHAJÍCÍ REGISTRACI

Podle českého zákona o střelných zbraních a střelivu jsou střelné zbraně podléhající registraci označovány jako zbraně kategorie B. Do této kategorie spadají palné zbraně, pro které je charakteristické užití náboje. Tyto zbraně se vyrábí z různorodých materiálů, mezi které patří kov, plast, keramika a také kombinace těchto materiálů. Kov bývá použit hlavně pro hlavně, kde při výstřelech vznikají velké tlaky, které by jiné materiály roztrhlo. K záměru studie jsou vybrány pouze krátké kulové zbraně základních typů, které jsou v podstatě základem zbylých palných zbraní. Jedná se o českou, rakouskou a americkou zbrojovku se svými zakládajícími modely. U české zbrojovky to byl model CZ 75 B, u rakouské zbrojovky Glock 17 a u americké zbrojovky Colt 1911. V dnešní době každá ze zbrojovek disponuje několika různými modely a velikostmi svých zbraní.

1.1 Česká zbrojovka s modelem CZ 75 B

Česká zbrojovka je tuzemská zbrojovka, která vznikla v roce 1936 v Uherském Brodě. Proslula výrobou nejen pistolí, ale i vzduchovek, malorážek, samopalů a útočných pušek. Jako první pistoli vyrobili podle návrhu Františka Kouckého již v 70. letech minulého století pod označením CZ 75. Tato pistole byla v ráži 9 mm a byla určená pro bezpečnostní sbory. CZ 75 je předchůdcem modelu CZ 75 B, která byla použita do provedeného experimentu.

U pistole s označením CZ 75 B se již objevila blokace zápalníku, která se od té doby vyskytuje ve většině zbraní vyráběných Českou zbrojovkou Uherský Brod. Tato zbraň se stala velmi oblíbenou nejen v České republice, ale i v zahraničí. Je vhodná jak pro služební účely ozbrojených složek, tak i pro sportovní účely. Mezi výhody tohoto modelu se řadí především dobré držení pro leváky i praváky, dvouřadový zásobník a přesnost střelby.

1.2 Rakouská zbrojovka s modelem Glock 17

Druhým základem zbylých střelných zbraní je rakouská zbrojovka, která byla založena v roce 1963 panem Gastonem Glockem. Podle něho je i zbrojovka označována. Největší úspěch z hlediska vývoje a výroby přinesl rok 1981, kdy vytvořil nové revoluční konstrukční řešení pistolí. Bylo to na popud toho, že rakouská armáda chtěla nahradit své dosavadně používané pistole Walther P38 za nové. Pistole Glock jsou jako CZ vhodné pro ozbrojené složky, jako služební pistole nebo pro sportovní účely či sebeobranu. Glock je hojně zastoupený na americkém trhu a to zhruba 60 %.

Pistole Glock 17 je jedinečný v tom, že má vnitřní automatické pojistky a proto na zbrani se nenajde manuálně ovladatelné vnější bezpečnostní prvky. Pouze jsou na ní ovládací prvky a z bezpečnostního prvku je součástí spouště bezpečnostní pojistka spouště. V dnešní době má Glock 5 generačních obměn všech svých modelů. Každá generační obměna jde s časem a díky tomu i s požadavky zákazníků, pro jeho lepší ovladatelnost, úchop, atd.

1.3 Americká zbrojovka s modelem Colt 1911

I za tzv. velkou louží je jedna zbrojovka, která je hojně kopírovaná. Touto zbrojovkou je Colt, který byl založen 1855 a tím pádem je to nejstarší zbrojovka ze základních typů, ze kterých vychází zbylé střelné zbraně. Zakladatelem a konstruktérem zbraní byl Samuel Colt, který při výrobě pistole Colt 1911 spolupracoval s vynikajícím konstruktérem zbraní a střeliva panem Johnem Browningem. Tato samonabíjecí pistole byla zařazena do americké výzbroje v roce 1911 a byla v ní v různých modifikacích až do roku 1985, kdy byla nahrazena.

Typické pro Colt 1911 je to, že oproti předchozím dvěma typům má manuální dlaňovou pojistku. Charakteristický je také systém uzamčení závěru a jednočinné spoušťové ústrojí. Tento systém uzamčení může být označován taky jako Browningův systém. K experimentu byla použita modifikace legendární pistole Colt 1911 pojmenovaná jako Dan Wesson PM7.

2. VYBRANÉ VOLNĚ DOSTUPNÉ KOPIE STŘELNÝCH ZBRANÍ PODLÉHAJÍCÍ REGISTRACI

Pod pojmem volně dostupné kopie střelných zbraní podléhající registraci je potřeba si představit veškeré střelné zbraně zařazeny podle zákona o střelných zbraních a střelivu do zbraní kategorie D. Je to z důvodu toho, že na ně není potřeba zbrojní průkaz, jak již bylo psáno výše a taky, že vzhledem připomínají právě zbraně, které registraci podléhají. V těchto

konkrétních případech se bavíme pouze o airsoftových nebo expanzních zbraních. Proto jsou v práci popsány tyto střelné zbraně, které jsou věrnými kopiemi výše popsaných zbraní.

Výrobců, kteří vyrábí věrné kopie právě zbraní podléhajících registraci je na českém trhu nepřeberné množství. Byly vybrány dvě věrné kopie (airsoftová a expanzní zbraň) ke každému typu zbraně podléhající registraci.

2.1 Airsoftové zbraně

Airsoftové zbraně jsou to plynové zbraně a jsou velmi oblíbené hlavně pro hru odvozenou od typu zbraní a tedy Airsoft. Jedná se o střelné zbraně, které místo klasických nábojů vystřelují sférické střely. Některé z těchto zbraní jsou věrnými kopiemi právě zbraní zařazených ve zbraních kategorie B. Existuje několik typů takových kopií. Mohou to být pouze „hračky" které „jen" vystřelují sférické střely na základě uvolnění stlačeného plynu, který je ve formě bombičky vložen do zásobníku nebo přepuštěn z lahve do zásobníku. Jiné mají naopak pohyblivý závěr zbraně, ale pouze na jeden výstřel (po každém výstřelu se musí znovu závěr natáhnout). Posledním typem airsoftových zbraní je právě typ, který vzhledem i manipulací věrně napodobuje právě „ostré" zbraně.

U těchto zbraní je k výstřelu potřeba natáhnout závěr pouze jednou a mít tam vložený zásobník s dostatečným množstvím poháněcího plynu. Jakmile se vystřelí poslední sférická střela, tak závěr zbraně zůstane v zadní poloze, jak je tomu právě u „ostrých" zbraní.

Článek se nezaobírá mechanizmy ani funkcí zbraní, ale pouze vizuální stránkou „ostrých" zbraní s jejich věrnými kopiemi, proto nebude dále řešeno střelivo ani funkčnost popisovaných střelných zbraní.

2.1.1 KP-09 CZ 75

Jedná se o věrnou kopii pistole CZ 75. KP-09 CZ 75 je vyrobena společností KJ Works a je celokovová. Umožňuje poloautomatickou střelbu. Pro udělení rychlosti sférické střele je použit Green Gas. Disponuje pohyblivým závěrem (nazývané u airsoftových zbraní jako BlowBack systém) a má kapacitu zásobníku na 28 sférických střel.

2.1.2 G17 Gen4

Pod označením G17 Gen 4 se skrývá kopie rakouské zbrojovky Glock, kterou vyrábí společnost WE. Je vyrobená z odolného ABS plastu a kovového závěru. Disponuje BlowBack systémem, pro svůj pohon používá GreenGas a kapacitu zásobníku má na 24 sférických střel.

2.1.3 Colt M1911

Airsoftová zbraň Colt M1911 je věrnou kopií Coltu STI M1911 Classic a je od společnosti KWC. Je vyrobena z ABS plastu a pro Colt je typické, že zásobník je pouze jednořadý a proto se do něj vleze pouze 12 sférických střel. Také postrádá BlowBack systém, tak se závěr musí před každým výstřelem znovu natáhnout. Do srovnání byl použit místo klasického Coltu STI M1911 Classic jeho náhrada v podobě Dan Wesson PM7.

2.2 Expanzní zbraně

Expanzní zbraně jsou to palné zbraně, stejně jako „ostré“ zbraně, do kterých se místo nábojů používají nábojky. Nevystřelují tudíž hmotnou střelu. Při nataženém závěru a stisknutí spouště dojde k chemické reakci a tlaku, který protrhne zátku nábojky. Nábojky mohou být trojího typu. První typ je pouze akustická, druhý je akustická doplněna o světelný efekt (výšleh plamene) a třetí je kombinace akustické s nějakou chemicky látkou (technický pepř, dusivou nebo slzotvornou).

Expanzní zbraně mají vždy pohyblivý závěr a není potřeba je plnit poháněcím plynem, jak tomu bylo u airsoftových zbraní. V hlavni expanzní zbraně jsou umístěny přepážky a i celá zbraň je vyrobena tak, aby do ní nebylo možné vložit náboj nýbrž pouze nábojky.

2.2.1 Kimar CZ-75

Expanzní zbraň Kimar CZ-75 je věrnou kopií CZ 75. Její výrobce je společnost Kimar a vyrábí samonabíjecí pistole s celokovou konstrukcí. Disponuje zásobníkem na 10 nábojek.

2.2.2 Atak Zoraki 917

Atak Zoraki 917 je označována věrná kopie Glocku 17 společností Atak Arms, která tuto expanzní zbraň vyrábí. Je vyrobená z polymeru a kovového závěru. Kapacita zásobníku je až 17 nábojek.

2.2.3 Colt Government 1911 A1

Umarex je výrobcem expanzní zbraně Colt Government 1911 A1, která je věrnou kopií vojenské pistole Colt Government 1911. Jedná se o celokovovou zbraň s kapacitou zásobníku na 8 nábojek. K věrnějšímu vzhledu je na zbrani vygravírované originální logo Colt přímo laserem.

3. ZJIŠTĚNÉ VÝZNAMNÉ MARKANTY SROVNÁVANÝCH STŘELNÝCH ZBRANÍ

Závěrečná část článku se zabývá hledáním významných markantů, díky kterým se jednotlivé střelné zbraně odlišují. I když jsou airsoftové a expanzní zbraně věrnými kopiemi zbraní zařazených ve zbraních kategorie B, tak i tak se najdou nepatrné rozdíly, kterými se od nich odlišují.

Jsou vytvořeny přehledné tabulky, ve kterých jsou uvedeny rozdílnosti. Jako referenční střelnou zbraní je vždy zbraň kategorie B. Na následujících obrázcích jsou uvedené rozdíly, které jsou zvýrazněny pro lepší pochopení a orientaci. V rámci rozsahu článku jsou zjišťované rozdíly omezeny pouze na levou a pravou stranu všech výše popsaných střelných zbraní. Barva zbraní není bráno jako rozdíl.

Červenou barvou jsou zvýrazněny markanty, díky kterým by se dala střelná zbraň rozpoznat s velkou pravděpodobností. Modrou barvou jsou zvýrazněny detaily, které jsou malé nebo mohou být úpravou odstraněny. Zvláštní nezvýrazněnou kategorií jsou botky zásobníků, které je možné modifikovat na různou velikost a tvar.

Vždy bude nahoře ukázána referenční zbraň zařazená ve zbraních kategorie B. Uprostřed bude airsoftová zbraň a dole expanzní zbraň.

3.1 Významné markanty u CZ 75 B

I když se na první pohled může zdát, že se jedná o jednu a tutéž zbraň, tak opak je pravdou. Mezi významné markanty, které byly odhaleny u CZ 75 B, jsou hlavně ty, které jsou zvýrazněny červeně. Ty méně významné jsou označeny modře. Je to z důvodu toho, že jsou malé a lehce přehlédnutelné nebo taky při úchopu přímo neviditelné či dokonce mohou být odstraněny.

Střelná zbraň	CZ 75 B	KP-09 CZ 75	Kimar CZ-75
Kohout	Zakulacen s dírkou	Do obloučku	Zakulacen s dírkou
Vyhazovací okénko	Lze vidět hlaveň a vyhazovač	Imitace kovu s náznakem vyhazovače	Lze vidět hlaveň a vyhazovač
Vyústění hlavně	Hlaveň mírně vyčnívá	Hlaveň výrazně vyčnívá	Hlaveň mírně vyčnívá
Záchyt závěru (pravá strana)	Standardní výstup záchytu závěru	Uměle simulovaný výstup záchytu závěru	Oválný, nepřesahující tělo zbraně výstup záchytu závěru
Logo na pažbičce	Bez loga	Logo na střence	Bez loga
Závěr (nápisy)	Označení zbraně, ráže a logo	Bez označení zbraně	Označení zbraně
Lučík	Přední strana lučíku rovná dále zakulacená	Celý lučík zakulacený	Přední strana lučíku rovná dále zakulacená
Záchyt závěru (levá strana)	Hranatý záchyt závěru	Malý zakulacený záchyt závěru	Standardní zakulacený záchyt závěru
Pojistka	Standardní tvar	Menší a zakulacená	Standardní tvar
Bobří ocas	Kratší a mírně ohnutý směrem dolů	Delší a rovný	Kratší a rovný

Tab. 5. Popis zjištěných markantů u vybraných střelných zbraní CZ

Obr. 7. Grafické zobrazení zjištěných markantů vybraných střelných zbraní CZ

3.2 Významné markanty u Glock 17

Střelná zbraň	Glock 17	G17 Gen4	Atak Zoraki 917
Hledí	Typické pro Glock, ale lze provést výměnu	Typické pro Glock	Hledí
Slide lock	Na potáhnutí	Na potáhnutí	Na rozepnutí
Závěr (nápisy)	Označení zbraně, ráže, logo, země	Označení zbraně a ráže	Označení zbraně
Záchyt závěru	Standardní velikost s částečným ohraničením	Standardní velikost s částečným ohraničením	Větší velikost s tři čtvrtě ohraničením
Lučík	Typické pro Glock	Typické pro Glock	Hrbolek vně lučíku a spoušť bez pojistky

Tab. 6. Popis zjištěných markantů u vybraných střelných zbraní Glock

Obr. 8. Grafické zobrazení zjištěných markantů vybraných střelných zbraní Glock

3.3 Významné markanty u Colt 1911

Střelná zbraň	Dan Wesson PM7	Colt M1911	Colt Government 1911 A1
Kohout	Obloukový s dírou	Zahnutý plochý	Zahnutý nahoru plochý
Výhozné okénko	Jde vidět část hlavně bez vyhazovače	Umělá atrapa hlavně bez vyhazovače	Jde vidět část hlavně s vyhazovačem
Závěr	Dvojí rýhování na závěru	Bez druhého rýhování	Bez druhého rýhování
Závěr (nápisy)	Bez jakéhokoliv označení	Označení zbraně	Označení zbraně a logo
Hledí	Stavitelné hledí	Pevné hledí	Pevné hledí
Bobří ocas	Delší a zahnutý nahoru	Kratší zahnutý dolů	Kratší zahnutý dolů

Tab. 7. Popis zjištěných markantů u vybraných střelných zbraní Colt 1911

Obr. 9. Grafické zobrazení zjištěných markantů vybraných střelných zbraní Colt 1911

ZÁVĚR

Jak již bylo v úvodu uvedeno, článek se zaměřoval na tři základní typy střelných zbraní, které jsou nejčastěji kopírované a vychází z nich zbylé střelné zbraně. Z těchto tří základních typů střelných zbraní byly vybrány jejich „ostré“ verze, které jsou zařazeny podle zákona o střelných zbraních a střelivu zařazeny do zbraní kategorie B a jejich volně dostupné kopie tudíž střelné zbraně zařazeny ve zbraních kategorie D. Ze všech zbraní, které jsou zařazeny do zbraní kategorie D, odpovídá „ostrým“ verzím pouze airsoftové a expanzní zbraně. Proto byl vybrán vždy jeden ze zástupců (airsoftové a expanzní zbraně) z celého portfolia výrobců. Byly určovány významné markanty, podle kterých se jednotlivé volně dostupné kopie od „ostré“ verze dají odlišit. Jsou uvedeny v přehledných tabulkách, na které navazují obrázky, v nichž jsou rozdíly zakresleny. U České zbrojovky Uherský Brod modelu CZ 75 B,

se dá „ostrá“ střelná zbraň rozpoznat převážně podle kohoutu, výhozného okénka, lučíku, záchyt závěru a bobřího ocasu. Jsou to prvky, na které se musí osoba, která chce střelné zbraně rozpoznat zaměřit úplně jako první, pokud se zbraní nemůže nijak manipulovat. Mezi další se řadí nápisy na závěru, pojistka a z pravé strany záchyt závěru. Nejvíce rozdílností na první pohled viditelných jsou z airsoftovou zbraní. U expanzní zbraně to již tak jednoznačné není. Jsou tam jen rozdíly pouze v záchytu závěru, nápisu na závěru a bobřím ocasu. Oproti tomu u Glocku 17 je rozpoznávacích míst méně než u CZ 75 B. U Glocku jsou to pouze hledí, slide lock, záchyt závěru, lučík se spouští a nápis na závěru. V tomto případě s „ostrým“ Glockem 17 je nejvíce nerozeznatelná airsoftová zbraň, kde na první pohled není možné rozeznat o jakou střlenou zbraň se jedná. Jsou tam jen malé detaily, které na první pohled nejsou vidět pouze po detailním zkoumání. U expanzní zbraně je odlišný lučík se spouští, záchyt závěru, slide lock i hledí. Nápis na závěru není kompetentní rozpoznávací znak, neboť může být odstraněn případně dodatečně dodělán. Colt 1911 je na tom podobně jako Glock. S tím rozdílem, že u Coltu 1911 jsou přesně rozeznatelné markanty na první pohled, kterými se odlišují věrné kopie od „ostré“ zbraně. Těmito rozdíly jsou kohout výhozné okénko, dvojí rýhování na závěru, hledí a bobří ocas. Na pravém Coltu 1911 je také absence označení zbraně, loga i ráže, které mají zbylé „ostré“ zbraně naražené na závěru. Mezi největší a nejvýznamnější rozdíly se řadí kohout, bobří ocas a dvojí rýhování na závěru, které se na žádné věrné kopii neobjevuje. Z toho celého vyplývá, že rozpoznat střelnou zbraň zařazenou ve zbraních kategorie B a jejich volně dostupné kopie lze, ale pouze s tím, že osoba, která chce zbraně rozpoznat, zná přesně „ostrou“ zbraň i její všechny možné modifikace. Bez těchto znalostí je to jinak velmi těžké rozpoznat věrné kopie od „ostrých“ zbraní aniž by na ně osoba mohla sáhnout.

Literatura

[1] ŠAFR, Miroslav a Petr HEJNA, c2010. Střelná poranění. Praha: Galén. ISBN 978-80-7262-696-0.

[2] JORGENSEN, Jorgen Joakim, Paal Aksel NAESS a Christine GAARDER. Injuries caused by fragmenting rifle ammunition. Injury [online]. 2016, 47(9), 1951-1954 [cit. 2018-08-23]. DOI: 10.1016/j.injury.2016.03.023. ISSN 00201383. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0020138316300675

[3] HANNA, Tarek N. et al., 2015. Firearms, bullets, and wound ballistics: An imaging primer. Injury [online]. 46(7), 1186-1196 [cit. 2017-08-15]. DOI: 10.1016/j.injury.2015.01.034. ISSN 00201383. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0020138315000601

[4] RIDDEZ, L. Wounds of war in the civilian sector: principles of treatment and pitfalls to avoid. European Journal of Trauma and Emergency Surgery [online]. 2014, 40(4), 461-468 [cit. 2018-08-23]. DOI: 10.1007/s00068-014-0395-6. ISSN 1863-9933. Dostupné z: http://link.springer.com/10.1007/s00068-014-0395-6

[5] JUŘÍČEK, Ludvík, 2016. Porovnání hloubky vniku šípu kuše a střely náboje ráže 22 Long Rifle do bloku náhradního materiálu biologických tkání v experimentální ranivé balistice. Bezpečnostní management v regionech [online]. 2(1), 12 [cit. 2017-02-09]. Dostupné z: http://www.bezpecnostnimanagementvregionech.cz/sites/bezpecnostnimanagementvregionech.cz/files/juricek_porovnani_hloubky_vniku_.pdf

[6] JUŘÍČEK, L., B. PLÍHAL a J. KOMENDA, 2003. Prediction of ballistic bodies penetration depth into alternative material biological tissues in ballistic experiment: Predikce hloubky vniku balistických těles do bloku náhradního materiálu biologických tkání v balistickém experimentu [online]. 2003(1), 23-35 [cit. 2017-08-15]. Dostupné z: https://www.scopus.com/record/display.uri?eid=2-s2.0-33751372268&origin=resultslist&sort=plf-f&src=s&st1=Ju%c5%99%c3%ad%c4%8dek+L.&st2=&sid=92E1D888063D500855F0283A28884DAD.wsnAw8kcdt7IPYLO0V48gA%3a60&sot=b&sdt=b&sl=23&s=AUTHOR-NAME%28Ju%c5%99%c3%ad%c4%8dek+L.%29&relpos=11&citeCnt=0&searchTerm#references

[7] GRACLA, Michal, Aleš CHOCHOLATÝ a Zdeněk MALÁNÍK, 2017. Analýza ranivého účinku základních zbraní kategorie D. In: BRADÁČ, Albert a Michal KŘIŽÁK. Sborník příspěvků konference Expert Forensic Science Brno 2017 (ExFoS 2017): XXVI. mezinárodní vědecká konference soudního inženýrství [USB disk]. Brno: Vysoké učení technické v Brně, Ústav soudního inženýrství, Purkyňova 464/118, 612 00 Brno, s. 327-336 [cit. 2017-01-31]. ISBN 978-80-214-5459-0. Dostupné z: www.exfos.cz

[8] MIKULICOVA, Michaela et al., 2017. Comparison of depth of incomplete penetration for different types of pellets for shooting weapon of category D. In: KRIVANEK, V. 2017 International Conference on Military Technologies (ICMT) [USB proceedings]. Brno: IEEE, s. 66-69 [cit. 2018-08-23]. DOI: 10.1109/MILTECHS.2017.7988732. ISBN 978-1-5090-5666-8. Dostupné z: http://ieeexplore.ieee.org/document/7988732/

[9] GRACLA, Michal a Vojtěch KŘESÁLEK, 2017. Determining the Wounding Potential of Shooting Weapons in the Course Forensic Science at the Faculty of Applied Informatics Tomas Bata University in Zlin. The Turkish Online Journal of Educational Technology [online]. 2017(October), 802-810 [cit. 2017-12-07]. ISSN 2146-7242. Dostupné z: http://www.tojet.net/special/2017_10_1.pdf

[10] GRACLA, Michal et al., 2017. Komparace ranivého potenciálu zbraní kategorie D přes oděvní materiál. In: KONEČNÝ, Jiří a Vladimír ADAMEC, ed. Krizové řízení a řešení krizových situací [online]. Uherské Hradiště: Univerzita Tomáše Bati ve Zlíně, s. 94-104 [cit. 2018-01-02]. ISBN 978-80-7454-717-1. Dostupné z: http://www.krizoverizeni-uh.cz/

TEORETICKÉ KONCEPTY, SPOJENÉ S KOMUNIKACÍ V PŘÍPADĚ ROPNÉ NOUZE

THEORETICAL CONCEPTS RELATED TO COMMUNICATION IN CASE OF OIL EMERGENCY

Mgr. Lukáš Harazin, Ph.D., Mgr. Oldřich Luža, Mgr. Oldřich Krulík, Ph.D.
Policejní akademie České republiky v Praze
Lhotecká 559/7, Praha 4
harazin@polac.cz; o.luza@polac.cz; krulik@polac.cz

ABSTRAKT

Cílem příspěvku je indikativně zmapovat možnosti aplikování „teorie komunikace“ na problematiku nedostatku ropy a ropných produktů. Podle názoru autorů existuje rovněž průsečík pro aplikování další existujících teoretických konceptů, které se tématu přímo či nepřímo týkají (koncept „hard power“ versus „soft power“), se kterými rezonují praktické zkušenosti ve vztahu ke komunikaci s veřejností během různých scénářů souvisejících s ropou (v nedávné i dávnější minulosti). Ropa, respektive omezení jejího exportu do určitých zemí, může být specifickou zbraní v mezinárodních konfliktech současnosti. Závěrem příspěvku je poukázání na nejednoznačnost a neprůkaznost jednoduchým pohledů na tuto problematiku, s tím, že daleko korektnější je integrovaný přístup, operující nezřídka s pojmem „smart power“.

KLÍČOVÁ SLOVA

Komunikace, teorie, ropná nouze.

ABSTRACT

The aim of the paper is to map out the possibilities of applying "theory of communication" to the potential oil shortage (or lack of petroleum products). According the opinion of the authors, there is also a point of intersection for the application of other existing theoretical concepts directly or indirectly related to the topic (“hard power” versus “soft power” concept) which resonate with practical experience in communicating with the public during various oil-related scenarios (in the recent and more distant past). Oil, or the restriction of its export to certain countries, may be a specific weapon in international conflicts of today. The result or conclusion of the paper is to point to the ambiguity and inconclusiveness of simple views on this issue, with the fact that an integrated approach, often operating with the notion of "smart power", is much more correct.

KEY WORDS

Communication, theory, oil emergency.

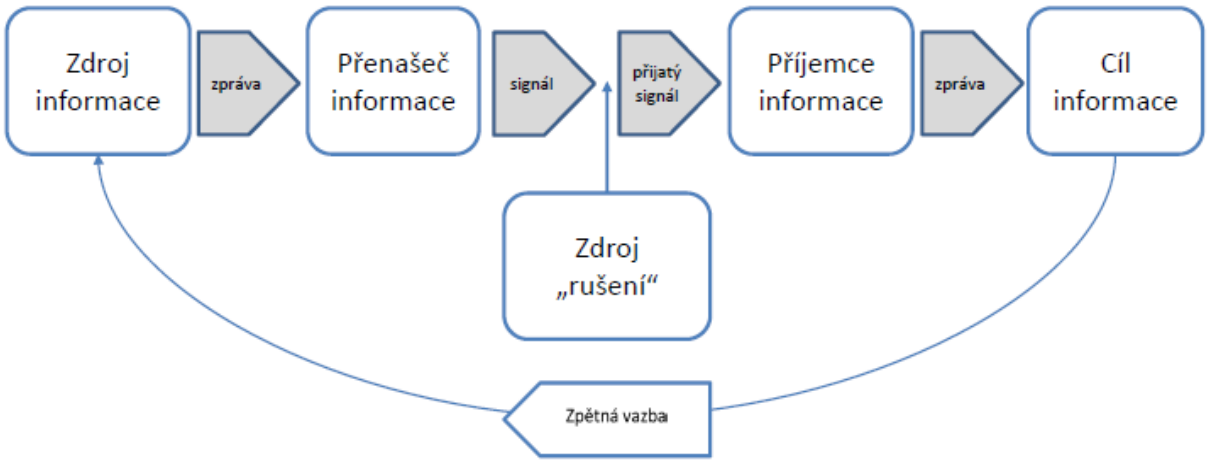
ÚVOD

V tomto příspěvku je pozornost věnována problematice „informování veřejnosti“ (obyvatel), zejména s ohledem na možný scénář ropné nouze. Tato eventualita je zároveň využita jako určitý **průsečík pro aplikování existujících teoretických konceptů, které se tématu přímo či nepřímo týkají** (teorie komunikace, koncept „hard power“ versus „soft power“), stejně

jako existující teoretické přístupy a praktické zkušenosti ke komunikaci s veřejností během různých scénářů souvisejících s ropou (v nedávné i dávnější minulosti).

1. TEORIE KOMUNIKACE JAKO KONCEPT

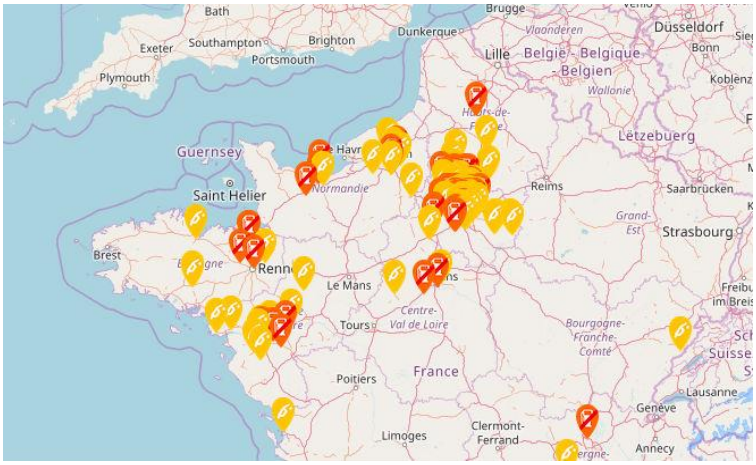
Pokud je řeč o teorii komunikace, pak jejím cílem je šířit přepodklad, že žádná moc (stát atd.) se nemůže opírat jen a pouze na modely, které se dosud odehrály, ale že se musí „učit“ a pružně reagovat na vývoj situace, respektive na chování společnosti, včetně sklonu části veřejnosti komunikační poselství obohatit o různé „šumy“. V případě zúžení problematiky nebo teorie na téma ropné nouze respektive na aspekt důvěry nebo nedůvěry veřejnosti v doporučení ohledně chování ze strany veřejné sféry, pak se jedná přímo o modelovou oblast, kterou lze v souvislosti s touto teorií zmínit. [5], [6], [9], [10]



Obrázek 1 Schematický pohled na možné znázornění procesu komunikace (vlastní zpracování na základě [6])

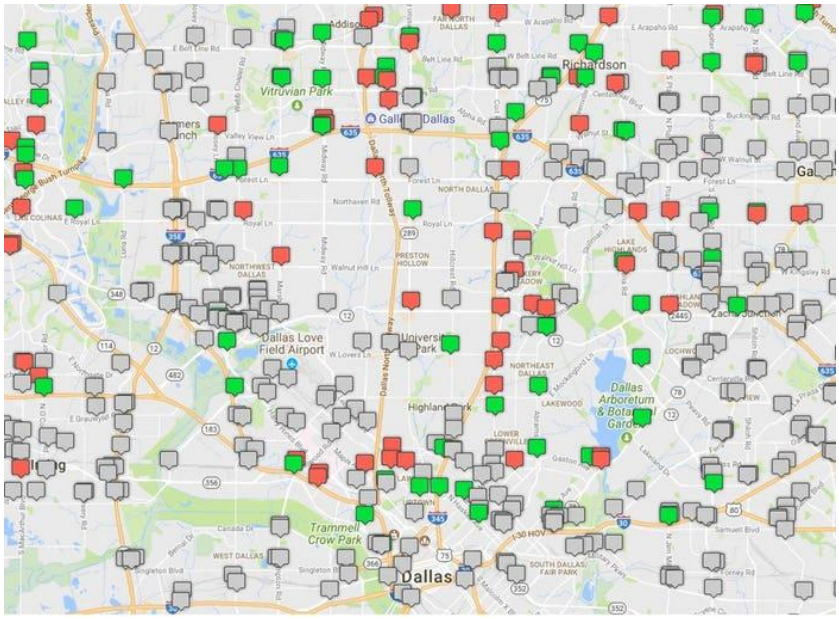
Příkladem „nezvládnutí komunikace” může být Francie. Po zkušenostech s posledním nedostatkem pohonných hmot ve Francii (rok 2010) se zdálo, že tato země bude připravena na možné problémy spojené s nedostatkem pohonných hmot. Jenže tomu tak nebylo. V květnu 2016 Francie opět čelila hrozbě nedostatku pohonných hmot. Záminkou stávek v rafinériích byl vládní návrh reformy pracovního práva. Dopad vleklého konfliktu na společnost byl značný a mnohovrstevnatý [8]

Nedostatek paliva přitom nebyl způsoben samotným nedostatkem této komodity, ale pravděpodobně to byl dopad strachu z obav motoristů, kteří se v nadcházejících dnech báli možnosti nedostatku pohonných hmot do svých automobilů. Zástupci vlády mírnili pesimismus a uvedli, že vše je pod kontrolou. Ministryně dopravy Elisabeth Borne opakovaně uvedla, že v některých oblastech není velký nedostatek ropy nebo potíže s dodávkami. **Vyzvala spotřebitele, aby nešířili paniku a tankovali jako běžně**. Navzdory skutečnosti, že vláda ujišťovala, že nehrozí žádný kolaps a nedostatek pohonných hmot ve Francii, začali motoristé šířit paniku. Zejména to platilo pro severní část Francie. Situace byla také vyhrocena v oblasti okolo Marseille a v blízkosti Lyonu. [15]



Obrázek 2 Portál, popisující čerpací stanice bez paliva [15]

Poněkud proaktivnější využití krizové komunikace ve vztahu k překlenutí ropné nouze lze zaznamenat roku 2017 ve Spojených státech amerických, které se potýkaly s následky hurikánu Harvey. Těžba v Texasu klesla asi o 25 %. V Dallasu se objevily stopy paniky v oblasti nedostatku pohonných hmot. Tím se krize ještě zhoršovala. Znepokojení řidiči neustále naplňovali své částečně plné nádrže, stejně jako nádrže vozidel, které jejich rodiny nevyužily tolik, protože se obávali, že čerpací stanice budou brzy bez pohonných hmot – a to by vedlo ke skutečnému nedostatku. Ceny benzínu vzrostly z 2,60 USD někdy na téměř 8 USD. Úřady požadovaly, aby veřejnost hlásila nadměrné ceny pohonných hmot na portál ochrany spotřebitele consumerreamergency@oag.texas.gov. [3]



Obrázek 3 Portál ochrany spotřebitele, navigující k čerpacím stanicím, kde je ještě k dostání palivo [3]

2. KONCEPT „HARD POWER“ VERSUS „SOFT POWER“

Pokud je zmínka o konceptu či konceptech tzv. „tvrdé“ a „měkké“ moci, pak je třeba zmínit Josepha Nye (ročník 1937), který v současnosti působí jako profesor mezinárodních vztahů na John F. Kennedy School of Government Harvardovy univerzity. [8], [9]

Obrázek 4 Schematický pohled na možné instrumenty „hard“ a „soft“ power (vlastní zpracování na základě [11] [16] a [17])

Tento teoretik mezinárodních vztahů, jeden z hlavních představitelů tzv. neoliberálního institucionalismu, v roce 1990 zavedl do mezinárodních vztahů pojem měkké moci, který se poprvé objevil jeho v knize Bound to Lead: The Changing Nature of American Power. Koncept pak dále rozvinul v díle Soft Power: The Means to Success in World Politics z roku 2004.

Mezi instrumenty „tvrdé síly“ tak podle Nye patří omezení dodávek nebo tranzitu ropy mezi aktéry mezinárodních vztahů, sankce týkající se obchodování s ropou a ropnými produkty, atd. Příkladem nejnovějších komentářů na dané téma může být práce G. Eberlinga[1] z roku 2014. Ten konstatuje, že hranice mezi „hard power“ a „soft power“ může být velmi proměnlivá. Konkrétně Čínská lidová republika se důvodně obává, že její růst, včetně růstu vojenské síly, je nemyslitelný, bez opatření pro zajištění dodávek ropy pro svůj průmysl. I z tohoto důvodu provozuje preventivní a značně oportunistickou diplomacii ve vztahu k zemím, jako je Gabun, Angola nebo země Perského zálivu. [4]

Naprosto průlomová role ropy může být zmíněna ve vztahu k izraelsko-palestinskému konfliktu. Proti sobě stojí přinejmenším dva propastně odlišné postoje. Podle prvního může těžba ropy v pobřežním šelfu pásma Gazy a Libanonu přispět k ekonomickému vzestupu těchto teritorií a otupit palestinský respektive protiizraelský radikalismus – nebo alespoň se spolupráce v oblasti těžby ropy ukáže nezbytnou, bez ní nedostane nikdo nic. [1]

Druhý názor naopak předpokládá, že případný výnos z ropy bude „investován“ do zvýšení „hard power“ Hizballáhu a dalších radikálních skupin a spíše situaci v regionu destabilizuje. Do třetice je pak možné zmínit taktiku protiizraelských teroristů, spočívajících v útocích

[1] Sám Eberling je zajímavou postavou, někdejší příslušník vojenského námořnictva Spojených států amerických, nyní publikující na řadu témat, souvisejících s energetickou bezpečnostním zejména ve vztahu k Čínské lidové republice jako supervelmoci pro XXI. století.

na ropnou plynovou (ale i zavlažovací) infrastrukturu Izraele, ve snaze „poškodit protivníka“ a snížit jeho ekonomickou i vojenskou sílu. [18:14nn]

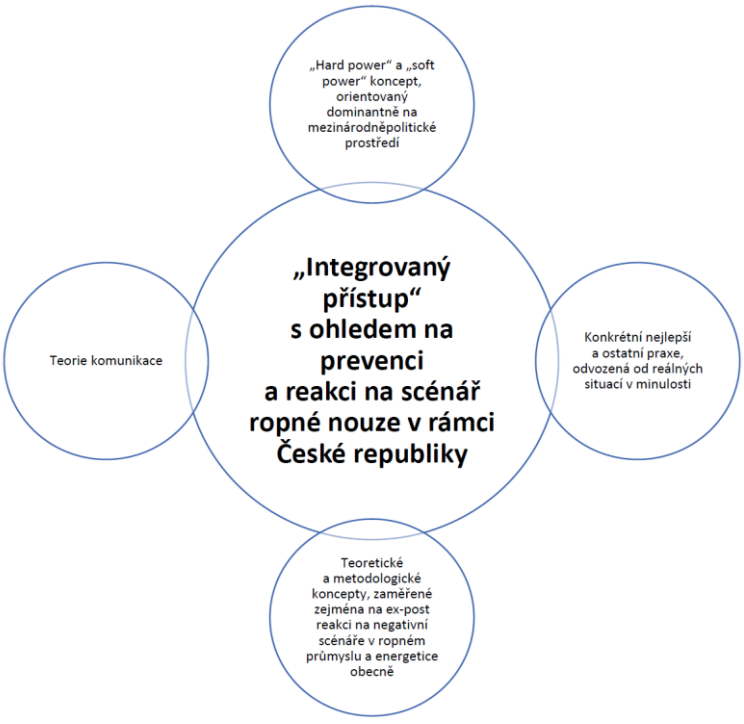
3. PŘEKONÁNÍ KONCEPTU A POSUN K INTEGROVANÉMU PŘÍSTUPU

Celý koncept byl přitom v nedávné době zrelativizován jak samotným profesorem Nye, tak dalšími badateli. [2]

Panuje například košatá diskuse o tom, zda jsou konkrétně zájmy Spojených států amerických v zahraničí lépe efektivněji prosazovány tvrdými silovými donucovacími prostředky, jako je vojenská síla nebo měkkou mocí, méně agresivní prostředky přesvědčování, jako je diplomacie, ekonomická pomoc a propaganda. Barack Obama svého času alespoň rétoricky vyzdvihoval měkkou moc. Byl ale kritizován z obou stran, a to že se tímto doporučením reálně neřídí, nebo že je naopak příliš měkký k protivníkům.

Někdy je používán dokonce specifický pojem „energetická síla“, tedy využívání výhod určité země nebo jiného aktéra co se týče výroby energie a energetických technologií, které podporují její (jeho) mezinárodněpolitické zájmy a mohou perspektivně oslabit priority jejích (jeho) konkurentů. To může znamenat například poskytování energie nebo přímo ropy spojencům (například viz aktivity Venezuely). „*Energetická síla může být využita k posílení vazeb s geostrategickým partnerem, jako je to v jaderné dohodě mezi Spojenými státy a Indií, nebo potrestání ze svého pohledu věrolomného souseda, jako v případě opakovaného rušení dodávek zemního plynu na Ukrajinu.* ***I když není tak tvrdá jako tvrdá síla, energetická síla může znamenat politiku, která stoupá nad úroveň měkké síly.***“ [7]

Sám Joseph Nye nyní svůj někdejší koncept posunul a propaguje spíše pojem nebo koncept „chytré síly“ (smart power). [12]



Obrázek 5: Průnik teoretických konceptů ve vztahu k tématu práce (vlastní zpracování).

V podobném duchu, navíc s přesahem do energetické bezpečnosti se vyjadřuje Michael Klare, přednášející v rámci Five College, Massachusets: Spojené státy podle jeho názoru musí znovu objevit, jak být „inteligentní mocí“. Spojené státy musely přejít od „vyvážení strachu“ k „inspirujícímu optimismu a naději“. Někdejší ministr obrany Robert Gates ostatně vyzval vládu, aby vynakládala více peněz a úsilí na měkké nástroje, včetně diplomacie, ekonomické pomoci a komunikace, protože armáda nemůže bránit americké zájmy na celém světě. [7]

ZÁVĚR

Zátěžová situace, která souvisí s omezením dodávek ropy a ropných produktů bývá obvykle komentována primárně optikou bezpečnostních studií nebo mezinárodních vztahů. Autoři se pokusili tento přístup rozšířit aplikací některých aspektů teorie komunikace nebo přístupu „hard power“ či „soft power“. Řadu badatelů je ostatně toho názoru, že „tvrdá síla“ sama o sobě nemůže dosáhnout žádoucích výsledků (co se týče třeba nátlaku ze strany státu vyvážejícího ropu na státy, které jsou jejími odběrateli). Je tedy chybou, pokud neexistuje adekvátní interagenturní proces pro rozvoj a financování inteligentní energetické strategie.

PODĚKOVÁNÍ

Příspěvek byl zpracován s využitím institucionální podpory na rozvoj výzkumné organizace poskytnuté Policejní akademii České republiky v Praze.

Literatura

[1] BUTT, Gerald. *Gaza Gas Stranded at Sea*. [online] Petroleum Economist, 16. I. 2018. [cit. 2018-03-22] Dostupné na WWW: http://www.petroleum-economist.com/articles/midstream-downstream/lng/2018/gaza-gas-stranded-at-sea

[2] BUZAN, B., (2016). *Confusing Public Diplomacy and Soft Power*. [online] China Policy Institute, 10. III. 2016. [cit. 2017-07-23] Dostupné na WWW: <https://cpianalysis.org/2016/03/10/confusing-public-diplomacy-and-soft-power/>

[3] DICHRISTOPHER, T., (2017) *Texas Faces Fuel 'Crisis' as Depleted Gasoline Stations Deal with Panic Buying*. [online] CNBC. 1. IX. 2017. [cit. 2018-01-02] Dostupné na WWW: <https://www.cnbc.com/2017/09/01/texas-faces-fuel-crisis-as-panic-gasoline-buying-ensues.html>

[4] EBERLING, G., G., (2014). *Future Oil Demands of China, India, and Japan: Policy Scenarios and Implications*. Lexington: Lexington Books, 2014.

[5] GEORGE, A., M., PRATT, C., B., (1997). *Case Studies in Crisis Communication*. Routledge: Abingdon on Thames.

[6] HARRISON, G., A., (2007). *Communication Strategies as a Basis for Crisis Management Including Use of the Internet as a Delivery Platform.* [online] Georgia State University, 1. XII. 2007. [cit. 2017-07-03] Dostupné na WWW: <http://scholarworks.gsu.edu/cgi/viewcontent.cgi?article=1021&context=english_diss>

[7] KLARE. M., T., (2015). *Hard Power, Soft Power, and Energy Power*. [online] Foreign Affairs, 3. III. 2015. [cit. 2017-07-03] Dostupné na WWW: https://www.foreignaffairs.com/articles/united-states/2015-03-03/hard-power-soft-power-and-energy-power

[8] KOTTASOVA, I., (2016). *One in Three Gas Stations in France is Running Dry*. [online] CNN, 25. V. 2016. [cit. 2018-01-02] Dostupné na WWW: <http://money.cnn.com/2016/05/25/news/france-gas-shortages-strike/index.html?iid=el>

[9] LASSWELL, H., (2006). The Structure and Function of Communication in Society. In. COBLEY, P. (ed.) *Communication Theories: Critical Concepts in Media and Cultural Studies*. Routledge: Abingdon on Thames. 2006.

[10] LENCI, D., MULLANE, J. *Communicating with the Public: How BP told the Macondo Story*. [online] Calumet Communications Group, 12. VI. 2010. [cit. 2017-07-03] Dostupné na WWW: http://www.ogj.com/articles/print/volume-108/issue-46/general-interest/comment-communicating-with-the-public.html

[11] MAZURIER, P., (2015). *The Nature of CyberPower*. [online] Cyberpolitics.eu. 2015. [cit. 2017-07-03] Dostupné na WWW: <http://www.cyberpolitics.eu/cyberpolitics_art_01_cyberpower.html>

[12] NYE, J., (2007). Smart Power. [online] HuffPost Blog, 29. XI. 2007. [cit. 2017-07-03] Dostupné na WWW: <http://www.huffingtonpost.com/joseph-nye/smart-power_b_74725.html>

[13] NYE, J., (2008). *Understanding International Conflicts: An Introduction to Theory and History*. New York: Longman.

[14] NYE, J., (2009). *Soft Power: The Means to Success in World Politics*. Public Affairs.

[15] *Panicked Drivers Cause Fuel Stations in France to Run Dry*. [online] The Local, 25. IX. 2007. [cit. 2018-01-02] Dostupné na WWW: https://www.thelocal.fr/20170925/map-here-are-the-fuel-stations-that-are-running-dry-in-france

[16] *Power, Soft Power & China*, (2012). [online] Value of Dissent. [cit. 2017-07-03] Dostupné na WWW: <http://valueofdissent.blogspot.cz/2012/07/power-soft-power-china.html>

[17] Soft Power vs Hard Power, (2016). [online] *Renaissance for Leaders*. 5. XI. 2016. [cit. 2017-07-03] Dostupné na WWW: <https://renaissanceforleaders.com/2016/11/05/soft-power-vs-hard-power/>

[18] TICHÝ, L., (2017). *Energetika jako strategický nástroj hnutí Hizballáh v konfrontaci s Izraelem*. In. Vojenské rozhledy, 2017, č. 1, s. 14nn.

EKONOMICKÉ ASPEKTY MIGRACE

ECONOMIC ASPECTS OF MIGRATION

Ing. Eva Hoke, Ph.D.
Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení
Studentské náměstí 1532, 686 01 Uherské Hradiště
hoke@utb.cz

ABSTRAKT

Migrace je v současné době jedno z nejvíce diskutovaných témat. Odborníci vedou dlouhé diskuse, které se týkají především humanitárních, bezpečnostních a ekonomických aspektů migrace. Právě ekonomické důvody jsou velmi silnou příčinou toho, proč lidé překračují hranice. Cílem příspěvku je sumarizovat příčiny, jež migraci vyvolávají a též důsledky, které způsobují. Pozornost bude zaměřena především na ekonomické aspekty, jako je stárnutí populace, únik mozků (brain drain) či otázka remitencí.

KLÍČOVÁ SLOVA

Migrace, migrační teorie, ekonomické aspekty, remitence, únik mozků

ABSTRACT

Migration is currently one of the most discussed topics. Experts have been conducting lengthy discussions, which mainly concern the humanitarian, security and economic aspects of migration. The very economic reasons are a very powerful cause of why people cross the border. The aim of the paper is to summarize the causes of migration and the consequences it causes. Attention will be focused primarily on economic aspects such as population aging, brain drain, or remittances.

KEY WORDS

Migration, migration theory, economic aspects, remittance, brain drain

ÚVOD

Migrací označujeme proces prostorového přemisťování osob přes hranice, spojený se změnou místa bydliště na dobu kratší či delší, případně natrvalo. Migrace je permanentně jednou ze společenských strategií k získávání zdrojů obživy a energií, vyrovnávání se s nepříznivými přírodními vlivy, řešení společenských konfliktů a dosahování inovací. Migrace bývají odpovědí na více či méně komplexní ekonomické, ekologické, sociální a kulturní podmínky existence člověka. [8] Příčin, proč lidé migrují je celá řada a dle toho se i jednotlivé migrace nazývají, např. ekonomická, environmentální, náboženská, politická apod.

1. UVEDENÍ DO KONTEXTU

Migrace obyvatelstva není žádným novodobým pojmem. Je všeobecně známo, že migrační procesy probíhaly již daleko do naší historie a v evropských dějinách již bylo několik krizí migrantů. Evropa čelila 700 000 žadatelům o azyl po pádu železné opony, situace ještě vážnější byla během a po skončení druhé světové války. Nedávno po vzniku války zahájené ruskými separatisty bylo 2,6 milionů obyvatel Ukrajiny nuceno opustit své domy na východní Ukrajině.

Nyní v současných vyspělých podmínkách jsme však svědky velkých masových přesunů, vyvolaných především krizí blízkého Východu. Budeme-li se migrační krizí či otázkou migrace zabývat, budeme se snažit najít odpovědi především na otázky typu: Jaké jsou příčiny migrace, proč k migraci dochází, z jakých důvodů dané skupiny lidí migrují a případně proč migrace v čase trvá nebo proč existuje reemigrace? Kdo jsou ti, kteří migrují a jaké jsou jejich charakteristiky a jak se liší od obecných charakteristik populace, z níž odcházejí? Jak lidé migrují, skupinově nebo samostatně; je migrace součástí jejich životního cyklu? Jaké je jejich chování v cílových zemích migrace: je jejich migrace trvalá nebo dočasná a jaké adaptační nebo integrační strategie zde volí, nebo volit musí? Co daná migrace způsobuje – u samotných migrantů, v místě přistěhování i v místě, odkud migrovali? [16]

Snažíme se tedy pochopit souvislosti z širšího spektra. Tento článek nemá za cíl detailně rozebrat pohnutky a motivy lidí, neboť otázka migrace je interdisciplinární záležitostí, která sahá do sociologie, ekonomie, etnologie, sociální geografie, práva, demografie, historie, psychologie, politologie a urbanismu a dalších věd. Příspěvek si klade za cíl shrnout a stroze pojednat právě o ekonomických aspektech, jež migraci zapříčiňují a způsobují.

2. MIGRAČNÍ TEORIE

Tak jak lidé migrovali, se utvářely též migrační teorie. Podle uchopení problematiky (filozofie i metodického přístupu) se teorie/koncepty dělí na mikro nebo makro-úrovňové. Zatímco prvá tradice se soustředí zejména na jedince, případně rodinu nebo domácnost a jejich chování svázané s daným mikrosociálním milié, makroúrovňová perspektiva zdůrazňuje ekonomické, sociální a politické okolnosti, jejichž kontext vytváří prostředí, ve kterém daný jedinec-migrant pohyb realizuje (Kulu-Glasgow 1992). [16]

Základem ekonomické teorie, zabývající se ekonomikou migrace, je poznatek o tom, že nejdůležitějšími determinanty migračních toků z méně bohatých zemí nebo oblastí do bohatších zemí jsou mzdové diferenciály, ekonomické rozdíly, rozdíly v HDP na obyvatele a míře nezaměstnanosti (viz například Hannan, 1970; Todaro 1969, Harris a Todaro, 1970, Walsh, 1974, 1987; Strielkowski a O'Donoghue, 2006, Glazar a Strielkowski, 2010; Strielkowski, 2012). Navíc do hry vstupují různé systémy sociálního zabezpečení, které mohou ovlivnit rozsah migrace. Například Cushing (1993), Faini et al. (1999) nebo de Haas (2005) ukazují, jak jsou sociální dávky pro nezaměstnané schopné zvýšit nebo ovlivnit migraci venkov-město nebo mezinárodní migraci. [4]

Tato analýza dokládá, že rozsah a velikost migrace závisí na migračním potenciálu obyvatelstva dané země. Pro obyvatelstvo zemí s vysokým migračním potenciálem je více přirozené reagovat na problémy doma zvýšenou emigrací do země s vyššími příjmy a nižší nezaměstnaností (viz např. Fidrmuc, 2002 nebo Glazar a Strielkowski, 2010). Strielkowski a Turnovec (2011) přichází s konceptem "indikátoru migračních nákladů", který je specifický pro konkrétní zemi a skládá se z hmotné (např. náklady na přesídlení nebo zabydlení se v nové zemi) a nehmotné (např. psychologické náklady migrace, porušení sociálních vazeb, odloučení od rodin nebo přátel, jazyková bariéra, apod.) složky. Ukazuje se, že pokud je tento indikátor vyšší než rozdíl mezi mzdami dvou nebo více států, pro pracovní sílu neexistuje motivace k migraci (v tomto případě je sklon k migraci roven nule). Ekonomické a psychologické náklady migrace jsou větší než výhody mzdových rozdílů plynoucích z migrace. V zemích, kde je tento indikátor vyšší než mzdy, je migrační potenciál (neboli sklon k migraci) nízký a její občané nemusí rychle reagovat na vidinu vyšších mezd a zaměstnanosti v bohatších zemích. [4]

Na přelomu 19. a 20. století v oblasti migračních teorií dochází k výrazné proměně tím, že věda nechápe migraci jen jako mechanické přemisťování z místa na místo, ale i jako proces vyvazování se ze sociálních vazeb ve zdrojovém prostoru a navazování nových sociálních vazeb v zemi cílové. [11]

2.1 Motivy migrace

Motivy, které jsou podstatné pro rozhodnutí k migraci, rozebral již koncem 19. století E. G. Ravenstein ve stále uznávané „push-pull theory". [10] Dle této teorie někteří lidé migrují, protože jsou vypuzováni tzv. „push faktory", jiní naopak proto, že jsou přitahováni do nové země tzv. „pull faktory", přičemž významnější roli hrají pull faktory. Mezi hlavní push faktory patří především nízká úroveň životních podmínek, nedostatek ekonomických a pracovních příležitostí, rychlý demografický růst, válečné, náboženské a národnostní střety, znečištěné životní prostředí, politická represe, přírodní katastrofy, válečné konflikty. Mezi pull faktory patří právě naopak ekonomická prosperita, lepší pracovní příležitosti, politická svoboda, přítomnost příbuzných, přátel či lidí ze stejné komunity, svoboda a možnost seberealizace apod. [12] Dříve hrály mezi migranty významnější roli push faktory, v poslední době se hovoří o posílení pull faktorů při rozhodování o migraci.

S odstupem času lze konstatovat, že Ravensteinovy závěry byly opravdu průkopnické a převratné, o čemž nás může přesvědčit i současná platnost některých jeho zjištění. Na druhou stranu je třeba vzít v úvahu faktor času, tj. že od formulace jeho zákonů uplynulo více než 120 let, proto by se platnost valné části Ravensteinových zákonů musela v současnosti znovu ověřit. [10]

2.2 Ekonomické stimuly

Ekonomické aspekty hrají podstatnou roli v utváření migračních toků. Mají přímý vliv na jejich intenzitu, trvání a směr, spolupodílí se na formulaci migračních politik dotčených zemí. Z pohledu ekonomické analýzy lze primárně rozlišit dvě základní problematiky, a sice ekonomické stimuly a ekonomické dopady.

Při zjišťování (odhadu) migračního potenciálu se užívají dva rozdílné postupy. První je založen na výstupech terénních dotazování, druhý, se opírá o ekonometrické modely pracující s reálnými makroekonomickými ukazateli, přičemž oba mají své klady i zápory. Ekonometrické odhady migračního potenciálu, primárně vycházejí z jednoduchého modelu formulovanému J. Hicksem, který za hlavní příčinu migrace označil mzdové diferenciály mezi cílovými a zdrojovými zeměmi očištěné o náklady migrace Vedle mzdových diferenciálů jsou sledovány také míry nezaměstnanosti, životní náklady nebo veřejné statky a transfery. Výhodou ekonometrických modelů je fakt, že jimi generované odhady migračních potenciálů jsou operativněji zjistitelné (lze je provést kdykoli pro libovolné země). Jak vyplývá z výše uvedeného migrační potenciál, a tudíž i reálnou migraci determinují zejména rozdíly ekonomické úrovně mezi zdrojovou a cílovou zemí, nejčastěji vyjadřované pomocí mzdových diferenciálů hrubých i čistých mezd. Jak uvádí Baštýř, důvody pro používání mezd, spíše než celkových příjmových rozdílů, jsou v zásadě dvojí. Prvním je skutečnost, že většina migrantů vstupuje na pracovní trh v postavení zaměstnance (počty samostatně podnikajících imigrantů jsou, až na výjimky, marginální), druhým je důvodem je lepší dosažitelnost mzdových dat oproti jiným příjmům. [5]

Mezi další faktory, které významným způsobem ovlivňují migrační potenciál, můžeme zařadit typ a strukturální charakteristiky pracovních trhů zdrojových i cílových zemí, jejich vyspělost a úroveň, dále vývoj nezaměstnanosti, pružnost a otevřenost pracovních trhů nebo legislativní

rámec trhu práce. Další faktory, které nejsou přímo spjaty s trhem práce, ale z pohledu migračních toků tvoří jeho komplementy, patří zejména geografická vzdálenost, vzdělání, věková struktura migrantů, rodinný stav a jazykovou vybavenost. [5]

2.2.1 Stárnutí populace

Rabušic a Burjanek publikují o dlouhotrvajících nízkých hodnotách plodnosti a prodlužující se naději dožití, což vyvolává ve vyspělých zemích debaty o tom, jakým způsobem reagovat na následky těchto dvou trendů. Zdá se totiž pravděpodobné, že jejich efektem bude populační úbytek a poměrně značné stárnutí obyvatelstva. [10] Tento trend zaznamenávají všechny ekonomicky vyspělé země. Mezi jeho ekonomické důsledky patří především rostoucí finanční zatížení systému důchodového zabezpečení a systému zdravotní péče. Jako indikátor tohoto zatížení se používá nejčastěji poměr počtu osob v poproduktivním věku ku počtu osob v produktivním věku (index závislosti seniorů). Tento ukazatel však porovnává pouze počty osob, nebere v úvahu rozdíly v jejich produkci a spotřebě ani rozdílné náklady na zdravotní péči. [2]

Podobně jako ve většině dalších vyspělých zemí prochází Česká republika populační krizí, která se projevuje v první řadě nízkou porodností. S prodlužující se střední délkou života a klesající plodností roste věkový medián v populaci a populace se stává starší, přičemž platí, že při úhrnné plodnosti 2,1 dítěte na 1 ženu ve věku 15 – 49 let bude populace zachována. Vysoká plodnost je dle OSN [2015] chápána jako 3,2 dítěte na jednu ženu, nízká pod 2,0 a velmi nízká pod 1,3 dítěte na 1 ženu. Vyšší i nižší úhrnná plodnost než 2,1 přináší své problémy. Pokud je vyšší, populace roste, což může působit problémy v mnoha zemích s nestabilní vládou, slabými státními institucemi a špatným zdravotnictvím a školstvím. Nižší plodnost zase vede ke stárnutí populace. Děti budou pro ekonomiku zemí vzácné, vlády se je možná budou snažit „nahradit“. [7]
Plodnost v ČR, tj. počet dětí připadající na jednu ženu v plodném věku, poklesla během prvních let 21. století na 1,14 dítěte, v roce 2010 vzrostla na zhruba 1,5 dítěte, ale stále je hluboko pod hranicí prosté reprodukce. [2]

S problematikou stárnutí populací ve světě navrhuje Magnus [2009] bojovat těmito způsoby:

- Ti, kteří mohou pracovat, budou pracovat déle a více,
- Podpořit vyšší produktivitu práce,
- Podpořit migraci za účelem většího výběru na trhu práce a odstranění dovednostních nedostatků,
- Podporovat úspory domácností za účelem vyhnutí se problémům v přerozdělování důchodů.

Je to právě migrační politika, která začíná být v současné době opět prvkem, o němž se v západoevropských zemích uvažuje jakožto o vážném faktoru populační politiky. Může být totiž potenciálně jedním ze způsobů, jak zmírnit efekty populačního úbytku a populačního stárnutí. Obnova obyvatelstva je tedy závislá na migračním saldu – i střední varianta projekce počtu obyvatel bez migrace (ČSÚ, 2009) totiž předpokládá pokles počtu obyvatel z 10,3 milionu (2010) na asi 8,12 milionu (2050), tedy čistý úbytek větší než dva miliony lidí. Nízká varianta projekce bez migrace by přinesla dokonce pokles počtu obyvatel pod 7,5 milionu. [2]

Samotná předpokládaná imigrace vyvolá poměrně značnou pravděpodobnost řady dalších jevů provázejících tento vývoj – především výrazné zatížení vzdělávacího systému výuky alespoň základní znalosti jazyka, pravděpodobně velmi nevhodné složení znalostní struktury imigrantů, tedy zatížení vzdělávacích programů pro jejich rychlé začlenění do pracovního

procesu. V souvislosti s tím je nutné vnímat i fakt, že i při relativně vysokém saldu migrace se celá ekonomika bude potýkat s dramatickým nedostatkem pracovní síly – v roce 2010 bylo v produktivním věku (20 až 65 let) asi 6,6 milionu lidí, v roce 2050 to i přes velkou imigraci (již zmíněné saldo 10 až 25 000 osob ročně) bude zhruba 4,2 až 4,6 milionu obyvatel země. [13]

2.3 Ekonomické dopady

Ekonomické dopady můžeme zkoumat z různých pohledů. První, z pohledu na zdrojovou zemi a dále na cílovou zemi. Imigrační dopady lze rozdělit na rozpočtové (daně a transfery - např. výplaty starobních důchodů, dávek státního pojištění, v nezaměstnanosti), dopady na makroekonomické indikátory (HDP, růst ekonomiky) a dopady na trh práce (mzdy, zaměstnanost, kvalifikační struktura, aj.).

Bereme-li do úvahu zdrojovou zemi, čili zemi, odkud imigranti pocházejí, tak je nejspíše největším problémem tzv. únik mozků (brain drain). Odliv mozků znamená odchod kvalifikovaných jedinců většinou kvůli nedostatku příležitostí či lepším podmínkám. Dopad odlivu mozků na rozvojové země je jedním z nejdiskutovanějších témat v oblasti migrace a rozvoje. Rozvinuté země usilují o přitahování kvalifikovaných migrantů z rozvojových zemí a zavádí různé programy, jako např. modré karty. Nejúspěšnější je ale v této oblasti USA a Austrálie, kam směřuje nejvíce vzdělaných odborníků (např. v Silicon Valley pracuje mnoho vědců indického a čínského původu). Podle některých není negativní vliv jednoznačný, protože lidé se často vracejí – bohatší o nové zkušenosti - a mohou tak pomoci rozvoji původní země (Tchaj-wan nebo Jižní Korea se i díky vzdělaným lidem navracejícím se v devadesátých letech po zkušenostech s prací převážně v USA staly jedničkou v oblasti vyspělých technologií). Na druhou stranu rozvojové země přichází o odborníky, např. odchod zdravotnického personálu z Afriky a Asie může v původních zemích podle odborníků brzy způsobit katastrofu. V Británii tvoří až třetinu zdravotnického personálu mimoevropští lékaři a zdravotní sestry. V Ghaně slouží 20 milionové populaci pouze 1500 lékařů, ale v Británii pracuje 300 ghanských lékařů a dalších 500 v USA. [12]

Česká republika, která se řadí v rámci EU mezi vyspělé země s relativně vysokým životním standardem a dlouhodobou malou ochotou obyvatel migrovat za prací tento problém nepociťuje nijak výrazně, na druhou stranu například sousední Polsko je jím zasaženo již více a státy jako Rumunsko (emigrovaly až 4 % obyvatelstva) či Litva ještě více.

V souvislosti s emigrací nelze však hovořit o čisté ztrátě, jelikož obyvatelé v zahraničí získávají zkušenosti a zpět posílají finanční prostředky ve formě tzv. remitencí, které mohou dosahovat řádově až procent HDP. Právě remitence hrají významnou roli v posuzování migrační politiky. Remitence jsou peníze zasílané zahraničními pracovníky do země původu. Objem těchto peněz celosvětově představuje 300 miliard dolarů, což je třikrát větší částka, než kterou jednotlivé vlády poskytují na rozvojovou spolupráci. Efektivní adresný nástroj, protože prostředky pomáhají konkrétním rodinám (na vzdělání, rozvoj drobného podnikání, zlepšení bydlení, zdravotní péči). Podle odhadů podporuje jeden člen rodiny pracující v zahraničí čtyři až pět lidí v zemi původu. Na rozdíl od rozvojové pomoci jsou ale remitence v zemích původu často použity pouze na materiální potřeby a negenerují tak další zisk. Mezi státy, které přijímají největší částku remitencí, patří Indie (27 miliard USD), Čína (25,7 mld. USD), Mexiko (25 mld. USD), Filipíny (17 mld. USD). Pokud se podíváme na procento HDP, největší část HDP tvoří peníze od občanů pracujících v zahraničí v Tádžikistánu a Moldavsku (36 % HDP), dále v Tongu (32 % HDP), Kyrgyzstánu (27 % HDP) a Hondurasu (26 % HDP). V ČR byla uskutečněna studie Remitence zasílané z České republiky a jejich

rozvojový dopad. Z ČR směřuje nejvíce remitencí na Slovensko (37 %), Ukrajinu (28 %) a do Vietnamu (11 %). [2]

Remitence jsou velmi špatně měřitelné, neboť existuje velmi málo datových zdrojů, a tak je odhad výše remitencí proto prováděn pomocí odhadů ČSÚ a sociologických šetření. [1]

Celkové množství odeslaných remitencí bylo v roce 2015 necelých 32 miliard Kč, z čehož dvě třetiny šly mimo země EU. Celkový přínos pracovní migrace lze nejlépe vyjádřit poměrem k makroekonomickým ukazatelům, v tomto případě k národnímu disponibilnímu důchodu. Přijaté remitence zahrnují dle metodiky národních účtů jak remitence z dlouhodobých pobytů v zahraničí, tak mzdy krátkodobých pracovníků v zahraničí. Stejně tak odeslané remitence zahrnují remitence z dlouhodobých pobytů cizinců v ČR, tak mzdy krátkodobých zahraničních pracovníků v ČR. Přínosem ovšem nejsou nejen remitence krátkodobých a dlouhodobých pracovníků, ale také mzdy vyplacené dlouhodobým zahraničním zaměstnancům v ČR. Celkový přínos, tedy rozdíl mezi přijatými a odeslanými remitencemi plus mzdy dlouhodobých zaměstnanců činí 3,5 % disponibilního důchodu v roce 2015. V absolutním vyjádření dosáhl přínos z migrace v roce 2015 144 mld. Kč. [1]

Rabušic (2001) považuje za ekonomický přínos migrace daně, které u nás pracující imigranti musejí ze svého příjmu odvést. Jelikož část imigrantů se po určité době vrací do země původu, nejsou jim zde v ČR vypláceny důchody a jejich příspěvek do důchodového systému je tak rozdělen mezi české důchodce. Dalším přínosem imigrantů je zvýšená nabídka práce. Často jsou imigranti ochotni vykonávat práci, kterou český zaměstnanec odmítá, navíc za nízkou mzdu. [9] Další z významných problémů je proto tzv. brain waste, tedy mrhání mozky. To znamená, že pracovní migranti z těchto zemí často berou práci hluboko pod svou kvalifikací (například vysokoškolák ve výkopech), ve které se dále nerozvíjejí. Zároveň v případě, kdy mají štěstí a naberou v zahraničí cenné zkušenosti, nejsou schopni je zužitkovat. [12]

V České republice v roce 2015 žilo 569 tisíc cizinců, což je 5,3 % obyvatel. Je to dvakrát více než před 10 lety a šestkrát více než v roce 1993, přesto je podíl cizinců velmi malý ve srovnání s ostatními evropskými zeměmi. 46,5% cizinců pochází ze zemí EU, z toho 35,7% ze zemí měnové unie. [14]

3. ŘEŠENÍ

Jak již bylo uvedeno výše, vyspělé evropské ekonomiky jsou zásadně oslabeny faktem, že počet potomků původních obyvatel se v každé další generaci snižuje. Pokud například dosáhneme v jedné generaci plodnost pouze 1,5 dítěte na ženu, v principu to značí, že následující generace bude o čtvrtinu méně početná. Jestliže tento fakt nemá znamenat naprosté zhroucení vyspělých ekonomik, pak nezbývá, než nechat „kolonie“ dále vcházet do „domu“, tedy nechat migraci z méně vyspělých do vyspělých států relativně volný průběh.

Přinejmenším ve smyslu „dodávek pracovní síly“. I tak budeme svědky značného přesunu ekonomické aktivity mimo nynější nejbohatší země, ale zmíněný úbytek obyvatel musí být prostě nahrazen, aby nedošlo k naprostému pádu systému.

Zvládnutí situace, načrtnuté v předchozích řádcích, si bude vyžadovat značnou koncentraci opatření a rozhodnutí především ekonomického charakteru, která však budou mít značné politické a sociální konsekvence. Vyspělé země se musí připravit na řadu kroků, které budou v mnoha případech hraničit s tradicemi a budou v kolizi s kulturními, sociálními a ekonomickými zvyklostmi vyspělých států. Bude nutné nikoliv reformovat, ale především

revidovat a redukovat důchodové systémy, bude nutné připustit, že v péči o zdraví existuje rovnost pouze do určité výše nákladů, bude nutné změnit celý školský systém a pojmout ho nejen jako oblast vzdělávání mládeže, ale také jako nástroj pro výkon nutné míry asimilace migrační dospělé populace. Co je ale nutné znovu zdůraznit, to je fakt, že nehledě na veškeré konsekvence, problém „stárnutí“ je otázkou v první řadě hospodářskou. Veškeré další souvislosti je možné řešit efektivním způsobem pouze tehdy, pokud budeme o věci přemýšlet jako o problému ekonomickém, tedy jako o otázce vývoje ekonomického prostředí, vývoje tržních vztahů či poptávky a nabídky. Jestliže v tomto přemýšlení převládnou ohledy politické nebo sociální, velmi pravděpodobně by to vedlo k prohloubení potíží ekonomických, nikoliv k jejich řešení. [13]

Migrace se stala předmětem společných politik v roce 1999 a od té doby je jedním z klíčových témat. V migračních politikách se postupně začal prosazovat rozvojový aspekt. Po zasedání Evropské rady v Tampere v roce 1999 platí při řízení migrace v EU zásada udržování rovnováhy mezi hospodářským prospěchem EU a rozvojovou situací v zemi původu a vytváření partnerství (EU podepsala readmisní smlouvy s Hong Kongem, Srí Lankou, Albánií, Macaem, probíhají další jednání). Na toto téma bylo publikováno několik komunikací a směrnic, naposledy Evropský pakt o migraci a azylu, který byl přijat v září 2008 a kde je téma migrace a rozvoje jedním z pěti klíčových (vedle legální migrace, boji proti nelegální migraci, kontroly hranic a azylového systému). Klíčové by mělo být partnerství se zeměmi původu migrantů a podpora rozvoje zemi původu, aby migranti neodcházeli. Na období 2007-2010 bylo na finanční a technickou podporu třetích zemí vyčleněno 205 milionů eur. EU se v oblasti migrace a rozvoje soustředí především na: spolupráci se třetími zeměmi podporu cirkulární migrace zejména u vzdělaných a kvalifikovaných migrantů ze třetích zemí tak, aby jejich odchod neměl negativní dopad na země původu snahu o omezení nákladů na remitence zařazení oblasti genderu do migračních politik podporu diaspory při rozvoji zemí původu. [12]

ZÁVĚR

Česká republika nepatří k zemím, kde migrace a remitence mají negativní vliv na ekonomiku. Migranti zde svou prací přispívají k tvorbě HDP, za svou práci dostávají mzdu, ze které platí sociální pojištění a daně. Migranty též můžeme označit za levnou pracovní silou pro domácí zaměstnavatele, vykonávají práce, kde by bylo obtížné získat jiné zaměstnance a často za nižší mzdu, než za kterou by pracoval rezident. Své vydělané peníze zde z části také utrácejí, čímž napomáhají dalšímu točení kol ekonomiky. Pracovní imigrace tak pomáhá udržet stabilní poměr mezi produktivní a poproduktivní populací a vytváří dodatečné zdroje pro ekonomiku a lze vyčíslit i přínosy pro státní rozpočet a důchodový systém. Zvládnutí ekonomického fenoménu migrace vyžaduje vhodnou migrační politiku, která v konečném důsledku může být výhodná pro hostitelkou zemi i zemi původu. Vhodná podpora migrace umožňuje se vyrovnat se stárnutí naší populace s chybějícími pracovníky v celé řadě profesí. V optimálním případě vhodná politika může zajistit, že Česká republika bude cílovou zemí, kde cizinci zůstanou natrvalo. Kde se stanou aktivními členy společnosti z právního, sociálního, ekonomického, vzdělávacího i kulturního hlediska. Efektivní imigrační politika by měla zahrnovat podporu přílivu kvalifikovaných zahraničních pracovníků a měla by bránit nelegální imigraci. V této oblasti bohužel není dořešena otázka válečných uprchlíků, kteří potřebují dočasný azyl, legálních ekonomických migrantů a nelegálních ekonomických migrantů. Nebezpečí, která při absenci migrační politiky hrozí, pramení zejména z xenofobních názorů stávající populace, což může vést k izolování přistěhovalé skupiny osob, uzavírání takové skupiny do sebe, a tím následně horší integraci do stávající společnosti. [14]

Literatura

[1] ČSÚ. 2016. [online]. Praha: Český statistický úřad 2016. [cit. 2018-8-14]. Dostupné na WWW: https://www.czso.cz/csu/czso/cizinci-v-cr

[2] FIALA, T., LANGHAMROVÁ, J. [online]. *Ekonomické důsledky stárnutí populace České republiky*. [cit. 2018-8-14]. Dostupné na WWW: https://kdem.vse.cz/resources/relik10/PDFucastnici/Fiala_Langhamrova.pdf

[3] HERZÁN, M. Svědectví z uprchlického tábora: Migranti jsou jako časovaná bomba, Unie ztratila soudnost. Novinky.cz [online]. Dostupné z: http://www.novinky.cz/domaci/393789-svedectvi-z-uprchlickeho-tabora-migranti-jsou-jako-casovana-bomba-unie-ztratilasoudnost.html

[4] KOWALSKA, K., STRIELKOWSKI, W. [online]. *ANALÝZA: Sklon k migraci a migrační potenciál ČR a Polska.* [cit. 2018-8-30]. Dostupné na WWW: http://www.demografie.info/?cz_detail_clanku&artclID=894

[5] LENOMAR, A. [online]. Mezinárodní pracovní migrace ve vybraných zemích střední Evropy [cit. 2018-8-14]. Dostupné na WWW: https://is.muni.cz/th/wvyzj/?so=nx

[6] MACHÁČEK, J. [online]. *Měli by ekonomové o efektech migrace mlčet?* [cit. 2018-8-30]. Dostupné na WWW: https://www.kzamysleni.cz/migrace-jako-prirozena-soucast-ekonomickeho-mysleni-cloveka/

[7] NEWBOLD, K. B. *Six billion plus: world population in the twenty-first century*. Vyd. 2. Lanham, Md.: Rowman & Littlefield Publishers, 2007. ISBN 978-0-7425-3928-0.

[8] PAVLÁT, M. Determinanty vzniku migrace a statistiky cizinců v Evropské unii. Praha: Key Publishing, 2012. ISBN 978-80-7418-228-0

[9] RABUŠIC, L. *Kde ty všechny děti jsou?* Sociologické nakladatelství. Praha: SLON, 2001. 266 s. ISBN 80-86429-01-6.

[10] RABUŠIC, L., BURJANEK, A. *Imigrace a imigrační politika jako prvek řešení české demografické situace?* Brno: VÚPSV, 2003, s. 9.

[11] RÁKOCZYOVÁ, M., TRBOLA, R. *Sociální integrace přistěhovalců v České republice*. Praha: SLON, 2012. ISBN 978-80-7419-077-3

[12] ROZVOJOVKA. [online]. Migrace a rozvoj. [cit. 2018-8-18]. Dostupné na WWW: http://www.rozvojovka.cz/publikace/11-migrace-a-rozvoj.htm

[13] SMRČKA, L., ARLTOVÁ, M. [online]. *Ekonomické aspekty stárnutí populace ve vyspělých zemích.* [cit. 2018-8-31]. Dostupné na WWW: https://www.researchgate.net/publication/290369902_Ekonomicke_aspekty_starnuti_populace_ve_vyspelych_zemich

[14] ŠIMKOVÁ, M. [online]. *Ekonomické aspekty pracovní migrace v ČR*. [cit. 2018-8-14]. Dostupné na WWW: http://www.czechdemography.cz/res/archive/002/000325.pdf?seek=1485543413

[15] ZPRÁVY O REMITENCÍCH JEDNOTLIVÝCH ZEMÍ. [online]. [cit. 2018-8-14]. Dostupné na WWW: http://www.worldbank.org/en/topic/migrationremittancesdiasporaissues/brief/migration-remittances-data

[16] UHEREK, Z., DRBOHLAV, D. [online]. Reflexe migračních teorií. [cit. 2018-8-14]. Dostupné na WWW: https://web.natur.cuni.cz/ksgrrsek/illegal/clanky/Uherek-Teorie.pdf

POUŽITÍ QUALITY ESSURANCE MATRIX METODY ŘÍZENÍ RIZIK S CÍLEM ZVÝŠENÍ VÝKONNOSTI VYBRANÉHO VÝROBNÍHO PROCESU

USING THE QUALITY ASSURANCE MATRIX INTERACTIVE RISK MANAGEMENT METHOD TO INCREASE THE PERFORMANCE OF A SELECTED PRODUCTION PROCESS

Ing. Lucie Hrbáčková
Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky
Mostní 5139
760 01 Zlín
lhrbackova@utb.cz

ABSTRAKT

Soudobé trendy ve zvyšování výkonnosti podnikových procesů jsou orientovány do oblasti řízení rizik s ohledem na kontext organizace. Jde o rizika, která mohou vzniknout při realizaci podnikatelské činnosti a projeví se odchýlením skutečných výsledků od plánovaných. Existuje několik metod pro posuzování rizik v procesu, které jsou firmami využívány pro řízení rizik. Tento článek se zaměřuje na metodu Quality Essurance Matrix (QAM), která slouží pro řešení rizik ve výrobním procesu, a je užívána zejména v automobilovém průmyslu. Autor popisuje použití metody QAM v procesu vstřikování plastů. Cílem článku je zhodnotit dopad metody Quality Essurance Matrix na výkonnost procesu vstřikování po jejím zavedení a využívání v procesu.

KLÍČOVÁ SLOVA

Výkonnost podnikových procesů, Quality Essurance Matrix, QAM, řízení rizik, podnikové procesy

ABSTRACT

Current trends in improving business process performance are focused on risk management according to the context of the organization. These are the risks that may arise in business and will be reflected by deviating from the actual results. There are several methods for risk assessment process, which are used by companies to manage risk. This article focuses on the Quality Assurance Matrix (QAM) method, which is used to address the risks in the manufacturing process and is used mainly in the automotive industry. The author describes the use of QAM in the plastic injection process. The aim of the article is to evaluate the impact of the Quality Assurance Matrix method on the performance of the injection process after its introduction and use in the process.

KEY WORDS

Business process performance, Quality Essurance Matrix, QAM, risk-based thinking, business processes

ÚVOD

Soudobým trendem v oblasti podnikových procesů je myšlení založené na rizicích, které by mělo začínat u strategického plánování, následovat fáze rozhodování, řízení a směřovat až do myšlení založeného na rizicích v jednotlivých procesech organizace. Rizika jsou chápána jako negativní jevy, které mohou nastat s určitou pravděpodobností a různými dopady na podniková aktiva i pasiva. Obecně lze rizika v podnikových procesech chápat jako negativní odchýlení se skutečných výsledků od plánovaných. Vlastníci procesů jsou odpovědní za řízení rizik a musejí volit metody a postupy pro zajištění možných negativních jevů. Norma ČSN EN ISO 9001: 2016 Systém managementu jakosti – Požadavky obsahuje kapitolu 6.1 Opatření pro řešení rizik a příležitostí. Organizace musí plánovat, integrovat a hodnotit efektivnost stanovených opatření pro řešení rizik a příležitostí do procesů systému managementu kvality. Doplňující normou pro systémy managementu a řízení rizik je v tomto roce aktualizovaná norma ISO 31000, která se zaměřuje na řízení rizik, přijímání rozhodnutí založené na rizicích a zlepšování výkonnosti. Tyto aktuální trendy jsou důvodem aplikace myšlení založeného na rizicích do podnikové kultury. MAPI and Deloitte (2015) označil aktivity zaměřené na řízení rizik, zejména v oblasti interních auditů a rozhodování o investicích, jako klíčové aktivity v získání přední pozice mezi konkurenty na trhu. Firmy, které budou správně implementovat a řídit tyto aktivity ve svých podnikových procesech, mají šanci se stát výkonným a významným hráčem na trhu.

1. LITERÁRNÍ REŠERŠE

Mezi externí faktory ovlivňující neustálé zlepšování v oblasti výrobních firem patří nové trendy publikované Mezinárodní organizací pro normalizaci (dále jen organizace ISO) zastoupenou v České Republice, Českým institutem pro akreditaci. Od roku 2016 došlo k aktualizaci několika norem, které požadují po organizacích zakomponovat myšlení založené na rizicích do celého systému řízení kvality.

1.1 Řízení rizik a ISO 9001:2016

V roce 2016 vyšla aktualizovaná norma ČSN EN ISO 9001: 2016 Systém managementu jakosti – Požadavky, která obsahuje nové prvky pro systém řízení kvality ve firmách zejména v oblasti řízení rizik v podnikových procesech. Tajemník ISO Kevin McKinley zdůrazňuje přínos v aktualizaci standardu ISO 9001 ve zvládnutí příležitosti organizací se adaptovat na měnící se svět (ISO 2015). Výzkum provedený IRCA QMS (Mezinárodní registr certifikovaných auditorů) označuje aktualizovanou normu za prospěšný nástroj pro vytváření konceptu moderního systémy řízení kvality v podnikovém prostředí (Fonseca et al., 2016).

Norma ISO 9001: 2015 organizacím doporučuje, aby definice rizik probíhala na základě kontextu a cílů organizace, zároveň jim nenařizuje způsob, jakým mají rizika řídit. Sitnikov a kol. (2017) popisují, že nová verze normy ISO 9001: 2015 představuje významnou příležitost k vytvoření integrovaného systému řízení výkonnosti, a to vytvořením významných vazeb mezi řízením kvality a neustálým zlepšováním na jedné straně a řízením podnikových rizik na straně druhé.

1.2 Výkonnost procesů a řízení rizik

Další aktualizovanou technickou normou, která se zabývá pojmem řízení rizik, je norma 31000: 2018 Risk management - Guidelines, která má zajistit organizacím prostřednictví

svých pokynů zvýšení dosažených cílů, zlepšení identifikace příležitostí a hrozeb a efektivní přidělení zdrojů pro řízení rizik a možnost zvýšení výkonnosti podnikových procesů. (ISO, 2018)

Kapitola 9 Hodnocení výkonnosti dle normy ČSN EN ISO 9001: 2016 doporučuje určení metod pro monitorování, měření, analýzu a vyhodnocování, které jsou potřebné pro zajištění platných výsledků (ISO 9001: 2016). Firmy musejí zvolit správné metody pro analýzu a zlepšování svých procesů.

Kohlbacher a Gruenwald (2011) uvádí, že vlastník procesu je odpovědný za měření výkonnosti a zlepšování procesu. Vlastník procesu se musí rozhodnout o druhu aktivity, metody či postupy pro řízení rizik a příležitostí pro zvýšení výkonnosti procesu, za něhož nese odpovědnost.

Herrinton (2012) doporučuje stanovit KRI (Key Risk Indicators), tedy klíčové indikátory rizika s cílem predikovat, modelovat a kontrolovat posouzení rizik. MetricStream (2018) tvrdí, že správné stanovení klíčových indikátorů rizik je kritické pro úspěšný proces řízení rizik v podniku.

1.3 Metody řízení rizik

Norma ČSN EN 31010: 2011 Management rizik – Techniky posuzování rizik poskytuje návod k volbě a aplikaci systematických technik pro posuzování rizik. Tato norma rozděluje metody hodnocení rizik podle stupně podrobnosti na kvalitativní, semikvantitativní a kvantitativní metody. Antušák (2013) pro kvantifikaci rizik dělí metody dle stupně podrobnosti a dle schopnosti kvantifikace míry rizika. Analytické metody založené na deterministickém přístupu mohou být kvalitativní, ale také semikvantitativní (Antušák, 2013). Pravděpodobnostní metody a modely lze v analýze rizik využít pouze v případě opakovatelnosti, u jedinečných událostí pozbývají smysl (Aven, 2010). Šefčík (2009) uvádí, že kritériem pro výběr vhodné metody je dostupnost dat, které metoda využívá.

Rizikové matice a rizikové diagramy jsou široce používané nástroje pro analýzu, posuzování a vizualizaci rizik v mnoha průmyslových odvětvích, a jsou používány značně pro účely řízení rizik. Problémem v těchto nástrojích je neurčitost vizualizace nejistoty (Goerlandt a Reniers, 2016).

1.4 Nástroj QAM

Metoda QAM patří mezi analytické metody založené na deterministickém přístupu. Jiránek (2007) uvádí, že tato metoda má vést k dosažení „nulové chyby“ ve výrobě či na montáži.

Tento nástroj pro zabezpečení kvality má předejít vzniku možných defektů/vad v procesu. Cílem této metody je odhalit prostřednictví již existujících tzv. bran kvality možné vady, a tím zabránit vzniku vady u interního i externího zákazníka. Dalšími přínosy využívání tohoto nástroje je zvýšení produktivity, zlepšení toku informací a snížení nákladů na opravu chyb. Tento metodický nástroj mohou pracovníci využívat v různých průmyslech výrobních společností. Metoda QAM je využívána v týmu, který se pravidelně schází a řeší vznik interních a externích vad. (Neises, 2015)

Lindqvist a kol. (2011) uvádí v závěru svého příspěvku, že při zajišťování kvality u vydefinovaných vad v metodě QAM pro zlepšení aktuálního stavu by se měli pracovníci zamýšlet nad následujícími body:

- Co by mělo být v procesu měřeno, řízeno a sledováno?

- Jak je důležitá role operátora v procese? (vliv na chybu a jeho odborná zdatnost)
- Jaký význam má každé konkrétní měření, a jaká je jeho důležitost?
- V případě specifické operace, dochází k měření ve specifických podmínkách? (separované měřící místnosti)
- Jak se provádí měření? (ruční, poloautomatické nebo plně automatické)
- Jaké máme k měření měřící nástroje?
- Kdy provádíme měření? A jak často se měření provádí ve vztahu k velikosti výrobní dávky?
- Kdo provádí měření? Jak je nastavena kompetence a požadavek na vzdělání k vykovávanému měření?

(Lindqvist a kol., 2011)

2. METODIKA

Metoda řízení rizik zvaná Quality Assurance Matrix (dále jen QAM) byla použita na základě předchozí případové studie, která srovnává využití metody FMEA (Failure Mode and Effect Analysis – Analýza možných vad a jejich následků, dále jen FMEA) a QAM. Výsledky této studie (Hrbáčková, 2016) poukazují na výhodu používání metody QAM z důvodu její interaktivity pro řešení již vzniklých vad ve výrobním procesu.

Autor použil kvantitativní výzkum ve formě případové studie ve vybrané společnosti ve výrobním procesu. Touto metodou se autor snaží zachytit detailně způsob použití metody QAM ve výrobním procesu vstřikování plastů. Cílem této studie je odpovědět si na následující vědeckou otázku: Zvýší se zavedením metody QAM výkonnost vybraného procesu? Metoda byla ve vybrané společnosti aplikována a používána po dobu 6 měsíců, po této době bylo vyhodnocena účinnost používání metody QAM s ohledem na snížení nekvality na vstřikolisovně a ovlivnění měřitelného ukazatele výkonnosti procesu vstřikování – produktivitu.

3. VÝSLEDKY PŘÍPADOVÉ STUDIE

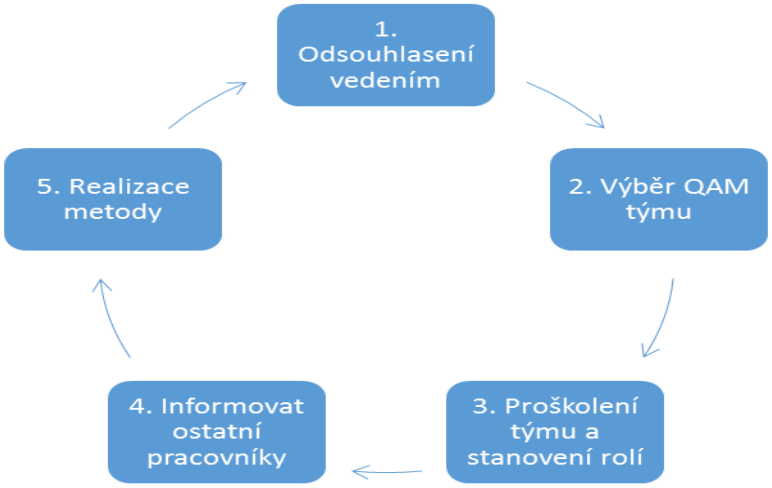
V této části výsledků autor popisuje způsob implementace metody QAM do procesu výroby plastů. Zmiňuje kroky, které jsou nezbytné pro úspěšné zavedení. Metoda QAM byla zavedena a používána 6 měsíců ve vybraném procesu a následně bylo zhodnoceno, jaký vliv má její používání na výkonnost procesu.

3.1 Implementace metody QAM

Pro zavedení metody QAM byl výrobním ředitelem jako vlastníkem procesu vybrán proces vstřikování plastů. Důvodem byla skutečnost, že od roku 2016 se společnost potýká s vyšší nekvalitou při procesu najíždění nové výroby a dále také nedochází k odhalování příčiny vzniku potenciálních, ani existujících chyb.

Pro aplikaci metody QAM muselo být její použití odsouhlaseno na poradě vedení jako pilotního nástroje pro řízení rizik. Výrobní ředitel určil QAM tým, který byl následně proškolen o definici a aplikaci metody QAM. Všichni pracovníci ve výrobě byli informováni o započaté aktivitě.

QAM tým byl složen z vedoucího vstřikolisovny (vedoucí týmu), technologa vstřikování, pracovnice technické kontroly, seřizovače a obsluhy vstřikolisů (dle směnnosti, 1-2 obsluhy na směnu). Vedoucí týmu má za úkol tým svolávat a moderovat, tj. pobízet tým k aktivitě. Setkávání QAM týmu je stanoveno pravidelně 1krát týdně, v případě vzniku externí reklamace okamžitě. Jednou měsíčně se QAM týmu účastnil technický a výrobní ředitel.



Obr. 1 Kroky implementace metody QAM (vlastní zpracování)

3.2 Realizace metody QAM

Výchozím a zásadním bodem pro realizaci metody je zpracování procesní FMEA pro vybraný proces. Všechna definovaná rizika procesu vstřikování včetně jejich příčin byla zanesena do formuláře QAM jako popis chyby či rizika s příčinou v závorce, viz. Obr. 2. Na obrázku můžeme vidět místo 3. vstřikolis a procesní krok vstřikování. Místem jsou myšleny prostory související s prostorem. V našem případě jde o dílnu mechaniků (procesní krok – příprava formy), sklad vstupního materiálu (procesní krok - příprava materiálu), vstřikolis (procesní krok – vstřikování) a skladový prostor (procesní krok – manipulace s kusy).

Místo	Procesní krok	Popis chyby / rizika [hlavní příčina v závorce]
3. Vstřikolis	Vstřikování	Znečištěný výlisek (rozjezdový kus znečištěn od konzervace formy)

Obr. 2 Definice chyb a rizik s příčinou (vlastní zpracování)

Následně jsou všechny chyby (rizika) hodnoceny z dvou hledisek – zamezení vzniku chybě (četnosti vzniku chyby) a možnosti odhalení chyby skrze různé tzv. brány kvality (kontrolní místa). Na obrázku 3 můžeme vidět chybu – znečistěný výlisek – který je hodnocený žlutou barvou z hlediska zamezení vzniku chybě, tzn. chyba se vyskytuje zřídka. U této chyby je dále hodnocena její možnost odhalení skrze různá kontrolní místa (vstupní kontrola, uvolnění materiálu, uvolnění formy, uvolnění 1.ního kusu, nastavení vstřikovacích parametrů, nastavení robotu, kontrola výlisku měřením, vizuální kontrola dílenská, vizuální kontrola operátorem, kontrola dle kontrolního plánu a 100% finální kontrola). Tato místa jsou

definována pracovníky firmy. Na základě těchto dvou hledisek – zamezení vzniku chybě a možnost odhalení chyby – je vyhodnocena celková rizikovost posuzované chyby (rizika).

	Brány kvality (Q-Tory)											
	Zamezení vzniku chybě	Možnost odhalení chyby										CELKOVÁ RIZIKOVOST
Popis chyby / rizika [hlavní příčina v závorce]		Vstupní kontrola	Uvolnění materiálu	Uvolnění formy	Uvolnění 1. Kusu	Nastavení vstřik.parametrů	Nastvení robotu	Kontrola výlisku měřením	Vizuální kontrola dílenská kontrola	Vizuální kontrola operátorem	Kontrola dle kont. Plánu	100% kontrola	
Znečištěný výlisek (rozjezdový kus znečištěn od konzervace formy)													

Obr. 3 Definice chyb a rizik s příčinou (vlastní zpracování)

Pro stanovení hodnoty hlediska – zamezení vzniku chybě – je využívána v případě metody QAM následující tabulka (Obr. 4), která nám pomáhá stanovit četnost výskytu chyby. V případě, že máme zpracovanou metodu FMEA pro daný proces, můžeme využít hodnoty z této analýzy pro hodnocení výskytu vady, které dle hodnotící tabulky FMEA nabývají hodnoty 1-10.

Barva	Popis	Poznámka	Příklad	FMEA
Zelená	Dostatečné zamezení vzniku chyby	Chyby se nevyskytují	Šroubování s automatickou kontrolou úhlu a dotahovacího momentu	1 - 2
Žlutá	Střední zamezení vzniku chyby	Chyby se vyskytují zřídka	Automatické šroubování bez automatického zastavení linky	3 - 6
Červená	Nestandardizovaný proces	Chyby se vyskytují opakovaně	Ruční šroubování	7 - 10

Obr. 4 Hodnocení četnosti výskytu chyb (Interní školící materiály společnosti Bosch, 2012)

Pro stanovení hodnoty hlediska – možnost odhalení chyby – je využívána v případě metody QAM následující tabulka, která hodnotí zajištění kontroly ve zkoumaném procesu, jak můžeme vidět na obrázku Obr. 5. I u tohoto hlediska lze využít pro hodnocení zajištění kontroly metodu FMEA, která taktéž hodnotí pravděpodobnost odhalení vady.

Barva	Popis	Poznámka	Příklad	FMEA
Zelená	100% kontrola, automatické zastavení linky	Chyba je vždy odhalitelná	Vyřazovací brána s automatickým zastavením linky	1 - 2
Žlutá	Kontrola, použití speciálních přípravků	Chyba nemusí být při nevýhodných podmínkách odhalena	Manuální nebo vizuální zkouška s jednoduchým odhalením chyby	3 - 6
Červená	Není možné provést kontrolu, nepravděpodobné odhalení chyby	Chyba nemůže být odhalena s jistotou	Vizuální zkouška zaměřená na závažné příznaky nebo na více příznaků	7 - 10

Obr 5 Hodnocení odhalení chyby (Interní školící materiály společnosti Bosch, 2012)

Riziková matice QAM hodnotí dvě hlediska pro stanovení rizikovosti v procesu. V následující tabulce na obrázku Obr. 6 můžeme vidět matici pro rozhodování o rizikovosti hodnocené chyby (rizika).

Odhalení chyby / Vyvarování se chybě	Zelená	Žlutá	Červená
Zelená	bezpečná	bezpečná	nutné další vylepšení
Žlutá	bezpečná	nutné další vylepšení	musí být zlepšeno s nejvyšší prioritou
Červená	nutné další vylepšení	musí být zlepšeno s nejvyšší prioritou	musí být zlepšeno s nejvyšší prioritou

Obr. 6 Matice zabezpečení kvality (Interní školící materiály společnosti Bosch, 2012)

Chyby, které mají žluté označení celkové rizikovosti, je třeba ošetřit, červené označení u celkové rizikovosti znamená okamžité zlepšení s nejvyšší prioritou, tzn., musí být řešeno okamžitě. Jiránek (2007) ve svojí práci uvádí místo pojmu celková rizikovost, pojem účinnost kontrolních bodů.

Popis chyby / rizika [hlavní příčina v závorce]	CELKOVÁ RIZIKOVOST	Vylepšení vyvarování se chybám				Efekt vylepšení				Vylepšení odhalení chyby			
		nápravná opatření				Počet reklamovaných dílů: zákazník / interně				nápravná opatření			
		popis (co)	odpovědnost (kdo)	termín (kdy)	Hotovo?	před zavedení opatření		po zavedení opatření		popis (co)	odpovědnost (kdo)	termín (kdy)	Hotovo?
						zákazník	interně	zákazník	interně				
Znečištěný výlisek (rozjezdový kus znečištěn od konzervace formy)		Před uvolněním výroby odstranit všechny rozjezdové kusy	Seřizovač / obsluha	KW 6	A	1	0	0	0				
Záměna kusů ve skladu (Špatný počet ks výlisků v balení - lidský faktor - externí zákazník)						1	0	0	8	Při lepení pásky je použit lis s konkrétní lisovací matrici na tento díl = 100% kontrola	Technolog	KW 40 / 2015	A

Obr. 7 Stanovení nápravných opatření (vlastní zpracování)

Takto vypracovaná QAM matice je vytištěná a umístěná na nástěnce ve výrobě, kde se tým pravidelně schází, nebo v případě externí reklamace řeší daný problém okamžitě. Aktualizaci dokumentu (matice QAM) má v odpovědnosti vedoucí QAM týmu. Cílem QAM matice je její neustálé rozšiřování o nové potenciální chyby a dále řešení hrozících závažných chyb a existujících již vzniklých vad v procesu.

3.3 Zhodnocení použití metody QAM na výkonnost procesu

Daná výrobní společnost má v oblasti zajištění nekvality na pracovišti vstřikování dlouhodobý cíl, udržení ztráty pod 4 %, kde ztráty z najíždění nesmí převýšit 1 % a ztráty z výroby 3 %. V roce 2016 a 2017 společnost eviduje zvyšující se nekvalitu při najíždění nové výroby (přetypování). Příčinou může být také snížení výrobních dávek a navýšení počtu zakázek.

	2013	2014	2015	2016	2017
Ztráty z najíždění	1,00%	0,80%	1,00%	**1,20%**	**1,30%**
Ztráty z výroby	1,80%	1,60%	2,20%	2,50%	2,80%
Ztráty celkem	**2,80%**	**2,40%**	**3,20%**	**3,70%**	**4,10%**

Obr. 8 Nekvalita na pracovišti vstřikování (interní materiály společnosti)

Snížení nekvality bylo sledováno u vytypovaných výrobků po dobu 6 měsíců. Šlo o výrobky, u kterých byly evidovány nejvyšší ztráty z najíždění a zároveň výrobky, u kterých se objevuje nejčetnější typ vady: pohledová vada – nečistoty. Na obrázku Obr. 9 nalezneme vyhodnocení snížení ukazatele nekvality za 6 měsíců u zmíněných výrobků. Vlivem používání metody QAM došlo ke snížení nekvality u sledovaných 3 výrobků o 4,1 %. Nelze jednoznačně tvrdit, že 100% podíl na tomto snížení má pouze používání této metody.

Název položky	Minulé období		Sledované období	
	Vyrobeno	**Zmetky**	**Vyrobeno**	**Zmetky**
Výrobek A	8 694	1716	6 654	234
Výrobek B	2400	180	6 654	1560
Výrobek C	4122	474	3588	150
	15 216	**2 370**	**16 896**	**1 944**
Ukazatel nekvality:	**15,60%**		**11,50%**	
Pokles ukazatele nekvality:	**4,10%**			

Obr. 9 Přepočet snížení ukazatele nekvality (interní materiály společnosti)

ZÁVĚR

Metoda QAM je interaktivní metoda pro řízení vzniklých i potenciálně hrozících rizik. V prvním kroku jsou pomocí nástroje FMEA vydefinovány všechny možné vady, které se mohou v procesu objevit. Metoda QAM stejně jako metoda FMEA využívá rizikovou matici pro hodnocení úrovně rizika neboli zajištění kvality. Metoda FMEA je matice o třech hodnotách, na rozdíl od metody QAM, která hodnotí jednotlivé vady ze dvou hledisek – četnosti výskytu a možnosti odhalení vady.

Důležitým prvkem metody QAM je skutečnost, že nápady na zajištění procesu jsou tlačeny zespodu směrem nahoru, co se týká stupně podřízenosti. Do řešení problémů jsou zapojeni přímo pracovníci, kteří jsou nejblíže výrobě a mohou ovlivnit vznik vad a návrh řešení.

Na základě případové studie bylo po dobu 6. ti měsíců pozorování procesu zjištěno, že díky aktivnímu sledování interní a externí nekvality, řešení příčin vzniku těchto vad a vyhodnocování dalších potenciálních hrozeb došlo ke snížení ukazatele ztráty z nekvality. Na základě zajištění kvality došlo k mírnému zvýšení množství produkce, které mělo pozitivní vliv na ukazatel produktivity

Literatura

[1] ANTUŠÁK, Emil. Krizová připravenost firmy. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2013, s. ISBN 978-80-7357-983-8.

[2] AVEN, T. Selective critique of risk assessments with recommendations for improving methodology and practise, Reliability Engineering & System Safety [online], Volume 96, Issue 5, May 2011, 2011, Pages 509-514, ISSN 0951-8320, [cit. 2018-03-15]. Dostupné z: http://dx.doi.org/10.1016/j.ress.2010.12.021. (http://www.sciencedirect.com/science/article/pii/S0951832010002772)

[3] ČSN EN 31010:2011 Management rizik – Techniky posuzování rizik. 2011. Praha: Český normalizační institut. Třídící znak: 010352.

[4] FONSECA, L., Domingues, J.P. ISO 9001:2015 Edition- Management, Quality and Value. International Journal for Quality Research, 2016, pp. 149-158. DOI – 10.18421/IJQR11.01-09

[5] GOERLANDT, F., Genserik, R. On the assessment of uncertainty in risk diagrams, Safety Science [online], Volume 84, 2016, Pages 67-77, ISSN 0925-7535, [cit. 2016-06-18]. Dostupné z:http://dx.doi.org/10.1016/j.ssci.2015.12.001. (http://www.sciencedirect.com/science/article/pii/S0925753515003215)

[6] HERRINGTON, How Mature is Your Risk Management? [online]. In: Harward Business Review. June 29, 2012 [vid. 2016-06-18]. Dostupné z: https://hbr.org/2012/06/how-mature-is-your-risk-manage

[7] HRBACKOVA, Lucie. Risk-based thinking in the Production Process Using the Methods of Quality Assurance Matrix and the FMEA Process. Journal of Systems Integration, 2016, roč. 2016, 7, č. 1, s. 1-28. ISSN 1804-2724.

[8] Interní školící materiály firmy Bosch, 2012

[9] Interní školící materiály vybrané společnosti

[10] ISO - INTERNATIONAL ORGANIZATION OF STANDARDIZATION. News. ISO 9001:2015 – Just published! [online]. Geneva: ISO, 2015 [vid. 2016-01-07]. Dostupné z: http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref2002

[11] ISO - INTERNATIONAL ORGANIZATION OF STANDARDIZATION. Popular Standards. ISO 31000 – Risk management. [online]. Geneva: ISO, 2018 [cit. 2018-08-15]. Dostupné z: https://www.iso.org/iso-31000-risk-management.html

[12] ISO /FDIS 9001:2015 Quality management system – Requirements. 2015. [pdf] Available at: <www.iso.org/tc176/sc02/public> [Accessed 9 September 2015].

[13] JIRÁNEK, Lukáš. Analýza zabezpečení kvality výrobního procesu metoda FMEA a QAM. Zlín, 2007. Bakalářská práce. Fakulta technologická. Ústav výrobního inženýrství.

[14] LINDGVIST, R., MATTSSON, L., JOSEFSSON, N., SALMELA, J. Implementation of the Quality Assurance Matrix and Methodology. [online]. QualityDigest, 2018 [cit. 2018-08-07] Dostupné z: https://www.qualitydigest.com/inside/twitter-ed/implementation-quality-assurance-matrix-and-methodology.html#

[15] NEISES, Armin, 2015. QAM: Qualitäts-Absicherungs-Matrix [online]. TQM.com. [cit. 2016-01-15]. Dostupné z: http://www.tqm.com/beratung/qam-firewall/qam

[16] KOHLBACHER, Markus a Stefan GRUENWALD, 2011. Process ownership, process performance measurement and firm performance. International Journal of Productivity and Performance Management, 2011, vol. 60, no. 7, pp. 709-720. ISSN 1741-0401. MAPI and Deloitte, Understanding risk assessment practices at manufacturing companies. Copyright © 2015 Manufacturers Alliance for Productivity and Innovation, Copyright © 2015 Deloitte Development LLC. All rights reserved. [cit. 2018-04-15]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-mfg-mapi-risk-assessment-paper-single-page-040715.pdf

[17] METRICSTREAM. The Power of Key Risk indicators (KRIs) in Enterprise Risk Management (ERM), © 2018 MetricStream Inc. All Rights Reserved. [cit. 2018-04-20]. Dostupné z: https://www.metricstream.com/insights/Key-Risk-indicators-ERM.htm

[18] SITNICOV, C., BOCEAN, C.G. and BERCEANU, D. Risk Management Model from the Perspective of the Implementing ISO 9001:2015 Standard Within Financial Services Companies. Amfiteatru Economic, 19(Special no. 11), 2017, pp. 1017-1034.

[19] ŠEFČÍK, Vladimír. Analýza rizik. 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 98 s. ISBN 978-80-7318-696-8

[20] ŠEFČÍK, Vladimír, TOMEK, M. a HRUŠKA, M. Krizové řízení v malých a středních podnicích. 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 181 s. ISBN 978-80-7318-867-2BEŇO, J., MAŇKOVÁ I. *Technológické a materiálové činitele obrábania*, Košice: VIENALA, 2004. ISBN 80-7099-701-X

VYBRANÁ RIZIKA SNIŽUJÍCÍ VÝKONNOST ŽELEZNIČNÍ DOPRAVNÍ INFRASTRUKTURY

SELECTED RISKS TO RAIL INFRASTRUCTURE PERFORMANCE

Ing. Peter Hrmel
phrmel@seznam.cz

ABSTRAKT

Železniční doprava představuje významnou dopravní infrastrukturu, jejímiž základními aspekty jsou bezpečnost a plynulost. Rizika spojená s provozováním dráhy a drážní dopravy mohou výrazně ovlivnit chod drážní infrastruktury s následným negativním vlivem na obyvatelstvo, výrobní i nevýrobní sféru a ostatní odvětví české společnosti. Článek rozebírá některá rizika dopravního provozu, která mohou způsobit snížení výkonnosti nebo úplné zastavení železniční dopravy. Následné dopady rizik do železničního provozu mohou fungování infrastruktury ovlivnit v závislosti na přijatých opatřeních uvnitř podniku provozovatele dráhy nebo drážní dopravy nebo ve spolupráci se složkami integrovaného záchranného systému a orgánů státního dozoru. Příspěvek zároveň poukazuje na různou výši dopadů při různé závažnosti příčin vzniku provozní mimořádnosti nebo mimořádné události v drážní dopravě.

KLÍČOVÁ SLOVA

Železniční doprava, drážní infrastruktura, riziko, plynulost dopravy,

ABSTRACT

Rail transport is an important transport infrastructure, the basic aspects of which are safety and fluidity. The risks associated with the operation of railways and rail transport can significantly affect the operation of the railway infrastructure, with a consequent negative impact on the population, production and non-production spheres and other branches of the Czech society. The article discusses some of the traffic risks that may cause a reduction in performance or a complete stop to rail transport. The consequent impacts of the risks to the railway operation may influence the functioning of the infrastructure depending on the measures taken within the operator of the railways or the rail transport or in cooperation with the components of the integrated rescue system and the state supervision authorities. At the same time, the contribution points to the different levels of impact of the various causes of the occurrence of operational emergency or extraordinary events in rail transport.

KEY WORDS

Rail transport, rail infrastructure, risk, traffic fluency,

ÚVOD

Železniční doprava v České republice (ČR) představuje významné dopravní odvětví, které zejména v historických souvislostech bylo klíčovým pro zabezpečení dopravní obslužnosti většiny průmyslových aglomerací české kotliny. V dobách plánovitého řízení hospodářství byl kladen velký důraz na maximální vytěžení výhod tohoto dopravního systému. Výstavba průmyslových center byla plánována s ohledem na možnost vzájemného propojení

a ve stejném duchu byla železniční doprava přiváděna do významných nově budovaných sídlišť a městských obvodů. Tato kritéria, někdy ignorující skutečnou ekonomickou realitu, stála u zrodu jedné z nejhustších železničních sítí na světě. Dnes hovoříme o dopravní infrastruktuře, jejíž úroveň výkonu je z vnějšího pohledu zákonitě nejvíce spojována s včasností a kvalitou uskutečněné osobní nebo nákladní přepravy. K uspokojování těchto potřeb je jednotlivými subjekty, které na dopravní infrastruktuře fungují, vydáván jízdní řád, tzv. grafikon vlakové dopravy (GVD), jehož plnění je hlavním ukazatelem spokojenosti zákazníků nebo odběratelů produktů procesu drážní dopravy. [1]

Ekonomické aspekty budování a provozu drážní infrastruktury, stavebně technické požadavky na zřízení a provozování dráhy, personální potřeba zabezpečení dopravního provozu a provozuschopnosti železnic stavějí drážní dopravu v konkurenci s eskalující dopravou silniční do nevýhodnějšího postavení. Tyto okolnosti se v historických souvislostech na úrovni drah projevovaly po celém světě dvojím způsobem. V zemích uplatňujících tržní principy hospodaření docházelo v rámci tvrdého konkurenčního boje k útlumu drah, zatímco ve státech s plánovitým řízením byly dráhy preferovány a k jejich liniím byly projektovány řady průmyslových podniků a účelových staveb. Tato přednost byla mnohdy „vyvažována“ nižší investiční činností v této oblasti, kdy zaostávala modernizace i běžná údržba.

1. PODMÍNKY BEZPEČNÉHO FUNGOVÁNÍ DRÁŽNÍ INFRASTRUKTURY

Bezpečnost železniční dopravy je jedním ze základních požadavků na provozování dráhy a drážní dopravy. Za tím účelem je prostředí železniční dopravy zasazeno do stávajícího legislativního rámce, který je stále se vyvíjejícím produktem státní správy, zabezpečujícím v současné době především bezpečné provozování dráhy a drážní dopravy, liberalizaci dopravního trhu, podmínky k přístupu na dopravní cestu a v neposlední řadě práva a povinnosti zúčastněných stran.

1.1 Legislativní východiska železniční dopravy

Hlavními legislativními východisky odvětví železniční dopravy jsou zejména:

- Zákon 266/1994 Sb., o dráhách ve znění pozdějších předpisů,
- Přípojek C Vyhlášky č. 8/1985 Sb., o Úmluvě o mezinárodní železniční přepravě (COTIF) ve znění pozdějších předpisů - Řád pro mezinárodní železniční přepravu nebezpečných věcí (RID),
- Nařízení vlády č. 1/2000 Sb., o přepravním řádu pro veřejnou drážní nákladní dopravu, ve znění pozdějších předpisů.
- Vyhláška č. 376/2006 Sb., o systému bezpečnosti provozování dráhy a drážní dopravy a postupech při vzniku mimořádných událostí na dráhách.
- Vyhláška Ministerstva dopravy č. 100/1995 Sb., kterou se stanoví podmínky pro provoz, konstrukci a výrobu určených technických zařízení a jejich konkretizace (Řád určených technických zařízení),
- Vyhláška Ministerstva dopravy č. 101/1995 Sb., kterou se vydává Řád pro zdravotní způsobilost osob při provozování dráhy a drážní dopravy, ve znění pozdějších předpisů,
- vyhláška MD ČR č. 173/1995 Sb. kterou se vydává dopravní řád drah,

- vyhláška MD ČR č. 177/1995 Sb. kterou se vydává stavební a technický řád drah,
- Nařízení vlády č. 208/2011 Sb., o technických požadavcích na přepravitelná tlaková zařízení,
- Zákon 77/2002 Sb., o akciové společnosti České dráhy, státní organizaci Správa železniční dopravní cesty a o změně zákona 266/1994 Sb. o drahách ve znění pozdějších předpisů.

Uvedený výčet představuje páteřní systém legislativy, vztažné k problematice železniční dopravy. Pro provozování dráhy a organizaci dopravního provozu jsou vydávány navazující resortní předpisy, které jsou v souladu s platnou národní i evropskou legislativou.

2. VÝKONNOST ŽELEZNIČNÍ DOPRAVNÍ INFRASTRUKTURY

Výkonnost dopravní infrastruktury je závislá na celé řadě ukazatelů. Jednou z hlavních veličin v této souvislosti je propustná výkonnost (propustnost) určitého dopravního bodu nebo úseku, která udává počet možných dopravních úkonů, např. jízd vlaků, za stanovenou dobu. Pro ilustraci propustné výkonnosti lze uvést vzorec [2] pro výpočet maximální nebo teoretické propustnosti:

$$N = \frac{T}{t_{obs}} \tag{1}$$

kde: N_{max} - výsledná propustnost v počtu úkonů za zvolené období

T - délka zvoleného období (např. 1440 minut, 60 – 240 minut apod.) [min],

t_{obs} - doba obsazení posuzovaného úseku technologickým úkonem (vlak, posun) [min],

Propustnost je dále ovlivňována celou řadou parametrů posuzovaného úseku. Jejich zohledněním lze docílit reálnějšího pohledu na výkonnost dopravní infrastruktury. Pro tyto případy se provádí výpočet tzv. praktické nebo technické propustnosti [2] dle následujícího vzorce:

$$n = \frac{T-(T_{výl}+ T_{stál})}{t_{obs}+ t_{dod}+ t_{ruš}} \tag{2}$$

kde: n – praktická propustnost technologických operací, [t. o.]

T – délka zvoleného období např. 1440 minut, 60, 120, 240 minut apod. [min],

$T_{výl}$ – doba výluk [min],

$T_{stál}$ – doba stálých operací [min],

t_{obs} - doba obsazení úseku technologickým úkonem (vlak, posun), [min],

t_{dod} – průměrná doba zálohy na jeden vlak [min],

$t_{ruš}$ – doba rušení [min],

Výkonost drážní dopravy je pak zohledněním vypočtených propustností jednotlivých úseků nebo kolizních bodů drážní infrastruktury v kontextu platného grafikonu vlakové dopravy a množství vyčerpané kapacity dráhy provozovateli drážní dopravy. Propustnost dopravní infrastruktury je zjišťována pro následující prvky dráhy:

- Traťové koleje,

- Mezistaniční úseky,
- Dopravní koleje stanic,
- Staniční zhlaví,
- Seřaďovací zařízení

Výpočet výsledné propustnosti je předmětem dalších složitých postupů různými metodami. Použít lze analytické metody, grafické metody, případně simulační modelování. K tvorbě nákresných jízdních řádů jsou nově vyvinuty provozní aplikace informačních technologií. [2]

2.1 Bezpečnost železniční dopravy

Základní podmínkou pro fungování jakéhokoli druhu dopravy je zajištění maximální bezpečnosti osob, majetku a životního prostředí v souvislosti s existencí dopravního procesu. V historickém kontextu docházelo v rámci legislativního vývoje k postupné implementaci bezpečnostních opatření do oblasti zákonů, právních a technických norem, předpisů a resortních opatření. V současné době lze konstatovat, že obor železniční dopravy je při dodržování všech předpisů z hlediska bezpečnosti na vysoké úrovni. Při srovnávání rizik újmy na zdraví nebo usmrcení lze jednoznačně konstatovat nižší dopady na osoby v pozici uživatele drážní dopravy ve srovnání s uživateli pozemní komunikace. Je to dáno robustnější konstrukcí drážních vozidel ve srovnání se silničními motorovými vozidly. Obzvláště při vzájemných kolizích na úrovňovém křížení dráhy s pozemní komunikací dochází k častějšímu zranění nebo úmrtí osob v silničních vozidlech. Vyšší bezpečnost je rovněž dílem skutečnosti, kdy strojvedoucí hnacího drážního vozidla určuje „pouze“ rychlost vlaku, intenzitu brzdění a směr jízdy vpřed a vzad, zatímco postavení výhybek a zabezpečení jízdních cest se děje z pozice základního nebo dálkového řízení dopravního provozu. O vjezdové koleji ve stanici rozhoduje výpravčí nebo traťový dispečer, zatímco strojvedoucí upravuje rychlost drážních vozidel, aby byl schopen zastavit na určeném místě a přitom dodržet stanovený GVD. Přes všechny tyto atributy železniční dopravy je stávající trend vývoje bezpečnosti dráhy a nehodovosti považován za neuspokojivý.

2.2 Plynulost drážní dopravy

Vypočtená propustnost prvku je jen dílčí podmínkou zajištění plynulosti drážní dopravy. V České republice je provozování dráhy svěřeno legislativně státní organizaci Správa železniční dopravní cesty (SŽDC). Tato funkce, mimo jiné, zahrnuje organizaci drážní dopravy a zajištění provozuschopnosti dráhy. [3] Dalším článkem, ovlivňujícím plynulost provozování drážní dopravy jednotlivými provozovateli, dopravci. Nastavení legislativního prostředí při přístupu na dopravní cestu má rovněž za cíl zajištění nejen bezpečnosti drážní dopravy, ale i pravidel, umožňující řízení dopravního provozu. Dopravci si zakupují trasy vlaků v ročním jízdním řádu nebo žádají o příděl kapacity dráhy na menší období dle svých potřeb. Požadavky na příděl kapacity dráhy lze uplatnit i v online režimu pro jednotlivé vlaky tzv. „ad hoc“. Každá trasa vlaku má své číslo vlaku a druh vlaku, který je rozhodující pro určení pořadí důležitosti vlaků a usnadňuje rozhodovací procesy pracovníků základního, dálkového i operativního řízení provozu.

Plynulým provozem lze nazvat stav, kdy vlaky v posuzovaném úseku jezdí oběma směry v souladu s platným GVD a požadavky dopravců, nedochází k nadměrnému hromadění zátěže vlivem přetížení kapacity dráhy na daném traťovém úseku nebo v železniční dopravně.

Za plynulý provoz lze považovat stavy, kdy dochází k čekání vlaků k upřednostnění jízdy vlaků vyšší důležitosti v kolizních bodech.

3. RIZIKA NARUŠENÍ FUNKČNOSTI DOPRAVNÍ INFRASTRUKTURY

Funkční dopravní infrastruktura je schopná zabezpečit provoz plynulé drážní dopravy. To znamená stav, kdy zavedené vlaky s přidělenou kapacitou dopravní cesty jsou v posuzovaném úseku dopravovány plynule s minimálními, provozně odůvodněnými vlivy na plnění GVD. Vlaky jedou podle schváleného pořadí důležitosti a v případě hromadění zátěže je pořadí vlaků v kolizních bodech řízen z úrovně operativního řízení provozu. Dispečeři operativního řízení mají kompetenci rozhodovat o pořadí důležitosti vlaků ve sporných případech za provozních mimořádností. [4] O vzniku mimořádností v provozu informují dispečeři operativního řízení všechny dotčené dopravce, kteří mohou přijmout opatření k efektivnějšímu provozování drážní dopravy (odklony vlaků, mimořádné obraty souprav, náhradní autobusová doprava, odřeknutí vlaků a podobně).

3.1 Omezení provozu

Plynulost železničního provozu je omezována z mnoha příčin. Omezení provozu lze definovat jako stav znemožňující realizovat zcela plynulý dopravní provoz, zohledňující platný GVD a přidělenou kapacitu dráhy. Provoz vlaků je zachován za podmínek snížené kapacity dráhy vlivem omezujícího faktoru, ale není na žádném úseku zcela přerušen. Omezujícím faktorem může být:

- snížená provozuschopnost dráhy,
- závada na straně dopravce,
- překážka v dopravní cestě dráhy.

Uvedené členění zdrojů rizik je zaměřeno na původ dopravního omezení, dle vlastníka rizika. Provozovatel dráhy je odpovědný za organizaci dopravního provozu a zajištění provozuschopnosti dráhy, tedy technického stavu dráhy, umožňující bezpečné a plynulé provozování drážní dopravy. Provozovatel drážní dopravy musí mimo jiné zajistit, aby jízdou vlaku nevzniklo ohrožení drážní dopravy, omezení nebo zastavení dopravního provozu. Ani třetím osobám není dovoleno svévolně poškozovat zařízení dopravní infrastruktury nebo ohrožovat provozovanou drážní dopravu a tím působit omezení nebo zastavení provozu.

Skutečnost je ovšem taková, že jsou denně zaznamenány desítky případů provozních mimořádností na všech stranách s negativním dopadem do dopravního provozu.

3.1.1 Rizika na straně provozovatele dráhy

Na straně provozovatele dráhy vznikají zejména tyto případy:

- poruchy trakčního vedení nebo jeho poškození,
- závady v napájení trakční proudové soustavy,
- závady na železničním svršku vzhledem k celistvosti kolejí,
- závady v geometrické poloze koleje,
- mechanické závady výhybek, kolejových křižovatek a výkolejek,

- poruchy staničních zabezpečovacího zařízení,
- poruchy traťových zabezpečovacích zařízení,
- poruchy přejezdových zabezpečovacích zařízení,
- poruchy sdělovacích systémů,
- mimořádné události v důsledku závad zařízení nebo pracovníků provozovatele dráhy.

3.1.2 Rizika na straně provozovatele drážní dopravy

Z důvodu na straně provozovatele drážní dopravy dochází k vlivu na dopravní provoz zejména v těchto případech:

- závady hnacích a tažených drážních vozidel,
- ložné závady nákladních vlaků,
- závady způsobené zákazníky,
- kompenzace předchozího zpoždění vlaků,
- nedodržení podmínek přístupu na dopravní cestu,
- Mimořádné události vlivem provozovatele drážní dopravy

3.1.3 Rizika vlivem třetích stran

Provozování dráhy a drážní dopravy může být negativně ovlivněno riziky vnějšího prostředí nebo třetích stran. K těmto rizikům lze zahrnou všechny případy, které v případě šetření nebudou přisouzeny do množiny rizik provozovatele dráhy nebo některého provozovatele drážní dopravy. Jedná se zejména o:

- povětrnostní vlivy[1],
- překážky v dopravní cestě dráhy,
- požadavky na součinnost se složkami IZS,
- mimořádné události vlivem třetích stran a vnějšího prostředí.

3.2 Zastavení provozu

Příčiny zastavení provozu na železniční infrastruktuře mohou být shodné s příčinami omezení provozu. Rozdíl je pouze v dopadech, kdy zastavení provozu lze definovat jako úplné zastavení pohybu drážních vozidel na určitém úseku nebo v kolizním bodě. Stav zastavení provozu často postupně přechází do stavu omezení provozu, kdy po vykonání určitých činností, záchranných a likvidačních prací nebo šetření MU, dochází k částečnému obnovení provozu s omezením. Při vzniku mimořádných událostí, například vykolejení drážního vozidla na dvojkolejné nebo vícekolejné trati, může být postupně obnoven provoz po jedné z traťových kolejích sníženou rychlostí do úplného odstranění následků MU. Zastavení provozu z kterékoli z příčin oznamuje provozovatel dráhy všem dotčeným dopravcům

[1] Výpravčí jedná v souladu s články 4098 - 4118 předpisu SŽDC D1 Dopravní a návěstní předpis [4]

a zavádí formou informace do provozních aplikací informačních systémů pro organizaci dopravního provozu.

4. VYBRANÉ VLIVY NA VÝKONNOST DOPRAVNÍ INFRASTRUKTURY

Příčiny snížené výkonnosti dopravní infrastruktury lze hledat ve všech výše uvedených oblastech. Neplatí žádná úměra mezi závažností následků daného stavu a následných dopadů na plynulost provozu. Některé případy MU lze efektivně řešit bez potřeby zastavení nebo omezení provozu a naopak některé jednoduché stavy vyžadují velká provozní omezení.

4.1 Výluková činnost

Mezi nejznámější a mediálně značně frekventovanou problematiku lze zařadit potřeby výstavby, oprav a rekonstrukcí dopravních staveb, zařízení nebo potřeby těchto prací v bezprostředním okolí dráhy. Za tím účelem jsou prováděny plánované výluky dopravního provozu s následkem omezení nebo úplného zastavení provozu. V těchto případech je dopravní provoz veden dle opatření zúčastněných stran. Dle závažnosti omezení provozu jsou vydávány výlukové jízdní řady, dopravci vedou vlaky po odklonových trasách, osobní doprava může být nahrazena autobusy. V případě plánovaných výluk je součástí opatření i informovanost veřejnosti a dopravců o omezujících aspektech a předpokládaných dopadech výlukové činnosti. Zejména v posledních letech dochází vlivem velkých investic do sektoru dopravní infrastruktury k velkému nárůstu počtu konaných výluk. Dopady výlukových činností mají mnohdy domino efekt, kdy narušení GVD z jedné výlukové akce negativně ovlivňuje nejen výkonnost dopravní infrastruktury, ale i průběh výlukových akcí a plnění GVD ve svém okolí. Velký počet investic do dopravní infrastruktury je potřebný, ovšem jejich stávající množství naráží na schopnost zhotovitelů staveb, tyto efektivně pokrýt personálem a následně včas dokončit. Zlepšení tohoto stavu je v kompetenci Ministerstva dopravy ČR, které upravuje toky investic a definuje priority dopravního sektoru.

Neplánované výluky se konají zpravidla v souvislosti s jinými závadami nebo mimořádnými událostmi v železniční dopravě a jejich dopady na drážní infrastrukturu lze chápat jako dopady těchto příčin.

4.2 Součinnost s IZS

Dopravní infrastruktura je svým síťovým charakterem a značným územním rozsahem vysoce zranitelná. Omezení výkonnosti dráhy může v tomto pohledu být snadno způsobeno s úmyslem poškodit chráněné zájmy nebo jako důsledek potřeby chráněné zájmy zabezpečit. K omezení nebo zastavení provozu dochází na základě oznámení o vzniku MU v drážní dopravě na ohlašovacím pracovišti provozovatele dráhy zpravidla v závislosti na charakteru a rozsahu MU.

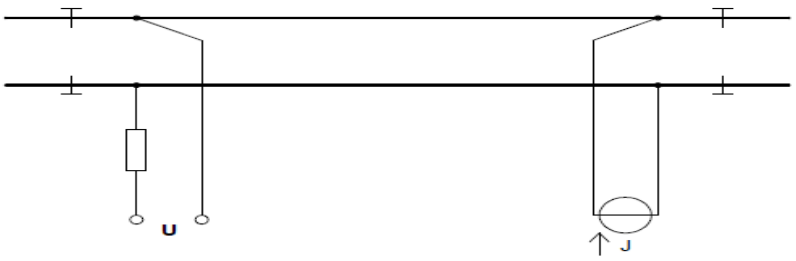
Při vzniku potřeby zásahu složek IZS v bezprostřední blízkosti dráhy nebo při předpokladu potřeby takového zásahu dochází k omezení nebo zastavení provozu na základě požadavku pracovníka IZS. Tyto požadavky bývají zpravidla, z důvodů přijetí různě srozumitelného primárního oznámení, velmi obecné a mohou být značně nadlimitní. V tomto stavu je navíc skryto další riziko, vyplývající z možnosti omylu při definování požadavku na rozsah požadovaného opatření. Nezřídka dochází k záměně v místopisném označení v obci obvyklém s označením stanic a zastávek na drážní infrastruktuře, která může mít fatální následky. Eliminace možných omylů není jednoduchá záležitost. Pro snadnější dorozumění a zároveň

pro možnost opravy nepřesných informací je potřeba komunikovat oboustranně. Znamená to omezení volání ze skrytých čísel na minimum, případně doplnit požadavek složek IZS o kontakt na oznamovatele požadavku. Jakákoli nepřesnost nebo omyl při zastavování provozu může vyústit v domino efekt následků na jiném traťovém úseku s mnohem většími dopady na funkčnost drážní infrastruktury a především na chráněné zájmy.

4.3 Pochybnost o sjízdnosti koleje

Pro indikaci volného úseku koleje jsou některá traťová a staniční zabezpečovací zařízení vybavena kolejovými obvody. Jedná se o elektrický obvod s funkcí vyhodnocení volnosti nebo obsazení dotčeného úseku koleje, (Obr. 1). Kolejové obvody na sebe bezprostředně navazují, čímž je zajištěna kontrola všech takto vybavených kolejí, včetně výhybek a kolejových křižovatek. Obsazení kolejového obvodu je indikováno obsluhujícímu zaměstnanci v případě fyzického obsazení koleje drážními vozidly, tj. Spojení obou kolejnicových pásů elektricky vodivým drážním dvojkolím nebo jiným vodivým předmětem. Současně dochází ke shodné indikaci při přerušení celistvosti nebo vodivého propojení některého z kolejnicových pásů. Z tohoto důvodu má kolejový obvod další funkci, indikaci celistvosti koleje. V případě indikace obsazení kolejového obvodu v situaci, že obsluhující zaměstnanec má nepochybně zjištěno, že v dotčeném kolejovém úseku se nenachází drážní vozidlo, se má za to, že nastává pochybnost o neporušení kolejnice daného úseku a sjízdnost koleje musí být spolehlivě zjištěna a prokázána. [5] Tato funkce, v duchu platné legislativy, přísluší jen odborně způsobilému zaměstnanci provozovatele dráhy na úseku zajištění provozuschopnosti, případně může být volnost a sjízdnost dotčeného úseku koleje zjištěna a potvrzena kontrolní jízdou samostatného hnacího drážního vozidla, zpraveného rozkazem o skutečnosti, že se jízda uskutečňuje za tímto účelem a dle podmínek stanovených vnitřními předpisy[2].

Do doby spolehlivého zjištění sjízdnosti kolejového úseku je provoz drážních vozidel zakázán a podle místa výskytu kolejového obvodu to znamená omezení nebo zastavení provozu. V případě zastavení provozu může být vliv na obnovení provozu navýšen o dojezdovou vzdálenost pohotovostního odborně způsobilého zaměstnance provozovatele dráhy, pokud je v mimopracovní době v režimu domácí pohotovosti.



Obr. 1 Schéma paralelního kolejového obvodu [6]

4.4 Indikace obsazení kolejového obvodu za výlukové činnosti

Z výše uvedeného vyplývá značné omezení provozu za existence výlukové činnosti. V případě konání nepřetržitých vícedenních výluk jedné z traťových kolejí na dvojkolejné trati dochází v okamžiku obsazení kolejového obvodu na jediné pojížděné koleji

[2] Obsluhující zaměstnanec jedná v souladu s článkem 4130 předpisu SŽDC D1 Dopravní a návěstní předpis [4]

k automatickému zastavení provozu a potřebě prohlédnutí inkriminovaného kolejového úseku odborně způsobilým zaměstnancem provozovatele dráhy nebo zjištění sjízdnosti dle článku 4130 předpisu SŽDC D1 Dopravní a návěstní předpis [5].

Při uvedené kombinaci rizik omezení nebo zastavení provozu drážní infrastruktury by zejména na vícekolejných, koridorových tratích s vyšší intenzitou dopravního provozu měla být součástí plánování výlukových akcí provedení posouzení rizik. Současně by měla být přijata opatření k zajištění lepší dostupnosti odborně způsobilých zaměstnanců spravující inkriminované úseky dotčené zvýšeným rizikem, případně jejich posílení a obnovení pohotovosti na pracovištích.

ZÁVĚR

Funkčnost dopravní infrastruktury je základním předpokladem jejího plného využívání. Jakékoli vlivy, které mají za následek omezení nebo zastavení drážní dopravy je potřeba co nejrychleji eliminovat nebo jim účinně předcházet. Absence posuzování rizik v této oblasti může vést k potlačení základního principu existence dopravní infrastruktury a následnému negativnímu vlivu na značnou část obyvatelstva nebo průmyslových podniků s dopady významně přesahujícími některé současně sledované úspory.

Součástí posuzování rizik by do budoucna mělo být posouzení schopnosti zhotovitelů stavebních a výlukových prací provést veškeré práce, vyžadující omezení provozu, v potřebném termínu a při nepřetržitých výlukách definovat přiměřený nárůst personálních stavů odborně způsobilých pracovníků provozovatele dráhy na úroveň potřebnou k minimalizaci dojezdových časů a dob nezbytného provozního omezení nebo zastavení provozu drážní infrastruktury.

Literatura

[1] VONKA J., MOLKOVÁ T., ŠIROKY J.: *Technologie a řízení dopravy II: GVD*. Vyd. 1. Pardubice: Univerzita Pardubice, 2000. 122 s. ISBN 80-7194-286-3

[2] MOLKOVÁ, T. a kol.: *Kapacita železničnich trati.* Pardubice: Univerzita Pardubice, 2010, ISBN 978-80-7395-317-1

[3] SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY. *O nás, Vznik SŽDC,* [online], C 2018, [cit.2018-08-10], Dostupné z WWW:< https://www.szdc.cz/o-nas/vznik-szdc.html>

[4] PROCHÁZKA, J., KERTIS, T., PROCHÁZKOVÁ, D., [online], *Zdroje rizik pro dopravu na železnici v ČR,* [cit.2018-8-15], SBORNÍK PŘÍSPĚVKŮ, JUFOS 2017, ISBN: 978-80-214-5486-6,

[5] SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY. *SŽDC D1 Dopravní a návěstní předpis (2013),*[online]. C 2013-2015, poslední aktualizace 30. 03. 2017 [cit. 2018-08-10].Dostupné z WWW: <http://provoz.szdc.cz/portal/ViewArticle.aspx?oid=869998>

[6] DORAZIL, P., *Základní vlastnosti kolejových obvodů bez izolovaných styků,* Bakalářská práce, [online], UPCE 2008, [cit. 2018-04-20] dostupné z WWW:<http://dk.upce.cz/bitstream/handle/ 10195/28903/text.pdf?Sequence=1>

SYSTÉMOVÉ VYMEZENÍ MODELU KYBERPROSTORU EKONOMICKÉ BEZPEČNOSTI

SYSTEMIC DEFINITION OF THE ECONOMIC SAFETY MODEL

Mgr. František Hřebík, Ph.D. [1], Ing. et Ing. Jiří Konečný, Ph.D. [2,3], prof. Ing. Jiří Dvořák, DrSc. [2,4], Ing. Martina Janková, BA (Hons), Ph.D. [5]

[1]Policejní akademie České republiky v Praze
Lhotecká 559/7, Praha 4
hrebik@polac.cz

[2]Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení
Studentské nám. 1532, Uherské Hradiště
[3]konecny@flkr.utb.cz; [4]jdvorak@flkr.utb.cz

[5]martina.jankova@email.cz

ABSTRAKT:

Cílem článku je seznámit odbornou veřejnost s možnostmi současného reálného prostředí ekonomické bezpečnostia systémově je vymezit tak, aby byl postupně vytvářen vhodný systémově vymezený model této ekonomické bezpečnosti. V tomto procesu jenezbytné vhodně systémově vymezit sociálně ekonomické prostředí pro funkce ekonomické kybernetiky a z tohoto pohledu také vyjádřit kybernetický prostor pro řízení ekonomických procesů moderní technologické a znalostní společnosti. V budoucnutento systémový model ekonomické bezpečnosti může být součástí modelování na prostředcích aplikované kybernetické a informační bezpečnosti a pro vědeckou práci pracovišť být přínosem pro projektování inteligentního kyberprostoru ekonomické bezpečnosti.

KLÍČOVÁ SLOVA:

kybernetický prostor, ekonomická bezpečnost, kybernetická bezpečnost, model bezpečnosti

ABSTRACT:

The aim of the article is to familiarize the public with the possibilities of the current real environment of economic security and to define them systemically so that a suitable systemic model of this economic security is gradually created. In this process, it is also necessary to systematically define the socio-economic environment for the functions of economic cybernetics and, from this point of view, also to express the cybernetic space for managing the economic processes of the modern technological and knowledge society. In the future, this systemic model of economic security maybe part of the modeling of cybernetic and informatik security tools and work place scientific work can be beneficial to designing inteligent cyberspace for economic security.

KEYWORDS:

cyberspace, economicsecurity, cybersecurity, security model

ÚVOD

Ve společenské praxi se setkáváme s procesy a jevy, které jsou objekty. Studium velkého počtu objektů v různých oblastech lidského poznávání světa ukázalo, že řadu postupů, které se osvědčují při studiu určitých objektů v jedné oblasti poznání, je možné dobře použít i při

studiu v jiné oblasti. Dále se také prokázalo, že existují četné analogie ve vztazích mezi částmi objektů a jejich celkem, i když jde o objekty zcela rozdílné povahy, např. fyzikální, technické, sociální, ekonomické nebo i objekty matematické.

Toto poznání vedlo ke snahám zobecnit charakteristiky vztahů mezi částmi objektů, objekty, jejich chováním apod.. To vyžadovalo vytvořit pojmový aparát, který by usnadňoval zobecnění poznatků získaných takovým studiem. L. von Bartalanffy ve známem článku „*General SystemTheory*“ určil důvody nového směru při **systémovém vymezení reálného prostředí** [2,3]**:**

- existuje obecná tendence ke sjednocování různých přírodních a společenských věd,
- takové sjednocení může být předmětem studia obecné teorie systémů,
- tato teorie se může stát významným prostředkem formování exaktních teorií o živé přírodě a o společnosti,
- rozvíjením sjednocujících principů, s nimiž se setkáváme ve všech oblastech vědění, nás obecná teorie přibližuje k dosažení cíle tohoto příspěvku –modelu **ekonomické bezpečnosti** ve specifickém prostředí.

1. SYSTÉMOVÉ VYMEZENÍ PROSTŘEDÍ

Obecná teorie systémů má velký vliv na rozvoj poznání. Představuje mohutný teoretický a metodologický nástroj pro poznávání struktur a závislostí mezi různými prvky složitých jevů a procesů, s nimiž se setkáváme ve společenské praxi. Terminologie vypracovaná v jejím rámci umožňuje používat téhož jazyka k popisu zcela různých objektů. [1,5]

V literatuřeje o teorii systémů v současné době podrobně popsána široká škála obecných modelů, matematických metod, metodických postupů a principů, které usnadňují analýzu systémů (rozpoznávání, identifikaci systémů apod.)**, tvorbu modelů a modelování systémů**, syntézu (kompozici, integraci) systémů v novém pojetí řízení a sdělování informacív tak zvaném**kybernetickém prostoru.** [8,10]

Systémy jsou tedy abstrakce, které si lidé vytváří v procesu poznání. Užíváme je při identifikaci reálného prostředí (analýze) jako nástroj poznání reálných objektů. Jsou to v podstatě logické a matematické konstrukce, které slouží v poznávacím procesu pro zobrazování systémových vlastností a souvislostí objektů a jevů vnějšího světa například **v ekonomické oblasti – konkrétně např. v ekonomické bezpečnosti**.

Pojem systém odráží a systémově vymezuje nejen podstatné systémové jevy reálného světa, ale vztahuje se i na abstraktní matematické objekty, které se skládají z množin, prvků a vztahů mezi nimi [6]:

Systém: $$S = \{ P , R \} \quad (1)$$

je účelově definovaná množina prvků P:

$$P = \{ p_i \} \quad (2)$$

kde $i \in J$ (J je množina indexů)

a množina vazeb (vztahů) R:

$$R = \{ r_{i,j} \} \quad (3)$$

kde $i, j \in J$ mezi prvky p_i a p_j

Množina všech vazeb (vztahů, relací) R = { $r_{i,j}$ } mezi prvky p_i a p_j systému tvoří strukturu systému a ta může být funkční, technická, informační, časová, organizační, apod. a tvoří ji tzv. hierarchická struktura, která vyjadřuje vztahy nadřízenosti a podřízenosti mezi jednotlivými prvky systému.

Prostředkem pro sdělování informací je vždy **jazyk.**

Takže proces popisu našeho systému S vede přes jeho definování k vytváření jeho vlastního modelu M:

$$S \rightarrow M \tag{4}$$

Z hlediska globálního hodnocení reálných objektů je v praxi zavedenodalší účelové dělení systémů na:

- **ekonomické** systémy - jsou to účelové systémy, kde se veličiny vstupů systému s mírou pro hodnotu a efekt, vhodně transformují na hodnotové vyjádření výstupů,
- **sociální** - jsou to opět účelově definované systémy, kde významnou množinu prvků tvoří soubor lidských individualit (s formální a neformální strukturou), vyznačujících se rozdílnými vlastnostmi (zdravotní stav, povaha, vzdělání, ...),
- *technické* - jsou účelově zavedené systémy, v nichž například transformační roli hrají stroje, zařízení atp. a roli vazeb v systému hrají manipulační trasy, materiálové toky apod.
- Zajímavými a moderními jsou **informační a komunikační systémy** (ICT), kde prvky systému jsou místa transformace a vazby v systému patří informačním tokům. [7]

2. VYMEZENÍ KYBERNETICKÉHO PROSTORU

Specifickou oblastí teorie systémů je zkoumání vnitřního uspořádání vlastních systémů. Jestliže z množiny prvků systému S vyčleníme jejich část a pojmenujeme ji jako řídicí podsystém, druhou skupinu prvků pojmenujeme jako řízený podsystém a nahradíme-li stávající vazby novými významnými vazbami, v nichž bude dominantní tzv. zpětná vazba, pak mluvíme o **kybernetickém systému.**

Kybernetika je věda, která zkoumá obecné vlastnosti a zákonitosti řízení v biologických, technických a společenských systémech apod.. Vedle:

- **teoretické kybernetiky** (využívající teorii regulace, teorii informace, teorii automatů, teorii učení, teorii her, teorii algoritmů a další teorie) je také,
- **aplikovaná kybernetika**, ke které řadíme:

✓ *technickou* kybernetiku,

✓ *lékařskou* kybernetiku,

✓ zde ***ekonomickou kybernetiku*** a další.

Jednotlivé dílčí podsystémy ekonomického systému jsou klasické modely kybernetického systému a modelující prostředí je nyní počítačové prostředí, tj. PC (obecně ICT) jako klasický kybernetický systém pro modelování a v tomto příspěvku jako **MODELU KYBERPROSTORU EKONOMICKÉ BEZPEČNOSTI**. Obdobně celé modelování systému je modelem kybernetického systému, kde rozpoznáváním prostředí získáváme údaje o stavu daného prostředí a zpětnou vazbu tvoří vyhodnocování procesu modelování.

Kybernetika definuje procesní inženýrství a studuje živé i neživé organismy, které musí mít schopnost zachovávat informaci. Aplikační prostory pro kybernetiku jsou: technika, **ekonomie** a další.

3. MODELOVÁNÍ EKONOMICKÉ BEZPEČNOSTI V MODERNÍM KYBERPROSTORU

„Praxe ekonomiky má svůj základ v hospodářské politice, praxe v ekonomické bezpečnosti se dotýká každodenního života občanů“ [9]

Bezpečnost má význam obecného atributu a má své systémové vymezení v řadě procesů charakterizujících podle: dimenze bezpečnosti, systémy moci a státu, řízení státu, procesy o morálce a normách chování, o modernímpojetí peněz, nové pojetí právního státu, zákonitosti o hospodářské počítačové a kybernetické kriminalitě, řešení korupce, zákonné vymezení podnikání, vlivy organizovaného zločinu a dalších velmi zajímavých oblastí také nutné pro organizaci bezpečnosti a metod kybernetické a informační bezpečnosti států i celé civilizace. [9]

Modelování ekonomické bezpečnosti je bezesporu moderním trendem na současné problematice řešení rizik, krizí nebo dalších jevech společnosti.

Modelování této oblasti v uvedeném kyberprostoru můžeme vyjadřovat na základě prostředků umělé inteligence (ArtificialIntelligence). Rozvoj tohoto perspektivního oboru je úzce spjat s rozvojem počítačů a sociotechnických prostředků rozpoznávání scén a prostředí. Technologie umělé inteligence jsou v současné době velmi rozmanité. Jsou zastoupeny aplikacemi vycházejícími z biologie (jako například neuronové sítě a genetické algoritmy), z fyziky, matematiky a logiky (jako jsou technologie modelující a identifikující chaos a technologie využívající neostrých množin). Tyto technologie tvoří skupiny založené na počítačových modelech řešení úloh se zásobou expertních informací (expertní systémy), na induktivním učení a tak podobně. Doménami umělé inteligence jsou expertní úlohy (například finanční analýzy), formální úlohy (hry a simulační úlohy), ostatní úlohy – například rozpoznávání přirozeného jazyka, procesy vnímání apod..

Nejvíce užívané technologie umělé inteligencejsou nyní:

- **Neuronové sítě**. Umělé neuronové sítě hledají využití principů, kterými se řídí lidský mozek – sítě neuronů. Existuje řada reprezentací neuronových sítí a jejich interpretací – **pro ekonomické úlohy** budou vhodné neuronové sítě vícevrstvé, kde lze lépe identifikovat nelineární vztahy v modelu,
- **Genetické algoritmy**. Podle analogie z biologie jsou u genetických algoritmů chromozomy jako řetězce bitů, polí, stromů, seznamů a jiných objektů. Chromozomy jsou nositeli podstatných informací o prvku systému. Zakódování informace do chromozomu je možné v binárním formátu (lze zakódovat více informací) nebo v jiných formátech. Při modelování jsou v první populaci všechny chromozomy generovány náhodně – je určena jejich hodnota pro další generace pomocí účelové funkce. Poté následuje reprodukce – selekce, crossover a mutace. Genetické algoritmy mohou sloužit kupříkladu k vyhodnocování výstupů neuronových sítí. V ekonomii se používají například **v optimalizačních úlohách** alokace aktiv nebo při obchodování s měnou. [1,4]

ZÁVĚR

Uvedené přístupy řeší v kyberprostoru systémovou analýzu a modelování jako kybernetické systémy, které mají vlastnosti: celistvosti objektu, rozložitelnost na části, existenci vazeb mezi částmi, interakce objektu jako celku s okolím, dynamičnosti objektu (**adaptabilnosti modelů ekonomické bezpečnosti**, schopnostiučení se) a podobně.

Vědecké práce navazují na uvedené procesy ekonomické bezpečnosti na obou fakultách a dále pokračují v trendech vyjádřených v mezinárodním pojetí nových aspektů technologického přínosu pro rozvoj makroekonomiky a nového směru modelování ekonomických procesů.

Literatura

[1] DVOŘÁK, J.; JANKOVÁ, M. *The ICT possibilities in thevirtualuniversitiescyberspace.* In Mathematics, Information Technologies and AppliedSciences 2014 (post-conferenceproceedingsofselectedpapersextendedversions). Brno: MITAV 2014, 2014. s. 59-65. ISBN: 978-80-7231-978- 7.

[2] DVOŘÁK, J.; JANKOVÁ, M. *Systemicallyintegratedelectronic business model*. Ekonómia a podnikanie, 2012, roč. 6, č. 2/ 2012, s. 79-84. ISSN: 1337- 4990.

[3] DVOŘÁK, J.; JANKOVÁ, M. *Optionsofelectroniccommerce modelling in a cyberspaceofneweconomy*. In EBES Conference. Rusko, Ekaterinburg: EBES, 2014. s. 43-51. ISBN: 978-605-64002-3- 0.

[4] DVOŘÁK, J.; JANKOVÁ, M. *Informační gramotnost pro moderní praxi*. In Daně-teorie a praxe 2012. Akademie Sting. Brno: Akademie Sting, 2012. s. 14-16. ISBN: 978-80-87482-10- 0.

[5] DVOŘÁK, J.; JANKOVÁ, M. *Rozpoznávání rizik v ekonomické kybernetice*. In Krizový management 2014. doc. Ing. Miloslav Hub, Ph.D. Pardubice: Univerzita Pardubice, 2014. s. 12-19. ISBN: 978-80-7395-871- 8.

[6] DVOŘÁK, J.; KONEČNÝ, J.; JANKOVÁ, M. *Možnosti identifikace útoků v kyberprostoru krizového řízení*. In Krizové řízení a řešení krizových situací 2015. Uherské Hradiště: Univerzita Tomáše Bati ve Zlíně, 2015. s. 64-69. ISBN: 978-80-7454-573- 3.

[7] DVOŘÁK, J.; KONEČNÝ, J.; JANKOVÁ, M. *Možnosti útoků v kyberprostoru bezpilotních prostředků*. In Krizový management 2015. Univerzita Pardubice. 2015. s. 5-13. ISBN: 978-80-7395-941- 8.

[8] JANÍČEK, P.; MAREK, J. *Expertní inženýrství v systémovém pojetí*. 1. vyd. Praha: GradaPublishing, 2013, 592 s. ISBN 978-80-247-4127-7.

[9] HŘEBÍK, F., SEKERKA, B. *Vybrané aspekty ekonomické bezpečnosti*. Praha Tigris. spol. s r.o. Holešov ISBN 978-80-7490-195-9.

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

ANALÝZA GENERACE Y A X Z POHLEDU VYUŽÍVÁNÍ SLUŽEB V KRÁTKODOBÉM CESTOVNÍM RUCHU V ČESKÉ REPUBLICE

ANALYSIS OF GENERATION Y AND X FROM THE VIEW OF THE USE OF SERVICES IN SHORT-TERM TOURISM IN THE CZECH REPUBLIC

Ing. et Ing. Monika Hýblová [1], Ing. Ottó Bartók [2]
Univerzita Tomáše Bati ve Zlíně
Faculty of Management and Economics
Mostní 5139, 760 01 Zlín
[1]E-mail: mhyblova@utb.cz
ORCID: 0000-0002-7788-6204

[2]Email: bartok@fame.utb.cz
ORCID: 0000-0001-6340-676X

ABSTRAKT

Krátkodobý turismus je významnou součástí cestovní ruchu. Generace Y společně s generací X se vyznačují právě velkým využíváním krátkodobého turismu. Generace Y má vyšší zdatnost ve využívání internetu. Díky čemuž se mění nákupní chování této generace oproti zvyklostem. Tato zdatnost umožňuje využívat širší paletu služeb při krátkodobém cestovním ruchu. Generace X je ovlivněna i zkušenostmi a do jisté míry i ne tak velkou mírou ochoty využívat nové technologické prostředky. Právě tyto rozdíly mají významný vliv na spektrum využívaných služeb. Využívanost služeb se liší nejen v četnosti, ale i v celkovém složení v rámci jednoho uživatele. V neposlední řadě je třeba neopomíjet celkový rozhodovací proces. Článek pojednává o těchto odlišnostech a představuje komplexní srovnání těchto dvou generací z pohledu využívanosti služeb v krátkodobém cestovním ruchu. Cílem výzkumu je zjistit, zda generace Y využívá internet k nákupu služeb při účasti na krátkodobém cestovním ruchu více, než generace X a jak generace X a generace Y využívá internet k nákupu služeb při účasti na krátkodobém cestovním ruchu.

KLÍČOVÁ SLOVA

krátkodobý cestovní ruch, generace Y, generace X, služby

ABSTRACT

Short-term tourism is an important part of tourism. Generation Y, together with the X generation, is characterized by the great use of short-term tourism. Generation Y is more proficient in using the internet. This makes the generations' purchasing behaviour different from their habits. This skill makes it possible to use a wider range of services for short-term tourism. Generation X is influenced by experience and, to a certain extent, by not too much willingness to use new technological means. These differences have a significant impact on the spectrum of services used. Usage of services differs not only in frequency but also in overall composition within a single user. Last but not least, the overall decision-making process must not be avoided. The article discusses these differences and represents a comprehensive comparison of these two generations from the point of view of the use of services in short-term tourism. The aim of the research is to find out whether generation Y uses the internet to buy short-term tourism services more than generation X and how generation X and generation Y use the internet to buy services for short-term tourism.

KEY WORDS

short-term tourism, generation Y, generation X, services

ÚVOD

V současné době dynamicky roste význam generace Y, která již je nebo se stává ekonomicky aktivním segmentem trhu. Tato generace je dle Kotlera (2007) velice významnou pro B2B trhy, neboť mají díky vysokému počtu velkou kupní sílu. Tato generace vyrostla v období prosperity a v mírovém prostředí, díky čemuž byla rozmazlována. Z těchto důvodů je pro současné i budoucí prodeje nutné pochopit tuto cílovou skupinu, brzy se totiž stane skupinou, která bude kompletně ekonomicky aktivní, a tedy zajímavá pro trh. Cestovní ruch je velice konkurenční prostředí, což je možné zejména díky rozvoji dopravy a dopravní infrastruktury. To umožnilo snížení nákladů na dálkové typy dopravy, a tak je umožněno cestovat téměř po celém světě velkému množství lidí. To je důvodem, proč je na světě tolik konkurenčních destinací. Základem pro cestování je i dobrý mírový stav a disponibilní důchod, který zákazníkům toto cestování umožňuje. Cestovní ruch je velice důležitým odvětvím pro světovou ekonomiku, dle Tsiotsou a kol. (2012) je podíl cestovního ruchu 9 % na světovém HDP, zaměstnává 260 milionů lidí, přičemž očekává nárůst o téměř 70 milionů zaměstnanců do roku 2021.

1. LITERÁRNÍ REŠERŠE

1.1 Cestovní ruch

V průběhu desetiletí zaznamenala cestovní ruch pokračující růst a prohlubování diverzifikace, aby se stal jedním z nejrychleji se rozvíjejících hospodářských odvětví na světě. Moderní cestovní ruch je úzce spjat s rozvojem a zahrnuje rostoucí počet nových destinací. Tato dynamika změnila cestovní ruch jako klíčový faktor socioekonomického pokroku. Dnes je obchod v cestovním ruch roven nebo dokonce překonává objem exportu ropy, potravinářských výrobků nebo automobilů. Cestovní ruch se stal jedním z hlavních hráčů v mezinárodním obchodě a zároveň je jedním z hlavních zdrojů příjmů mnoha rozvojových zemí. Tento růst jde ruku v ruce s rostoucí diverzifikací a konkurencí mezi destinacemi. Toto globální rozšíření cestovního ruchu v průmyslových a rozvinutých státech přineslo výhody v mnoha souvisejících sektorech – od stavebnictví až po zemědělství nebo telekomunikace (UNWTO, 2017)

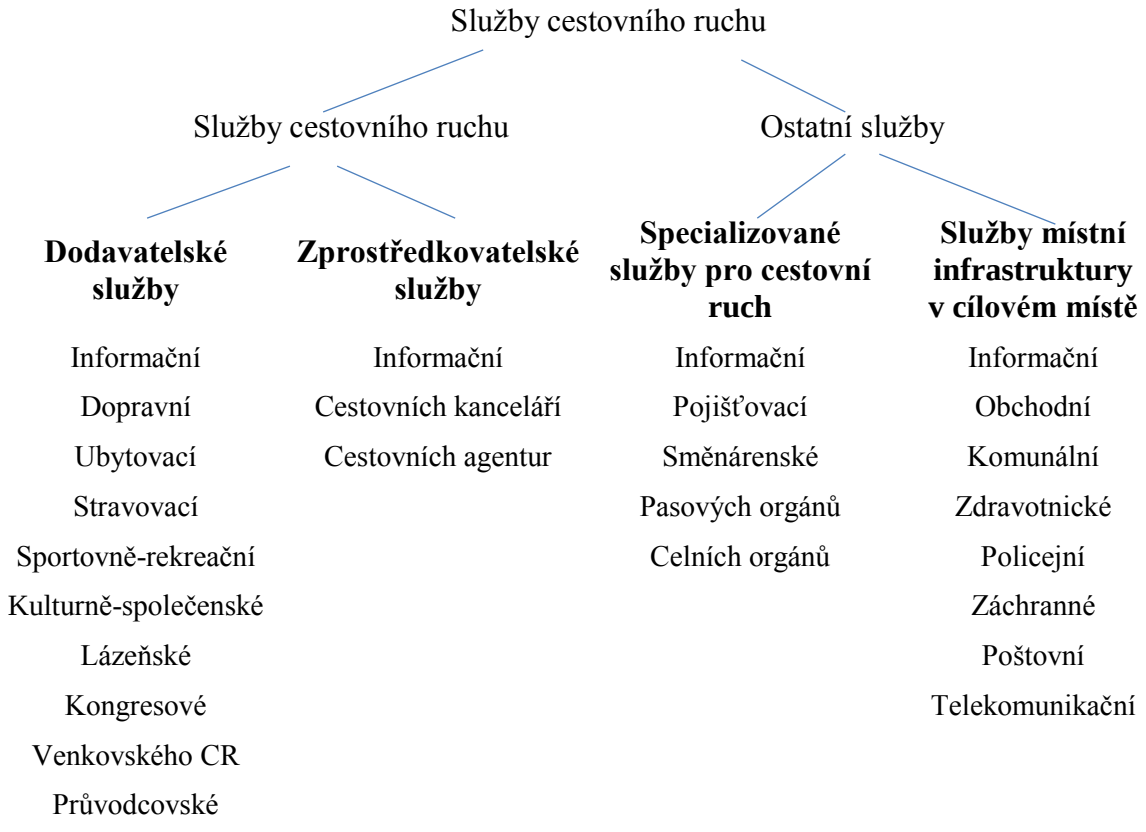
Cestovní ruch je významným odvětvím v oblasti služeb, a to i v podmínkách České republiky. Podíl cestovního ruchu na HDP se pohybuje nad 3 %. Již v roce 2015 dle CzechTourismu přiblížily příjmy z cestovního ruchu 150 mld. Kč. za rok (CzechTourism). Česká republika je pro zahraniční turisty velmi atraktivní zemí, jen za první ¾ roku 2017 navštívilo naši republiku více než 7,8 mil zahraničních návštěvníků, nejvíce z Německa. (ČSÚ 2017) I přesto, že dle Vajčnerové a Ryglové (2017) má Česká republika potenciál, rozvoj návštěvnosti není samozřejmý. Vysoká návštěvnost České republiky je tvořena nejen zahraničními návštěvníky, ale i vnitrostátním cestovním ruchem, který je pro Čechy variantou k zahraničnímu cestování.

1.2 Služby cestovního ruchu

Zeithaml (1981) zdůrazňuje u služeb cestovního ruchu jejich charakteristické vlastnosti – heterogenita, nehmotnost, neoddělitelnost a netrvanlivostí. Tsiotsou (2012) dodává, že zvláštnosti odvětví cestovního ruchu označovány jako sezónnost, globalizace, nízká

loajalita a složitost poptávky. Sezónnost Butler (2001) chápe jako časovou nerovnováhu ve fenoménu cestovního ruchu, která může být vyjádřena, počet návštěvníků, výdaji návštěvníků, dopravou na dálnicích a dalších formách dopravy. Sezónnost je považována za závažný problém cestovního ruchu, protože vede turistické firmy k tomu, aby najímali pracovníky na částečný úvazek. Neustálé najímání nových sezónních zaměstnanců vede ke zvýšení nákladů na zácvik a dalších nákladů spojených s nestabilitou zaměstnanců. V některých případech dosahuje 80 % příjmů z cestovního ruchu během dvouměsíčního období hlavní sezóny. Globalizace v cestovním ruchu znamená, že podniky cestovního ruchu mají schopnost působit a prodávat se nejen na místní, ale i celosvětové úrovni, zatímco mnohé z nich se rozhodly pro konkurenceschopnou strategii internacionalizace (Knowles a kol., 2001). V oblasti cestovního ruchu globalizace ovlivňuje jak nabídku, tak poptávku různými způsoby. Při poskytování služeb cestovního ruchu se nejběžnější trendy týkají vývoje velkých celosvětových dodavatelů a zprostředkovatelů, mohou vést k oligopolům. Na straně poptávky je globalizace spojena se snížením nákladů na leteckou dopravu, s přístupem k novým a levným destinacím a také s relativně nízkými sociálními standardy. Tsiotsou a Wirtz (2012) zdůrazňují velice nízkou loajalitu zákazníků, kteří chtějí zkoušet pořád nové zážitky a navštěvovat různé destinace cestovního ruchu. Řešením může být vytváření nadnárodních společností, které poskytují služby v mnoha různých destinacích, kdy zákazník nakupuje služby v různých destinacích, ale od stejného dodavatele globálních služeb. Tsiotsou (2012) vidí problém u služeb cestovního ruchu i v množství dodavatelů, kteří vytváří soubor služeb – od ubytování, stravování, dopravu nebo návštěvu atraktivit. Špatná kvalita jedné služby může přinést negativní dojem z cestovního ruchu, i přestože ostatní služby byly v očekávané kvalitě.

Hesková (2006) rozděluje služby cestovního ruchu do následujícího schématu, na přímé služby cestovního ruchu a ostatní služby.



Asistenční

Animační

Tabulka 1 Služby cestovního ruchu

1.3 Generační segmentace a její vliv na trh cestovního ruchu

Při četných pokusech o interpretaci současného cestovního ruchu jsou otázky, které se stávají stále naléhavější, ty, které se týkají sociálně demografických změn a trendů, které ovlivňují chování turistů nebo v širším slova smyslu volnočasovou aktivitu jako celek. Demografické změny mají vliv na mnoho aspektů cestovního ruchu, především na sílu a typ poptávky po cestovním ruchu, stejně jako na trh práce v oblasti cestovního ruchu (Grimm et al 2009). Mezi standardní determinanty činnosti cestovního ruchu, preference a následně i tvorba turistického prostoru jsou sociální a demografické rysy. Důležitou proměnnou je věk, ale mnozí autoři poukazují na etapy životního cyklu a také na generační rozdíly (Opperman 1995, Kowalczyk – Anioł, 2007). Definice může popisovat generaci jako skupinu lidí (také zvířata nebo rostliny) přibližně ve stejném věku a lidé dospívající s podobnými nebo stejnými zkušenostmi. Myšlenka interpretace socioekonomických problémů z pohledu generačních kohort není nová. Ve společenských vědách má dlouhou tradici od 20. let 20. století (Mannheim) a často se uplatňuje v sociologii (např. Teorie generací formulovaná americkými sociology, Howe & Strauss, 1991), psychologii nebo politické vědě. V posledních letech věnují lidé i marketingový specialisté svou pozornost těmto otázkám. Rozsáhlé společensko-politické debaty o probíhajících globálních demografických změnách stále častěji zahrnují otázky mezigeneračních vztahů.

Koncepce rozdělení žijící populace na jednotlivé generace není novým problémem, rozdělení na generace řešil již Mannheim (1952). Generační teorie se snaží pochopit a charakterizovat kohorty lidí podle jejich členství v generaci (Benckendorff et al, 2010). Z tohoto pohledu se také stalo zásadním důrazem na zorientování se v cestovním ruchu. Zajímavou a obzvláště důležitou otázkou pro pochopení dnešní situace je srovnání chování jednotlivých generací, zejména pokud jde o tři velké skupiny na současném trhu cestovního ruchu. Tyto generace jsou jmény: nejstarší je generace Baby Boomer, střední je generace X, zatímco nejmladší – generace Y. Generace Baby Boomer (BB), X a Y (nejdůležitější kvůli jejich současným číslům) byly popsány různými autory v detailu (např. Howe, 1991, Mitchell, 1995). Věkové rozmezí jsou "teoretické", takže autoři odkazují na mírně odlišné období týkající se roků narození členů určitých věkových kohort. Například v jeho publikaci v roce 2005 Kotler předpokládal, že generace Y (v USA – poznámka autora) byla produktem dobrých ekonomických časů a internetu a jeho členové jsou narozeni v letech1978-94. Pro jiné autory (např. Lawrence) se Generace Y skládá z Američanů narozených mezi lety 1977 a 1999. Kotler a Armstrong (2010) představuje nejširší časový úsek pro generaci Y (tzv. miléniálové nebo echo boomers) nebo i-Pod generace, net generace, Generace next) - mezi lety 1977 a 2000. Mileniálové jsou většinou děti baby boomers. Zatímco většina (83 %) generace BB je bílá, 45 % generace Y patří k jiným rasám (Kotler & Armstrong, 2010).

Čína		Generace po 50. letech (1950-1959)	Generace po 60. letech (1960-1969)	Generace po 70. letech (1970-1979)	Generace po 80. letech (1980-1989)		Generace po 90. letech (1990-1999)
Indie	Tradiční generace (1948-1968)			Netradiční generace (1969-1980)	Generace Y (po roce 1981)		
Jižní Korea		Generace 475 (1950-1959)	Generace 386 (1960-1969)	Generace X a generace Y (po roce 1970)			
Japonsko	1.generace Baby Boomer (1946-1950)	Danso generace (1951-1960)	Generace shinjinrui (1961-1970)	2. generace Baby Boomer (1971-1975)	Post Bubble (1976-1987)	Generace shinjinrui junior (1986-1995)	Yutori (1987-2002)
Rusko	Baby Boomers (1943-1964)		Generace X (1965-1980)		Generace Y (generace „Pu“) (1983-2000)		
Bulharsko	Poválečná generace (1945-1965)		Komunistická generace (1965-1980)		Demokratická generace (po roce 1980)		
Česká republika	Baby Boomers (1946-1964)		Generace X „Husákovy děti“ (1965-1982)		Generace Y (1983-2000)		
Jižní Afrika	Baby Boomers (1943-1970)			Generace X (1970-1989)			Generace Y (po roce 1990)
Brazílie	Baby Boomers (1946-1964)		Generace X (1965-1980)		Generace Y (1981-2001)		
USA	Baby Boomers (1946-1964)		Generace X (1965-1980)		Generace Y (1981-2001)		

Tab. 1 Porovnání generací v jednotlivých státech světa (Bejtkovský 2016)

Členové generace Y jsou v současné době v mladé dospělé fázi života, plní vitality a testující hodnoty. Generace a generační jednotky jsou neformálně definováni demografy, médii, kulturou, výzkumníky a členy generace (Prendergast, 2007). Rozdělení na generace je dle Oh & Reevse (2011) jsou rozdíly mezi jednotlivými generace diskutovány v tisku, na konferencích i workshopech. Přitom rozdělení na jednotlivé generace se u jednotlivých autorů liší, toto rozdělení není nijak standardizováno. Někteří autoři se liší i v názvu jednotlivých generací, také generaci Y můžeme najít pod názvy miléniálové, gen-Y, Baby Busters, NetGen, Nexters, Generace Why, Generace Search, síťová generace, Generace dot.com, Generace Einsteinů, Echo Boomers, Generace We, Peter Pan Generation nebo digitální generace. Spitzer (2014) označuje tuto generaci i jako zlomovou. Obecně se dá říct, že většina autorů zahájení této generace datuje do roků 1978-1985 a konec v letech 1995-2003. Tato generace je dle Bergha (2016) zvyklá na velké množství podnětů, je těžké je ohromit nebo udržet jejich pozornost, pro co se nadchnou, hned realizují. Dle Benckendorffa et al (2010) se jedná o generaci se zaměřením na značky, přátele, zábavu a digitální kulturu. Členové Generace Y jsou přesvědčiví a uvolnění, konzervativní a nejvíce vzdělanou generací vůbec. Byli chráněni, ale měly vysoké očekávání a bezpečnost berou jako nejdůležitější. Jsou netrpěliví a zaměření na sebe, přesto vyzdvihují týmy a spolupráci. Jedná se o multitaskery, kteří jsou silně ovlivnění přáteli a vrstevníky.

1.4 Charakteristika generace Y

Generace Y je také také známá jako Millennials, echo-boomers, Generation We, Net Generation, Peter Pan Generation a děti baby boomers (Bleedorn, 2013). Neexistuje žádný pevný a konsenzuální časový rámec pro narození generací Y (Bolton, Hoefnagels, Migchels, Kabadayi, Loureiro & Solnet, 2013). Obecně platí, že lidé, kteří se narodili v letech 1980 až 1999, jsou široce definováni jako Millennials (Bolton et al., 2013). Podle Teller (2009), Millennials čítá více než 75 milionů lidí, a proto se řadí na druhé místo v početnosti po Baby Boomers (ti byli narozeni v letech 1946 a 1960). Generace Y se odlišuje od jiných generací prostřednictvím několika jedinečných vlastností. Za prvé, miléniálové se vyznačují

přirozeným využíváním technologií, které se kterými vyrostli. Na rozdíl od svých předchůdců jsou vázány na technologii i na emocionální bázi (Bolton et al., 2013), což vysvětluje jejich každodenní používání různých elektronických zařízení, jako jsou smartphony, notebooky a tablety, a to jak pro osobní, tak i pro obchodní účely. Někteří vědci také naznačili, že miléniálové považují za důležité (srov. Brown, Carter, Collins, Gallerson, Giffin, Greer, Griffith, Johnson & Richardson, 2009) stabilní rovnováhu mezi pracovním a soukromým životem, stejně jako flexibilitu v jejich pracovní pozici. Je tedy zřejmé, že hodnota rodiny se v této generaci stala ještě významnějším faktorem. Dále se uvádí, že mileniálové jsou známí svým optimismem, vzděláváním, schopnostmi spolupráce, otevřeností a pohonem (Spiro, 2006). Respektují své nadřízené a snaží se dodržovat jejich pravidla. Současně se také předpokládá, že spíše plní úkoly s profesionálním týmem než na individuálním základě (Brown et al., 2009). Ellin (2014) potvrdil a doplnil, že "V ideálním miléniálském kancelářském prostředí by všichni spolupracovali s menším důrazem na starých školách" (str. 59). Na rozdíl od lidí z jiných generací jsou však peněžní pojmy považovány za méně důležité (Crampton & Hodge, 2009), protože preferují více času s dětmi a zlepšují nebo udržují vztahy (Spiro, 2006). Když si stanovili cíl, jsou však velice nadšeni, když je ho dosaženo (Yeaton, 2008). Generace Y má také tendenci utrácet tolik peněz během ekonomické krize jako ve stabilním prostředí, aby udrželi své hodnoty a životní styl. Jsou tedy označeny za "nejoptimističtější generaci" (Bleedorn, 2013, s. 26). Pokud jde o neustálý rozvoj technologie, studie Brown et al. (2009) naznačuje, že používají webové stránky sociálních sítí častěji než respondenti, kteří nejsou generací Y. Jejich záměr využívání technologií se výrazně odlišuje od svých předchůdců, nepoužívají je pouze pro vyhledávání informací, ale také pro zábavu a komunikaci (Bleedorn, 2013, Bolton a kol., 2013, Chordas, 2008). Počítače považují pouze za součást života, říká Yeaton (2008, s. 69). V návaznosti na tento pojem je přirozeným očekáváním, že se budou spoléhat na vyhledávání informací na internetu a rozhodovat na základě dostupných informací na internetu (Ellin, 2014). Sociální média jsou proto významným zdrojem informací pro generaci Y, neboť tato technologie dokáže usnadnit komunikaci včas s rychlým vyhledáváním informací.

1.5 Generace Y a používání internetu

Jedním z největších rozdílů, mezi generací Y a předchozími generacemi je ten, že se jedná o první generaci, která strávila celý svůj život v digitálním prostředí; (Bennett et al., 2008, Wesner a Miller, 2008). Generace Y je dle Prenskyho (2006) první generací informačního věku a z tohoto důvodu jsou známí jako digitální domorodci.

K roku 2014 se podíl populace používající internet v oblasti cestování a ubytování vzrost na zhruba 47 %, což představuje téměř 60 % všech uživatelů internetu. Přičemž průměr EU 28 dosahoval z pohledu populace necelých 39 %, z pohledu uživatelů internetu téměř 50 %. Tyto výsledky staví Českou republiku na úroveň Francie nebo Velké Británie. Z výše uvedeného je tedy patrné, že i přesto, že Češi jako národ nenakupují na internetu v takové míře, jako nejvyspělejší státy Evropské unie, v oblasti cestovního ruchu jsme vysoko nad průměrem EU a vyrovnáváme se i nejvyspělejším zemím. Je tedy patrné, že oblast cestovního ruchu a ubytování je pro Čechy velice zajímavá a populární, a proto je vhodné se jí více věnovat. Navíc rozšiřování služeb cestovního ruchu a jejich prodej na internetu zvýšilo konkurenci a nabídku na tomto trhu. Nyní je zcela běžné nakoupit nebo porovnat nabídku služeb se zahraničím, i bez nutnosti znát cizí jazyky na vysoké úrovni (ČSÚ, 2015)

Překvapivý výsledek v roce 2017 zjistila svým výzkumem agentura PPM faktum. Původní předpoklad totiž byl, že procentuálně nejvíce na internetu nakupuje nejmladší generace Z, která se ve světě technologií pohybuje od narození. Vysvětlením tohoto jevu je v tom,

že generace Y již plně vydělává a má tak již dostatečné příjmy, ovšem mnohem méně volného času. Proto tedy volí nákup přímo na internetu, oproti generaci Z, kteří zboží a služby na internetu vyberou, ale poté jsou nákup uskutečnit osobně.

Tato mladí, kteří jsou buď studenti nebo relativně noví účastníci pracovní síly, jsou často označováni jako technologicky zdatní a nejvíce vizuálně sofistikovanou generací. Potřeba interakce s ostatními je klíčovým důvodem pro používání sociálních médií (Palfrey and Gasser, 2008). Uživatelé sociálních médií ve věku 18 až 34 let mají větší předpoklady než starší věkové skupiny preferovat sociální média pro interakce se známými, přáteli i rodinou. Jsou více ocení názory ostatních v sociálních médiích a budou se cítit důležití, když poskytnou zpětnou vazbu o značkách nebo produktech, které používají (eMarketer, 2011).

Richards (2007) říká, že generace prozkoumá další destinace, tráví více času cestováním, jsou hladoví po zkušenost a informacích. Dále zachycuje ducha generace Y v prohlášení: "Cestování je cesta života. Určitá míra rizika je součástí cestování, ačkoli to může být minimalizováno díky pečlivému plánování " Světová organizace cestovního ruchu (WTO) dodává, že unikátní motivy mladých cestujících dělá tento trh mimořádně důležitý v globálním programu cestovního ruchu (WTO, 2008). WTO (2008) uzavřela svou zprávu o záležitostech pro mladé cestující: porozumění globálnímu fenoménu cestování mládeže zdůrazňující, že mládežnické a studentské cestování je hlavní složkou globálního cestovního ruchu a má pozitivní vliv na osobní a sociální rozvoj mladých lidí. Také WTO přiznala, že studentské a mládežnické cestování představuje jedinečný trh, který musí být pochopen pro naplnění specifických potřeb. WTO (2008) konstatuje, že 70 % všech cest mladých lidí jsou motivovány touhou prozkoumat cizí země, pracovat nebo studovat v zahraničí.

1.6 Cestování generace Y

Dle Kowalczyk-Anioł (2012) je zejména ve vyspělých státech jako je Velká Británie nebo Spojené státy americké trendem rok volna mezi školou a vysokou školou, nebo před začátkem zaměstnání. Dle jejího výzkumu tento rok volna využívají pouze 4 % polských mladých v generaci Y. Oproti tomu je velmi populární cestování v rámci programu ERASMUS a CEEPUS. V roce 2010/2011 se v Polsku do tohoto programu zapojilo témě 15 tisíc studentů. Dle jejího výzkumu polská generace Y nejčastěji cestuje s přáteli, až ze 70 %, naopak velice zřídka cestují sami, asi 7 % odpovědí. Tato generace v Polsku také nejméně cestuje s rodinou, může to být i z důvodu, že oproti starším generacím je pouze31 % této generace vdaných nebo ženatých, u ostatních generací je to 59 %. Tyto hodnoty potvrzují polskou tradici a důraz na rodinu. Dále bylo zjištěno zaměření cestovatelů z generace Y na aktivní dovolenou a hledání zábayy, druhou velkou a zdánlivě protichůdnou skupinou jsou cestovatelé se zaměřením na pobyt v přírodě a autentičnost daného místa. Benckendorff (2012) stanovuje obecné trendy generace Y, kdy lidé více a častěji cestují, poznávají více destinací, mají větší útraty při cestování, při rezervacích více využívají internetové prostředí, snaží se pochopit jiné kultury, hledají si více informací, plánují výlety a nenechají se tolik vyvést z míry přírodními katastrofami nebo terorismem. Benckendorff (2012) zdůrazňuje generaci Y jako cestovatele kvůli práci. Rovněž potvrzuje, že tato generace cestuje častěji a do více destinací. Kueh a Voon (2007) označili asijskou generaci Y jako nejnáročnější na kvalitu služeb. Kromě vysoké kvality služeb očekávají i rychlost, spolehlivost, estetičnost nebo i pěkně upravený personál. Morton (2002) zdůrazňuje ovlivnění rozhodování této generace v cestování prostřednictvím zkušeností a názorů přátel, oproti tomu nevěří masmédiím. Výzkum Benckendorffa (2012) zjistil, že pro generaci Y jsou lákavou destinací velká města, víc je láká tenis a golf.

V důsledku výše zmíněného byly stanoveny tyto hypotézy a výzkumné otázky.

H1: Generace Y využívá internet k nákupu služeb při účasti na krátkodobém cestovním ruchu více, než generace X.

H2: Existuje statisticky významná zavilost mezi nižším věkem a ochotou využívat internet k nákupu služeb při účasti na krátkodobém cestovním ruchu.

VO1: Jak generace X a generace Y využívá internet k nákupu služeb při účasti na krátkodobém cestovním ruchu.

VO3: Které služby mají nejvyšší četnost nákupů v rámci krátkodobého cestovního ruchu za využití internetu.

***VO3*:** Které služby mají nejvyšší četnost nákupů v rámci krátkodobého cestovního ruchu bez využití internetu.

2. METODY

2.1 Účastníci

Kvantitativní výzkum byl proveden za pomocí dotazníkového šetření s generací X a generací Y. Respondenti byli selektování na základě kritérií související se specifiky generací X a Y, dále respondenti museli být účastnici krátkodobého cestovního ruchu v průběhu posledních 365. Celkový počet dotázaných respondentů byl 347 z toho lze přiřadit 166 respondentů do skupiny generace X a 144 respondentů do skupiny generace Y. Zbylých 37 respondentů neodpovídalo žádnému z kritérií pro členění a bylo vyřazeno. Generace X se vyznačovala průměrným věkovým zastoupením 38.5 let *(SD = 3,84)* přičemž mužů bylo 51 % a žen 49 %. Generace Y se vyznačovala průměrným věkovým zastoupením 23.2 let *(SD = 4.12)* přičemž mužů bylo 53 % a žen 47 %. Skupinou, na kterou je práce zaměřena, je generace Y v České republice. Ta je pro použití v práci specifikována věkovým rozmezím 18 až 34 let. To odpovídá rokům narození 1984 až 2000. Toto rozpětí podle Stanimira (2015), Sineka (2016) a Gronbacha (2008) odpovídá definici generace Y nebo jejich rokům narození. Tato generace dle posledního sčítání obyvatel čítá téměř 2 miliony obyvatel v České republice. Toto číslo bude ovlivněno přirozenou úmrtností a migrací.

2.2 Měření

Pro otestování přístupu k cestování generace Y probíhá pilotní ověření prostřednictvím dotazníkového šetření. To je zaměřeno na krátkodobý cestovní ruch a jeho nákup přes internet. Pro pilotní ověření bylo vypracováno dotazníkové šetření, kde jsou dosud sbírá-na data pro pozdější statistické vyhodnocení. Dotazníkové šetření bylo provedeno za využití Likertovy škály pro postojové otázky při využití škály 1 (zcela nesouhlasím) až 5 (zcela souhlasím Dále dichotomické otázky pro demografické rozlišení a výčtu položek pro analýzu služeb. Dotazníkové šetření zahrnovalo celkem 25 otázek, které se soustředily na analýzu využívaných služeb v krátkodobém cestovním ruchu v České republice. Pro otázky (N = 18) využívající Likertovu škálu byl proveden test reliability, tento test byl proveden pro tři specifické oblasti. Pro první oblast: služeb (α = .79), pro druhou oblast: internetové a počítačové zdatnosti (α = .76) a pro třetí: krátkodobého cestovního ruchu (α = .84). Dotazník byl sestaven až po stanovení cílů dotazníku. Dotazník byl pretestován na vzorku (N = 30) osob. Na základě jejich komentářů a doporučení byly doplněny odpovědi, které by mohli dotazovaným chybět. Dotazníkové šetření bylo zpracováno v elektronické po-době a touto cestou také šířeno a vyplňováno. Tento způsob je rychlý a má velice nízké náklady.

Navíc je možné dosáhnout i širokého geografického rozsahu v rámci České re-publiky bez nutnosti cestovat.

2.3 Proces zpracování

Dotazník byl šířen za pomocí elektronického odkazu dostupného na síti Google Forms. Šíření proběhlo v rámci jednotlivých skupin na sociálních sítích, ale i za využití databáze e-mailů, která disponuje schválením pro zasílání elektronických zpráv. Jako zdroj primární dat sloužilo dotazníkové šetření, které proběhlo v květnu roku 2018. Sekundární zdrojem dat byl Český statistický úřad a CzechTourism. Dotazníkové šetření bylo rozděleno do několika dílčích částí, tak aby respondent odpovídal relevantně a byl naplněn výzkumný cíl.

2.4 Analýza dat

Data z dotazníkového šetření byla analyzována za pomocí Cronbachovo alfa. Pro test normality byl využít Shapiro-Wilk test, pro testy hypotéz byl využit t-test a dále Pearsonova korelace pro vzájemné závislosti.

3. VÝSLEDKY

Data získaná v rámci dotazníkového šetření byla podrobena testu normality pro skupinu generace X $t(166)$ ($p = .34$) a pro skupinu generace Y $t(144)$ ($p = .29$) v obou případech mají data normálové rozdělení. Pro ověření hypotézy, že generace Y využívá více internet k nákupu služeb než generace X. Byl zvolen párový t-test, tento test ukázal, že využívání internetu k nákupu služeb v rámci krátkodobého cestovního ruchu je vyšší u skupiny generace Y ($M = .89$, $SD = .08$) než u skupiny generace X ($M = .56$, $SD = .31$), $t(310) = 11.7$, $p < .001$, $d = 0.68$. V důsledku výše zmíněného hypotéza byla přijata.

Ověření hypotézy, věnující se závislosti mezi věkem a ochotou využívat internet k nákupu služeb při účasti na krátkodobém cestovním ruchu, je provedeno za pomocí Pearsonovy korelace $r(210) = .72$, $p < .001$. Provedená korelace ukazuje středně silnou zavilost mezi nižším věkem účastníka a vyšší mírou ochoty využít internet pro nákup služeb v rámci krátkodobého turismu. V důsledku výše zmíněného hypotéza byla přijata.

Z dotazníkového šetření vyplynulo, že dotazovaní mají vztah k cestovnímu ruchu, i když se jednalo pouze o zaměření na krátkodobý cestovní ruch. Pouze 10.6 % všech respondentů vůbec nejezdí na pobyty v délce do tří dnů. Naopak, více než 22 % jezdí na takovéto pobyty čtyřikrát nebo i vícekrát za rok. Podobných výsledků dostáhly možnosti, že respondenti jezdí na takové pobyty 2x (28.2 %) nebo 1x (29.6 %) za rok. Téměř 6 % dotazovaných se krátkodobého cestovního ruchu účastní třikrát ročně.

Nejčastěji nakupovanými službami z pohledu generace X byly: služby cestovních kanceláří 77.7 % a wellness služby 53.6 %, v případě generace Y byly: ubytovací služby 60.4 % a dopravní služby 53.4 %. Generace X nejčastěji využívala internet pro nákupy ubytovacích služeb v 74.3 % stejně tomu bylo u generace Y nakupovanou službou v případě generace Y při využití internet pro nákup ubytovacích služeb v 95.1 %.

Nejméně nakupovanými službami z pohledu generace X byly: služby spadající do oblasti animačních služeb 68.1 % a kulturně společenské služby 56.1 % v případě generace Y: služby animačních služeb 88.7 % a průvodcovské služby 77.9 %. Generace X nejméně využívala internet pro nákupy asistenčních služeb 98.7 % a animačních služeb 96.7 %, přičemž

generace Y nejméně využila internet pro kongresové služby 99.7 % a animačních služeb 96,6 %.

4. DISKUZE

Výzkum o vztahu cestování a generaci Y byl uskutečněn v Polsku. Tam zjistili, že mladá polská generace má značný zájem o cestování. Bohužel výzkum byl proveden již v roce 2012 a popisuje velmi pozitivní vztah a postoj těchto mladých lidí k cestování v rámci studia a bezprostředně po něm. Ovšem již v této době byl zdokumentován zájem o cestování u části této generace. Část generace bohužel pro nízký věk nebyla oslovena, není předpoklad, že by již samostatně cestovali. Na základě zjištění, lze konstatovat, že generace Y v České republice využívá internet četněji, než generace X. Toto tvrzení lze přijmout i v důsledku přijaté hypotézy *H1*. Rovněž i věk účastníka v rámci krátkodobého cestovního ruchu má vliv na jeho ochotu využít internet k nákupu služeb. Mladí lidé projevovali vyšší ochotu k využití internetu, což je dáno i ochotou akceptovat vyšší riziko v rámci celé transakce. Tato vazba byla přijata v rámci *H2*. Nejvyužívanější službou v rámci krátkodobého cestovního ruchu z pohledu generace Y jsou ubytovací služby, kdy nadpoloviční většina respondentů tyto služby nakupuje, a to pro obě generace shodně i nejčastěji prostřednictvím internetu. Důvody k tomuto využívání můžeme spatřovat v široké nabídce, ale i v množství srovnávacích portálů (Trivago, Booking a dalších), kteří nabízí poměrně komfortní služby s jednoduchým ovládáním. Podobného zjištění nalezla i studie (Anderson, 2012). Naopak nejméně využívanými službami byly animační služby, tyto služby byly shodně nejméně využívanými pro obě generace X a Y. Toto zjištění je dáno charakterem a specifiky krátkodobého cestovního ruchu. Animační aktivity jsou využívány u déle trvajícího cestovního ruchu (Salazar, 2012). V případě nejméně využívané služby k nákupu přes internet v rámci krátkodobého cestovního ruchu lze zmínit v případě generace X asistenční služby. Toto zjištění může mít příčinu, že mnoho lidí z generace X již je pojištěno či vlastní nějaký druh krytí v případě krátkodobého cestovního ruchu, jak zmiňuje kolektiv autorů Li, Xu, Tang, Wang a Li (2018) nebo autoři Andergassen, Candela a Figini (2013) a proto nevyužívá právě tyto služby, jelikož je již aktivně užívá. Pokud vezmeme v úvahu generaci Y, jednalo se o kongresové služby, generace Y je aktivní a tyto služby jsou využívány v rámci pracovních výjezdů, jak zmiňuje výzkumný tým Celotto, Ellero, a Ferretti (2012) což pro tuto generaci není příliš časté. Obdobné výsledky jako tento výzkum má i studie autorů Jin, Moscardo a Murphy (2017) jenž zkoumala chování napříč generacemi v Číně. Tento rozdíl byl nejvíce znatelný u mladších generací. Díky schopnosti ovládat internet byla tato generace značně zvýhodněna a měla možnost získat více služeb i informací v rámci krátkodobého turismu oproti jiným generacím kupříkladu „ztracené generaci“.

ZÁVĚR

Zkoumání zvyků a pochopení postojů generace Y je velmi důležité pro pochopení, co tato generace chce a potřebuje a zároveň umožňuje této generaci nabídnout služby přímo na míru. Pochopení tohoto chování je důležité nejen pro organizace cestovního ruchu, ať již to jsou cestovní kanceláře a agentury, centrály a pobočky cestovního ruchu, ale i pro informační centra, provozovatele atraktivit, města, obce, kraje i stát, kde je možné vhodně podpořit rozvoj cestovního ruchu investicemi. Tato generace je z části pracující, z části studující, ovšem všichni jsou považováni za dobře finančně zajištěné a brzy bude tato generace hlavní skupinou zaměstnanců na trhu práce. Současné výzkumy generace Y se z velké části věnují právě oblasti zaměstnávání této generace, nikoli jejich nákupnímu chování. Provedený výzkum soustřeďující na krátkodobý cestovní ruch z pohledu generace X a generace Y.

Přičemž cílem výzkumu bylo zjistit, zda generace Y využívá internet k nákupu služeb při účasti na krátkodobém cestovním ruchu více, než generace X a jak generace X a generace Y využívá internet k nákupu služeb při účasti na krátkodobém cestovním ruchu. Hypotéza H1že, generace Y využívá internet k nákupu služeb při účasti na krátkodobém cestovním ruchu více, než generace X. Byla přijata stejně jako hypotéza H2, že Existuje statisticky významná zavilost mezi nižším věkem a ochotou využívat internet k nákupu služeb při účasti na krátkodobém cestovním ruchu. Výzkum dále ukázal na nejvyužívanější služby v rámci jednotlivých generací při využívání krátkodobého cestovního ruchu. Mezi které se řadili v případě generace X služby cestovních kanceláří a welness služby, kdy u generace Y se jednal o ubytovací služby a dopravní služby. Nejčastěji bylo využito prostředků na dálku k nákupu služeb v případě ubytovacích služeb, což je dáno propracovanými a široce dostupnými srovnávacími weby nabízející pohodlný a snadný nákup, přičemž internet byl nejméně využit pro nákup kongresových a animačních služeb což koreluje s následujícím uvedeným zjištěním. Naopak nejméně nakupovanými službami z pohledu generace X se jednalo o animační služby a kulturně společenské služby, kdy generace Y nejméně využila služeb animačních a průvodcovských.

Omezení výzkumu lze spatřovat ve volbě oblasti, kterou je Česká republika. V odlišných oblastech může být dosáhnuto jiných výsledků, avšak tyto výsledky lze vztáhnout k zemím, které si prošli obdobným historickým vývojem jako Česká republika – Polsko, Maďarsko, Slovensko. Určité omezení mohou představovat respondenti samotní, kdy skupina respondentů neobsahovala, některé věkové skupiny. Je důležité zmínit, že výzkum byl právě zaměřen na specifika generace Y a generace X, tudíž výsledky nejsou tímto ovlivněny a rozložení v rámci těchto skupin bylo rovnoměrné. Další omezení lze spatřit v počtu cest, které respondenti absolvují. Nesmíme však opomenout, že vzorek lidí koresponduje s daty, které jsou k dispozici v rámci Czech Tourism a více méně kopíruje tato data. Lze tedy tvrdit, že vzorek respondentů byl vhodný i po této stránce.

LITERATURA

[1] Agentura CzechTourism [online]. Praha: Česká centrála cestovního ruchu, ©2005-2017. Retrieved from: https://czechtourism.cz/

[2] Andergassen, R., Candela, G., & Figini, P. (2013). An economic model for tourism destinations: Product sophistication and price coordination. *Tourism Management, 37*, 86-98. doi:10.1016/j.tourman.2012.10.013

[3] Anderson, E. (2012). Evaluating visualization using cognitive measures. *BELIV'12*, 4.

[4] Bahr, N., & Prendergast, D. (2007). The millennial adolescent. Melbourne: ACER Press.

[5] Bejtkovsky, J. (2016). The Employees of Baby Boomers Generation, Generation X, Generation Y and Generation Z in Selected Czech Corporations as Conceivers of Development and Competitiveness in their Corporation. Journal of Competitiveness, 8(4), 105-123. doi:10.7441/joc.2016.04.07

[6] Bennett, M., & Sani, F. (2008). Childrens subjective identification with social groups: A group-reference effect approach. British Journal of Developmental Psychology, 26(3), 381-387. doi:10.1348/026151007x246268

[7] Bergh, J. V., & Behrer, M. (2016). How cool brands stay hot branding to generation Y. London: Kogan Page.

[8] Bleedorn, G. (2013). Say hello to the millennial generation. ABA Bank Marketing, 45 (1), 24-28

[9] Bolton, R. N., Parasuraman, A., Hoefnagels, A., Migchels, N., Kabadayi, S., Gruber, T., . . . Solnet, D. (2013). Understanding Generation Y and their use of social media: A review and research agenda. Journal of Service Management, 24(3), 245-267. doi:10.1108/09564231311326987

[10] Brown, K. S., Marean, C. W., Herries, A. I., Jacobs, Z., Tribolo, C., Braun, D., . . . Bernatchez, J. (2009). Fire As an Engineering Tool of Early Modern Humans. Science, 325(5942), 859-862. doi:10.1126/science.1175028

[11] Celotto, E., Ellero, A., & Ferretti, P. (2012). Short-medium Term Tourist Services Demand Forecasting with Rough Set Theory. *Procedia Economics and Finance, 3*, 62-67. doi:10.1016/s2212-5671(12)00121-9

[12] Crampton, S. M., & Hodge, J. W. (2011). Generation Y: Unchartered Territory. Journal of Business & Economics Research (JBER), 7(4). doi:10.19030/jber.v7i4.2272

[13] Diamantis, D., Knowles, T., & El-Mourhabi, J. B. (2004). The globalization of tourism and hospitality.: A strategic perspective. International Thomson Publs.

[14] Ellin, A. (2014). The beat (Up) generation. Psychology Today, 47 (2), 56-62.

[15] Grimm, B., et al. (2009), The impact of demographic change on tourism and conclusions for tourism policy, Federal Ministry of Economics & Technology, Berlin. (PDF) Current and Future Trends in Tourism and Hospitality. The Case of Greece.

[16] Hesková, M. (2006). Cestovní ruch: Pro vyšší odborné školy a vysoké školy. Praha: Fortuna.

[17] Chordas, L. (2008). Y New Technology? Best's Review, 109 (6), 88–90.

[18] Jin, H., Moscardo, G., & Murphy, L. (2017). Making sense of tourist shopping research: A critical review. *Tourism Management, 62*, 120-134. doi:10.1016/j.tourman.2017.03.027

[19] Kotler, P., & Armstrong, G. M. (2010). Principles of marketing. Upper Saddle River: Prentice Hall.

[20] Kotler, P., & Keller, K. L. (2007). Marketing management. Praha: Grada.

[21] Kowalczyk-Anioł, J. (2012). Tourism Trends Among Generation Y in Poland. Tourism, 22(2). doi:10.2478/v10106-012-0007-y

[22] Lawrence, J. (2012). Engaging Gen Y: Leading well across the generations. Cambridge, England: Grove Books.

[23] Li, J., Xu, L., Tang, L., Wang, S., & Li, L. (2018). Big data in tourism research: A literature review. *Tourism Management, 68*, 301-323. doi:10.1016/j.tourman.2018.03.009

[24] Mannheim, K. (1952). The Problem of Generations. In P. Kecskemeti (Ed.), Essays on the Sociology of Knowledge (pp. 276-320). London: Routledge and Kegan Paul

[25] Mitchell, V. (1995). Organizational Risk Perception and Reduction: A Literature Review. British Journal of Management, 6(2), 115-133. doi:10.1111/j.1467-8551.1995.tb00089.x

[26] Moscardo, G., Pendergast, D., & Benckendorff, P. (2010). Tourism and generation Y. Cambridge, MA: CAB International.

[27] Oficiální stránky Českého statistického úřadu. Retrieved from http://www.czso.cz/

[28] Oppermann, M. (1995). A Model of Travel Itineraries. Journal of Travel Research, 33(4), 57-61. doi:10.1177/004728759503300409

[29] Prensky, M. (2006). "Don't bother me Mom, I'm learning!": how computer and video games are preparing your kids for twenty-first century success and how you can help!. St. Paul, Minn.: Paragon House, ISBN 1-55778-858-8.

[30] Ryglová, K., Burian, M., & Vajčnerová, I. (2011). Cestovní ruch - podnikatelské principy a příležitosti v praxi. Praha: Grada.

[31] Salazar, N. B. (2012). Tourism Imaginaries: A Conceptual Approach. *Annals of Tourism Research, 39*(2), 863-882. doi:10.1016/j.annals.2011.10.004

[32] Spiro, C. (2006), Generation Y in the Workplace. Defense AT&L, pp. 16-19.

[33] Spitzer, M. (2014). Digitální demence: Jak připravujeme sami sebe a naše děti o rozum. Brno: Host.

[34] Strauss, W., & Howe, N. (1991). Generations: The history of Americas future, 1584 to 2069. New York: William Morrow.

[35] Teller Vision (2009). Know Your Gen Y Customers: Tech Savvy and Harder to Please. (1386), pp. 1-3.

[36] Tsiotsou, R. H., & Goldsmith, R. E. (2012). Strategic marketing in tourism services. Bingley: Emerald Group.

[37] World Tourism Organization UNWTO | Specialized agency of the United Nations. (n.d.). Retrieved from http://www2.unwto.org/

[38] Yeaton, K., & Hall, N. (2008). Expatriates: Reducing failure rates. Journal of Corporate Accounting & Finance, 19(3), 75-78. doi:10.1002/jcaf.20388

[39] Zeithaml, V. (1981). How Consumer Evaluation Processes Differ Between Goods and Services. Chapel Hill.

GREEN MARKETING V PŘÍPADĚ ENVIRONMENTÁLNÍ KRIZE

GREEN MARKETING IN ENVIRONMENTAL CRISIS

Ing. Eva Jaderná, Ph.D., doc. Ing. Jana Přikrylová, Ph.D., Mgr. Radka Picková, Ph.D., Bc. Martin Mlázovský
ŠKODA AUTO Vysoká škola, o. p. s.
Na Karmeli 1457
293 01 Mladá Boleslav
Česká republika
eva.jaderna@savs.cz, jana.prikrylova@savs.cz, radka.pickova@savs.cz, edu.martin.mlazovsky@savs.cz

ABSTRAKT

Příspěvek má za cíl poskytnout pohled na vnímání zelené marketingové komunikace automobilek českými spotřebiteli a především nastínit nutnost komunikace v případě environmentální krize. Zelená řešení jsou velmi diskutovaným tématem, spotřebitele zajímá ochrana životního prostředí a především to, jak automobilky nakládají s přírodními zdroji a jak přistupují k ochraně životního prostředí při své činnosti. Zelená řešení často bývají reakcí na environmentální skandály provázející automobilový průmysl. Automobilky musí se zákazníky komunikovat a reagovat novými opatřeními na krize plynoucí z environmentálních problémů.

KLÍČOVÁ SLOVA

Zelená řešení, green marketing, environmentální krize, emise, automobilový průmysl

ABSTRACT

The paper aims to present consumers´ perception of green marketing communications by Czech consumers in automotive industry, stressing necessity of the crisis communication in case of any environmental crisis. Green solutions have been discussed over the time globally and current customers becoming more and more interested in car producers green behaviour. As we have witnessed many scandals connected with the air pollution, the automotive producers should react and present their results of the green solutions. They should communicate that they have taken care about environment from their first purchase of natural resources through the car production ending with the after-sale care; and the final recycling at the end of the car life.

KEY WORDS

Green solutions, green marketing, environmental crisis, emissions, pollution, automotive industry

ÚVOD

Automobilový průmysl je ostře sledovaným odvětvím národního hospodářství v souvislosti se znečišťováním životního prostředí. Jsou neustále zpřísňována opatření týkající se emisí automobilů, emisí při jejich výrobě a automobilky jsou také pod drobnohledem v rámci dalších zelených řešení, kterými se nejen snaží eliminovat dopady své činnosti na životní prostředí, ale také naopak přispět k jeho obnově a zlepšení.

Evropské regulace se zaměřují především na emise CO_2 , přičemž lze uvést údaj týkající se osobní dopravy, která v rámci emisí CO_2 představuje pouze 0,2 % na světové tvorbě

CO_2 ,
a to včetně výroby celého vozu. (Dvořák, 2016) Přesto je na automobilové společnosti neustále vyvíjen tlak k výrobě vozů s co nejnižší mírou emisí CO_2 . Tyto regulace jsou navíc v některých státech Evropské unie ještě přísnější, a tak např. v Nizozemí musí automobilky každým rokem reagovat na stále se zpřísňující limity emisí CO_2 , které pak určují daňové zatížení vozů. (Přikrylová, Jaderná, 2016)

Tento neustálý tlak některé automobilky ve vývoji nových vozů nezvládají a jejich snaha tyto regulace obejít pramení v environmentální skandály typu Dieselgate. Tyto skandály velmi negativně ovlivňují pozici značky na trhu a důvěru spotřebitelů v to, co automobilky v rámci svého green marketingu komunikují.

1. KOMUNIKACE ZELENÝCH ŘEŠENÍ V AUTOMOBILOVÉM PRŮMYSLU

V 60. letech minulého století se začaly rozvíjet mnohé regulace, v souvislosti se vznikajícími principy environmentalismu. (Newton, Cantarello, 2014) V dnešní době je nejen významné environmentální právo, ale i environmentální regulace ve výrobě. Lze jmenovat normy ISO (ISO 26000, ISO 50001 a ISO 14001), které popisují postup provádění činnosti a definují požadavky pro danou problematiku. Získání certifikátu v některých zemích je dokonce legislativně vyžadováno. V automobilovém průmyslu jsou povinné certifikace ISO 9000 popisující systém řízení kvality a ISO 14000 týkající se environmentálního managementu (směrnice 2009/1/ES).

Automobilový průmysl je dále zatěžován regulacemi, které souvisí především s emisemi CO_2 . V Evropské unii jsou emise regulovány emisní normou Euro. Ta stanovuje maximální množství emitovaných částic. Testy jsou však prováděny v laboratorních podmínkách, které nejsou zcela relevantní vzhledem k tomu, že není možné zohlednit povětrnostní podmínky, stoupání, zapojení dalších funkcí (topení, klimatizace), narušení aerodynamiky střešním boxem aj.

Nařízení ES č. 443/2009 navíc stanovuje maximální flotilové hodnoty CO_2 nově vyrobených vozů v Evropské unii. Aktuálně činí 130 g/km, od roku 2020 má být pouze 95 g/km, což nutí automobilky působící na evropském trhu využívat elektrický či vodíkový pohon ve své produkci.

Emise výfukových plynů řeší také samostatně státy Evropské unie či dokonce velká města některých zemí. Německý Spolkový správní soud umožnil vydávat vyhlášky upravující vjezd automobilů se staršími motory, čehož využilo jako první město Hamburk, následují Cáchy a Stuttgart. (Havlíček, 2018; Burger, 2018; Jankov, 2018) Jednání o zavedení podobného opatření probíhá v Düsseldorfu, Berlíně, Kolíně nad Rýnem, Mohuči, Essenu, Kasselu, Freiburgu, Dortmundu a Mnichově. (Česká televize, 2018) Zákazy vjezdu vozů vyrobených před rokem 1997 se ale týkají také Paříže, která dokonce do roku 2020 plánuje některé ulice vyhradit pouze pro elektromobily. Velmi diskutované jsou také dieselové motory, jimž chce vjezd zakázat Madrid, Londýn nebo Atény. (Česká televize, 2017)

S ohledem na tyto regulace, vyhlášky je otázka emisí CO_2 stále diskutovanějším tématem, které vzbuzuje rozporuplné reakce veřejnosti. Trendem dnešní doby je zelené chování a smýšlení, proto se jeví jako podstatné řešit zelenost právě i v automobilovém průmyslu.

1.1 Green marketing v automobilovém průmyslu

Vzhledem k negativnímu postoji veřejnosti vůči činnosti automobilek jako jednomu z největších znečišťovatelů životního prostředí se automobilové společnosti snaží komunikovat svou zelenost. Využívají nástroje green marketingu. Ten je vnímán jako spojení klasického marketingu a ochrany životního prostředí. Jde tedy o dosažení zisku i udržitelnosti zároveň. (Baker, 2003)

Automobilky tak provádějí změny nejen ve vývoji produktu, ale také marketingové komunikaci tak, aby byly vnímány jako společensky odpovědné. Jejich reputace zeleně smýšlející společnosti je v dnešní době klíčová. Jako příklad lze uvést společnost ŠKODA AUTO se svou strategií „GreenFuture“ nebo Toyotu se svým projektem „Toyota Environmental Challenge 2050“.

Automobilky se zaměřují na prezentaci ekologických aspektů svých vozů a v rámci svého CSR reportu uvádějí mnohá zelená řešení spojená s vývojem a produkcí automobilů. Nejčastějšími zelenými řešeními v automobilovém průmyslu jsou redukce odpadů, vývoj produktů co nejméně znečišťující životní prostředí, ekologická řešení stávajících produktů, transformace a zlepšení výrobních procesů, rozvoj zeleného dodavatelského řetězce nebo kontrola dopadu využití produktu v rámci celého dodavatelského řetězce a využívání obnovitelných zdrojů (Mahamuni a Tambe, 2014)

Všechna tato zelená řešení se automobilky snaží co nejvíce komunikovat tak, aby byly vnímány jako společensky odpovědné a jejich produkty jako co nejvíce ekologické. Důležitá je však v tomto kontextu důvěra spotřebitelů v takto komunikované aspekty. Spotřebitelé se stávají rezistentní vůči některým nástrojům marketingové komunikace, ale zelený marketing může v určitých ohledech být zajímavým a poutavým pro stále více environmentálně edukované české spotřebitele.

Spotřebitel vnímá green marketing různě. Někdo ho považuje pouze za reakci na environmentální regulace nebo jako přijetí odpovědnosti firem. Oproti tomu stojí spotřebitelé, kteří jsou skeptičtí a považují green marketing pouze za možnost, jak prodat více s ohledem na zelený trend současnosti. (Arseculeratne, Yazdanifard, 2013).

Zde je důležité poznat současného spotřebitele, jeho postoje, preference a především reakce na marketingové podněty plynoucí od společností, které jsou primárně vnímány jako jedny z největších znečišťovatelů životního prostředí.

2. METODIKA

Článek prezentuje dílčí výsledky marketingového výzkumu, který byl realizován v rámci projektu studentské grantové soutěže s názvem Zelený produkt automobilek a jeho vnímání různými generacemi českých spotřebitelů. Tento projekt je v první fázi zaměřen na výzkum postojů různých generací českých spotřebitelů vůči zeleným produktům a zeleným aktivitám firem v automobilovém průmyslu. Je stěžejní poznat reakci spotřebitelů na zelená řešení automobilek, abychom mohli využívat vhodné nástroje green marketingu.

Se stále rostoucím zájmem o emisní skandály celosvětových automobilek, je nutné mimo klasické nástroje green marketingu řešit krizovou komunikaci v případě environmentální krize. Jak může firma zachovat svou zelenost v myslích zákazníků využitím vhodných komunikačních nástrojů.

Nejprve bylo nutné zjistit, jak spotřebitelé vnímají zelená řešení automobilek a zda jim v souvislosti s komunikací své zelenosti důvěřují. V rámci marketingového výzkumu provedeného formou dotazníkového šetření byla ke sběru dat využita externí agentura, která oslovila reprezentativní vzorek českých respondentů, čímž autorům pomohla k získání

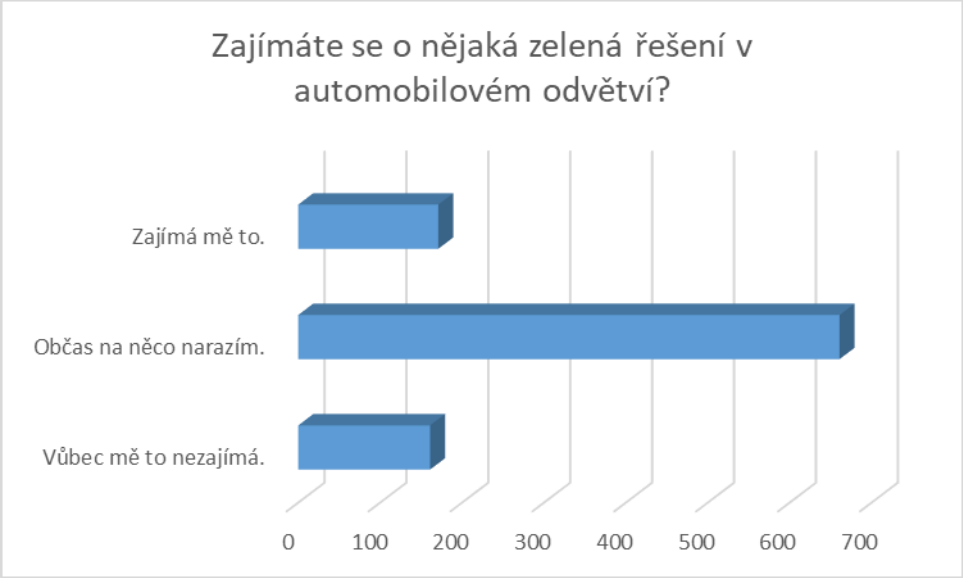
relevantních dat. Na základě úvodního briefu a přímé součinnosti s agenturou vznikl dotazník, který měl mimo jiné zodpovědět výzkumnou otázku: „Jak český spotřebitel vnímá zelená řešení automobilek a jejich komunikaci?“

Data byla sebrána během května 2018, kdy bylo osloveno více než 1000 respondentů. Přesně 1000 dotazníků pak bylo využito při analýze a interpretaci dat. V rámci tohoto článku, kde cílem je vnímání zelených řešení českými spotřebiteli a následně to, jak důvěřují zelené komunikaci, bude k interpretaci dat využita relativní, resp. absolutní četnost sledovaných proměnných.

3. VÝSLEDKY

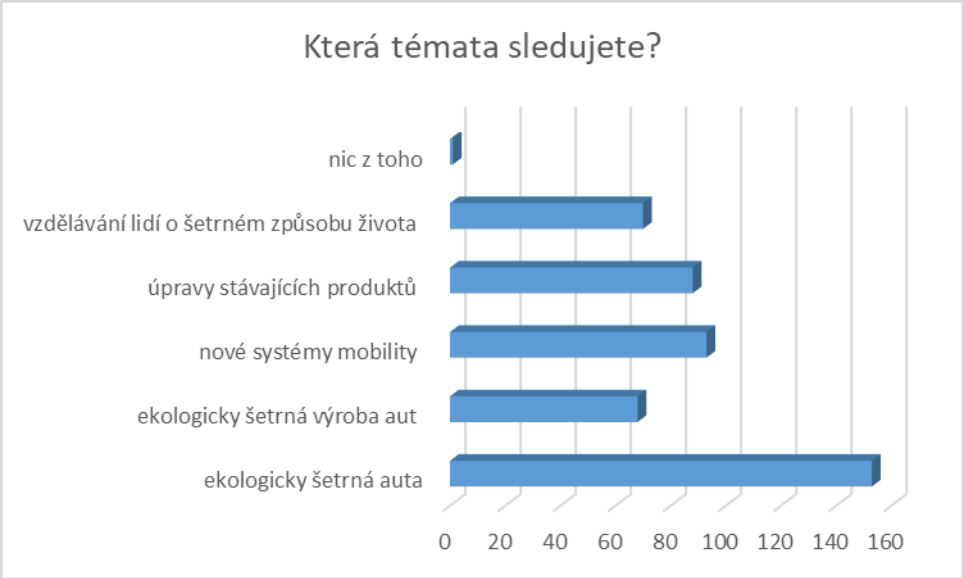
Český spotřebitel je svým postojem vůči environmentálním otázkám velmi specifický. Proto je nutné nejprve poznat, jak reaguje na podněty green marketingu, které jsou v automobilovém průmyslu velmi intenzivní.

První ze zásadních otázek se týkala zájmu o zelená řešení, která automobilky ve svém působení zavádějí. Jak naznačuje obrázek 1, aktivně hledá tyto informace pouze 171 (17 %) respondentů a 661 (67 %) z 1000 oslovených respondentů přiznává, že občas na nějaké informace narazí, ale aktivně je nevyhledává. Tedy nelze říci, že by potenciální zákazníci projevovali aktivní zájem o to zjistit, zda automobilky zelená řešení ve své činnosti zavádějí.



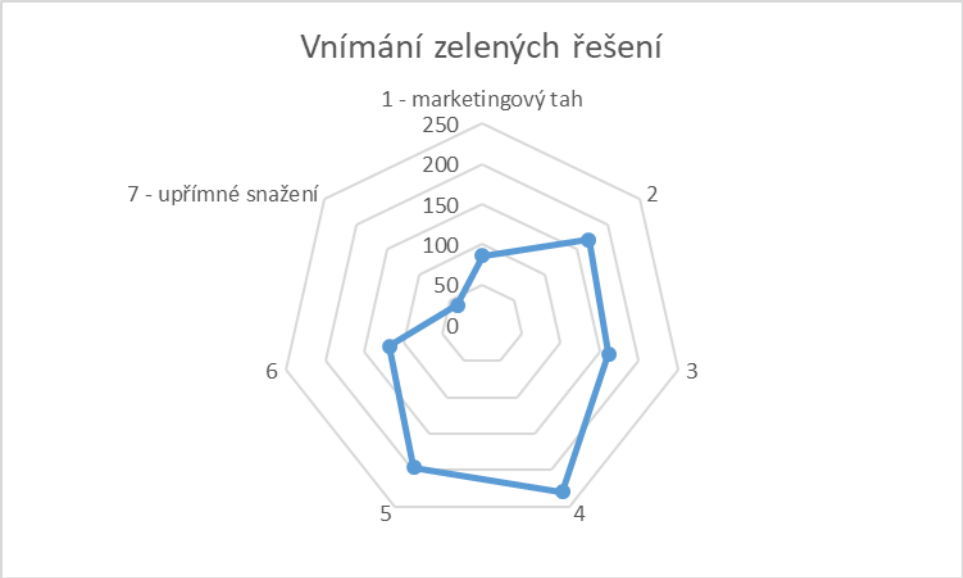
Obr. 1 Zájem o zelená řešení automobilek

Zájmem autorů bylo také zjistit, která témata spotřebitelé nejčastěji sledují (viz obrázek 2). 89 % spotřebitelů, kteří se zajímají o zelená řešení v automobilovém odvětví, má zájem o informace týkající se ekologicky šetrných aut, mezi které řadíme hybridy, vozy na vodíkový pohon atp. Ostatní sledované aspekty jsou pro spotřebitele zajímavé podobně (v rozmezí 40 – 55 %).



Obr. 2 Sledovaná témata

S ohledem na účinnost green marketingu je však stěžejní odpověď na otázku, jak spotřebitelé vnímají zelená řešení firem. Respondenti měli na škále od 1 do 7 rozhodnout, zda vnímají zelená řešení jako marketingový tah (1) nebo upřímné snažení automobilek (7). Paprskový graf (obrázek 3) naznačuje, že čeští spotřebitelé spíše inklinují k tomu, že zelená řešení považují za marketingový tah. Konkrétně pouze 39 (4 %) respondentů vnímá zelená řešení automobilek jako upřímné snažení (na škále označilo 7). 230 (23 %) respondentů označilo 4, tedy číslo ve středu škály naznačující nejasný postoj.



Obr. 3 Vnímání zelených řešení spotřebiteli

Otázkou tedy zůstává, do jaké míry je snažení automobilek v zavádění zelených řešení přínosné pro vnímání jejich firmy jako zeleného producenta. Tyto výsledky poukazují na nevalný zájem a také nízkou důvěru v zelená řešení automobilek. To ztěžuje také následnou komunikaci v případě environmentálních krizí, se kterými se automobilky v posledních letech potýkají a na které musí reagovat.

4. GREEN MARKETING V PŘÍPADĚ ENVIRONMENTÁLNÍ KRIZE

Výsledky výzkumu poukazují na nepříliš zásadní význam zelených řešení automobilek pro české spotřebitele. Navíc český spotřebitel spíše inklinuje k tomu považovat zelená řešení za marketingový tah, což jejich důvěru v zelenost snižuje.

Významným problémem, se kterým se nyní trh automobilů potýká, jsou emisní skandály. Automobilový průmysl je významně zatížen regulacemi, které řeší striktně emise CO_2 při užívání vozů (viz kapitola 1). Výrobci se snaží reagovat vývojem nových vozů, ale některé limity jsou natolik tvrdé, že se pokusili v minulosti manipulovat se softwary vykazujícími emise. První vyšetřování započalo v roce 2014 v koncernu Volkswagen, který se později přiznal k „upravujícímu softwaru“. Postiženo bylo 11 milionů vozů celého koncernu (1,2 milionů vozů ŠKODA). (ČTK, 2016)

Při dalších šetřeních se ukázalo, že falsifikace údajů není problém jedné automobilky, ale je to obecná praxe dalších značek, jako jsou Mercedes, BMW, Audi, Mitsubishi, Opel nebo Fiat. Každá z firem přistupovala k úpravě emisí svým originálním způsobem, nicméně byly touto environmentální krizí zasaženy.

Jak tedy v případě problémů vzniklých v souvislosti s ochranou životního prostředí postupovat? Koncern Volkswagen byl zpočátku velmi nekomunikativní a naopak popřel jakékoliv manipulace s měřením emisí. Posléze ale svou chybu přiznal a začal řešit vzniklé škody, přislíbil odkoupit nebo opravit postižené vozy a nabídl významné odškodné.

Nejdůležitějším aspektem krizové komunikace je znovunastolení důvěry. Důvěra je klíčový element podporující fungující vztah se zákazníkem (Kang a Hustvedt, 2014) a pokud je v případě nenadálé environmentální krize ohrožena, je to zásadní moment pro PR manažery. Důvěra a image se buduje desítky let, zatímco zničit ji lze snadno, levně a rychle. V případě emisních skandálů je situace na českém automobilovém trhu vážnější také tím, že důvěra českých spotřebitelů v zavádění zelených řešení automobilek čistě z vlastního přesvědčení je velmi malá. Proto je nutné brát v úvahu jejich postoj a především s nimi komunikovat a dávat jasná stanoviska. Na druhou stranu automobilkám nahrává fakt, že i sami zákazníci již vnímají některé regulace a stále se snižující limity emisí za přehnané.

Přesto je nutné reagovat na vzniklou situaci a nepraktikovat strategii mrtvého brouka. Rozhodně nelze v globalizovaném světě, nabízejícím komunikaci mnoha kanály, počítat s tím, že se krize samovolně utiší. Emisní skandály se týkaly desítek milionů vozů napříč všemi značkami. O zákazníky, kteří si vůz zakoupili, je nutné znovu bojovat.

V souvislosti s green marketingem je vhodné, aby automobilky o problému emisí více hovořily. Aby komunikovaly význam problému a vlastní zelená řešení, která vedou k tomu, aby minulá krize opět nenastala. Český spotřebitel přišel do styku s informacemi o dieselgate a pokud se rozhoduje o koupi nového vozu, marketéři by měli být schopni komunikovat zelená řešení v celém procesu od nákupu po recyklaci vozu. Nabízí se celá řada nástrojů green marketingu. Zákazník musí znovu získat důvěru ve vlastní snahu automobilek o zelenost své činnosti a opravdovost zelených řešení.

Důsledky emisního skandálu značky VW byly rozsáhlé jako snížení ceny akcií nebo snížení zisku v roce 2015, nicméně prodeje koncernu jako celku za prvních 9 měsíců roku 2016 rostly o 2,4 %. (ČTK, 2016b) Z toho je patrné, že i významné skandály nemusí být v případě dobré krizové komunikace likvidační, ale podmínkou je přiznat pochybení, sjednat nápravu a také ukázat opatření v celém procesu od vývoje po likvidaci vozů jako ekologické.

ZÁVĚR

Green marketing má v dnešním „zeleném světě“ své opodstatnění. Zákazníci čekají komunikaci produktů, při níž je kladen důraz na environmentální aspekty. Vyhledávají produkty s ekologickým značením. Co se týče zájmu českých spotřebitelů o zelená řešení automobilek, není to pro většinu téma, které by aktivně vyhledávali. Nicméně přicházejí s těmito informacemi do styku a zajímají je především ekologicky šetrné vozy. Čeští spotřebitelé na druhé straně ale příliš nedůvěřují tomu, že automobilky provádějí zelená řešení z jiného důvodu, než je nutná regulace a marketingový záměr. Jsou vůči komunikaci zelenosti celkem skeptičtí.

Důvodů k tomuto postoji může být mnoho. Jedním z nich je také stále aktuální emisní skandál koncernu Volkswagen, do kterého patří také největší český producent vozů ŠKODA AUTO, ale i dalších značek, které patří mezi často nakupované. Skandály jednotlivých značek vytvořily významnou environmentální krizí pro celý automobilový průmysl. Její řešení by mělo být příkladem toho, jak důležitá je pravdivá, důvěryhodná komunikace a reakce producentů na vzniklý problém.

V případě nejen environmentální krize je nejúčinnější zbraní marketérů komunikace. Firmy musí mít plán krizové komunikace a musí reagovat nejen prezentací nových opatření, ale také dlouhodobých zelených řešení. Musí si také uvědomit a změřit sílu pocitu nedůvěry v očích zákazníků a soustředit se na následnou komunikaci, která by měla mít za cíl obnovit důvěru v oblíbenou značku vozů.

PODĚKOVÁNÍ

Příspěvek byl řešený v rámci projektu SGS/2018/01 Jaderná Zelený produkt automobilek a jeho vnímání různými generacemi českých spotřebitelů na katedře Marketingu a Managementu ŠKODA AUTO Vysoké školy, o. p. s.

Literatura

[1] ARSECULERATNE, D., YAZDANIFARD, R. How Green Marketing Can Create a Sustainable Competitive Advantage for a Business. *International Business Research*, 2014, vol. 7, iss. 1, pp. 130-137. ISSN 1913-9004

[2] BAKER, J. *The marketing book*. 5. vydání, Boston: Butterworth-Heinemann, 2003. ISBN 0750655364

[3] *Burger* [online]. German court paves way for German city of Aachen to ban diesel cars, poslední úpravy 8. 6. 2018, [cit. 2018-8-26]. Dostupné na WWW: <https://www.reuters.com/article/us-germany-emissions-aachen/german-court-paves-way-for-german-city-of-aachen-to-ban-diesel-cars-idUSKCN1J41D9>

[4] *Česká televize* [online]. Germany: V Hamburku začal platit zákaz vjezdu do centra pro auta se starým dieselovým motorem, poslední úpravy 31. 5. 2018, [cit. 2018-8-26]. Dostupné na WWW: <https://ct24.ceskatelevize.cz/ekonomika/2495167-v-hamburku-zacal-platit-zakaz-vjezdu-do-centra-pro-auta-se-starym-dieselovym/>

[5] *Česká televize* [online]. Města bez dieselů? V Německu řeší zákaz 16 soudů, ve zbytku Evropy je trend podobný, poslední úpravy 15. 8. 2017, [cit. 2018-8-26]. Dostupné na WWW: <https://ct24.ceskatelevize.cz/ekonomika/2211514-mesta-bez-dieselu-v-nemecku-resi-zakaz-16-soudu-ve-zbytku-evropy-je-trend-podobny/>

[6] *Česká tisková kancelář* [online]. Jaká Dieselgate? Prodeje VW Group rostou nejvíce od emisního skandálu, poslední úpravy 14. 10. 2016b, [cit. 2018-8-26]. Dostupné na WWW: <http://www.auto.cz/jaka-dieselgate-prodeje-vw-group-rostou-99238>

[7] *Česká tisková kancelář* [online]. Rok po začátku Dieselgate žalují Volkswagen další spolkové země. Koncern prodal více aut než loni, poslední úpravy 18. 9. 2016, [cit. 2018-8-26]. Dostupné na WWW: <https://zpravy.aktualne.cz/ekonomika/auto/rok-po-zacatku-dieselgate-zaluji-volkwagen-dalsi-spolkove-ze/r~fa0458f27d5f11e682470025900fea04/>

[8] *Dvořák* [online]. Automobilky se chystají na nové testy emisí, ale předpisy se stále mění, poslední úpravy 14. 11. 2016, [cit. 2018-8-26]. Dostupné na WWW: <http://auto.idnes.cz/hrdlicka-co2-vyvoj-motor-skoda-emise-dbx-/automoto.aspx?c=A161109_005723_automoto_fdv/>

[9] *Havlíček* [online]. Německá města mají zelenou. Mohou zakázat vjezd starších dieselů, poslední úpravy 21. 5. 2018, [cit. 2018-8-26]. Dostupné na WWW: <https://www.autorevue.cz/zakaz-dieselu-v-nemecku-2018>

[10] *Jankov* [online]. Další vyhánění dieselů v Německu, nechce je automobilový Stuttgart, poslední úpravy 17. 7. 2018, [cit. 2018-8-26]. Dostupné na WWW: <https://auto.idnes.cz/diesel-stuttgart-zony-zakaz-vjezdu-dbk-/automoto.aspx?c=A180717_072413_automoto_Fdv/>

[11] KANG, J., HUSTVEDT, G. Building Trust between Consumers and oprorations: The Role of Consumer Perceptions of Transparency and Social Responsibility. *Journal of Business Ethics*, 2014, vol. 125, iss. 2, pp. 253–265. ISSN 0167-4544

[12] MAHAMUNI, A., TAMBE, M. Green Marketing in Automobile and Ancillary Industry: Issues and Implications. *Journal of Commerce and Management Thought*, 2014, vol. 5, iss. 3, pp. 363-377. ISSN 0975-623X

[13] NEWTON, A., CANTARELLO, E. *An Introduction to the Green Economy: Science, Systems and Sustainability*, New York: Routledge, 2014. ISBN 978-0-415-71160-9

[14] PŘIKRYLOVÁ, J., JADERNÁ, E. Green Marketing Practice of Car Producers. In: *INPROFORUM 2016 – Threatened Europe? Socio-Economic and Environmental Changes: 10th International Scientific Conference: November 3–4, 2016, České Budějovice, Czech Republic*. České Budějovice: Jihočeská univerzita v Českých Budějovicích, 2016. s. 241-245, ISBN 978-80-7394-607-4

PORANĚNÍ OBLIČEJE ČLOVĚKA PO ZÁSAHU PLYNOVKOU

FACE INJURY CAUSED BY GAS EXPANSIVE GUNSHOT

doc. Ing. Ludvík Juříček, Ph.D. [1], Ing. Martin Ficek [2], MUDr. Norbert Moravanský, PhD. [3], JUDr. Ing. Olga Vojtěchovská, Ph.D. [4]

[1]Ústav bezpečnosti, Vysoká škola Karla Engliše, a.s.,
Mezírka 775/1, 602 00 Brno, Česká republika,
telefon: +420 728 232 698, e-mail: ludvik.juricek@vske.cz

[2]Ústav bezpečnostního inženýrství, Fakulta aplikované informatiky, Univerzita Tomáše Bati ve Zlíně,
Nad Stráněmi 4511, 760 05 Zlín, Česká republika,
telefon: +420 731 829 550, e-mail: ficek@fai.utb.cz

[3]Ústav súdneho lekárstva, Lekárska fakulta, Univerzita Komenského v Bratislave, Sasinkova 4,
811 08 Bratislava, Slovenská republika,
telefon: +421 905 160 789, e-mail: info@lekarznalec.sk

[4]Katedra bezpečnosti a práva, Vysoká škola regionálního rozvoje a Bankovní institut – AMBIS, a.s. Praha,
Lindnerova 575/1, 180 00 Praha 8, Česká republika,
telefon: +420 603 300 064, e-mail: o.vojtechovska@atlas.cz

ABSTRAKT

Popis kazuistiky reálného střelného poranění člověka plynovou pistolí turecké výroby zn. EKOL model AGENT ráže 9 mm P.A.B. v oblasti obličeje, ke kterému došlo v roce 2015 v Ostravě při fyzickém incidentu mezi dvěma muži středního věku v uzavřeném prostoru chodby činžovního domu. V příspěvku jeho autoři provedli hodnocení způsobu použití krátké plynové zbraně proti člověku a balistickou analýzu ranivého potenciálu zplodin hoření akustické a plynové nábojky stejné ráže při střelbě z relativní blízkosti (střelba do 0,5 m). V závěru je provedeno soudnělékařské hodnocení klinické závažnosti střelného poranění způsobeného akustickou nábojkou a podrobná analýza rizik použití posuzovaného zbraňového systému proti člověku.

KLÍČOVÁ SLOVA

Expanzní zbraň, plynovka, plynová nábojka, akustická nábojka, ranivý potenciál, ranivý účinek, zraňující agens, výmetná náplň, chemická krystalická látka.

ABSTRACT

The paper reveals case report from 2015 of real gas expansive face gunshot wound caused by Turkish gas expansive gun EKOL, model Agent cal. 9 mm P.A.B. The incident passed in Ostrava, Czech Republic while two middle-age men conflict at the close apartment hall. The authors evaluated the manner of gas expansive gun use against man, ballistic analyze of wounding potential of combustion expansive products of acoustic and gas cartridge the same caliber in close distance (up to 0.5 m). The conclusion is also the medico-legal evaluation of wound range and risks of gas expansive gun use against human being.

KEY WORDS

Expansive gas gun, gun cartridge, acoustic cartridge, wounding potential, wounding effect, wounding agent, expansive cartridge, chemical crystal substance.

ÚVOD

Článek tematicky navazuje na naše příspěvky přednesené na konferencích pořádaných FLKŘ UTB ve Zlíně z předešlých let a orientuje se na případ kazuistiky reálného střelného poranění obličeje člověka plynovkou, kdy střelba byla vedena z relativní blízkosti, jako obrana proti fyzickému násilí jiné osoby. K případu střelného poranění muže středního věku došlo v září 2014 v Ostravě a byl projednáván KS v Ostravě.

Základním podkladem k vypracování společného příspěvku se stal ZP č. 008/2015, který byl na žádost advokáta obžalovaného, vypracován prvním autorem příspěvku, a to ve znaleckém oboru střelivo a výbušniny, se specializací na ruční palné zbraně a jejich účinky, munici a její účinky, ranivou balistiku.

Úloha znalce, při posouzení uvedeného případu, byla vymezena otázkami advokáta na znalce a spočívala ve vyjádření se ke způsobu použití plynové zbraně při incidentu ze dne 11. 9. 2014 na místě činu (MČ), jak jej popisují poškozený v protokolu o jeho výslechu a obviněný v protokolu o výslechu. Která z výpovědí těchto osob je z hlediska znalce technicky přijatelnější? Dále měl znalec popsat rozdíly v účincích akustické nábojky a plynové nábojky s dráždivou chemickou látkou dané ráže, včetně uvedení informací, které jsou z hlediska účinků těchto nábojek laickou veřejnosti dosažitelné. Při vlastních zjištěních byla pozornost znalce věnována analýze rizik, která vznikají v souvislosti s nevhodným použitím krátkých expanzních zbraní v rámci ochrany osob a majetku jejich uživateli [1].

1. POPIS PŘEDMĚTNÉ UDÁLOSTI JEJÍMI ÚČASTNÍKY

Při hodnocení předmětné události znalec vycházel ze spisového materiálu [2], který byl tvořen Úředními záznamy o podání vysvětlení obviněného a poškozeného (svědka) z 11. a 12. 9. 2014 a Protokoly u výslechu obviněného a poškozeného (svědka) z 11. a 17. 2. 2015. Obsahové zaměření výpovědí obou účastníků bylo směrováno na popis událostí, ke kterým došlo na MČ tak, jak je oba vnímali ze svého pohledu. Specifickým znakem tohoto případu byla skutečnost, že na jejím začátku vystupoval **poškozený** (svědek) jako agresor (útočník), který běh popisovaných událostí uvedl do pohybu a **obviněný** se ocitl v roli oběti jeho agrese.

1.1 Popis předmětné události obviněným

Obviněný uvedl, že si plynovou pistoli zakoupil pouze ke své ochraně. V komoře této pistole má vždy vložen slepý náboj se zelenou hlavičkou, který působí pouze tlakovou vlnu. Další náboje uložené v zásobníku jsou již pepřové s červenou hlavičkou, pro případ, že by útočník i přes varovný výstřel pokračoval v dalším útoku na mou osobu. Svou plynovou pistoli dnes použil poprvé k varovnému výstřelu, aby odradil cizího muže před dalším fyzickým útokem vůči své osobě.

Dále popisuje vlastní incident s poškozeným tak, že k němu došlo na chodbě domu, kde bydlí, v okamžiku, kdy vystoupil z výtahu v přízemí. Došlo ke vzájemnému fyzickému kontaktu, kdy jej poškozený uchopil pravou rukou za krk a levou se napřahoval k úderu pěstí. Naše vzájemné postavení bylo takové, že jsme stáli čelem k sobě, ale ne přímo, kdy já jsem stál spíše po jeho pravém boku. Nevěděl jsem, jak se bránit, tak mne napadlo, že vystřelím z plynové pistole, kterou mám v tašce a že by se mohl rány leknout, a zatím co on mě držel, tak jsem dal ruku do své příruční tašky a při vytahování jsem ji odjistil a natáhl kohoutek. Po jejím vytažení z tašky, jsem vystřelil. Jak jsem vystřelil, tak vůbec nemám potuchy, kam

střela mohla jít. **V okamžiku výstřelu pistole mohla být svým ústím v poloze někde pod pravým ramenem útočníka?**

1.2 Popis předmětné události poškozeným

Co se týče pana obžalovaného, tak si myslím, **že měl zbraň (plynovou pistoli) s největší pravděpodobností již v ruce ve chvíli, kdy výtah přijel do přízemí a po otevření roztahovacích dveří výtahu, vystřelil z této zbraně**, kdy si nevybavuji, zda šlo o jeden nebo dva výstřely, a to přímo do mého obličeje, čímž mě v danou chvíli úplně paralyzoval. Tento muž mě zcela bezdůvodně a beze slova varování napadl na chodbě v přízemí domu u výtahu a zranil v obličeji.

Na dotaz, zda poškozený (svědek) pana obviněného před výtahem nějak napadl, uvedl, že ne, vůbec jsem se jej nedotkl, ihned po mě vystřelil.

2. ODBORNÁ VYJÁDŘENÍ DALŠÍCH ÚČASTNÍKŮ ŘÍZENÍ

2.1 Lékařské zprávy ošetřujících lékařů

Popis charakteru zranění poškozeného a jeho klinická závažnost provedli dva lékaři, specialisté *(MUDr. Tomáš Veis a MUDr. Radovan Hranický)* ve svých lékařských zprávách [2] s těmito závěry:

- poškozený utrpěl zranění v souvislosti s napadením známým pachatelem. Bez předchozího konfliktu nečekaně střelen z těsné blízkosti plynovou pistolí do oblasti obličeje a obou očí,
- došlo k závažnému pohmoždění obou očních koulí, mnohočetná cizí tělíska v oblasti rohovek i spojivek obou očí (zejména na pravém oku), lehké popálení kůže obličeje. Vznik možné komplikace v podobě reálného nebezpečí poúrazového odchlípení sítnice, zejména vpravo.
- způsob vzniku poranění a jeho závažnost odpovídá okolnostem tak, jak je uvádí poškozený.

2.2 Znalecké posudky znalců z oboru zdravotnictví, odvětví soudní lékařství

Popis charakteru střelného poranění a mechanismu jeho vzniku provedli postupně dva soudní lékaři ve svých ZP *MUDr. Margita Smatanová, Ph.D.* z 23. 1. 2015 a *prof. MUDr. Miroslav Hirt, CSc.* z 14. 4. 2015 s následujícími závěry [2]:

- ZP z oboru zdravotnictví, odvětví soudní lékařství *MUDr. Margity Smatanové, Ph.D.* z 23. 1. 2015.

Ve svém znaleckém posudku vycházela z odborného vyjádření *MUDr. Radovana Hranického,* ordinace všeobecného praktického lékaře Vratimov ze dne 6. 11. 2014. Jedná se o závažné zhmoždění obou očních koulí, mnohočetná cizí tělíska v oblasti rohovek a spojivek obou očí, lehké popálení kůže obličeje. Porucha vidění, bolesti a řezání obou očí, slzení, nízká zraková výdrž, nyní s časovým odstupem od poranění dle odborného nálezu nebezpečí odchlípení sítnice, zejména na pravém oku, nutné lokální kapání ošetřování, maximální šetření zraku a dále žádná fyzická zátěž.

Lokalita objektivizovaných zranění svědčí pro vzájemné čelní postavení střelce a poškozené osoby v době výstřelu z předmětné plynové zbraně, a to z relativní blízkosti s namířením dlouhé osy hlavně do oblasti obličeje více vpravo.

- ZP z oboru zdravotnictví, odvětví soudní lékařství č. 2954/263 *prof. MUDr. Miroslava Hirta, CSc.* z 14. 4. 2015.

K předmětu znaleckého zkoumání se váže odpověď na otázku č. 1 výše uvedeného znalce, zda objektivně zjištěná poranění poškozeného mohla být způsobena při průběhu útoku popisovaného obviněným v protokolu o jeho výslechu, čj. KRPT-260501-37/TČ-2014-070771-0103 ze dne 11. 2. 2015?

Ano, popisované zranění naprosto odpovídá výstřelu z krátké vzdálenosti ze zbraně nabité slepým nábojem. I když je evidentní, že vzdálenost střelby do 0,5 metru (což by tak asi mohlo být) je naprosto dostačující, aby vzniklo projednávané zranění. **Definitivní posouzení účinnosti zbraně na danou vzdálenost nemůže dělat lékař, ale balistik.**

2.3 Odborné vyjádření z oboru kriminalistika, odvětví balistická expertíza

Ze dne 13. 2. 2015, čj. KRPT-4806-1/KT-2014 [2].

- *Ke zkoumání bylo předloženo:*

Pistole, zásobník, 5 ks nábojek, 1 ks vystřelená nábojnice.

- *Zkoumáním má být zjištěno:*

- určit druh a kategorii předložené zbraně, ráži, značku, typ, původ, dobu výroby a charakteristiku,
- zjistit technický stav střelné zbraně, její způsobilost ke střelbě, činnost mechanismů, možnost nežádoucího výstřelu, dodatečné úpravy nebo opravy, případně výskyt závad nebo poškození,
- zjistit případnou přesnost střelby zbraně,
- zda s předloženou zbraní nebyl spáchán neobjasněný trestný čin,
- určit druh, ráži, původ a stav zajištěného střeliva,
- posoudit způsob výroby nebo úprav předložených nábojnic,
- zda je předložené střelivo použitelné v předloženém typu zbraně,
- porovnat nábojnici v ÚSBS.

- *Výsledek zkoumání:*

- expanzní zbraň turecké výroby v provedení SA samonabíjecí pistole, zn. EKOL model AGENT ráže 9 mm P.A.B., výrobního čísla EVL-12120543 s příslušným zásobníkem naplněným 5 ks nábojek, pistole vyrobená v roce 2012,
- prohlídkou mechanismů zbraně nebylo v jejich činnosti zjištěno závad a nebyly zjištěny stopy po prováděných úpravách, které by změnily její původní charakter. Orientační pádová zkouška s negativním výsledkem vyloučila možnost nechtěného výstřelu. Způsobilost zbraně ke střelbě byla ověřena zkušební střelbou – zbraň v předloženém stavu je schopná střelby,
- spáchání dosud neobjasněného TČ nebylo prokázáno,

- konstrukce expanzních zbraní neumožňuje střelbu jednotným nábojem,
- k přesnosti střelby se nelze vyjádřit,
- 5 ks nábojek vyjmutých ze zásobníku zbraně,
- jedná se o nábojky německé výroby zn. WADIE ráže 9 mm P.A.B., s *náplní chemické dráždivé látky ozn. PV* (technický capsaicinod). Nábojky jsou v dobrém technickém stavu a jsou rážově příslušné k předložené zbrani,
- 1 ks volně ložená, vystřelená mosazná nábojnice z *akustické nábojky* tuzemské výroby zn. Sellier & Bellot ráže 9 mm P.A.B,
- vystřelená nábojnice je rážově příslušná k předložené zbrani. Povrch vystřelené nábojnice nenese stopy po prováděných úpravách, které by změnily původní charakter akustické nábojky. Nábojnice byla průmyslově vyrobena. Porovnání nábojnice v databázi ÚSBS bylo negativní.

3. VLASTNÍ RANIVĚ BALISTICKÁ ANALÝZA

K hodnocení podmínek, za kterých došlo ke vzniku poranění obličeje a očí poškozeného, znalec provedl rozsáhlou analýzu dostupných zdrojů informací nutných k posouzení *ranivého potenciálu* a *ranivých účinků* nábojek (akustická a s dráždivou chemickou látkou) zbraňového systému plynovky různých ráží a balistického výkonu.

Dostupné zdroje podrobené analýze:

- běžné tištěné zdroje (knihy, studijní texty, VŠ kvalifikační práce, internet) [3] a [4],
- návod na použití akustických pistolí (plynovek) EKOL AGENT Cal.: 9 mm P.A. Knall,
- převzaté výsledky balistických experimentů jiných odborných pracovišť zaměřených na přechodovou balistiku expanzní zbraně (plynovky).

3.1 Analýza a hodnocení informací z dostupných literárních zdrojů

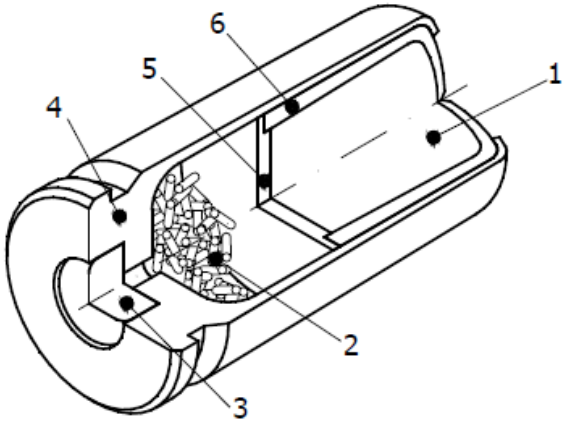
- *Konstrukce dostupných typů plynovek:*

Konstrukce plynovek vychází z jejich předlohy, kterou jsou klasické krátké palné zbraně (pistole, revolver), jenom s tím rozdílem, že jsou konstruovány tak, aby nemohlo dojít k vystřelení střely klasické konstrukce standardního náboje stejné ráže a nemohly být k tomuto účelu ani upraveny [3].

Na trhu se vyskytují plynovky ve třech základních rážích 6, 8 a 9 mm. V praxi jsou u těchto zbraní realizovány tři konstrukční typy spoušťového a bicího mechanismu zbraně, a to SA, DA a DAO.

- *Střelivo pro plynovky (konstrukce a účinky):*

Střelivem pro plynovky (palné expanzní zbraně) jsou *plynové* nebo *akustické nábojky*. Nábojka je složená zpravidla z mosazné nebo ocelové nábojnice, iniciátoru (zápalky) se zápalkovou složí, výmetné prachové náplně představované bezdýmným prachem (akustické nábojky) nebo směsí prachové náplně a krystalků nebo granulí chemické dráždivé látky (nábojky s dráždivou látkou). Jednotlivé druhy nábojek jsou barevně odlišeny k snadné identifikaci. Barevné šablonování (označení) se aplikuje na plastovou zátku zeslabenou dvěma na sebe kolmými zářezy, která uzavírá sestavu nábojky (obr. 1).



Obrázek 1 Plynová (plynovková) nábojka. 1 – dráždivá látka, 2 – výmetná prachová náplň, 3 – zápalka, 4 – nábojnice, 5 – dno, 6 – kontejner [3]

Krystalky účinné dráždivé látky se při výstřelu působením vysoké teploty odpaří (sublimují), plynná fáze tvořená parami dráždivé látky a zplodinami hoření výmetné prachové náplně opouští hlaveň. V relativně chladné atmosféře páry dráždivé látky kondenzují a vytvářejí před hlavní aerosolový oblak, jehož velikost závisí nejen na ráži nábojky, ale i na konstrukci hlavně použité zbraně (zejména na tvaru a rozměrech výtokového kanálu).

K základním účinným látkám plynových nábojek patří jednak původem vojenské dráždivé látky CN (C_8H_7ClO) a CS ($C_{10}H_5ClN_2$), a dále relativně nové dráždivé látky typu pepř (OC a PAVA). Dráždivá látka CN (chloracetofenon) je poměrně zastaralá a méně účinná látka se silným dráždivým, zejména na oční sliznici. Dráždivá látka CS je extrémně dráždivá, avšak téměř netoxická. Při zasažení organismu se vyznačuje širokým spektrem účinků (palčivé bolesti očí, spojené s nadměrným slzením a nedobrovolným uzavíráním očních víček, pálení nosní sliznice, zvýšení sekrece hlenu, silné dráždění ke kašli, dýchací potíže, tíživé pocity v hrudní krajině, přecitlivělost (pálení) vlhké pokožky a závratě, pocity „plavání“ hlavy. Uvedené příznaky se objevují bezprostředně po zasažení a přetrvávají několik minut až několik desítek minut. Jsou charakteristické i pro velmi nízké (prahové) koncentrace látky CS v aerosolovém oblaku. Při vyšších koncentracích se mohou přidružit pocity nucení na zvracení a velmi silné až nesnesitelné podráždění očí, sliznic i kůže, která dočasně zrudne. Podle některých autorů látka CS ovlivňuje i nervovou soustavu.

K dráždivým látkám typu pepř se řadí jak látky přírodní (OC – Oleoresin Capsicum) vyrobené z kajenského pepře. Její dráždivé účinky jsou obdobné jako u látky CS. Je však považována za účinnější proti osobám, které jsou pod vlivem alkoholu a drog. Syntetickou látkou je dráždivá látka známá jako *nonivamid* (PAVA – Peralgonyl Acid Vanil Amid, $C_{17}H_{27}NO_3$). Jsou dostupné ve více variantách a u různých výrobců se od sebe liší množstvím chemické dráždivé látky, která se pohybuje v rozmezí 20 až 45 mg na jednu nábojku. O toto množství je přirozeně sníženo množství výmetné prachové náplně v nábojce. Předností uvedených látek je skutečnost, že ani při velmi vysokých, v praxi nedosažitelných koncentracích, je ohrožení zdraví v důsledku toxicity látky vysoce nepravděpodobná.

V praxi dosahuje délka oblaku aerosolu až několik metrů a jeho průměr je minimálně 50 cm. Výrobci udávají účinnou vzdálenost střelby v rozmezí 1 až 7 m, optimální vzdálenost od cíle pro jejich použití pak kolem 3 až 4 m. Účinné jsou proti lidem i zvířatům a jsou chemicky stálé (s časem nevyprchají). Jejich účinek je ale omezený proti lidem pod vlivem některých návykových látek (alkohol a některá léčiva).

- *Testování plynovek experimentální střelbou:*

Testování plynových nábojek s dráždivou látkou se ve většině případů provádí ve vnitřních krytých prostorách (střelnicích) se standardní výbavou (měřící a snímací technika) zvlášť pro plynovkové pistole a revolvery. K dispozici jsou výsledky testů více druhů zbraní od různých výrobců. Testování je obvykle zaměřeno na maximální dostřel a měření funkční vzdálenosti. Z výsledků testování vyplynulo, že *maximální dostřel* (dosah oblaku zplodin hoření náplně nábojky) se u pistole a revolveru pohyboval v rozmezí 2 až 3 m, *funkční vzdálenost* pak 1 až 2 metry v závislosti na jejich ráži a balistickém výkonu.

Testování *ranivého účinku* plynových nábojek s dráždivou látkou je realizováno střelbou ze vzdálenosti 10 a 30 cm na cílovou plochu kancelářského papíru gramáže 80 $g.m^{-2}$ formátu A4, který byl jednak volně zavěšen nebo upevněn v obvodovém rámu. Měří se plocha (průměr) zakouřené plochy papíru, příp. jeho perforace působením tlaku, teploty a pevných částic dráždivé látky.

Podobné testy provedl rovněž *Jiří Mandík* s *akustickými nábojkami* ráže 6 a 8 mm střelbou na různé materiály (papír, mýdlo, dřevo) ze vzdálenosti 10 cm a kontaktní střelby. Výsledky těchto testů uvádí výše zmíněný článek v odborném časopise *Střelecká revue č. 12/2013.*

- *Střelná poranění člověka nábojkou plynovky:*

Mechanismus vzniku střelného poranění (ranivého účinku) člověka popsali autoři *MUDr. Miroslav Šafr a doc. MUDr. Petr Hejna, Ph.D., MBA* ve své monografii [6] v 10. kapitole *Střelné poranění expanzními zbraněmi.*

Na str. 127 až 136 autoři uvádí: „Expanzní zbraně lze považovat za neletální střelné zbraně.“ Ačkoliv jejich použití je v praxi velmi široké lze je s výhodou použít k *sebeobraně.*

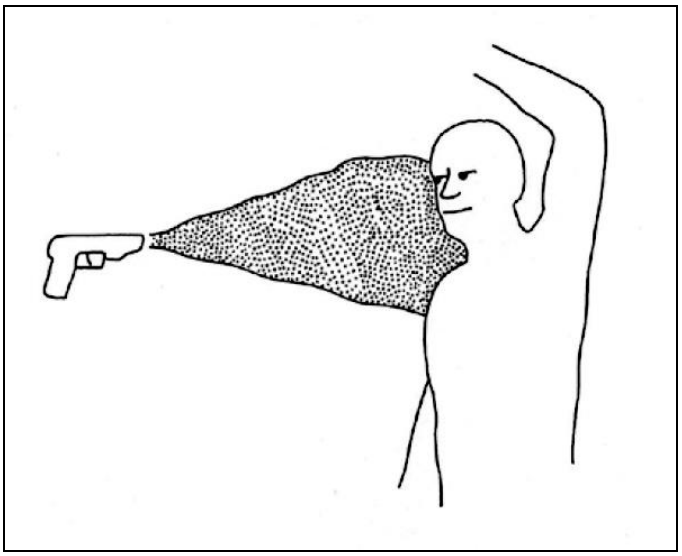
Střelivem pro expanzní zbraně jsou průmyslově vyráběné akustické a plynové nábojky. Hlukového efektu u akustických zbraní je dosaženo prudkou expanzí intenzivně spalované výmetné prachové náplně *akustické nábojky* v okamžiku, kdy spalné plyny opouštějí vývrt hlavně. Účinnou náplní *plynových nábojek* jsou granule (krystaly) dráždivé látky, které jsou v rámci nábojky uloženy buď v samostatném plastovém kontejneru před výmetnou náplní, nebo ve směsi s prachovou složí výmetné náplně. Při výstřelu dochází vlivem vysoké teploty k odpaření (sublimaci) krystalů dráždivé látky. Takto vzniklá plynná fáze (páry) pak společně se zplodinami hoření opouští hlaveň a v okolním chladnějším prostředí kondenzuje a tvoří aerosolový oblak, jehož velikost a tvar je závislý na ráži nábojky a rozměrech hlavně.

Dosah oblaku aerosolu může být řádově až *několik metrů*, přičemž účinný dosah se nachází v rozmezí v rozmezí 1,5 – 4 m (viz obr. 2).

Účinek dráždivé látky je dán typem a množstvím uvolněné látky a citlivostí tkání zasažené části těla. Intenzita a trvání příznaků jsou výrazně individuální. Podstatným faktorem účinku je rovněž velikost prostoru, kde dojde k použití takové dráždivé látky (vyšší koncentrace chemické látky v malém, uzavřeném prostoru).

Riziko použití plynových zbraní obecně spočívá v nedodržení doporučené vzdálenosti použití, tedy ve výstřelu z *relativní blízkosti* (řádově do několika desítek centimetrů) či *absolutní blízkosti* (přiložení) proti oblasti oka, obličejových otvorů, krku, ale i hrudníku a břicha.

Přímo i nepřímo zraňujícím faktorem jsou *zplodiny hoření* výmetné náplně, které pod tlakem a za vysoké teploty opouštějí ústí hlavně (v případě plynovek v kombinaci s účinnou dráždivou látkou) a *rázová tlaková vlna.*



Obrázek 2 Schematické znázornění zasažení člověka oblakem účinné látky po výstřelu z expanzní zbraně (plynovky).
ZDROJ: Obrázek 2 byl převzat s laskavým souhlasem autorů monografie ŠAFR, Miroslav, HEJNA, Petr. Střelná poranění. 1. vydání. Praha: Galén, 2010, s. 127 – 136. ISBN 978-80-7262-696-0.

3.2 Návod na použití akustických pistolí (plynovek) EKOL AGENT Cal.: 9 mm P.A. Knall

Informace pro zákazníky poskytnuté dovozcem plynovek firmou J.G.S. TRADE, s.r.o., Na Louži 5/939, 101 00 Praha 10 a volně dostupné na internetu.

Plynová zbraň tureckého výrobce **Ekol Agent** v ráži 9 mm PA má střenky vyrobené z odolného tvrzeného plastu, tělo ze slitiny kovu s pojistkou pro zajištění zbraně. Kapacita zásobníku je 5+1 ran a díky svým kompaktním rozměrům se jedná o ideální plynovou zbraň do dámské kabelky.

POZOR: Pistole je prodejná jen osobám starším 18 let!

Pistole je standardní koncepce s výrobním provedením „plynovky“, tedy do nábojové komory nelze nabít ostrý náboj (jiná délka a tvar), v hlavni jsou dva příčné kolíky (přepážky) proti výstřelu klasického náboje se střelou. Materiál hlavně by neodolal tlaku standardního kulového náboje a došlo by k havárii součástí zbraně (roztržení hlavně, nábojové komory nebo jejich vydutí).

Běžně se pro tuto ráži používají 9 mm nábojky s náplní „technický pepř“ s hnědým nebo červeným označením. Je možné ještě použít 9 mm nábojky s náplní CS „dráždivá na oči a dýchací cesty“ se žlutým označením. Na označování se nedá spolehnout. Vyskytuje se ještě barva zelená s látkou na bázi „CN“ (dráždí jen dýchací cesty), ale tato náplň je již velmi málo účinná.

Označování (šablonování) složení účinné chemické látky upravuje norma 370/2002 Sb., pojednávající o dovoleném výrobním provedení plynové zbraně, expanzní zbraně a střelivu [8].

Bezpečnostní pokyny:

Dovozce v Návodu na použití zbraně formuluje jednotlivé bezpečnostní pokyny, z nichž nejdůležitějším je zákaz používání plynové pistole na kratší vzdálenost než 1 m. Bohužel ani výrobce, ani dovozce posuzované zbraně neuvádí, k jakému typu nábojky (akustická nebo s dráždivou látkou) se tento údaj vztahuje!

3.3 Převzaté výsledky balistických experimentů zaměřených na přechodovou balistiku plynovek

Výsledky balistického experimentu provedeného *doc. Ing. Janem Komendou, CSc.* za účelem kvantifikace ústťového projevu (ústťové charakteristiky) plynovky neznámého původu v rámci přípravy znaleckého posudku. Jednalo se o ověření soudem projednávané střelby z plynovky ze vzdálenosti cca 1,0 m. Jakým typem KKZ se střílelo, zda se jednalo o pistoli nebo revolver, nebylo jasné, protože ani zbraň, ani střelivo (nebyla zajištěna nábojnice) nebyly policii zajištěny [2].

V rámci přípravy ZP výše jmenovaný znalec provedl tři střelecké experimenty se dvěma expanzními zbraněmi:

- plynovou pistolí ráže 8 mm a
- plynovým (akustickým) revolverem ráže 9 mm R s 2´´ hlavní. Ke střelbě byl použit zcela nový revolver.

- *Výsledky střeleckých experimentů:*

Střelba byla prováděna vstoje z volné ruky (bez opory) se zamířením na střed cílové plochy (volně zavěšené listu kancelářského papíru, gramáž 80 $g.m^{-2}$) formátu A3 ze vzdálenosti 0,3 až 1,0 m. Okolní teplota vzduchu 20° C. Ke střelbě byly použity 3 různé nábojky:

- *plynová nábojka 8 mm CS* – na vzdálenost 1 m 5 průrazů papíru, na vzdálenost 0,5 m 14 průrazů. Z experimentu lze odhadnout, že testovaná nábojka splňuje požadavek vyhlášky (neprůraz papíru gramáže 120 $g.m^{-2}$ na vzdálenost 1,5 m),
- *akustická nábojka 8 mm Blank* – hodnocen výrazně větší účinek – na 1 m 20 průrazů, na 0,5 m několik set průrazů,
- *akustická nábojka 9 mm R Blank* – na vzdálenosti 1,0 m i 0,5 m bez účinku, na vzdálenost 0,3 m byly zjištěny 4 průrazy papíru.

- *Závěry znalce:*

- Všechny identifikované průrazy byly velmi malých rozměrů (cca desetiny mm), žádná kovová částice (střepinka) nebyla experimenty zaznamenána.
- Na 1 m byly částice prachu rozptýleny na plochu o minimálním průměru cca 30 cm, z jejich hustoty vyplývá, že zásah oka je spíše náhodný, tzn., že v oku mohou být 1 – 2 zrnka.
- Obecně lze říci, že nežádoucí účinky akustických nábojek jsou větší než nábojek plynových, přičemž u akustických nábojek mohou být zaznamenány značné rozdíly v jejich účinku.

4. POSUDEK ZNALCE SE ZÁVĚRY A ODPOVĚĎMI NA ZADANÉ OTÁZKY

1. ***Vyjádřete se ke způsobu použití zbraně při incidentu ze dne 11. 9. 2014 jak jej popisuje poškozený v protokolu o jeho výslechu jako svědka ze dne 17. 2. 2015***

a obviněný v protokolu o výslechu tohoto obviněného ze dne 11. 2. 2015. Která z výpovědí těchto osob je z hlediska znalce technicky přijatelná?

Zásadní rozpor ve výpovědích **poškozeného** ze dne 17. 2. 2015 a **obviněného** ze dne 11. 2. 2015 spočívá v následujících tvrzeních :

- Poškozený uvádí, že v okamžiku, když chtěl vejít do výtahu, tak se ozval výstřel, který jej zasáhl přímo do očí. „V tom okamžiku jsem nic neviděl, viděl jsem ale, že se jedná o střílející osobu pana obviněného. Na dotaz, zda poškozený (svědek) pana obviněného před výtahem nějak napadl, uvedl, že ne. „Vůbec jsem se jej nedotkl."
- obviněný naproti tomu uvádí, že když sjel výtahem do přízemí domu, a po otevření dveří výtahu, uviděl před výtahem stát pana poškozeného (svědka), kterého se snažil při vystupování obejít. *„V tuto chvíli mne uchopil pravou rukou za krk a levou se napřahoval mne udeřit. Ve snaze se bránit jsem vystřelil z plynové pistole, kterou jsem měl u sebe. V okamžiku výstřelu jsme stáli čelem k sobě, ale ne přímo, já jsem stál spíše po jeho pravém boku."* Jak jsem vystřelil, tak vůbec nemám potuchy, kam střela mohla jít, v době, jak jsem vystřelil, tak pistole mohla být v té době někde pod pravým ramenem.

Z uvedených výpovědí *poškozeného* i *obviněného*, výsledků lékařských vyšetření hodnotících rozsah a klinickou závažnost střelného poranění, závěrů znalců z oboru zdravotnictví, odvětví soudní lékařství i vlastních zjištění, se znalec při hodnocení technických podmínek použití zbraně (plynové pistole) na MČ kloní k výpovědi obviněného.

K výstřelu došlo ze samonabíjecí plynové pistole s jednočinným provedením spoušťového a bicího mechanismu SA (Single Action), zn. EKOL model AGENT, ráže 9 mm P.A.B., v. č. EVL-12120543, r. v. 2012. K jedinému výstřelu a zásahu poškozeného došlo z relativní blízkosti (cca 0,2 až 0,4 m) povýstřelovými zplodinami akustické nábojky stejné ráže. Pokud by byla pravdivá výpověď obviněného a tento byl před použitím zbraně držen poškozeným za krk, nebylo možno zbraň použít na výrobcem předepsanou minimální vzdálenost 1 metru. Z lékařského hodnocení střelného poranění vyplývá, že závažnější poranění utrpěla pravá strana obličeje zasaženého. Tato skutečnost ukazuje na nemířený výstřel z plynové pistole akustickou nábojkou směrem vpravo od podélné osy těla poškozeného. Při uvážení možných radiálních rozměrů zplodinového mraku to podporuje i tvrzení obviněného, že v okamžiku výstřelu bylo ústí hlavně pistole někde pod pravým ramenem, kdy zplodiny hoření výmetné prachové náplně a také nespálená prachová zrna mohla zasáhnout přednostně pravou stranu obličeje poškozeného. Z takto hodnocené vzdálenosti střelby se na vzniku a rozsahu poranění podílel přetlak na čele rázové vlny a také vysoká teplota prachových plynů vytékajících z hlavně.

Zásahy hlavy kinetickými tělesy se obecně hodnotí velmi špatně, a to z důvodu značných stupňů volnosti, kterými tato anatomická oblast (krk a hlava) těla člověka disponuje. V okamžiku výstřelu, kdy hlava zasaženého není v přímé pozici, ale mírně natočena vlevo, může celou situaci výrazně ovlivnit.

2. ***Popište rozdíly v účincích akustických nábojek a nábojek s dráždivou látkou, včetně uvedení informací, které jsou ohledně účinků těchto nábojek laickou veřejnosti dosažitelné.***

Z dostupných zdrojů uvedených znalcem v části 3.1 je zřejmé, že účinky (ranivý potenciál) **akustických nábojek** na člověka jsou vyšší než účinky nábojek s **dráždivou látkou.** Tato disproporce v účincích je vedle typu a ráži zbraně a stavu vývrtu u jednotlivých druhů nábojek různá v závislosti na ráži, použitém typu chemické dráždivé látky i jejím stáří.

Je to dáno vyšším balistickým výkonem expanzní (akustické) nábojky, která obsahuje zpravidla vyšší hmotnost výmetné prachové náplně než nábojka náboje klasické (standardní) konstrukce s letálními účinky. Údaje některých výrobců uvádí, že toto množství může být téměř dvojnásobné. Je to vynuceno potřebou vývinu dostatečného tlaku prachových plynů v hlavni k zajištění pohonu automatiky zbraně při absenci střely a nové nabití zbraně před dalším výstřelem. Tyto údaje nejsou výrobci střeliva běžně uváděny ve firemní literatuře a laická veřejnost se k nim tedy dostává jen obtížně.

Nábojky plynové, obsahující chemickou dráždivou látku, disponují menším objemovým množstvím výmetné prachové náplně, které je sníženo o objem této chemické látky. Proto také v úsťové charakteristice zbraně po výstřelu nábojky s dráždivou látkou převládá oblak aerosolu této látky a projevy tlaku a vysoké teploty zplodin hoření výmetné prachové náplně jsou poněkud potlačeny.

Na tomto místě je nutné uvést jeden z nepřekonaných mýtů, kterému bohužel podléhá značná část laické veřejnosti. Je to názor, že **akustická (cvičná) nábojka** se projevuje pouze akusticky (vytváří hluk, třesk) a ostatní projevy (tlakový a tepelný účinek) jsou nepodstatné. Výrobce (či dovozce) zbraní neupozorňuje totiž v návodu ke zbrani na vyšší účinnost akustických nábojek a z podstaty slovního označení "akustické" nábojky se pak laici a někdy i odborná veřejnost nutně logicky domnívají, že akustická nábojka má naopak nižší účinnost či ranivost.

Seriózní hodnocení ranivého potenciálu akustické a plynové nábojky a jejich vzájemné porovnání by vyžadovalo přípravu a provedení balistického experimentu znalcem s doličnou zbraní a střelivem použitých v hodnoceném případu.

4.1 Vlastní zjištění znalce

Studiem doručeného spisového materiálu znalec nezjistil žádné další skutečnosti, které by z hlediska své odbornosti považoval za důležité v posudku uvést a podrobněji vysvětlit.

ZÁVĚR

Cílem příspěvku bylo odbornou, ale také laickou veřejnost upozornit na relativně vysokou nebezpečnost expanzních zbraní (plynovek), pokud jsou použity proti člověku v rozporu s obecně platnými doporučeními jejich výrobců. Jeho autoři neměli ambici se v příspěvku zabývat právní stránkou hodnoceného případu.

I když jsou tyto zbraně podle zákona č. 119/2002 Sb., zákona o zbraních a střelivu zařazeny do kategorie D (ostatní zbraně) a nepodléhají zvláštnímu povolovacímu režimu, praxe ukazuje, že jsou-li použity proti člověku na kratší vzdálenost, než je výrobcem doporučováno, mohou způsobit vážné poranění nebo dokonce i smrt [7].

Především akustické nábojky jsou spojovány s problematickým terminálně balistickým chováním a disponují vyšším ranivým potenciálem jak nábojky plynové stejné ráže. Naše znalecké ranivě balistické zkoumání prokázalo, že je-li zbraň použita z relativně blízké vzdálenosti střelby nebo dokonce s přiložením (kontaktní střelba) jsou takovou střelbou způsobována komplikovaná střelná poranění se značnou devastací měkkých tkání působením kouřové dutiny včetně termického účinku na kožní kryt v okolí zásahu.

Literatura:

[1] RYBÁŘ, Vadim. *Zadání znaleckého posudku s otázkami na znalce*. Ostrava: Advokátní kancelář Mgr. Vadim Rybář, Tyršova 1714/27, Moravská Ostrava, PSČ 702 00 z 20. 5. 2015.

[2] JUŘÍČEK, Ludvík. *Odpovědi na otázky advokáta AK Mgr. Vadima RYBÁŘE ze dne 20. 5. 2015 a vyjádření se k možným podmínkám, za kterých došlo ke zranění poškozeného Viléma KOŠMIDERA*. [Znalecký posudek č. 008/2015 zpracovaný pro AK Mgr. Vadima RYBÁŘE, Tyršova 1714/27, PSČ 702 00 Ostrava-Moravská Ostrava]. Brno: Vaculíkova 529/6, 638 00 Brno, 2015, 15 s.

[3] JUŘÍČEK, Ludvík a kol. *Ranivá balistika. Technické, soudnělékařské a kriminalistické aspekty*. Ostrava: KEY Publishing, s.r.o., Nádražní 733/176, 702 00 Ostrava – Přívoz. Tisk: NOVPRESS, s.r.o., nám. Republiky 15, 614 00 Brno, 2017, 614 s. ISBN 978-80-7418-274-7.

[4] JUŘÍČEK, Ludvík. *Ranivý potenciál malorážových střel a jeho hodnocení.* Ostrava: KEY Publishing, s.r.o., Nádražní 733/176, 702 00 Ostrava – Přívoz. Tisk: NOVPRESS, s.r.o., nám. Republiky 15, 614 00 Brno, 2015, 158 s. ISBN 978-80-7418-222-8.

[5] KLEIN, Leo, FERKO, Alexander, a kol. *Principy válečné chirurgie.* 1. vydání. Praha: GRADA Publishing, a.s., 2005. 140 s. ISBN 80-247-0735-7. [C-kapitola v knize, RIV/60162694: G44_/05: # 00001291]. Praha: Grada, 2005, s. 49-54.

[6] ŠAFR, Miroslav, HEJNA, Petr. *Střelná poranění.* 1. vydání. Praha: Galén, 2010, 259 s. ISBN 978-80-7262-696-0.

[7] Zákon č. 119/2002 Sb., zákon o zbraních a střelivu.

[8] Vyhláška MPO č 370/2002 Sb., o dovoleném výrobním provedení plynové zbraně, expanzní zbraně a střeliva, ve znění vyhlášky MPO č. 179/2017.

SOUVISLOSTI ŘÍZENÍ V OCHRANĚ OBYVATELSTVA

CONTEXT OF MANAGEMENT IN CIVIL PROTECTION

doc. Ing. Jaromír Novák, CSc.
Mgr. Vítězslav Prukner, Ph.D.
Univerzita Palackého v Olomouci, Fakulta tělesné kultury
Třída Míru 117,
E-mail: jarminov@seznam.cz
vitezslav.prukner@upol.cz

ABSTRAKT

Věci, jevy a procesy v současné společnosti jsou velmi složité, chaotické a prudce se měnící. Jejich řízení vyžaduje jejich poznávání, vyvozování závěrů a adekvátní reakci. Pojmy jako řízení, bezpečnost, hrozby, rizika, krizové řízení, ochrana obyvatelstva, ochrana člověka za mimořádných událostí jsou v dnešní společnosti pojmy silně frekventovanými. Ochrana obyvatelstva je nedílnou součástí dnešního světa takřka na všech úrovních. Problematika ochrany obyvatelstva má široké i úzké souvislosti. Vyžaduje v procesech jejího řízení odpovídající přístupy, metody a postupy. Za základní přístupy je možno považovat systémový přístup, cílově optimalizační přístup, heuristický přístup. Tyto přístupy napomáhají rozhodovacím procesům v ochraně obyvatelstva.

KLÍČOVÁ SLOVA

Bezpečnost, ochrana obyvatelstva, řízení, proces, systém, společnost

ABSTRACT

Things, phenomena and processes in nowadays society are very complicated, chaotic and fast changing. Their management demands their knowing, making consequences and adequate reactions. Phenomena like management, safety, threats, risks, crisis management, civil protection, human protection during unexpected circumstances are highly frequented phenomena. Civil protection is inseparable parts of nowadays world almost everywhere. Problematic of civil protection has a lot of consequences. Demands in it management processes adequate approach, methods and sequences. As a basic we can see system approach, optimization approach, and heuristic approach. These approaches help decision processes in civil protection.

KEY WORDS

Security, civil protection, management, proces, system, society

ÚVOD

Dnešní společnost je společností vysoce složitou, prudce se vyvíjející, rychle se měnící a zejména obtížně řiditelná. Lze se domnívat, že řiditelnost všech věcí, jevů a procesů je velmi obtížně zvládnutelná a i přes vývoj informačních technologií se ukazuje stále větší stochastičnost, obtížné či nemožné předvídání vývojových tendencí takřka ve všech oblastech existence společnosti. Podstatou řízení je transformace informací. Rozvinutěji vyjádřeno je to optimální využívání zdrojů, které jsou pro řízení k dispozici – zdrojů lidských, finančních, materiálních, časových a informačních. Jednouché vyjádření, avšak složité řešení.

V souvislosti se složitostí existence společnosti a jejím řízením nabývají v dnešním přetechnizovaném a přetechnologizovaném světě na významu pojmy jako bezpečnost, ochrana obyvatelstva a krizové řízení.

Vše, co se děje, má svou minulost, přítomnost a budoucnost. Dějiny člověka jsou dějinami násilí, válek a třídních bojů, dějinami ohně. Jsou také dějinami nadějí, víry a lásky. Dějiny jsou dějinami erotiky a sexu. Dějiny jsou dějinami náboženské temnoty, ale i tvoření a realizace tvůrčího ducha. Dějiny jsou dějinami pokroku, ale i dějinami katastrof. Dějiny jsou dějinami řešení rozporů. A tak bychom mohli v charakteristice pokračovat. Dějiny jsou pestrým mixem všeho zde uvedeného, ale mnohem více zde neuvedeného.

Dějiny jsou také dějinami společenské a společné odpovědnosti všech lidí. Dnes je frekventovaným pojmem společenská odpovědnost firem. Někdy, žel, jde spíše o marketingový tah mající veřejnost firemní i mimofiremní orientovat tak, aby byla přesvědčena o správném řízení firmy a jejího vlivu na zaměstnance, uživatele jejich produktů a firemní okolí. To se může ukázat jako kontraproduktivní a také nebezpečné.

Podívejme se trochu do minulosti a berme to jako ilustraci s přínosem pro dobu dnešní a budoucí, pro její řízení, bezpečnost. Kdysi velmi populární vědec Bertrand Rusell, žijící v letech 1872 – 1970, nositel Nobelovy ceny za literaturu (1950), se věnoval zejména matematice a filosofii. Napsal řadu knih, uvědomoval si složitost společnosti a snažil se aktivně působit na poli mezinárodním. Napsal mimo jiné knihu Logika, věda, filozofie, společnost (Rusell, 1993).

V této knize se zabývá také společenskou odpovědností vědců v projevu k Pugwashskému hnutí vědců pro atomové odzbrojení v roce 1959, tedy před 59 lety. A ta odpovědnost se přeneseně týká každého z nás. Proto aspoň pár slov z jeho myšlenek. V moderním světě nemůže vědec čestně prohlásit, že je jeho posláním získávat poznatky a nenést odpovědnost za to, jak se jeho poznatků využívá. Poznání může padnout do rukou lidí či institucí, kteří se zasvětili zcela nečestným cílům. Upozorňuje na množství peněz, které je vynakládáno na zbrojení a přitom by bylo užitečnější je dávat na potravinové zabezpečení ve světě a na snížení nárůstu populace (požadavek dnešního presidenta USA Trumpa je zvýšit množství peněz pro NATO ve výši 2 – 4% HDP, k čemu?). Tím, jak se svět neustále technicky sjednocuje, stává se život ve „slonové věži“ stále více nemožným. A nejen to. Člověk, který se postaví proti mocným institucím, které kontrolují většinu lidských aktivit, se přestává nacházet ve slonové věži s širokým výhledem na prosluněnou krajinu a ocitá se v temné jeskyni, nad níž byla slonová věž vystavěna. Je v naší moci vytvořit dobrý svět; a proto, ať již s jakoukoli námahou, je naší povinností jej vytvořit! (Rusell, 1993).

Uvážíme-li léta, která od jeho projevu uplynula a stav dnešního světa – jsme světem vyspělým? Opravdu jsou tzv. západní demokracie vyspělými a nám příkladnými?

1. VZTAH ŘÍZENÍ A OCHRANY OBYVATELSTVA

Vývoj je vždy dialektickou jednotou minulosti, přítomnosti a budoucnosti. Je tomu tak i s podmínkami pro život člověka, ochranu jeho žití, jeho širokou bezpečnost. Člověk se zcela zákonitě chránil před vlivy počasí, před sebou samým, před ostatními lidmi, kmeny, státy. Chránil se před dalšími vlivy důsledků chování systémů fauny a flóry. A také před důsledky chování systémů převážně s lidskou strukturou. V raných dobách ještě nevěděl nic o kybernetice a systémové teorii. Jeho rozhodování bylo zřejmě zkušenostní a možná i primitivní z dnešního pohledu. Nejprve využíval nabídky přírody a tuto využíval ve svůj prospěch, postupně ji přetvářel a jejích možností využíval stále více a tak si přírodu podmaňoval. Dnes jsme v situaci, kdy důsledky tohoto podmaňování jsou na zlomové hranici.

Člověk si bere pro své přežití a potřeby nutné i nadbytečné, či zbytečné, či pro své pohodlí z přírody řadu zdrojů, které už teď chybí nebo v budoucnu budou chybět. Svými aktivitami si vyrábí odpady-vykořisťuje přírodu, ve kterých se dusí a které ho obrazně řečeno mohou pohltit jakožto svou součást.

Člověk se musí chránit před zdroji, které sám produkuje a které se obrací či mohou obracet proti němu. A tak se stále rozvíjí disciplina zvaná ochrana obyvatelstva. Vztah mezi řízením a ochranou obyvatelstva je velmi úzký a jedno ovlivňuje druhé.

Lidský faktor je rozhodujícím, neboť jen člověk může reálně a kvalifikovaně posuzovat věci, jevy a procesy související s ochranou obyvatelstva a přijímat odpovídající rozhodnutí a tato pak do teorie i praxe ochrany zavést. Role lidí, přes všechny proklamace, je nedoceňována. Je naopak přeceňována role technických prostředků, informačních systémů a informačních technologií a dalších prostředků materiální povahy. Jde často o byznys ve prospěch firem, které se chopily příležitosti a chtějí na úkor státu a nás občanů vydělávat.

Příprava lidí na krizové situace a jejich předcházení se musí odehrávat ve zvýšené míře na úrovni nejen řídící, ale také na úrovni veškerého obyvatelstva. Svoji vyšší roli zde musí sehrát i masmédia. Místo zbytečných a trapných slovních soubojů politiků v televizi by mohl být věnován prostor problematice krizových faktorů.

V lidech bylo odstraněno nebo do nich nebylo vloženo povědomí, že bezpečí (obrana, ochrana před negativními vlivy) je možností, povinností, nutností každého občana. Nejen profesionálů. Je pravděpodobné, že počet mimořádných událostí poroste. Položme si otázku, zda jsme připraveni. Kdo má a bude řešit důkladnou prevenci, odstraňování následků a obnovu normálu? Máme dostatek profesionálních složek patřičně vybavených? Chce obyvatelstvo být připraveno k sebeochraně?

Pro řízení rizik, krizí, ochrany obyvatelstva existuje celá řada speciálních způsobů a metod. Některé jsou jednoduché a některé velmi složité a lidi, kteří se musí či mají podílet na ochraně obyvatelstva (řídící funkcionáři různého typu v orgánech státní správy, samosprávy, firmách, školách i obyčejní občané) ve většině případů odrazují, protože jim nerozumí a nemají čas se je učit. V další části příspěvku budou rozebrány některé obecnější možnosti, které však při tvůrčím využití mohou pomoci řešení problematiky ochrany obyvatelstva. Pro názornost můžeme brát problematiku ochrany obyvatelstva v konkrétních podmínkách organizace jako projekt. Projektový přístup je dnes hojně používán.

2. PRINCIPY PROJEKTOVÁNÍ V OCHRANĚ OBYVATELSTVA

Principy vyjadřují nejobecnější požadavky na činnost při projektování, stanoví zásadní orientaci tím, že odráží objektivní zákonitosti a tak působí na kvalitu projektování.

Princip cílovosti vychází z nutnosti, potřeb a možností řešení problému, stanovit určitý budoucí stav, kterého je třeba dosáhnout. Podle tohoto principu systém hlavního cílů a dílčích cílů projektování ochrany obyvatelstva představuje kriteriální funkci. Stanovení cílů musí vycházet z budoucích potřeb a hodnot. Jde o stanovení a uspořádání cílů podle úrovně, obsahu a časových parametrů. Stálé, průběžné sledování plnění cílů a slaďování procesu při jejich naplňování a provádění potřebných korekcí.

Princip komplexnosti ve všestranném postižení všech faktorů v jejich proporcích, vlivech a konkrétním vývoji.

Princip systémovosti vyjadřuje přístup k projektování jakožto systému, tedy jednotě parametrů, času, funkce a informace. Vyžaduje chápání projektování ochrany obyvatelstva

jako uspořádaného souboru prvků vzájemně spojených k funkčnímu účelu a přihlížení k objektivním podmínkám (okolí) za kterých se ochrana obyvatelstva realizuje k dosažení stanoveného cíle v určitém čase.

Princip hierarchičnosti vyjadřuje uspořádání, posloupnost funkcí ochrany obyvatelstva ve vertikální rovině, rozlišení jejich významnosti. Umožňuje stanovit rozhodující stránky ochrany obyvatelstva a jejich vliv na ostatní, stanovit rozhodující faktory, rozlišit podstatné. Jde také o správné rozložení úkolů na různých stupních hierarchie řízení, o vymezení kompetencí řídících a výkonných orgánů, jejich vzájemného vztahu, odpovědnosti a výměny informací. S tím také souvisí stanovení míry centralizace a decentralizace funkcí jednotlivých složek systému, podílejících se na ochraně obyvatelstva.

Princip adaptivnosti spočívá v možnosti přizpůsobování se realitě v důsledku vnitřních i vnějších vlivů.

Princip komplementarity vyžaduje sledování jak vlivy, zásahy a opatření vyvolávají změny, jak napomáhají či naopak narušují plnění stanovených cílů, jak ovlivňují proporcionalitu. Při projektování ochrany obyvatelstva existuje celá řada omezení obsahových, časových, finančních, materiálních a dalších. Omezení jsou dána jak vlivy subjektivní povahy, která jsou dána úrovní tvůrců, tak vlivy objektivní povahy, která lze jen s obtížemi měnit, či je nelze měnit vůbec.

Princip efektivnosti je založen na komplexním pojetí efektivnosti. Efektivnost zde lze chápat jako respektovaný a vzájemně úzce spjatý vztah mezi užitečností a vynaloženým úsilím. Efektivnost v širším pojetí se vztahuje k nové úrovni ochrany obyvatelstva, ve vyšší kvalitě. V užším pojetí pak jde o použití takových metod, forem a postupů při práci na projektování, které minimalizují vynaložené úsilí, náklady.

Uvedené principy se možná jeví příliš teoretické, je však třeba si je aspoň v jejich podstatě a tím také transformace do praxe uvědomit. Principy, jejich osvojení, mohou napomoci jak při tvorbě dokumentace, tedy preaktivní etapy řešení problematiky ochrany, tak také při zásazích a posléze jejich vyhodnocování.

3. PŘÍSTUPY K PROJEKTOVÁNÍ OCHRANY OBYVATELSTVA

Projektování problematiky ochrany obyvatelstva je podmíněno složitou strukturou objektivních podmínek a subjektivních faktorů. Změny obecného charakteru vyvolávají změny charakteru zvláštního a naopak.

Za základní, určující faktory lze považovat:

- potřeby a možnosti celospolečenského řádu, jeho vývoje minulého, přítomného i budoucího
- potřeby a možnosti konkrétní problémové reality –
- perspektivnost vývoje problému a předvídání jeho charakteru
- normativní akty - zákony, vyhlášky, normy, příkazy apod.
- zdrojové možnosti – lidé, finance, potřeby a možnosti techniky a technologií, informace a čas

Je možné využívat některé přístupy při řešení projektování krizového řízení, např.: systémový přístup, cílově optimalizační přístup, heuristický přístup, funkční přístup a empiricko-intuitivní přístup.

3.1 Systémový přístup

Systémový přístup vychází z teorie systémů a umožňuje řešit problémy spojené s projektováním ochrany obyvatelstva. Lze vydělit následující hlavní podsystémy systému projektování ochrany obyvatelstva: obsah a rozsah ochrany obyvatelstva, informační, organizační, časový, finanční, materiálový, personální, projektování, korekce.

Uvedené podsystémy jsou vzájemně propojeny, pronikají se, ovlivňují, jsou rozdílné a mohou být obsaženy v sobě navzájem. K základním podsystémům patří:

- obsah dané problematiky ochrany obyvatelstva – obecné a konkrétní problémy
- jednotlivé organizační složky ochrany a jejich hierarchické uspořádání
- veškeré informační procesy – sběr, zpracování, uchování a využití, přenosy informací v textové i obrazové formě
- časová propojenost, posloupnost, rychlost a kapacita přenosu informací
- finanční podsystém umožňuje korigovat vztah mezi potřebou a zdroji financí
- materiálové potřeby, jejich inovace, obměna, skladování, doprava apod.
- personální zabezpečení kvalifikovanými lidmi a jejich dostatkem i možnostmi jejich přípravy
- korekce projektů ochrany obyvatelstva, jejich aktualizace

3.2 Cílově optimalizační přístup

Cílově optimalizační přístup je úzce spjat s cílovostí a optimalizací. Jeho podstata spočívá v tom, že možné stavy a vztahy v systému ochrany obyvatelstva jsou chápány jako důsledek určité cílové funkce systému.

Tento přístup využívá do značné míry i exaktních metod, např. statistiky, síťové analýzy, hodnotové analýzy, dynamického programování apod.

Systém ochrany obyvatelstva je složen z podsystémů a prvků, které mají své vlastní, dílčí cíle, své chování, své kriteriální funkce.

Cíl je vždy spojen s budoucím stavem ochrany obyvatelstva. Stanovení cílů má svá kritéria, protože zpravidla půjde o výběr z množiny cílů, jejich variant a optimalizace.

3.3 Heuristický přístup

Heuristický přístup využívá logiky a obecného rozumu. Je nástrojem k modelování tvořivých činností a využití těchto modelů v tvořivých procesech. Využití heuristického přístupu při projektování ochrany obyvatelstva umožňuje na základě psychologických a logických podmínek zvýšit efektivnost myšlenkových postupů.

Heuristické přístupy se uplatňují všude tam, kde je obtížná formalizace exaktními metodami. Jde o použití metod, které optimalizují řešení úloh projektování ochrany obyvatelstva. Psychologické poznatky potvrzují, že člověk většinu problémových situací řeší bez použití algoritmů řešení.

Využití heuristického přístupu spočívá ve třech složkách:

Za prvé v analýze podmínek, spočívající v rozboru jednotlivých prvků, jejich charakteristických znaků a vztahů mezi nimi na různých úrovních

Za druhé je to analýza cílů jednotlivých prvků

Za třetí porovnání cílů s dosahovanými výsledky řešení.

3.4 Funkční přístup

Funkční přístup je přístupem umožňujícím zaměřit se na funkce ochrany obyvatelstva jako celku i jeho jednotlivých složek. Významem funkčního přístupu pro projektování ochrany obyvatelstva je poznávat jak co nejlépe zajistit funkce ochrany obyvatelstva.

Ochrana obyvatelstva v daných případech má svoji hlavní funkci a také funkce vedlejší, které doplňují a pomáhají naplňovat funkci hlavní. Tyto funkce se mohou projevovat pozitivně, negativně či neužitečně.

Při projektování ochrany obyvatelstva je třeba zvažovat, jak který faktor působí, jak se podílí na plnění funkcí. Cílem je dosáhnout potlačení či odstranění negativních a neužitečných funkcí.

3.5 Empiricko-intuitivní přístup

Empiricko-intuitivní přístup je založen na zkušenostech, intuici a pragmatičnosti a má své místo v ochraně obyvatelstva zejména tam, kde problematika je velice složitá ve své obtížné předvídatelnosti. Je třeba zde podotknout, že tento přístup je a zřejmě bude stále častěji využíván. Je však vhodné či nutné jej doplňovat exaktnějšími metodami rozhodování, bude-li to možné.

Uvedené přístupy nejsou jediné. Přístupy se navzájem prolínají, doplňují a ovlivňují.

Zásadní jednoduché otázky, které je vhodné si klást při projektování ochrany obyvatelstva:

1. Jaký je to problém, co to je, co je jeho podstatou?
2. Jaká je struktura řešeného problému?
3. Jakou funkci daný prvek, podsystém plní?
4. Která funkce je hlavní, kriteriální?
5. Které jiné funkce je třeba začlenit?
6. Co může zajistit plnění funkce?
7. Jaká je personální, finanční, materiálová, časová a informační náročnost?
8. Jaká je možnost náhradního řešení?
9. Jaké jsou proporce kvality a kvantity?
10. Které myšlenky a nápady, přístupy, řešení rozvíjet?
11. Jaké podmínky vytvářet pro realizaci nových myšlenek?
12. Jak překonat překážky, jak je obracet v příležitost?
13. Jak lze využít základních principů, zákonu a kategorií filosofické discipliny – dialektiky, neboť jejich návod k řešení problémů může být významnější, než složitý a drahý informační systém

ZÁVĚR

Smyslem příspěvku je poukázat na některé teoretické nástroje, které jsou v teorii i praxi ochrany obyvatelstva a jejího projektování využitelné a které by mohly napomoci ke zlepšení kvality práce při řešení problémů ochrany obyvatelstva. Mají obecnější platnost, jsou nástrojem k praktickému využití při řešení konkrétních úkolů ochrany obyvatelstva.

V textu je také připomenuto prostředí i minulost problematiky ochrany obyvatelstva a řízení z hlediska principu všeobecné souvislosti a principu komplexnosti. To proto, aby ochrana byla chápána z širšího pohledu.

Literatura

[1] JIRÁSEK,J. *Agenda příštích let*. Praha: Professional Publishing, 2006. ISBN 80-86946-04-5

[2] KUTTA,F.,SOUKUP, M. *Řízení v období vědeckotechnické revoluce.* Praha:Svoboda 1973

[3] NOSEK, V. a kol. *Malá encyklopedie vědeckého řízení*, Praha: Naše vojsko, 1976

[4] NOVÁK, J. *Projektování výuky*, Vyškov: VVŠ PV, 1991

[5] NOVÁK, J. Možné vývojové tendence okolí managementu. *In Sborník konference GEMAN 04 "General management"*. Plzeň: Sdružení EVIDA Plzeň, 2004

[6] VLČEK, J. a kol.:*Systémové řízení,* Praha: Institut řízení, 1976

[7] VLČEK, R. a kol.:*Hodnotová analýza*, Praha: SNTL, 1973

[8] RUSELL, B. *Logika, věda, filosofie, společnost*, Praha: Svoboda – Libertas, 1993. ISBN 25-068-93-02/3

VYUŽITÍ PROCESNÍHO MANAGEMENTU VE VÝROBNÍCH PODNICÍCH V ČESKÉ REPUBLICE: BUSINESS PROCESS MANAGEMENT V KONTEXTU KRIZOVÉHO ŘÍZENÍ

THE USE OF BUSINESS PROCESS MANAGEMENT IN THE PRODUCTION COMPANIES IN THE CZECH REPUBLIC: BUSINESS PROCESS MANAGEMENT IN CONTEXT OF CRISIS MANAGEMENT

Ing. Pavel Ondra
Univerzita Tomáše Bati ve Zlíně, Fakulta managementu a ekonomiky
Mostní 5139, Zlín, 760 01
ondra@utb.cz

ABSTRAKT

Společnými jmenovateli dynamicky se měnících podmínek podnikových procesů jsou úlohy zákazníka, nejistota dosažení budoucího úspěchu a inovace, ve výrobních podnicích především inovaci organizace a řízení výroby. Proto je nutné se zabývat se řízením podnikových procesů, včetně jejich výkonnosti, a krizovým managementem. Procesní řízení bylo vyvoláno nutností změny v řízení organizací, tzn. jistou krizí v tomto směru. Příspěvek je zaměřen na využívání principů procesního řízení ve výrobních podnicích v ČR. Hlavním cílem příspěvku je identifikovat a popsat přístup výrobních podniků v ČR při využívání procesního řízení. Příspěvek poskytuje odpovědi na výzkumné otázky týkající se využívání procesního řízení a jeho podpůrného IT řešení v podmínkách výrobních podniků v ČR, sledování, měření a hodnocení podnikových procesů a využívané ukazatele podnikových procesů. V příspěvku jsou shrnuty výsledky online dotazníkového šetření mezi 400 výrobními podniky v ČR.

KLÍČOVÁ SLOVA

Management, podnikové procesy, procesní řízení, krizové řízení, výrobní podniky, Česká republika

ABSTRACT

The common denominators of the dynamically changing business process conditions are customer tasks, uncertainty of future success and innovation, especially in manufacturing companies, mainly innovating organization and production control. Therefore, it is necessary to address the management of business processes, including their performance, and crisis management. Business Process Management was triggered by the need for a change in organization management, a certain crisis in this direction. The paper focuses on the use of the principles of Business Process Management in manufacturing companies in the Czech Republic. The main objective of this paper is to identify and describe the approach of manufacturing companies in the Czech Republic in using Business Process Management. This paper provides answers to research questions on the use of Business Process Management and its software support solution in terms of manufacturing companies in the Czech Republic, monitoring, measurement and evaluation of business processes and used business process indicators. The paper summarizes the results of the online questionnaire survey among 400 manufacturing companies in the Czech Republic.

KEY WORDS

Management, Business Processes, Business Process Management, Crisis Management, Manufacturing and Processing Industry, Czech Republic

ÚVOD

Současnost je pro podniky turbulentním a dynamickým prostředím. Od počátku 90. let minulého století se neustále objevují nové a nové manažerské praktiky, techniky, nástroje a metody, čímž se vytváří podmínky pro tzv. management v podmínkách kritických změn (Antušák a Vilášek, 2016). Uvnitř i vně podniku dochází neustále ke změnám, které mohou mít jak menší, tak i větší dopad na daný podnik. Takové změny však nemusí mít na podnik nutně jen pozitivní efekt, ale mohou mít kritické nebo až krizové důsledky. Podnik se může do krizové situace dostat z důvodu neadekvátní reakce na různé změny, anebo i z neschopnosti jakékoli reakce. Takový vývoj si vyžaduje nové styly řízení a nové tvůrčí přístupy, které dokáží vyřešit vzniklé problémy a využít nového prostředí v prospěch daného podniku (Zuzák a Königová, 2009).

Podnikové procesy představují základní aktivum firem. Mají přímý vliv na atraktivitu výrobků a služeb, které vnímá trh. Rozhodují o úkolech, pracovních místech a odpovědnostech, čímž formují práci každého zaměstnance. Procesy spojují systémy, data a zdroje uvnitř podniku a jakékoli selhání může způsobit ukončení života podniku. Procesy předurčují schopnost podniku přizpůsobit se novým okolnostem a dodržovat legislativní požadavky. Procesy ovlivňují jak potenciální výnosy, tak stojí za vznikem nákladových položek podniku. Na rozdíl od jiného firemního bohatství, jako jsou výrobky, služby, pracovní síla, značka, fyzická nebo finanční aktiva, nebyl podnikovým procesům dlouhou dobu přikládán moc velký důraz. A to i navzdory skutečnosti, že procesy jsou krví, kterou podniky potřebují k životu. Rostoucí požadavky na globalizaci, integraci, standardizaci, inovaci, efektivnost a hledání možných optimalizací podnikových systémů nakonec dopomohly ke zvýšení zájmu a zlepšování podnikových procesů.

Vzhledem k dynamicky se měnícím podmínkám podnikových procesů a inovacím organizace a řízení výroby je nutné se z hlediska manažerských přístupů zabývat řízením podnikových procesů, včetně jejich výkonnosti. V souvislosti s řízením podnikových procesů často přichází na řadu procesní řízení, které bylo vyvoláno nutností změny v řízení podniků, tzn. jistou krizí v manažerském myšlení. A jak je známo, při každé krizi se nám nabízí ji pozitivně využití a vytěžit z ní co nejvíce, takže můžeme v tomto smyslu krizi chápat i jako výzvu ke změnám. (Klouček, 2011; Řepa, 2012; Zuzák a Königová, 2009; Dumas, 2013)

1. TEORETICKÁ VÝCHODISKA

1.1 Procesní řízení a jeho role v řízení podniku

Procesní management neboli procesní řízení je možno definovat různými způsoby. Nejprve je však potřeba porozumět slovu „proces“, se kterými je možné se potkat na každém kroku. Carr a Johansson (1995) definují proces jako soubor provázaných činností, které vezmou vstup, transformují jej a vytvoří výstup. Obdobně definuje proces i Řepa (2007), když uvádí, že proces je objektivně přirozenou posloupností činností, konaných v úmyslem dosažení daného cíle v objektivně daných podmínkách. Dle Basla, Glasla a Tůmy (2002) je proces tokem práce, postupujícím od jednoho člověka k druhému, a v případě větších procesů pravděpodobně z jednoho útvaru do druhého. Weske (2012) uvádí, že proces je složen z řady aktivit, které jsou prováděny v rámci organizačních a technických podmínek podniku

za účelem dosažení podnikového cíle. Šmída (2007) zmiňuje, že proces je organizovaná skupina vzájemně souvisejících činností a/nebo podprocesů, které procházejí jedním nebo více organizačními útvary a spotřebovávají materiální, lidské, finanční a informační vstupy a jejichž výstupem je produkt, který má hodnotu pro externího nebo interního zákazníka.

Řepa (2007) a Grasseová, Dubec a Horák (2008) definují dva typy procesů – klíčové, tzv. hlavní, primární procesy, které jsou zpravidla velmi specifické pro každý podnik, jelikož se odvíjejí od zaměření podniku, ale všechny obsahují aktivity různých oddělení, které vedou k tvorbě produktů nebo obecněji k tvorbě přidané hodnoty pro koncového zákazníka, a podpůrné, vedlejší, sekundární procesy, které slouží k podpoře klíčových procesů, jelikož jim poskytují nebytné zdroje a vstupy, ale nejsou součástí klíčových procesů. Reijers (2003) a Fotr (2012) uvádějí, že se ke klíčovým a podpůrným procesům běžně připojují i procesy řídící, které zabezpečují řízení výkonu podniku a vytvářejí podmínky pro fungování ostatních procesů. Grasseová, Dubec a Horák (2008) dodává, že každý proces má vlastníka, zákazníka, vstupy, výstupy, rizika, omezení, činnosti, začátek a konec a je měřitelný pomocí ukazatelů.

Měření je základním principem řízení procesů, protože bez vhodných ukazatelů procesu a znalosti jejich hodnot není možné proces řídit (Melan, 1989). I proto je možné najít celou řadu důkazů o řešení této problematiky (Hulthén, Näslund a Norrman, 2016; Josifovski a Minovski, 2015; Kleindienst a Biedermann, 2017; Nadarajah a Sharifah Latifah Syed, 2016; Rodrigues, Pigosso a McAloone, 2016; Tuček a Novák, 2014; Van Looy a Shafagatova, 2016; Vuksic, Glavan a Susa, 2015). Dle Šmídy (2007) systém měření výkonnosti podnikových procesů pomocí procesních ukazatelů účinně podporuje jejich fungování a zlepšování, čímž zásadně přispívá k vyšší efektivnosti. Parmenter (2010) rozděluje měřitelné ukazatele procesů na klíčové ukazatele výsledků, ukazatele výkonnosti a klíčové ukazatele výkonnosti. Klíčové ukazatele výkonnosti (Key Performance Indicators, KPI) dle Janišové a Křivánka (2013) měří naplnění strategických cílů a jsou základním kamenem Balanced Scorecard, vyrovnaného systému cílů a měřitelných ukazatelů výkonnosti podniku. Výběr KPI je velmi důležitý, jelikož tyto ukazatele slouží k posouzení výkonnosti procesů (Šmída, 2007). Jednotlivé ukazatele KPI se mohou lišit svou povahou, včetně finančních, kvantitativních, kvalitativních nebo časových údajů, a jsou závislé na specifikách každého podnikového procesu (vom Brocke et al., 2014). Dumas (2013) uvádí jako obecně využitelné KPI například cyklový čas výrobní operace, čas zpracování objednávky, provozní náklady, úroveň externí a interní kvality aj. Parmenter (2010) kromě řady další ukazatelů uvádí například tržní podíl, procentuální ztrátu zákazníků, index spokojenosti zákazníků, počet zrušených objednávek, procento odpadu, cash flow, hodnotu rozpracované výroby, investice do výzkumu a vývoje apod. Ať už si podnik chce zvolit jakékoli KPI ke svým procesům, Šmída (2007) dodává, že dobrý ukazatel procesu musí být přesný, aktuální, objektivní, srozumitelný, finančně nenáročný a snadno spočitatelný.

Smith a Fingar (2003) definují procesní řízení jako systém, který umožňuje realizaci jakékoli existující teorie managementu a podporuje pohotovější vytváření a osvojení nových teorií do podnikové reality. S tím souhlasí Šmída (2007), když zmiňuje, že procesní řízení představuje systém, postupy, metody a nástroje trvalého zajištění maximální výkonnosti podnikových a mezipodnikových procesů, které vycházejí z jasně definované strategie podniku a jejichž cílem je naplnit stanovené strategické cíle. Burlton (2001) upřesňuje, že procesní řízení je samo o sobě procesem, který zajišťuje neustálé zlepšování výkonnosti podniku. Dumas (2013) dodává, že procesní řízení je umění i věda, která spočívá v kontrole toho, jak je prováděna práce v podniku, aby se zajistily konzistentní výsledky a využily příležitostí ke zlepšení.

Procesy a procesní řízení jsou prostředky pro efektivní tvorbu hodnot, jelikož vedou podniky k přemýšlení o svých procesech z pohledu zákazníka a z hlediska výsledků. Podnikové

procesy jsou klíčovými nástroji pro organizování činností a lepší pochopení jejich vzájemných vztahů (Weske, 2012). Procesní řízení je účinným řízením podniku na bázi procesního modelu, kdy jsou jednoznačně definované cíle podniku, které plní očekávání vlastníka, naplňovány neustále zdokonalovanými procesy. Z průzkumu Michaela Hammera vyplývá, že při vyřizování objednávek došlo ke zkrácení času o 60 až 90 % a současně k 25% nárůstu počtu včasných a bezchybných objednávek; náklady související s nákupem materiálu klesly o více než 80 %, spotřeba času se snížila o 90 %, úspěšnost zavádění výrobků se zvýšila o 30 až 50 % a čas na zavedení se zkrátil o 50 až 75 % (Šmída, 2007).

Mallya (2007, s. 23) tvrdí, že v procesně řízeném podniku je základem všeho procesní přístup, díky kterému dochází ke spojení individuí a každé z nich pak do podniku přináší svůj vlastní názor a úhel pohledu ze svého hlediska. K tomu Tůma (2003) dodává, že procesně řízený podnik má jasně stanovené ukazatele výkonnosti, jasně identifikované klíčové a podpůrné procesy a práce je řízena jako ucelený proces, který se člení na vzájemně propojené subprocesy. Tyto procesy se neustále zlepšují a jejich napomáhají k naplnění strategických cílů. Podle Závadského (2005) je procesní řízení systematickou identifikací, vizualizací, měřením, hodnocením a neustálým zlepšováním podnikových procesů s využitím nástrojů, které jsou založené na procesním přístupu. Zde však dodává Řepa (2007), že v praxi však často zaniká podstata, že přemýšlet procesně znamená důkladně změnit tradiční úhel pohledu na všechno v životě podniku, tzn. například opustit klasickou funkční hierarchickou organizační strukturu, zapomenout na mýtus manažerské odpovědnosti za práci podřízených (a tedy neodpovědnosti podřízených) nebo pochopit smysl vývoje technologií a roli technologií při vývoji podniku. U takového podniku se následně předpokládá patřičná pružnost a variantnost postupů. Fotr (2012) doplňuje, že mnoho firem o sobě sice často tvrdí, že jsou procesně orientovány, ale přitom stále respektují funkční strukturu a tím ve výsledku představují určité hybridy, ve kterých se do řízení promítají jak prvky procesního, tak i funkčního managementu. Oproti tomu Galbraith (1995), Hendry (1995), Cameron (1986) a Majchrzak a Wang (1996) tvrdí, že existuje řada firem, které v minulosti začaly využívat procesní řízení, ale přitom nezměnily svou strukturu z funkční na procesní, protože měly dobře nastaven systém řízení a koordinace, autonomie, motivace a učení, a tak procesní úroveň byla v těchto případech chápána jen jako další úhel pohledu na strukturu podniku.

Hlavní problém při implementaci procesního řízení je dle Fišera (2014) u lidí, protože nejsou ochotní změnit své stereotypní chování plynoucí z funkčního řízení. Jeston (2006) dodává, že zaměstnanci se sami z vlastní potřeby neobětují, aby bylo dosaženo nějaké změny, dokud tomu dostatečně nevěří. I přesto, že přechod na procesní řízení není zcela lehký a nese s sebou řadu náročných úkolů, Hammer a Champy (2000) uvádějí několik důvodů, proč k tomuto přechodu z funkčního na procesní řízení přistoupit, a těmi jsou: zjednodušení, zrychlení a zefektivnění proces, konzistentní a transparentní procesy, soulad s regulačními a výkonnostními požadavky a neustálé zlepšování podnikových procesů a optimalizace výkonnosti. Šmída (2007) uvádí, že procesní řízení vede ke snižování nákladů a zvyšování rychlosti a kvality, možnosti kvantifikace jevů a lepšímu odhadování budoucích událostí, schopnosti dosáhnout navzájem nekompatibilních cílů a podpoře disciplíny, týmového ducha, týmové práce a angažovanosti. Současně také dodává, že orientace na podnikové procesy umožňuje předcházet budoucím problémům v nich s využitím různých zlepšovacích programů (Šmída, 2007).

Součástí implementace procesního řízení je také mapování a modelování podnikových procesů. Procesní modelování je součástí procesní analýzy, pomocí které dochází k identifikaci a specifikaci procesů, jejich struktury a charakteristik. Procesní modely představují přehled procesů v podniku a z jednotlivých modelů se skládá procesní mapa podniku. Jelikož každý podnik disponuje velkým množstvím procesů, a s přesáhnutím jejich

úměrně zvladatelného množství rapidně klesá jejich přehlednost a čitelnost, díky procesní mapě je umožněno jejich přehlednost zajistit a zachovat. Procesy jsou organizovány do skupin a vznikají tak celé hierarchie procesů a procesních modelů. (Davis, 2001; Davis, 2008; Davis a Brabander, 2007)

Pomocí procesních modelů se jednodušeji získávají informace a celkový přehled o podnikových procesech. Existuje několik metodik a každý podnik by si měl vybrat tu, která je pro něj nejvhodnější, aby mu co nejvíce sloužila k uspokojení vlastních požadavků. K modelování procesů je možné použít obecné modelovací nástroje nebo speciální nástroje určené pouze pro modelování procesů, například s využitím notace BPMN. Jedním z nástrojů je ARIS Architect & Designer, který je základním nástrojem řady ARIS Platform. (Davis, 2001; Davis, 2008; Davis a Brabander, 2007)

Většina modelovacích nástrojů v dnešní době disponuje možnostmi simulování, např. ADONIS, ARIS Business Designer, IBM Websphere Business Modeler, OpenText ProVision, Oracle Business Process Analysis (BPA) Suite, Savvion Process Modeler, Signavio Process Editor a TIBCO Business Studio. Obecně vzato se však funkcionalita jednotlivých nástrojů dost výrazně odlišuje. (Dumas, 2013)

1.2 Krizové řízení v kontextu procesního řízení

Jak již bylo zmíněno, impulsem pro příchod procesního řízení byla jistá krize řízení v podnikatelském světě, která si vyžádala změnu manažerského přístupu v tomto směru. Ve světě podniků můžeme dle Šefčíka, Tomka a Hrušky (2009) chápat krizi jako neočekávanou událost, která může mít negativní vliv na hospodářský výsledek podniku a může výrazně zhoršit její tržní postavení. A i když krize může mít i jiné podoby, jejím řízením se zabývá krizový management. Haddow, Bullock a Coppola (2014) uvádějí, že krizový management neboli krizové řízení je disciplína zabývající se minimalizací rizika, která zahrnuje přípravu na krizové stavy a mimořádné události, před tím než se stanou, reakce na ně, stejně tak jako podporu a obnovení. Dle Špačka (2008) se jedná o systematickou reakci na neočekávané události, u kterých se předpokládá, že by mohly ohrozit lidi, majetek, finanční či operační stabilitu podniku. A dále dodává, že krizový management není v žádném případě souborem mechanických pravidel, postupů a aktivit, ale souborem promyšlených procesů a postupových kroků zaměřených na předjímání komplexní podstaty krize (Špaček, 2008). Blanchard et al. (2007) tvrdí, že krizové řízení je manažerskou funkcí, která vytváří rámec pro omezení zranitelnosti vůči rizikům. Antušák a Vilášek (2016) definují krizové řízení jako soubor přístupů, postupů, nástrojů a metod využívaných manažery k zajištění funkčnosti podniku během působení nepříznivých vlivů, kdy na zvládnutí krizové situace nestačí jejich běžné kompetence ani prostředky. A dodávají, že se jedná o kontinuální nikdy nekončící proces (Antušák a Vilášek, 2016).

Proces krizového managementu je možné rozdělit na proces řízení rizik, s cílem minimalizace ztrát plynoucích s hrozeb, a proces řízení krizí, s cílem dostat krizi pod kontrolu (Antušák a Vilášek, 2016). Pokud chce podnik minimalizovat rizika uvnitř svého podnikového systému, musí mít přehled o svých podnikových procesech, takže by je měl mít důsledně zmapované a monitorované, a měl by se zabývat jejich neustálým zlepšováním, což indikuje propojení procesního řízení a krizového řízení. Smejkal a Rais (2013) tuto myšlenku podporují konstatováním, že procesně řízený podnik se neobejde bez řízení rizik a krizových situací z hlediska ekonomiky podniku a makroekonomického úhlu pohledu. Procesně řízený podnik se obdobně neobejde ani bez neustálého zlepšování procesů (Elliott, Swartz a Herbane, 2010; Smith, 2005), což je možno označit jako neustálé provádění změn k dosažení lepšího stavu. Propojení krizového řízení a neustálého zlepšování potvrzují i Zuzák a Königová (2009) tím,

že kdo nehledá nové cesty a nereaguje na změny, směřuje do krize. Tato tvrzení podporuje také Řepa (2012), jelikož dle něj komplexní přístup k procesní změně zdůrazňuje silnou potřebu propojení procesního řízení s řízením znalostí, řízením změn, řízením rizik a krizovým řízením z hlediska podnikatelských jednotek.

Kushnareva, Rychkova a Le Grand (2015) tvrdí, že manažeři zabývající se procesním řízením hrají klíčovou roli v krizovém managementu podniku. Smith (2005) a Šmída (2007) zmiňují, že jedním z kritických faktorů úspěchu procesního řízení v podniku je vzdělávání zaměstnanců v oblasti identifikace a řízení rizik a krizového managementu. Smith (2005) dodává, že takové vzdělávání může kdykoli selhat a kvůli tomu se v podniku vytváří prostředí vhodné pro tvorbu a udržování náchylnosti a citlivosti na rizika a krize. Hofmann, Betke a Sackmann (2015) uvádí, že aplikace principů procesního řízení v oblasti krizového řízení je považována za slibný přístup vzhledem k obecným podobnostem podnikových procesů a cílů procesního a krizového řízení. Problematikou zlepšování a podpory krizového řízení aplikací procesního řízení se zabývalo již několika autorů (Fahland a Woith, 2009; Marjanovic a Hallikainen, 2013; Rüppel a Wagenknecht, 2007; Sell a Braun, 2009). Kushnareva, Rychkova a Le Grand (2015) se ve svém výzkumu zaměřili na modelování podnikových procesů pro automatizovanou podporu krizového řízení. Franke a Charoy (2010) navrhli systémový rámec procesního řízení, který spolupracuje při reakci na krizovou situaci a tím podporuje průběh procesu krizového řízení. Nunavath a Prinz (2015) namodelovali proces krizového řízení v podmínkách Norska s využitím notace Business Process Modeling Notation. Weske (2012) konstatuje, že systém procesního řízení, včetně procesních modelů, podporuje provádění činností v rámci krizového řízení, konkrétně ve fázi reakce na krizi. Systém procesního řízení by měl v takovém případě dle Tahir et al. (2008) zajistit poskytnutí všech relevantních informací o vzniknuté krizi. I tak však přímé aplikaci procesního řízení zpravidla brání specifické podmínky, jako jsou jedinečné procesy, náhlé a neočekávané události, časový tlak či urgentnost, masivní zapojení osob, nedokonalé informace atd. (Chen et al., 2008; Franke and Charoy, 2010; Swenson, 2010).

2. CÍL A METODIKA

Hlavním cílem příspěvku je identifikovat a popsat přístup výrobních podniků v ČR při využívání procesního řízení. Na základě stanoveného cíle má tento příspěvek poskytnout odpovědi na následující výzkumné otázky:

- VO1: Jak přistupují výrobní podniky v ČR k využívání procesního řízení?
- VO2: Jak výrobní podniky v ČR softwarově podporují procesní řízení?
- VO3: Jaké podnikové procesy ve výrobních podnicích v ČR patří mezi nejvíce sledované, měřené a hodnocené?
- VO4: Jaké ukazatele procesů jsou sledovány ve výrobních podnicích v ČR?
- VO5: Kolik klíčových ukazatelů výkonnosti podnikových procesů je sledováno ve výrobních podnicích v ČR?

Za účelem zodpovězení výše uvedených výzkumných otázek a naplnění hlavního cíle byla potřebná data o výrobních podnicích v České republice získána pomocí online dotazníkového šetření. Dotazník byl vytvořen online pomocí služby Google Forms a distribuován e-mailem průmyslovým a procesním inženýrům, výrobním manažerů a majitelům výrobních podniků napříč celou Českou republikou. Záměrem bylo dosáhnout co největšího počtu respondentů z různých sektorů národního hospodářství ze všech regionů České republiky. Dotazníkové šetření probíhalo v průběhu roku 2017. Celkově bylo získáno 460 kompletně vyplněných

dotazníků. Vzhledem k zaměření na výrobní podniky byly z původního souboru dat vyloučeny podniky, které ve své charakteristice uvedly, že jsou zaměřeny na poskytování služeb. Konečný soubor dat zahrnoval odpovědi ze vzorku 400 výrobních podniků z různých oborů. Velikost tohoto výzkumného vzorku je považována za dostatečně reprezentativní. Výzkumu se zúčastnilo přibližně 10 % kontaktovaných podniků. Získané dotazníky a odpovědi respondentů byly následně převedeny ze služby Google Forms na databázi v aplikaci MS Excel. V tomto programu byly taktéž zpracovány základní popisné statistiky pomocí kontingenčních tabulek a provedeny základní popisné a srovnávací analýzy získaných dat.

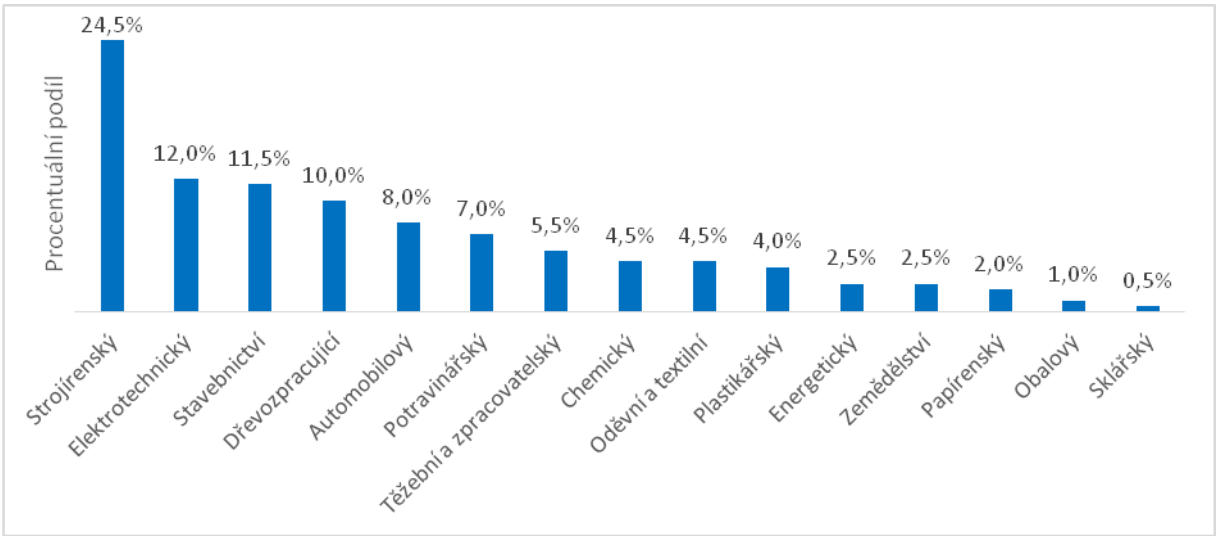
3. VÝSLEDKY

V níže uvedené tabulce (Tab. 1) jsou zachyceny základní charakteristiky výzkumného vzorku výrobních podniků v ČR. Ze znázorněných dat je patrné, že ve vzorku jsou nejvíce zastoupeny malé a střední podniky s 11 až 250 zaměstnanci, dále podniky, které figurují na trhu v ČR již více než 20 let a také podniky, výrobní proces má charakter kusové a sériové výroby.

Počet zaměstnanců			**Doba existence na trhu**			**Typ výrobního procesu**		
Do 10	64	16,0 %	Nad 20 let	202	50,5 %	Kusová	160	40,0 %
11 až 50	114	28,5 %	11 až 20 let	106	26,5 %	Sériová	158	39,5 %
51 až 250	122	30,5 %	6 až 10 let	66	16,5 %	Hromadná	82	20,5 %
251 až 500	58	14,5 %	Do 5 let	26	6,5 %			
Nad 500	42	10,5 %						

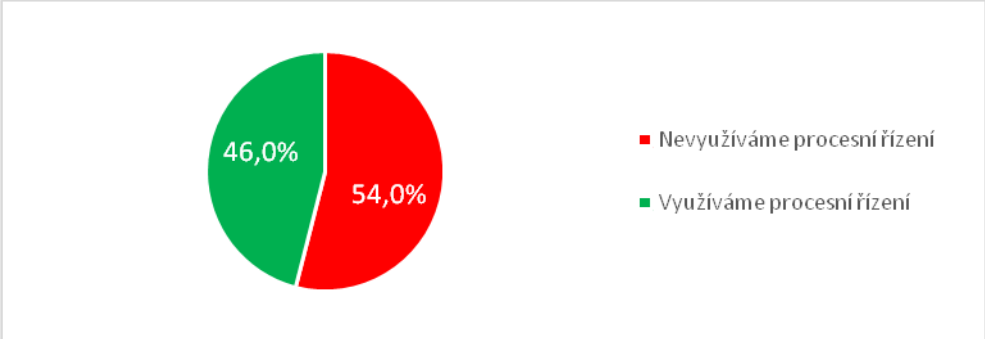
Tab. 8 Základní charakteristiky výzkumného vzorku (Vlastní zpracování)

Následující graf (Obr. 1) znázorňuje strukturu výzkumného vzorku vzhledem k oborové příslušnosti jednotlivých výrobních podniků. Je na první pohled patrné, že ve vzorku jsou nejvíce zastoupeny podniky působící ve strojírenském průmyslu (98 podniků; 24,5 %), které jsou dále následovány podniky zabývajícími se výrobou elektrotechnických komponentů (48 podniků; 12,0 %), stavebnictvím a výrobou stavebního materiálu (46 podniků; 11,5 %) a zpracováním dřeva (40 podniků; 10,0 %).



Obr. 10 Struktura výzkumného souboru dle průmyslového zaměření (Vlastní zpracování)

Aby bylo možné zodpovědět první výzkumnou otázku *(VO1: Jak přistupují výrobní podniky v ČR k využívání procesního řízení?)*, bylo nutné se podívat na danou problematiku z více úhlů pohledu. Níže uvedený graf (Obr. 2) znázorňuje v základním pojetí, jak výrobní podniky využívají či nevyužívají procesní řízení (BPM). Není zde zohledněno, zda podniky, které BPM v současné době nevyužívají, mají či nemají zájem o jeho využívání v budoucnosti.

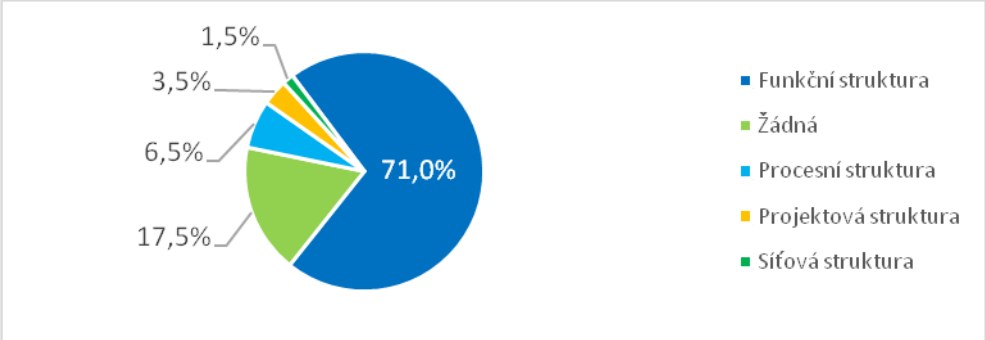


Obr. 11 Využívání procesního řízení (Vlastní zpracování)

Z grafu (Obr. 2) je patrné, že BPM využívá pouze 46,0 % podniků. Není zde však řešena úroveň vyspělosti takto využívaného systému BPM, což znamená, že některé podniky se tímto mohou zabývat důsledněji a výrazně delší dobu než podniky jiné. Z výzkumu vyplývá, že 27,78 % podniků bez BPM se na trhu pohybuje méně jak 10 let, přičemž v případě podniků s BPM je tato hodnota na úrovni 17,39 %. Na druhou stranu 72,22 % podniků bez BPM je na trhu více jak 10 let, ale u podniků s BPM je tato hodnota na úrovni 82,61 %. Je tedy patrné, že podniky se zavedeným BPM se na trhu pohybují delší dobu. Z hlediska velikosti podniku dle počtu zaměstnanců je možné říct, že 58,34 % podniků bez BPM má do 50 zaměstnanců, kdežto 71,74 % podniků s BPM má více jak 50 zaměstnanců. Toto rozdělení potvrzuje také členění dle ročního obratu, jelikož 77,78 % podniků bez BPM vykazuje roční obrat především do 10 milionů eur a 58,69 % podniků s BPM dosahuje ročního obratu většího jak 10 milionů eur. Rozdíl mezi těmito dvěma skupinami podniků je také v charakteru výrobního procesu. Podniky bez BPM jsou více charakteristické kusovou výrobou (48,15 %), kdežto u podniků

s BPM převládá spíše sériová výroba (48,91 %). V případě hromadné výroby nejsou patrné žádné zásadní rozdíly (20,37 % u podniků bez BPM a 20,65 % u podniků s BPM). Další rozdíly mezi podniky s a bez BPM jsou patrné také z hlediska sledování, měření a hodnocení procesů a ukazatelů. Mezi podniky bez BPM je 12,04 % takových, které nesledují žádné podnikové procesy a 75,93 %, které nesledují žádné KPI. Naopak v případě podniků s BPM je pouze 3,26 % takových, které nesledují žádné podnikové procesy a 52,17 % nesleduje žádné KPI.

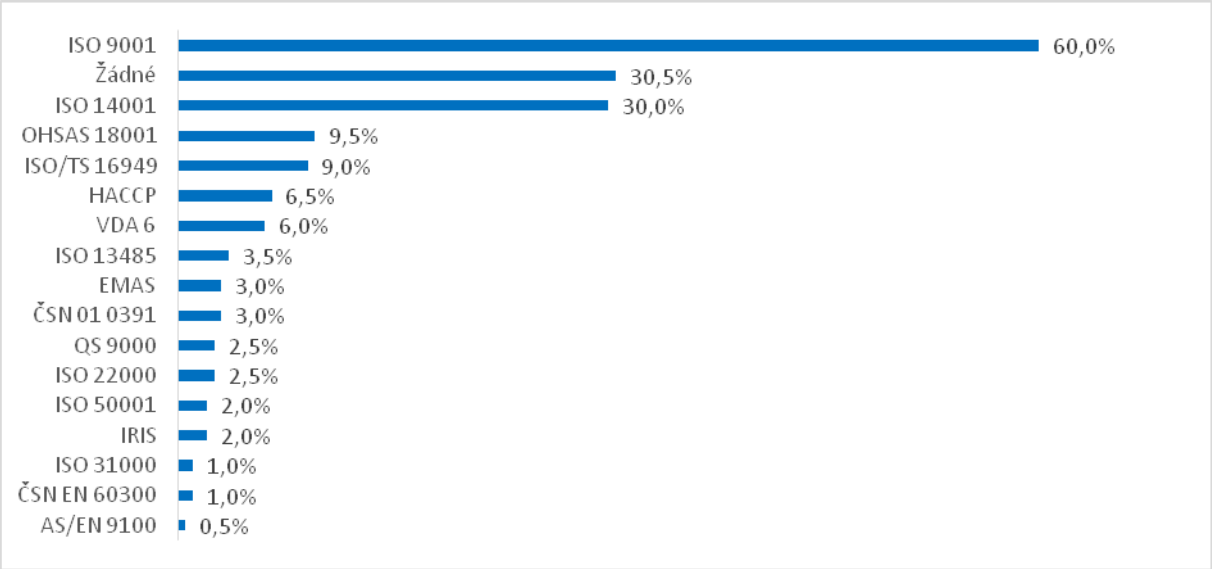
Vhodné je také zmínit, že mezi podniky s BPM je 76,09 % podniků s funkční organizační strukturou, což může být vysvětleno postupným přechodem na procesní řízení nebo ne zcela nutnou přeměnou funkční struktury na procesní či jinou podobnou strukturu, jak je uvedeno v literární rešerši. Pouze 3,26 % podniků s BPM nemá stanovenu žádnou organizační strukturu podniku. Naopak v případě podniků bez BPM jde o 29,63 % podniků bez organizační struktury a v podstatě všechny ostatní podniky v této skupině využívají funkční organizační strukturu. Zastoupení organizačních struktur v celém vzorku podniků je znázorněno na grafu (Obr. 3).



Obr. 12 Organizační struktury podniků (Vlastní zpracování)

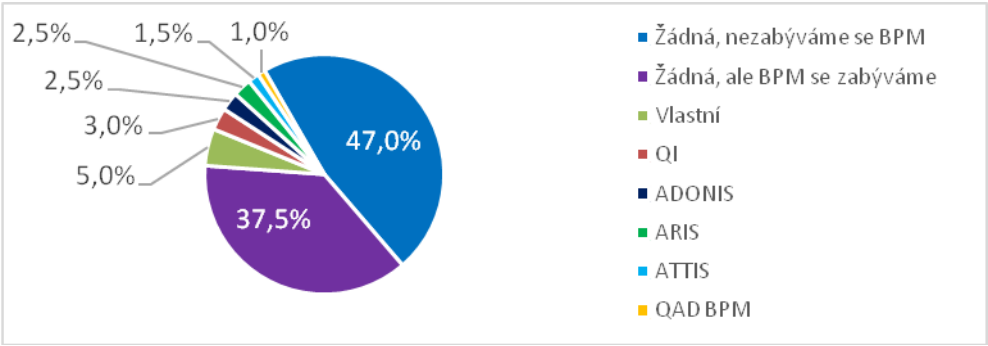
Většina podniků (71,0 %) má stanovenu funkční organizační strukturu a procesní organizační struktura je zastoupena pouze nepatrně (6,5 %). I přesto však 92,31 % podniků s procesní organizační strukturou působí na trhu více než 10 let, v 53,85 % případů zaměstnávají do 50 zaměstnanců a 69,23 % podniků s procesní strukturou spadá do strojírenského, automobilového a elektrotechnického průmyslu. Celkem 70 podniků (17,5 %) uvedlo, že nemají stanovenu žádnou organizační strukturu, a 91,43 % z těchto podniků nevyužívá BPM. Na druhou stranu využívá BPM přibližně 49,3 % podniků, které mají stanovenu funkční organizační strukturu. A všechny podniky, které mají stanovenu procesní nebo síťovou organizační strukturu také využívají BPM, u podniků s projektovou organizační strukturou BPM využívá přibližně 50 %.

Vzhledem k tomu, že na procesním řízení jsou založeny normy ISO řady 9000 a tyto tím pádem dávají podnikům jistý základ procesního řízení v oblasti managementu kvality, je v rámci dalšího grafu (Obr. 4) znázorněno i využití této normy ve výrobních podnicích v ČR. Pro porovnání jsou zde současně uvedeny i další normy, které jsou v podnicích využívány. Je na první pohled patrné, že ISO 9001 je nejvíce využívanou normou, jelikož její využití uvedlo 60,0 % podniků. Mimo to však 30,5 % podniků uvedlo, že při výkonu své činnosti žádné obdobné normy nevyužívají. Z výzkumu dále vyplývá, že i když podniky nevyužívají BPM, tak využívají ISO 9001 ve 44,44 % případů. Mimo to bylo zjištěno, že 77,17 % podniků využívajících BPM také současně využívá ISO 9001 a že 59,66 % z těch, co využívají ISO 9001, současně využívají také BPM.



Obr. 13 Využití norem v podnicích (Vlastní zpracování)

Níže uvedený graf (Obr. 5) poskytuje odpověď na druhou výzkumnou otázku *(VO2: Jak výrobní podniky v ČR softwarově podporují procesní řízení?)*, jelikož znázorňuje využití softwarové (IT) podpory procesního řízení u výrobních podniků v ČR. Celkem 47,0 % podniků uvedlo, že nevyužívají žádnou softwarovou podporu, jelikož se procesním řízením nezabývají a dále 37,5 % podniků taktéž nevyužívá žádnou softwarovou podporu, i když využívají BPM. Vzhledem k tomu, že výzkumem bylo zjištěno, že 54,0 % podniků nevyužívá BPM, je zde jistý nesoulad, takže i když 15,5 % podniků využívá nějakou softwarovou podporu BPM, přibližně polovina z nich se nezabývá procesním řízením. Tím pádem je tedy možné předpokládat, že tento software zkoušejí pro možné budoucí využití, příp. jim umožňuje jiné funkcionality, které jejich dosavadní podnikový software neumožňuje, bez ohledu na využívání procesního řízení. Jedná se většinou o software vytvořený nebo upravený pro vlastní potřeby podniku.



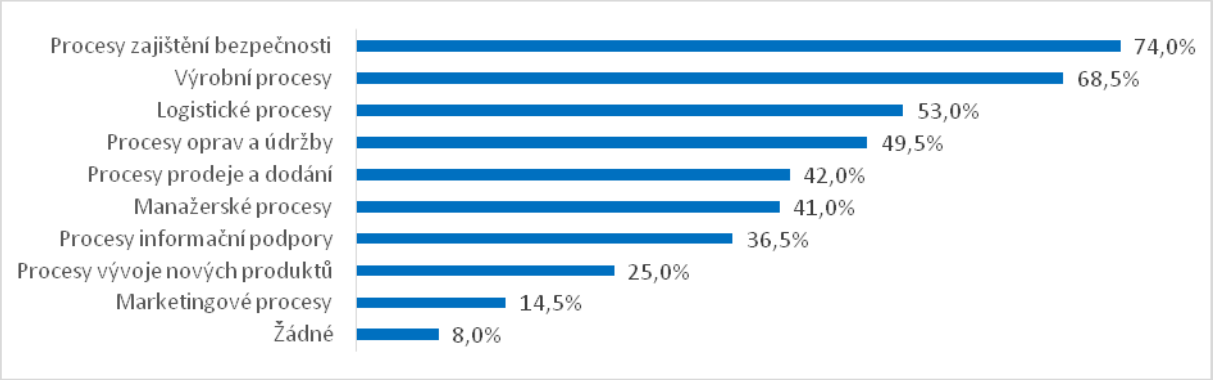
Obr. 14 Využití softwarové (IT) podpory procesního řízení (Vlastní zpracování)

Dále bylo u jednotlivých konkrétních podpůrných řešení zjištěno, u monitoringu kterých procesů se nejvíce využívají:

- ADONIS (BOC Group) – Procesy zajištění bezpečnosti, Procesy oprav a údržby, Výrobní procesy

- ARIS (Software AG) – nebyly identifikovány žádné konkrétní procesní oblasti, obecnější využití
- ATTIS (ATTN Consulting) – Procesy zajištění bezpečnosti, Manažerské procesy, Výrobní procesy
- QAD (QAD Inc.) – Procesy zajištění bezpečnosti, Procesy informační podpory, Logistické procesy, Procesy prodeje a dodání, Výrobní procesy
- QI (QI GROUP) – Procesy oprav a údržby, Procesy prodeje a dodání
- Vlastní – Manažerské procesy, Výrobní procesy, Procesy zajištění bezpečnosti

Následující graf (Obr. 6) odpovídá na třetí výzkumnou otázku *(VO3: Jaké podnikové procesy ve výrobních podnicích v ČR patří mezi nejvíce sledované, měřené a hodnocené?)*, jelikož ilustruje sledované, měřené a hodnocené procesy. Nejvíce podniků sleduje, měří a hodnotí procesy související se zajištěním bezpečnosti (74,0 %). Dále jsou také pod dohledem podniků i procesy výrobní (68,5 %), což lze u výrobních podniků očekávat, stejně jako se očekávalo, že tyto procesy budou zastoupeny daleko více, jelikož vzorek byl složen jen z výrobních podniků.



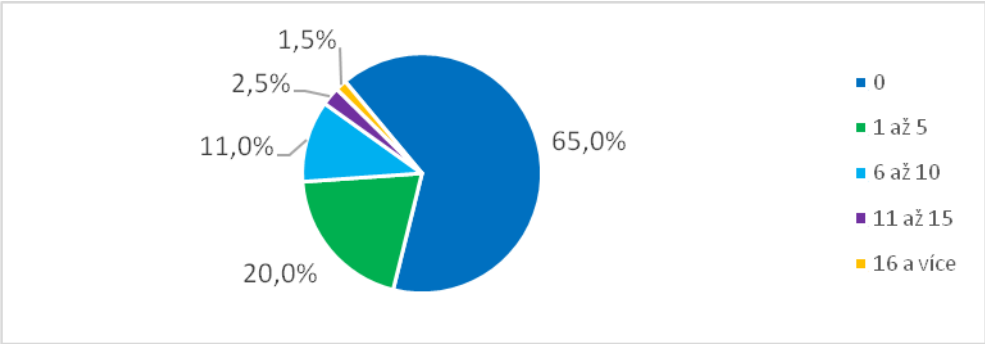
Obr. 15 Sledované, měřené a hodnocené procesy (Vlastní zpracování)

Nejméně podniků (8,0 %) nesleduje, neměří a nehodnotí žádné procesy, přičemž 18,75 % z těchto podniků dle výzkumu využívá BPM, tudíž by měly své procesy sledovat, měřit a hodnotit. Jedná se primárně o podniky zaměstnávající maximálně 50 zaměstnanců, působící na trhu méně jak 10 let a dosahující ročního obratu do 2 milionů eur.

Níže uvedený graf (Obr. 7) odpovídá na čtvrtou výzkumnou otázku *(VO4: Jaké ukazatele procesů jsou sledovány ve výrobních podnicích v ČR?)*. Z výzkumu vyplývá, že nejčastěji sledovaným ukazatelem podnikových procesů jsou náklady na daný proces (56,5 %). Dále výrobní podniky sledují kvalitu procesu (46,0 %), plnění norem výkonu (45,5 %), produktivitu na pracovníka (45,5 %) a hodnotu realizované produkce (45,0 %). Přibližně 11,0 % podniků nesleduje žádné ukazatele podnikových procesů. Všechny tyto podniky navíc nevyužívají procesní řízení. Přesto však 59,09 % z nich sleduje, měří a hodnotí alespoň jeden podnikový proces, ale není zde patrné, na základě jakých měřítek či ukazatelů takové hodnocení probíhá. Opět se jedná primárně o podniky zaměstnávající maximálně 50 zaměstnanců, působící na trhu méně jak 10 let a dosahující ročního obratu do 2 milionů eur.

Obr. 16 Sledované ukazatele výkonnosti procesů (Vlastní zpracování)

Následující graf (Obr. 8) dává odpověď na pátou výzkumnou otázku *(VO5: Kolik klíčových ukazatelů výkonnosti podnikových procesů je sledováno ve výrobních podnicích v ČR?).* Z výsledků výzkumu je patrné, že 65,0 % podniků nesleduje ani jeden klíčový ukazatel výkonnosti. Z těchto podniků však 86,92 % podniků sleduje a hodnotí alespoň jeden procesní ukazatel, přičemž tento ukazatel není klíčovým ukazatelem výkonnosti. Zbylých 13,08 % těchto podniků nesleduje žádné ukazatele procesů. Vhodné je doplnit, že 36,92 % z podniků, které nesledují ani jeden ukazatel KPI, využívá procesní řízení, takže by se v těchto případech očekávalo, že nějaké KPI sledovat budou. Dále se ukazuje, že podniky preferují sledování menšího počtu KPI (s rostoucím počtem sledovaných KPI klesá počet podniků, které je sledují), např. 1 až 5 KPI v tomto případě sleduje 20 % podniků, ale pouze 1,5 % podniků sleduje 16 a více KPI.



Obr. 17 Počet sledovaných klíčových ukazatelů výkonnosti (Vlastní zpracování)

ZÁVĚR

Hlavním cílem příspěvku bylo identifikovat a popsat přístup výrobních podniků v ČR při využívání procesního řízení. Pro účely naplnění tohoto cíle byl realizován výzkum formou online dotazníkového šetření, do kterého se zapojilo 460 podniků v ČR, z nichž bylo pro další zpracování využito údajů od 400 výrobních podniků.

V rámci literární rešerše, která zkoumala procesní a krizové řízení a jejich vzájemný vztah, bylo zjištěno, že procesně řízený podnik se neobejde jak bez krizového řízení a řízení rizik, tak ani bez neustálého zlepšování procesů, protože kdo nehledá nové cesty a nereaguje na změny, směřuje do krize. Komplexní přístup k procesní změně totiž zdůrazňuje silnou potřebu propojení procesního řízení s řízením znalostí, řízením změn, řízením rizik a krizovým řízením. I proto je pro úspěch procesního řízení důležité vzdělávání zaměstnanců v oblasti identifikace a řízení rizik a krizového managementu.

Dále bylo položeno pět výzkumných otázek, na které byly v rámci výzkumu nalezeny odpovědi. *VO1:* Bylo zjištěno, že BPM využívá pouze 46,0 % výrobních podniků v ČR. Předmětem však nebylo zjistit úroveň vyspělosti využívaných systémů BPM. Z výzkumu vyplývá, že podniky s BPM se na trhu pohybují delší dobu než podniky bez BPM a jsou větší, jak dle počtu zaměstnanců, tak i dle ročního obratu. Rozdíl mezi podniky s BPM a bez BPM je také v charakteru výrobního procesu. Další rozdíly jsou patrné také z hlediska sledování, měření a hodnocení procesů a ukazatelů. Mezi podniky s BPM je 76,09 % podniků s funkční organizační strukturou, což může být vysvětleno postupným přechodem na procesní řízení nebo ne zcela nutnou přeměnou funkční struktury. Obecně má většina výrobních podniků stanovenu funkční organizační strukturu a procesní organizační struktura je zastoupena pouze nepatrně. I přesto všechny podniky s procesní nebo síťovou strukturou využívají BPM.

VO2: Celkem 47,0 % výrobních podniků uvedlo, že nevyužívají žádnou softwarovou podporu, jelikož nevyužívají BPM. Dalších 37,5 % výrobních podniků nevyužívá žádnou softwarovou podporu, i když využívají BPM. Zajímavé je, že 15,5 % výrobních podniků využívá nějakou softwarovou podporu BPM, ale přibližně polovina z nich nevyužívá BPM. U jednotlivých konkrétních podpůrných řešení bylo zjištěno, u monitoringu kterých procesů se nejvíce využívají.

VO3: Nejvíce podniků sleduje, měří a hodnotí procesy související se zajištěním bezpečnosti. Dále jsou také pod dohledem podniků i procesy výrobní, což lze u výrobních podniků očekávat. Nejméně podniků (8,0 %) nesleduje, neměří a nehodnotí žádné procesy, přičemž 18,75 % z těchto podniků využívá BPM, tudíž by měly své procesy sledovat, měřit a hodnotit.

VO4: Nejčastěji sledovanými ukazateli podnikových procesů jsou náklady na proces, kvalita procesu, plnění výkonnostních norem, produktivita na pracovníka a hodnota realizované produkce. Přibližně 11,0 % podniků nesleduje žádné ukazatele.

VO5: Z výzkumu je patrné, že 65,0 % podniků nesleduje ani jeden klíčový ukazatel výkonnosti. Z těchto podniků však 86,92 % podniků sleduje a hodnotí alespoň jeden procesní ukazatel, přičemž tento ukazatel není klíčovým ukazatelem výkonnosti. Dále se ukazuje, že podniky preferují sledování menšího počtu KPI (s rostoucím počtem sledovaných KPI klesá počet podniků, které je sledují).

Tato studie doporučuje výrobním podnikům více využívat procesní řízení, a to v kombinaci s krizovým řízením a řízením rizik, jelikož se jedná o nástroj spolupracující s těmito dvěma nástroji managementu, který podporuje jejich společné aktivity. Vyžívání procesního řízení dopomáhá k lepšímu organizování činností, pochopení jejich vzájemných vztahů, neustálému zlepšování podnikových procesů a zvyšování jejich výkonnosti, naplňování strategických cílů a zvyšování konkurenceschopnosti podniku.

PODĚKOVÁNÍ

Tento příspěvek byl zpracován jako jeden z výstupů projektu financovaného Interní grantovou agenturou FaME UTB, č. IGA/FaME/2017/015 Vliv vybraných metod průmyslového inženýrství na celkovou výkonnost podniku a výkonnost jeho procesů.

Literatura

[1] ANTUŠÁK, Emil a Josef VILÁŠEK, 2016. *Základy teorie krizového managementu.* Praha: Univerzita Karlova v Praze, Karolinum Press, 130 s. ISBN 978-80-246-3443-2.

[2] BASL, Josef, Vít GLASL a Miroslav TŮMA, 2002. *Modelování a optimalizace podnikových procesů.* Plzeň: Západočeská univerzita v Plzni, 140 s. ISBN 80-7082-936-2.

[3] BLANCHARD, Wayne B. et al., 2007. Principles of Emergency Management. In: *International Association of Emergency Managers* [online]. Falls Church [cit. 2018-08-08]. Dostupné z: http://bit.ly/2MprPCQ

[4] BURLTON, Roger T., 2001. *Business Process Management: Profiting From Process.* Indianapolis: Sams, 416 s. ISBN 978-06-723-2063-7.

[5] CAMERON, Kim S., 1986. Effectiveness as Paradox: Consensus and Conflict in Conceptions of Organisational Effectiveness. *Management Science* [online]. Linthicum: Institute for Operations Research and the Management Sciences, 32(5), 539-553 [cit. 2018-08-08]. ISSN 0025-1909. Dostupné z: http://bit.ly/2LlRRS2

[6] CARR, David K. a Henry J. JOHANSSON, 1995. *Best Practices in Reengineering: What Works and What Doesn't in the Reengineering Process.* New York: McGraw-Hill Professional, 288 s. ISBN 978-00-701-1224-7.

[7] DAVIS, Rob, 2001. *Business Process Modelling with ARIS: A Practical Guide.* London: Springer, 556 s. ISBN 978-18-523-3434-5.

[8] DAVIS, Rob, 2008. *ARIS Design Platform: Advanced Process Modelling and Administration.* London: Springer, 408 s. ISBN 978-18-480-0110-7.

[9] DAVIS, Rob a Eric BRABANDER, 2007. *ARIS Design Platform: Getting Started with BPM.* London: Springer, 364 s. ISBN 978-18-462-8612-4.

[10] DUMAS, Marlon, 2013. *Fundamentals of Business Process Management.* Berlin: Springer, 399 s. ISBN 978-3-642-33142-8.

[11] ELLIOTT, Dominic, Ethné SWARTZ a Brahim HERBANE, 2010. *Business Continuity Management: A Crisis Management Approach.* 2nd ed. New York: Routledge, 338 s. ISBN 978-0-415-37109-4.

[12] FAHLAND, Dirk a Heiko WOITH, 2009. Towards Process Models for Disaster Response. In: *Business Process Management Workshops (BPM 2008)* [online]. Milano, September 2008. Berlin: Springer, 17, 254-265 [cit. 2018-08-08]. ISBN: 978-3-642-00328-8. DOI: 10.1007/978-3-642-00328-8_25. Dostupné z: http://bit.ly/2NgeRUE

[13] FIŠER, Roman, 2014. *Procesní řízení pro manažery: Jak zařídit, aby lidé věděli, chtěli, uměli i mohli.* Praha: Grada, 173 s. ISBN 978-80-247-5038-5.

[14] FOTR, Jiří, 2012. *Tvorba strategie a strategické plánování: Teorie a praxe.* Praha: Grada, 381 s. ISBN 978-80-247-3985-4.

[15] FRANKE, Jörn a François CHAROY, 2010. Design of a Collaborative Disaster Response Process Management System. In: *9th International Conference on Designing Cooperative Systems* [online]. Aix-en-Provence, May 2010. London: Springer, 57-77 [cit. 2018-08-08]. ISBN: 978-1-84996-211-7. DOI: 10.1007/978-1-84996-211-7_5. Dostupné z: http://bit.ly/2wejkAL

[16] GALBRAITH, Jay R., 2001. *Designing Organizations: An Executive Guide to Strategy, Structure, and Process Revised.* 2nd ed. San Francisco: Jossey & Bass, 196 s. ISBN 978-0787957452

[17] GRASSEOVÁ, Monika, Radek DUBEC a Roman HORÁK, 2008. *Procesní řízení ve veřejném sektoru: Teoretická východiska a praktické příklady.* Brno: Computer Press, 266 s. ISBN 978-80-251-1987-7.

[18] HADDOW, George D., Jane A. BULLOCK a Damon P. COPPOLA, 2014. *Introduction to Emergency Management.* Fifth edition. Amsterdam: Elsevier, 422 s. ISBN 978-0-12-407784-3.

[19] HAMMER, Michael a James CHAMPY, 2000. *Reengineering - radikální proměna firmy: Manifest revoluce v podnikání.* 3. vyd. Praha: Management Press, 212 s. ISBN 80-726-1028-7.

[20] HENDRY, John, 1995. Process Reengineering and the Dynamic Balance of the Organisation. *European Management Journal* [online]. Oxford: Elsevier, 13(1), 52-58 [cit. 2018-08-08]. ISSN 0263-2373. Dostupné z: http://bit.ly/2OZFFsr

[21] HOFMANN, Marlen, Hans BETKE a Stefan SACKMANN, 2015. Process-oriented Disaster Response Management: A Structured Literature Review. *Business Process Management Journal* [online]. Bradford: Emerald, 21(5), 966-987 [cit. 2018-08-08]. ISSN 1463-7154. DOI: 10.1108/BPMJ-07-2014-0069. Dostupné z: http://bit.ly/2N7012u

[22] HULTHÉN, Hana, Dag NÄSLUND a Andreas NORRMAN, 2016. Framework for Measuring Performance of the Sales and Operations Planning Process. *International Journal of Physical Distribution & Logistics Management* [online]. Bradford: Emerald, 46(9), 809-835 [cit. 2018-08-08]. ISSN 0960-0035. Dostupné z: http://bit.ly/2o32AI5

[23] CHEN, Rui, Raj SHARMAN, H. Raghav RAO a Shambhu J. UPADHYAYA, 2008. Coordination in Emergency Response Management. *Magazine Communications of the ACM* [online]. New York: ACM, 51(5), 66-73 [cit. 2018-08-08]. DOI: 10.1145/1342327.1342340. Dostupné z: http://bit.ly/2BC5QUw

[24] JANIŠOVÁ, Dana a Mirko KŘIVÁNEK, 2013. *Velká kniha o řízení firmy: Praktické postupy pro úspěšný rozvoj.* Praha: Grada, 2013, 394 s. ISBN 978-80-247-4337-0.

[25] JESTON, John, 2018. *Business Process Management: Practical Guidelines to Successful Implementations.* Fourth edition. London: Taylor & Francis, 653 s. ISBN 978-1-138-73840-9.

[26] JOSIFOVSKI, Darko a Robert MINOVSKI, 2015. Defining a Performance Measurement System as an Improvement to the New Product Development Process. *Annals of the Faculty of Engineering Hunedoara* [online]. Hunedoara: Faculty of Engineering Hunedoara, 13(2), 25-28 [cit. 2018-08-08]. ISSN 1584-2665. Dostupné z: http://bit.ly/2LlstMg

[27] KLEINDIENST, Bernd a Hubert BIEDERMANN, 2017. Involving Employees in the Development Process of Performance Measurement and Management Systems. *Annals*

of the Faculty of Engineering Hunedoara [online]. Hunedoara: Faculty of Engineering Hunedoara, 15(2), 17-24 [cit. 2018-08-08]. ISSN 1584-2665. Dostupné z: http://bit.ly/2N8jgZn

[28] KLOUČEK, Jan, 2011. Management kvality a jeho důležitost v období po Světové hospodářské krizi. In: *Construction Maeconomics Conference* [online]. Praha: České vysoké učení technické v Praze, 12. 10. 2011 [cit. 2018-08-08]. Dostupné z: http://bit.ly/2nQYz9v

[29] KUSHNAREVA, Elena, Irina RYCHKOVA a Bénédicte LE GRAND, 2015. Modeling Business Processes for Automated Crisis Management Support: Lessons Learned. In: *2015 IEEE 9th International Conference on Research Challenges in Information Science (RCIS)* [online]. Athens, IEEE, May 13-15, 2015, 388-399 [cit. 2018-08-08]. ISBN: 978-1-4673-6630-4. DOI: 10.1109/RCIS.2015.7128900. Dostupné z: http://bit.ly/2PvgnDB

[30] MAJCHRZAK, Ann a Qianwei WANG, 1986. Breaking the Functional Mind-Set in Process Organizations. *Harvard Business Review* [online]. Boston: Harvard Business Review, 74(5), 92-99 [cit. 2018-08-08]. ISSN 0017-8012. Dostupné z: http://bit.ly/2Ndb0ro

[31] MALLYA, Thaddeus, 2007. *Základy strategického řízení a rozhodování.* Praha: Grada, 246 s. ISBN 978-80-247-1911-5.

[32] MARJANOVIC, Olivera a Petri HALLIKAINEN, 2013. Disaster Recovery – New Challenges and Opportunities for Business Process Management Research and Practice. *Pacific Asia Journal of the Association for Information Systems* [online]. Association for Information Systems, 5(1), 23-43 [cit. 2018-08-08]. ISSN 1943-7544. Dostupné z: http://bit.ly/2MpZLzr

[33] MELAN, Eugene H., 1989. Process Management: A Unifying Framework for Improvement. *National Productivity Review* [online]. New York: Wiley Periodicals, 8(4), 395-406 [cit. 2018-08-08]. ISSN 0277-8556. Dostupné z: http://bit.ly/2PtmYi9

[34] NADARAJAH, Devika a A. Kadir SHARIFAH LATIFAH SYED, 2016. Measuring Business Process Management Using Business Process Orientation and Process Improvement Initiatives. *Business Process Management Journal* [online]. Bradford: Emerald, 22(6), 1069-1078 [cit. 2018-08-08]. ISSN 1463-7154. DOI: 10.1108/BPMJ-01-2014-0001. Dostupné z: http://bit.ly/2BFivpL

[35] NUNAVATH, Vimala a Andreas PRINZ, 2015. Norwegian Emergency Management Process by Using Business Process Modeling Notation. In: *8th IADIS International Conference Information Systems* [online]. Madeira, March 2015, 205-210 [cit. 2018-08-08]. ISBN: 978-9-8985-3333-3. DOI: 10.13140/RG.2.1.5146.4403. Dostupné z: http://bit.ly/2MHRhDa

[36] PARMENTER, David, 2010. *Key Performance Indicators: Developing, Implementing, and Using Winning KPIs.* 2nd ed. Hoboken: John Wiley, 299 s. ISBN 978-0-470-54515-7.

[37] REIJERS, Hajo A., Monique H. JANSEN-VULLERS, Michael ZUR MUEHLEN a Winfried APPL, 2007. Workflow Management Systems + Swarm Intelligence = Dynamic Task Assignment for Emergency Management Applications. *Business Process Management* [online]. Berlin: Springer, 4714, 125-140 [cit. 2018-08-08]. DOI: 10.1007/978-3-540-75183-0_10. Dostupné z: http://bit.ly/2wf8ycD

[38] RODRIGUES, Vinícius P., Daniela C. A. PIGOSSO a Tim C. MCALOONE, 2016. Process-related Key Performance Indicators for Measuring Sustainability Performance of Ecodesign Implementation into Product Development. *Journal of Cleaner Production* [online]. Oxford: Elsevier, 139, 416-428 [cit. 2018-08-08]. ISSN 0959-6526. DOI: 10.1016/j.jclepro.2016.08.046. Dostupné z: http://bit.ly/2w9oZYw

[39] RUEPPEL, Uwe a Armin WAGENKNECHT, 2007. Improving Emergency Management by Formal Dynamic Process-Modelling. In: *24th Conference on Information Technology in Construction* [online]. Maribor, June 2007, 559-564 [cit. 2018-08-08]. Dostupné z: http://bit.ly/2wf459y

[40] ŘEPA, Václav, 2007. *Podnikové procesy: Procesní řízení a modelování.* 2., aktualiz. a rozš. vyd. Praha: Grada, 281 s. ISBN 978-80-247-2252-8.

[41] ŘEPA, Václav, 2012. *Procesně řízená organizace.* Praha: Grada, 301 s. ISBN 978-80-247-4128-4.

[42] SELL, Christian a Iris BRAUN, 2009. Using a Workflow Management System to Manage Emergency Plans. In: *6th International Conference on Information Systems for Crisis Response and Management* [online]. Gothenburg, May 2009, 41, 43-50 [cit. 2018-08-08]. Dostupné z: http://bit.ly/2OZ3W1M

[43] SMEJKAL, Vladimír a Karel RAIS, 2013. *Řízení rizik ve firmách a jiných organizacích.* 4., aktualiz. a rozš. vyd. Praha: Grada, 483 s. ISBN 978-80-247-4644-9.

[44] SMITH, Denis, 2005. Business (not) as Usual: Crisis Management, Service Recovery and the Vulnerability of Organisations. *The Journal of Services Marketing* [online]. Santa Barbara: Emerald, 19(5), 309-320 [cit. 2018-08-08]. ISSN 0887-6045. DOI: 10.1108/08876040510609925. Dostupné z: http://bit.ly/2Mtssv6

[45] SMITH, Howard a Peter FINGAR, 2003. *Business Process Management: The Third Wave.* Tampa: Meghan-Kiffer Press, 292 s. ISBN 09-296-5233-9.

[46] SWENSON, Keith D., 2010. *Mastering the Unpredictable: How Adaptive Case Management Will Revolutionize the Way that Knowledge Workers Get Things Done.* Tampa: Meghan-Kiffer Press, 354 s. ISBN: 978-0929652122.

[47] ŠEFČÍK, Vladimír, Miroslav TOMEK a Miroslav HRUŠKA, 2009. *Krizové řízení v malých a středních podnicích.* Zlín: Univerzita Tomáše Bati ve Zlíně, 181 s. ISBN 978-80-7318-867-2.

[48] ŠMÍDA, Filip, 2007. *Zavádění a rozvoj procesního řízení ve firmě.* Praha: Grada, 293 s. ISBN 978-80-247-1679-4.

[49] ŠPAČEK, Miroslav, 2008. Krizový management a jeho zvládání. In: *Moderní řízení* [online]. Praha [cit. 2018-08-08]. Dostupné z: http://bit.ly/2BtSidt

[50] TAHIR, Omar et al., 2008. A Collaborative Information System Architecture for Process-Based Crisis Management. In: *12th International Conference on Knowledge-Based Intelligent Information and Engineering Systems (KES 2008)* [online]. Zagreb, 2008. Berlin: Springer, 5179, 630-641 [cit. 2018-08-08]. ISBN: 978-3-540-85567-5. DOI: 10.1007/978-3-540-85567-5_78. Dostupné z: http://bit.ly/2OVrLYr

[51] TUČEK, David a Zdeněk NOVÁK, 2014. Process Management and Performance Measurement in Energy Area of Czech Production Plants. In: *Proceedings of the 6th European Conference on Intellectual Capital (ECIC 2014)* [online]. Bratislava, Slovak Univ Technol, Fac Mat Sci & Technol, April 10-11, 2014, 273-282. ISBN: 978-1-909507-24-1. Dostupné z: http://bit.ly/2wnCMdi

[52] TŮMA, Miroslav, 2003. Jak zavést procesní organizaci podniku. In: *SystemOnLine* [online]. Praha [cit. 2018-08-08]. Dostupné z: http://bit.ly/2BuRULQ

[53] VAN LOOY, Amy a Aygun SHAFAGATOVA, 2016. Business Process Performance Measurement: A Structured Literature Review of Indicators, Measures and Metrics. *SpringerPlus* [online]. Heidelberg: Springer, 5(1), 1-24, [cit. 2018-08-08]. DOI: 10.1186/s40064-016-3498-1. Dostupné z: http://bit.ly/2BKkxoe

[54] VOM BROCKE, Jan, Theresa SCHMIEDEL, Jan RECKER, Peter TRKMAN a Willem MERTENS, 2014. Ten Principles of Good Business Process Management. *Business Process Management Journal* [online]. Leuven: Emerald, 20(4), 530 [cit. 2018-08-08]. Dostupné z: http://bit.ly/2Mvm1aU

[55] VUKSIC, Vesna Bosilj, Ljubica Milanovic GLAVAN a Dalia SUSA, 2015. The Role of Process Performance Measurement in BPM Adoption Outcomes in Croatia. *Economic and Business Review for Central and South - Eastern Europe* [online]. Ljubljana: University of Ljubljana, Faculty of Economics, 17(1), 117-143, 149-150 [cit. 2018-08-08]. ISSN 1580-0466. Dostupné z: http://bit.ly/2MQLprm

[56] WESKE, Mathias, 2012. *Business Process Management: Concepts, Languages, Architectures.* Berlin: Springer, 368 s. ISBN 978-3-642-28616-2.

[57] ZÁVADSKÝ, Ján, 2005. *Systémové pojednání o procesním řízení.* Praha: Alfa Publishing, 82 s. ISBN: 978-80-868-5115-0

[58] ZUZÁK, Roman a Martina KÖNIGOVÁ, 2009. *Krizové řízení podniku.* 2., aktualiz. a rozš. vyd. Praha: Grada, 253 s. ISBN 978-80-247-3156-8.

ŘÍZENÍ RIZIK SPOJENÝCH S BEZPEČNOSTNÍ LETECKÝCH PODVOZKŮ

RISK MANAGEMENT RELATED TO SAFETY AIRCRAFT LANDING GEAR

RNDr. Jan Procházka, Ph.D., doc. RNDr. Dana Procházková, DrSc., Ing. Jan Král
ČVUT v Praze Fakulta dopravní
Konviktská 20
Praha 1, 110 00
prochj31@fd.cvut.cz

ABSTRAKT

Pro zajištění bezpečnosti lidí a všech základních chráněných aktiv je třeba řídit rizika ve všech odvětvích lidské činnosti. Práce uvádí příklad nástroje pro řízení rizik z oblasti strojírenství, tj. kontrolní seznam. Předmětný seznam se používá pro bezpečnostní audit před testem tlumení nárazu podvozku letounu v okamžiku přistání proto, aby výsledky testu byly správné a spolehlivé a aby měly dobrou vypovídací hodnotu. O výsledky testu se lze pak opřít při vyslovení závěru o tom, zda dané zařízení je bezpečné a spolehlivé a kvalitně plní svou funkci.

KLÍČOVÁ SLOVA

Bezpečnost; ochrana do hloubky; strojírenství; kontrolní seznam; podvozek;

ABSTRACT

For ensuring the safety of humans and all basic protected assets, there is necessary to manage the risks in all branches of human activities. The paper gives the example of tool for the risk management from the field of engineering. This check list is used for safety audit before the test of dumping the aircraft landing gear bump test at moment of landing from the reason, so the test results may be correct, reliable and good validity. On such test results it is possible to lean on when we make the outcome whether the given device is safe, reliable and fulfil its function with high quality.

KEY WORDS

Safety; defence in depth; engineering; check list; landing gear;

ÚVOD

Bezpečnost je v současném celosvětovém dění velice častým diskutovaným tématem, neboť je záležitostí celé řady odvětví lidské činnosti, mezi které také patří doprava. Se stále rostoucím počtem dopravních prostředků narůstá také počet různých nehod a tragických událostí. Proto je potřeba, aby dopravní prostředky splňovaly přísnější standardy, normy a předpisy, tj. neustále se zvyšují nároky na bezpečnost strojních zařízení.

Bezpečnosti leteckého provozu je v jednotlivých zemích i na mezinárodní úrovni věnována značná pozornost, neboť případné selhání techniky nebo lidského faktoru v předmětné oblasti může vést jak k velkým materiálním škodám, tak ke ztrátám na životech a zdraví značného počtu lidi. Proto jsou všechny činnosti související s leteckým provozem celosvětově poměrně

přísně regulovány. Většina zemí má pro danou oblast vytvořen soubor zákonů, směrnic a standardů, které usměrňují všechny činnosti s touto oblasti související.

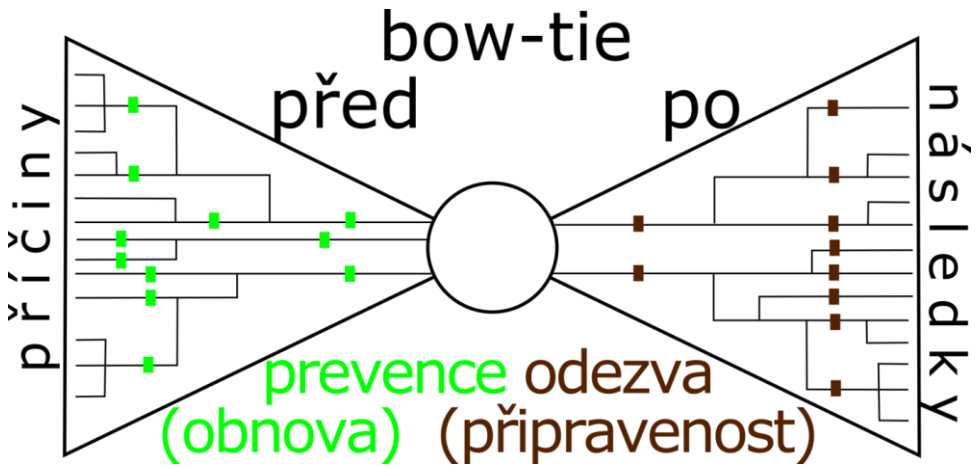
Speciální místo v souborech dokumentů mají předpisy stanovující technické požadavky na konstrukci letecké techniky a zejména požadavky na její bezpečnost. Dokumenty mají zpravidla závazný charakter a každý výrobce, který chce leteckou techniku vyrábět, je musí akceptovat a jejich dodržení stanoveným způsobem prokazovat [1]. Znalost příslušných dokumentů a požadavků, které jsou v nich specifikovány, je nevyhnutným předpokladem pro úspěšnou realizaci předvýrobních (vývojových) etap u každého výrobků leteckého průmyslu. Testování letadel a jeho jednotlivých částí je dnes rozsáhlým vědním oborem, který souvisí s rychlým rozvojem letectví. Jednou z nejdůležitějších částí letadla je přistávací zařízení, které je zejména při přistání vystaveno značnému zatížení. Letecká názvoslovná norma ČSN 31 0001 definuje pojem „Přistávací zařízení“ jako část letadla umožňující vzlet, přistání, popř. pojíždění. Podvozek je v dané normě definován jako základní konstrukční skupina přistávacího zařízení [1]. Jeho porušení může mít za následek poškození až zničení celého letadla, včetně ohrožení bezpečnosti cestujících. Z uvedených a mnoha dalších důvodů se od přistávacího zařízení požaduje velká bezpečnost a vysoká spolehlivost po celou dobu životnosti letounu, která u některých letounů může znamenat až desítky tisíc vzletů a přistání. Proto je potřeba jak při návrhu nového přistávacího zařízení, tak i při jeho pravidelných kontrolách a revizích věnovat patřičnou pozornost bezpečnosti, a to hlavně řízení jednotlivých rizik vyplývajících z konstrukce, funkce a způsobu řízení, montáže a údržby. Musí být provedena taková opatření, aby se závažná rizika eliminovala nebo snížila na úroveň, která je akceptovatelná.

Přeložená práce obsahuje výsledek výzkumu, který je detailně popsán v práci [1], a to kontrolní seznam [2] pro bezpečnostní audit před testem tlumení nárazu podvozku letounu v okamžiku přistání. Předmětný výrobek hraje zásadní roli při přistání.

1. VÍCEÚROVŇOVÝ PŘÍSTUP „OCHRANA DO HLOUBKY“

Defence in depth, volně přeloženo ochrana do hloubky, je označení pro původně vojenskou strategii obrany za využití mnoha menších obraných opatření místo jednoho obřího opevnění. Do civilní bezpečnosti se poprvé dostala tato strategie v oblasti jaderné bezpečnosti [3]. V dnešní době je využívána především v oblasti bezpečnosti v anglosaském světě v kybernetických, informačních a řídicích systémech. Své uplatnění má ale ve všech oblastech bezpečnosti.

Základní přístup strategie spočívá v tom, že každý prvek obrany, každá bezpečnostní bariéra může někdy selhat, model švýcarského sýru [4]. Příkladem takového selhání v oblasti jaderné energetiky je například havárie jaderné elektrárny Fukušima. Většina prvků areálu byla proti přílivové vlně chráněna pouze zdí. Nepočítalo se možností selhaní zdi, přičemž výška zdi byla určena predikcí na základě příliš krátkého časového období dat. Jako příklad správné aplikace strategie „defense in depth“ můžeme uvést identifikaci všech scénářů během „Bow-tie“ analýzy, obrázek 1.



Obr. 1 Schéma bow-tie analýzy, bezpečnostní bariéry preventivní zeleně a reaktivní hnědou barvou

Bow-tie analýza se skládá z identifikace všech možných příčin, které mohou vést k studované události, s tím, že se do příčin počítají i nežádoucí vzájemné závislosti (Fault-tree analýza). Druhou částí jsou pak všechny scénáře, které za vlivů nejrůznějších faktorů mohou následkem studované události nastat (Event-tree analýza). Aplikace strategie defense in depth pak vyžaduje použití více úrovní bariér. Nevytváříme obranu jenom proti bezprostředním příčinám pohromy, ale i proti okolnostem a podmínkám, které mohou zhoršit okolnosti problémů (problematika skoro-nehod). V oblasti reaktivní odezvy se pak musíme připravit na zvládnutí nouzových situací o rozměrech paradigmatických, kritických až extrémních, což opět tvoří sérii bariér.

Výsledkem aplikace strategie defense in depth tak je série ochranných vrstev, preventivních i reaktivních, kde u nejrůznějších pohrom spoléháme, že neselžou všechny a některá z nich zajistí ochranu chráněných zájmů. Základní chybou v této strategii pak může být dopuštění degradace některého z opatření s tím, že problém bude zvládnut předchozími či následujícími bezpečnostními bariérami. Taková to selhání pak jsou v praxi vysvětlována mýtickými označeními „black swan“ či „dragon king“ ale většinou jde o kombinaci znalostního deficitu a porušení principu předběžné opatrnosti jako například v případě havárie plošiny Deepwater Horizon [5].

2. BEZPEČNOST LETECKÝCH PODVOZKŮ

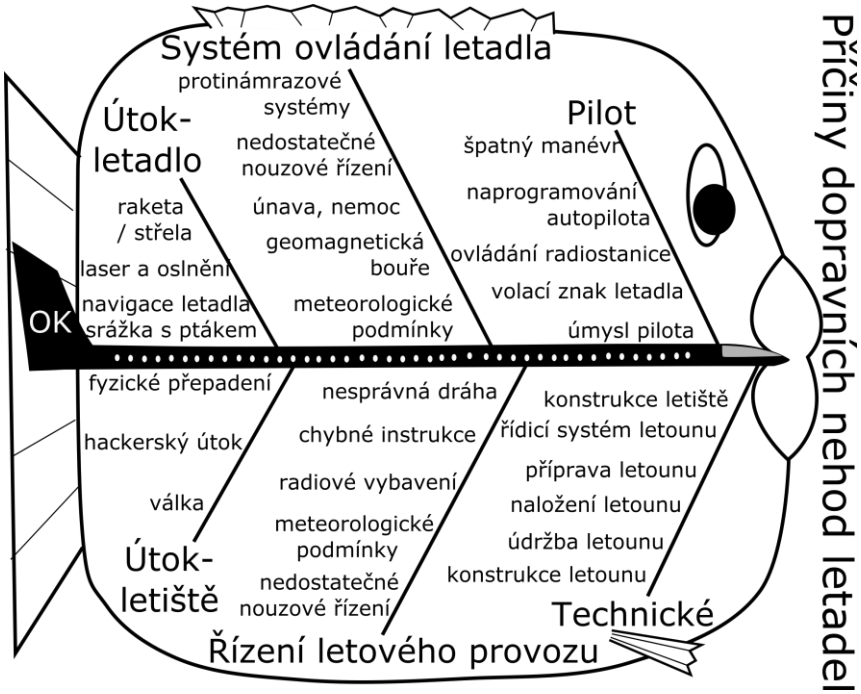
V případě bezpečnosti letecké přepravy můžeme příčiny leteckých havárii rozdělit podle příčin na celou řadu nejrůznějších odvětví, obrázek 2, [6]. Zajištění bezpečí celého systému je pak nutné zajistit bezpečnostními opatřeními na všech úrovních řízeného systému, v tomto případě letecké dopravy. V článku [6] jsou doporučení pro bezpečnost na nejvyšší úrovni řízení, tedy řízení letecké dopravy. Vedle toho je potřeba nastavit opatření na úrovni řízení letadla, technická / lidský faktor s ohledem na požadavky zbytku systému a konečně je nutné zajistit bezpečnost i na úrovni dílčích prvků systému. Například součástí letadla jako je motor [7] nebo třeba podvozek.

2.1 Historický vývoj podvozku letounu

Jedno z prvních skutečných přistávacích zařízení na letadlech (jednoduchý a spolehlivý tříbodový podvozek, často s příďovým kolem) bylo použito v roce 1903, kdy byl k pohonu letounu použit spalovací motor. Do té doby byly používány většinou lyže a starty byly

realizovány z kolejnic za pomoci katapultu (bratři Wrightové). V průběhu 1. světové války se z důvodu vpředu umístěné vrtule velkého průměru ustálila koncepce dvoukolového hlavního podvozku a jednoduché ostruhy v zadní části letadla. Tlumení přistávacího rázu bylo řešeno pomoci gumového lana omotaného kolem osy hlavního podvozku a podvozkové nohy[1].

S rostoucí rychlostí letadel ve 20. letech 20. století se začínají vyrábět první zatahovací podvozky, které měly snížit aerodynamický odpor letounu. Koncem 2. světové války se začaly vyrábět první letouny vybavené reaktivním pohonem a při stále se zvyšujících rychlostech se začal opět používat podvozek s příďovým kolem, který usnadnil vzlet a hlavně přistání. I když konstrukce letadel od této doby prošla celou řadou změn, tak k žádným výrazným změnám v koncepci podvozků nedošlo. Podvozky s ostruhou lze vidět na některých amatérských konstrukcích a na moderních letounech stavěných speciálně pro leteckou akrobacii [1].



Obr. 2 Příčiny dopravních nehod letadel

2.2 Požadavky na podvozek letounu při přistání

Speciální místo v souborech dokumentů zajišťujících bezpečnost letectví mají předpisy stanovující technické požadavky na konstrukci letecké techniky a zejména požadavky na bezpečnost a spolehlivost letecké techniky po celou dobu životnosti. Předmětné dokumenty mají zpravidla závazný charakter a každý výrobce, který chce leteckou techniku vyrábět, je musí akceptovat a jejich dodržení stanoveným způsobem prokazovat. Znalost příslušných dokumentů a požadavků, které jsou v nich specifikovány, je tedy nevyhnutelným předpokladem pro úspěšnou realizaci předvýrobních (vývojových) etap u každého výrobků leteckého průmyslu.

Testování letadel a jeho jednotlivých částí je dnes rozsáhlým vědním oborem, který souvisí s rychlým rozvojem letectví. Jednou z nejdůležitějších částí letadla je přistávací zařízení, které je zejména při přistání vystaveno značnému zatížení. Jak již bylo uvedeno, jeho porušení může mít za následek poškození až zničení celého letadla, včetně ohrožení bezpečí cestujících. Z těchto a mnoha dalších důvodů se od přistávacího zařízení požaduje vysoká

bezpečnost a spolehlivost po celou dobu životnosti letounu, která u některých letounů může znamenat až desítky tisíc vzletů a přistání [8]. Proto je potřeba jak při návrhu nového přistávacího zařízení, tak i při jeho pravidelných kontrolách a revizích věnovat patřičnou pozornost bezpečnosti, včetně posouzení jednotlivých rizik vyplývajících z konstrukce, funkce a způsobu řízení, montáže a údržby. Musí být provedena taková opatření, aby se různá rizika eliminovala nebo snížila na takovou úroveň, aby byla akceptovatelná [8,9].

Nejzávažnější zatížení letounu bývá od přistání. Přistávající letadlo se přibližuje k zemi klouzavým letem. Při plavání letadla blízko nad zemí nastane ustálený stav, kdy aerodynamický vztlak vyváží sílu tíže letadla a zvýšený aerodynamický odpor zabrzďuje pohyb, až nastane částečná ztráta vztlaku, propadání letadla a náraz na přistávací plochu. Tato fáze přistání je nejdůležitější pro přistávací zařízení, neboť vytváří počáteční podmínky pro jeho funkci [10]. Při ideálním přistání se letoun v okamžiku „podrovnání“ a ztráty vztlaku již dotýká koly podvozku země. Klesací rychlost je téměř nulová a přistávací náraz je minimální. Toto je ideální případ. Prakticky ale dochází k tomu, že letoun má při dotyku se zemí jistou nezanedbatelnou klesací rychlost, nebo v případě brzkého podrovnání dojde ke ztrátě vztlaku ještě před dotykem se zemí. Konstrukce podvozku musí přenést a utlumit zatížení i od těchto mimořádných přistání, ke kterým zejména dochází u méně zkušených pilotů, případně za zhoršených podmínek viditelnosti [1,10].

2.3 Dynamické zkoušení leteckých podvozků

Ve stavbě letadel je dnes hlavním cílem zvyšování životnosti leteckých podvozků [1,8]. Proto se soustavně studují skutečné poměry v provozu a usiluje se o co nejvěrnější napodobování jejich namáhání v leteckých zkušebnách. To platí i o zkoušení přistávacích zařízeni, především podvozků, které jsou při rozjezdu a zejména při přistání velmi namáhány. Pro laboratorní zkoušky podvozků byl v ČR vyvinut v padesátých letech minulého století a uveden do provozu v Aeru Radotín (později Technometra Radotín) první „Padostroj“ PS-1, který umožňoval provádět první dynamické zkoušky na pohlcení mechanické práce (pádové zkoušky) leteckých podvozků na dopadovou plošinu [1].

V šedesátých letech minulého století byl uveden do provozu ve Výzkumném a zkušebním leteckém ústavu v Praze Letňanech (VZLÚ) nový víceúčelový zkušební stroj. Jedná se o univerzální padostroj, na němž lze se samotným podvozkem napodobit přistání skutečného letadla, za působení hlavních činitelů, které přistání ovlivňuji, jako je dopředná rychlost letadla, jeho hmota, rychlost klesání, vztlaková odlehčující síla atd., a to pro případy symetrického i nesymetrického přistání. Relativní pohyb letadla vůči zemi se simuluje pádem vozu s podvozkem na roztočený buben setrvačníkového zařízení, sleduje se převzetí kinetické energie svislého pohybu letadla prací tlumicí soustavy podvozku a zabrzdění dopředné složky pohybu letadla až do jeho zastavení přeměnou kinetické energie v teplo, dané prací brzd na kolech podvozku při zanedbání aerodynamických, event. jiných (např. brzdicí padáky) odporů [1,10], který dovoluje komplexní vyšetřování přistávacích zařízení [1].

3. DATA POUŽITÁ PRO SESTAVENÍ KONTROLNÍHO SEZNAMU

Pro zajištění bezpečnosti každého strojního zařízení a bezpečí obsluhy je velice důležité identifikovat všechna možná nebezpečí vyplývající z konstrukce nebo způsobu předpokládaného používání daného zařízení [11]. Proto je třeba mít nástroj a postup pro identifikaci nebezpečí a stanovení rizik, abychom včas identifikovali, že něco je nesprávné a určili místo, kde je třeba pro dosažení správného výsledku provést opatření. Předmětný nástroj je třeba správně použít tak, aby ve sledovaném případě byl test kvalitní a dal správné

výsledky. Proto jsme zvolili nástroje, a to postup ve formě bezpečnostního auditu podle nástroje kontrolní seznam [2,12], které jsou nástroji rizikového inženýrství [13].

Cílem je zajistit, aby testy podvozků byly správné a spolehlivé a aby měly dobrou vypovídací hodnotu. Proto byly použity jak teoretické znalosti [1,2,11-13], technická dokumentace a postupy pro provádění zkoušek na Padostroji PS 1 s nohou hlavního podvozku levou/pravou (nebo příďového, kde se uvažuje předepsané vztlakové vyvážení) včetně úplného kola za daných klimatických podmínek (20°C +/-5°C) [1], tak experimentální data z prováděných testů na Padostroji PS-1 [1]. Pro civilní letouny je test stavu podvozku prováděna podle požadavků předpisu EASA CS-23/FAR (letouny kategorie normální, cvičná, akrobatická a pro sběrnou dopravu) Part 23, AMDT. 23-55, § 23.725, § 23.726, §23.727 [8,9]. Pro vojenské letouny je zkouška prováděna podle požadavků technických podmínek vydaných výrobcem na základě požadavků zadavatele [8].

Kontrolní seznam (Check List [14]) je postup sloužící k systematické kontrole plnění předem stanovených podmínek vycházejících z předešlých zkušeností. Jedná se vlastně o seznam kontrolních otázek podle kterých je možno jednoduše ověřit stav sledovaného objektu a zajistit tak, že nejsou přehlédnuty žádné neshody. Pomocí kontrolního seznamu můžeme sledovat stav plnění nějakého souboru činností. Kontrolní seznamy otázek lze použít pro různé činnosti v kterékoliv fázi jejich životního cyklu. Jednou z možných činností může být kontrola strojního zařízení a lidského faktoru. V našem případě se jedná o postup prací na Padostroji PS-1 při testu tlumení nárazu podvozku letounu v okamžiku přistání. Kontrolní seznamy se mohou také značně lišit, co se týče úrovně detailů, a mohou být využívány k označení splnění standardů a zvyklostí. V případě navrhovaného kontrolního seznamu je snahou vyhovět v rámci jednoho dokumentu jak obsluze stroje, tak řídícím a kontrolním orgánům.

4. KONTROLNÍ SEZNAM PRO BEZPEČNOSTÍ AUDIT SLOUŽÍCÍ K PROVĚŘENÍ STAVU PADOSTROJE PŘED TESTEM PODVOZKU

Při sestavení kontrolního seznamu pro sledovaný proces jsme dbali na splnění požadavků uvedených v pracích [2,12], tj. kontrolní seznam musí být jasný, stručný a srozumitelný pro všechny strany a musí být zamezeno i jakékoliv dvojsmyslnosti. Jelikož podle [2,12] má analýza rizik pomocí kontrolního seznamu dva zásadní kroky a to: odpovědi na otázky; a celkové vyhodnocení, tak jsme pro bezpečnostní audit testu navrhli následující postup:

- odpovědi na otázky kontrolního seznamu ANO či NE,
- v případě, že se vyskytne odpověď NE, tak žádat dohlížejícího kontrolora o posouzení důležitosti činnosti, tj. o rozhodnutí: zda lze dále pokračovat v auditu a procesu testu, anebo
  je nutné provést nápravná opatření, aby požadavek byl splněn.

Vytvořený kontrolní seznam je uveden v tabulce 1.

číslo	Otázka	ano	ne
	1. Administrativní úkony		
1	Je platné povolení úřadů k provádění testů podvozků? (platnost Oprávnění vydaného ÚCL a Osvědčením ke zkoušení vydaným OVL MO)		
2	Jsou splněny podmínky uvedené v Příručce podnikové jakosti? (Příručka jakosti rozpracovává a popisuje systém řízení jakosti a uvádí jeho základní úroveň)		
3	Je podepsán předávací protokol testovaného podvozku?		
4	Je vydáno zadání (metodika, technické podmínky a specifikace) pro zkoušku		

	podvozku daného typu?		
5	Je vydán postup instalace senzorů na podvozek daného typu pro zkoušku?		
6	Je testovaný podvozek správně upevněn, aby nedošlo k ovlivnění výsledků testů?		
7	Souhlasí výrobní číslo zkoušeného podvozku se zadáním?		
8	Je přítomen osvědčující pracovník (kontrolor), který průběh testu sleduje?		
2. Bezpečnost práce			
9	Jsou při obsluze Padostroje PS-1 dodržovány zásady bezpečnosti práce?		
10	Je pracovní prostředí vhodné k provádění příslušných zkušebních prací z pohledu znečištění zkušebních prostor?		
11	Je pracovní prostředí vhodné k provádění příslušných zkušebních prací z pohledu dostatečného osvětlení?		
12	Je pracovní prostředí vhodné k provádění příslušných zkušebních prací z pohledu hladiny hluku?		
13	Byla provedena kontrola teploty pracovního prostředí, zda odpovídá podmínkám pro provádění zkoušky? (20°C +/-5°C)		
3. Kontrola Padostroje PS-1 před vlastní zkouškou			
14	Byla provedena kontrola knihy údržby Padostroje PS-1 zda má platný interval do další kontroly?		
15	Byla provedena vizuální kontrola stavu stroje?		
16	Byla provedena kontrola olejoznaku hydraulického systému na olejové nádrži v horní části stroje?		
4. Instalace senzorů na testovaný podvozek			
17	Jsou k dispozici senzory určené k instalaci na testovaný podvozek?		
18	Je testovaný podvozek řádně a bezpečně upevněn na transportním přípravku?		
19	Je provedena instalace senzorů na podvozek daného typu pro zkoušku podle vydaného postupu a průvodky práce?		
20	Jsou řádně připevněny konektory senzorů a propojovací kabeláž k testovanému podvozku?		
5. Instalace přípravku sloužícího k upnutí zkoušeného podvozku k pohyblivému stolu Padostroje PS-1, za předpokladu, kdy není instalováno závaží a pohyblivý stůl je spuštěn na bezpečnostní podpěře			
21	Má přípravek sloužící k upevnění testovaného podvozku k Padostroji PS-1 platnou revizi?		
22	Je vertikálně pohyblivý vůz podepřen bezpečnostní podpěrou?		
23	Byly provedeny úkony potřebné k instalaci přípravku sloužícího k upnutí zkoušeného podvozku k pohyblivému stolu Padostroje PS-1? (prodloužení manipulační délky hydraulického systému)		
24	Je přípravek bezpečně ustaven na manipulačním vozíku?		
25	Je přípravek ustaven a spojen s danou soustavou vhodnými svorníky dle technické specifikace a průvodky práce?		
26	Je vertikálně pohyblivý vůz spuštěn s nainstalovaným přípravkem na bezpečnostní podpěru?		
27	Byly provedeny zpětné úkony potřebné k instalaci přípravku sloužícího k upnutí zkoušeného podvozku k pohyblivému stolu Padostroje PS-1 ? (zkrácení manipulační délky hydraulického systému)		
6. Naložení závaží na pohyblivý stůl			
28	Je vertikálně pohyblivý vůz pomocí hydraulického systému zdvižen do horní krajní polohy Padostroje PS-1 k zásobníku závaží? (kontrola volného chodu pohyblivého vozíku)		
29	Je potřebný počet závaží - desek (dle technické specifikace a průvodky práce) uvolněno na vertikálně pohyblivý vůz?		
30	Je zbylé závaží v horní části stroje řádně zajištěno v nosných tyčích zajišťovacími kolíky? (pozor - řádně překontrolovat, nebezpečí úrazu!!!)		
31	Je vertikálně pohyblivý vůz pomocí hydraulického systému spuštěn do dolní polohy a opřen o bezpečnostní podporu? (kontrola volného chodu pohyblivého vozíku)		
32	Jsou desky závaží zajištěny na pohyblivém stole sponami?		
33	Je vertikálně pohyblivý vůz se závažím dovážen pytli s olověnou drtí podle technické specifikace zkoušeného podvozku a průvodky práce?		
7. Instalace podvozku do přípravku na pohyblivém stolu			
34	Je do přípravku instalován testovaný podvozek včetně kola, případně brzdy dle		

	průvodky práce?		
35	Je zkontrolován plnící tlak v tlumiči a v pneumatice testovaného podvozku pomocí kalibrovaných manometrů?		
36	Je spojeno měřící lanko celkového propérování podvozku s unášečem pásového měřítka?		
	8. Seřízení polohy „nula“ celkového propérování		
37	Je seřízená poloha lanka a pásového měřítka celkového propérování nastaveného na hodnotu „nula“ okamžiku dotyku kola a dopadové desky?		
	9. Simulace vztlakové síly pomocí pružných provazců		
38	Jsou instalovány držáky lan do vodících trubek ve vztlakových křídlech a nasunuty na dvojice vodících tyčí?		
39	Je potřebný počet lan stejnoměrně rozdělen a zaháknut do ok držáků pružných lan? (pozor - lana nesmí být překřížena!!!),		
40	Jsou v „nulové“ poloze podvozku (dotyk kola s dopadovou deskou) zajištěny držáky na vodících tyčích maticemi?		
	10. Předpětí pružných provazců		
41	Je provedena změna předpětí pružných provazců v horní části padostroje? (pozor - provádět při uvolněných lanech!!!)		
	11. Kontrola hmotnosti zkoušené soustavy		
42	Je připojen měřící zesilovač k senzoru síly?		
43	Je provedeno zahřátí, řádné nastavení a vynulování měřícího zesilovače síly?		
44	Je připojen senzor síly k měřící aparatuře, včetně senzorů umístněných na zkoušené podvozkové noze (senzor propérování a statického přetížení), senzor celkového propérování (senzor absolutního lineárního odměřování)?		
45	Jsou propojovací kabely mezi měřící ústřednou a senzory uspořádány tak, aby nebránili při vlastním měření a aby nedošlo také k jejich poškození?		
46	Je zapnuté napájení měřící ústředny a obslužný software PC pro sledování měřených parametrů, v tomto případě hmotnost zkoušené soustavy?		
47	Jsou v případě použití vztlakových lan tato lana odpojena?		
48	Je zkoušená soustava po odstranění bezpečnostní podpěry spuštěna na dopadovou desku?		
49	Je odjištěn zámek dopadového vozíku? („odhoz“ z nulové výšky)		
50	Bylo provedeno odečtení a zaznamenání hodnoty hmotnosti zkoušené soustavy z displeje zesilovače, zda odpovídá požadované velikosti?		
51	Bylo provedeno odečtení a uložení hodnoty hmotnosti zkoušené soustavy z displeje PC, zda odpovídá požadované velikosti?		
52	Je po kontrole hmotnosti zkoušené soustavy vertikálně pohyblivý vůz zdvižen a zajištěn zámek dopadového vozíku?		
53	Je vložena bezpečnostní podpora a vůz spuštěn na tuto podporu?		
54	Je potřeba soustavu dovážit a opakovat vážení zkoušené soustavy?		
55	Jsou v případě použití vztlakových lan tato lana znovu připojena?		
	12. Pádová zkouška		
56	Je zkoušená soustava zdvižena na předepsanou pádovou výšku dle technické specifikace a průvodky práce?		
57	Je řádně nastaven měřící zesilovač pro měření dopadové síly?		
58	Je správně nastaveno měřící lanko celkového propérování?		
59	Je zapnuté napájení měřící ústředny a obslužný software PC pro sledování měřených parametrů?		
60	Je vynulována poloha celkového propérování prostřednictvím software – proveden reset?		
61	Je odstraněna bezpečnostní podpora?		
62	Je spuštěna ochranná klec do dolní polohy?		
63	Je odjištěn zámek odhozu zamáčknutím žlutého tlačítka na ovládacím pultu?		
64	Je spuštěn záznam měřící aparatury software - PLAY?		
65	Je proveden odhoz s následnou vizuální kontrolou celé soustavy, zda nedošlo k nepředvídatelným událostem ohrožující bezpečnost obsluhy Padostroje PS-1?		
66	Je vyzdvižena ochranná klec do horní polohy?		
67	Je proveden odečet měřených parametrů a jejich zápis do tabulky naměřených hodnot?		
68	Je vypnut záznam měřící aparatury a provedena kontrola naměřených dat s následným		

	vyhodnocením testu?		
13. Zpětné zapojení pohyblivého stolu			
69	Je otevřen regulační ventil hydraulického systému a spuštěn vůz ke stolu?		
70	Jsou čelisti zámku řádně zapadnuty za ozuby na trnu vozu?		
71	Je zámek zajištěn zamáčknutím stříbrného tlačítka?		
72	Je provedena kontrola zapadnutí západky zámku?		
73	Je uzavřen regulační ventil hydraulického systému umožňující spouštění vozu?		
74	Je zdvižena zkoušená soustava do patřičné výšky v případě pokračování zkoušky?		
75	Je v případě ukončení zkoušky vložena bezpečností podpora a vůz je spuštěn na tuto podporu?		
14. Odstranění simulace vztlakové síly pokud byla použita			
76	Jsou v nulové“ poloze podvozku (dotyk kola s dopadovou deskou) odstraněny držáky na vodících tyčích sejmutím matic?		
77	Jsou odstraněny držáky lan vodících trubek ve vztlakových křídlech?		
78	Jsou vysunuty dvojice vodících tyčí vztlakové síly?		
15. Demontáž podvozku			
79	Je odpojeno měřící lanko celkového propérování s unášečem pásového měřítka?		
80	Jsou odpojeny vodiče od senzorů umístněných na zkoušené podvozkové noze (senzor propérování a statického přetížení?		
81	Je z přípravku vyjmuta testovaná podvozková noha dle průvodky práce?		
16. Sejmutí závaží (desek) z pohyblivého stolu			
82	Jsou odstraněny pytle s olověnou drtí, jsou-li použity?		
83	Jsou sejmuty zajišťovací spony desek na pohyblivém stolu?		
84	Je vertikálně pohyblivý vůz pomocí hydraulického systému zdvižen do horní krajní polohy Padostroje PS-1 k zásobníku závaží? (kontrola volného chodu pohyblivého vozíku)		
85	Jsou řádně zajištěny desky závaží v nosných tyčích zajišťovacími kolíky? (pozor - řádně překontrolovat, nebezpečí úrazu!!!)		
86	Je prázdný stůl bez závaží spuštěn do dolní polohy a opřen o bezpečnostní podporu?		
87	Je při spouštění zkontrolován volný chod vozíku?		
17. Demontáž přípravku sloužícího k upnutí zkoušeného podvozku k pohyblivému stolu			
88	Je vertikálně pohyblivý vůz podepřen bezpečnostní podpěrou?		
89	Byly provedeny úkony potřebné k vyjmutí přípravku sloužícího k upnutí zkoušeného podvozku k pohyblivému stolu Padostroje PS-1? (prodloužení manipulační délky hydraulického systému)		
90	Je přípravek rozpojen s danou soustavou vyjmutím svorníků dle technické specifikace a průvodky práce?		
91	Je vertikálně pohyblivý vůz spuštěn bez přípravku na bezpečnostní podpěru?		
92	Byly provedeny zpětné úkony vedoucí ke zkrácení manipulační délky hydraulického systému a uvedení Padostroje PS-1 do výchozího stavu pro další možné práce?		
18. Provedení zápisu do evidenční knihy zkoušek			
93	Je do evidenční knihy proveden záznam pádové zkoušky se všemi náležitostmi?		
19. Vyhodnocení zkoušky			
94	Je zpracován záznam a vyhodnocení zkoušky dle technické specifikace a průvodky práce?		
95	Je vystaven protokol o provedené zkoušce?		

Tab. 1. Kontrolní seznam pro prověření stavu padostroje před testem podvozku

Kontrolní seznam a předmětný postup bezpečnostního auditu je takový proto, že otázky sledují lineární proces, ve kterém jednotlivé úkony na sebe navzájem navazují a nelze je obsluhou samovolně vynechat bez souhlasu nadřízených orgánů. Tato podmínka vyplývá z dokumentu „Příručky zkušebny přistávacích zařízení“ [15], pro kterou se nástroj vytvářel, a ve které se říká, že jakákoliv změna postupů, metodik aj. je možná pouze za souhlasu dozorových podnikových a státních orgánů, a to formou dodatků k platným povolením prováděných zkoušek daného pracoviště, což mimo jiné představuje nemalou administrativní zátěž a časovou prodlevu. V daném případě se hodnotový systém zužuje pouze na hodnocení vynikající, neboť následující krok v kontrolním seznamu může následovat pouze za podmínky

splnění předchozího kroku. Případnou výjimku může jednorázově schválit pouze řídící pracovník při potřebných konstrukčních úpravách, a to pouze v rámci podnikových testů, a to za předpokladu řádného dodržování bezpečnosti při práci.

ZÁVĚR

Práce ukazuje příklad použití nástrojů rizikového inženýrství ve strojírenství, a to pro ocenění rizik při testu tlumení nárazu podvozku letounu v okamžiku přistání. Výsledek testu ukazuje, zda testované přistávací zařízení je či není bezpečný výrobek. Výsledek je důležitý pro bezpečnost letového provozu a hlavně pro lidi, které k přepravě letadla používají.

PODĚKOVÁNÍ

Práce je sepsána v rámci projektu „Řízení rizik a bezpečnost složitých technologických objektů (RIRIZIBE)“ CZ.02.2.69/0.0/0.0/16 _018/000. Za projekt i podporu děkují autoři EU, MŠMT a ČVUT v Praze.

Literatura

[1] KRÁL, J. *Ocenění rizik při testu tlumení nárazu podvozku letounu v okamžiku přistání.* Praha: ČVUT 2015. Diplomová práce, 157 p.

[2] PROCHÁZKOVÁ, D. *Analýza a řízení rizik.* Praha: ČVUT 2011. ISBN 978-80-01-04841-2, 405p.

[3] *INSAG*. [online]. *DEFENCE IN DEPTH IN NUCLEAR SAFETY*, IAEA: Poslední úpravy Červen 1996 [cit.20018-7-26], dostupné z https://www-pub.iaea.org/MTCD /publications/PDF/Pub1013e_web.pdf

[4] REASON, J. *Human error: models and management*, BMJ **320**, 768, 2000.

[5] Office of the Maritime Administrator. *DEEPWATER HORIZON Marine Casualty Investi Gation Report*, IMO Number: 8764597, report Official Number: 2213, vydáno 17.08.2011 [cit.20018-7-26], dostupné z http://www.register-iri.com/forms/upload/ Republic _of_the_Marshall_Islands_DEEPWATER_HORIZON_Marine_Casualty _Investigation_Report-Low_Resolution.pdf

[6] PROCHAZKOVA, D. PROCHAZKA, J. *Causes of accidents in civilian aircraft operation and tools for management of selected risks*, London: Taylor & Francis Group 2017, Safety and Reliability – Theory and Applications ISBN 978-1-138-62937-0, p. 3057.

[7] PROCHAZKOVA, D. PROCHAZKA, J. *Tool for risk reduction at specific component aircraft engine welding*, London: Taylor & Francis Group 2018, Safety and Reliability – Safe Societies in a Changing World ISBN 978-0-8153-8682-7, p. 3138.

[8] SLAVĚTINSKÝ, D. *O letadlech. Koncepce přistávacího zařízení*. Poslední úpravy 25.4.2010 [cit.20016-2-10]. Dostupné na http://www.slavetind.cz/stavba/koncepce /Koncepce_prist_ zar.aspx\

[9] TŮMA, J. *Letadla*. Praha: SNTL 1981. Opora pro učební a studijní obory na SOU.

[10] PETRÁSEK, M. *Základy konstrukce letadel*. Brno: VUT 1999.

[11] MAREK, J. a kol. *Management rizik v konstrukci výrobních strojů*. Praha: Průmyslové spektrum, speciální vydání., 2009. ISSN 1212-2572.

[12] PROCHÁZKOVÁ, D. *Metody, nástroje a techniky pro rizikové inženýrství*. Praha: ČVUT 2011. ISBN: 978-80-01-04842-9, 369p.

[13] PROCHÁZKOVÁ, D. *Bezpečnost složitých technologických systémů.* Praha: ČVUT 2015. ISBN: 978-80-01-05771-1, 208p.

[14] HRUŠKA, Z., SVITÁK, P. *ČSN 31 0001 aneb o leteckém názvosloví*, Letectví + kosmonautika 83 2007. ISSN 0024-1156, p. 98.

[15] *Aero Vodochody Aerospace*. *Interní materiály* – technická dokumentace, technické postupy, bezpečnostní dokumentace.

ČLOVĚK A BEZPEČNOSTNÍ ROZHODOVÁNÍ

MAN AND SAFETY DECIDING

doc. Ing. Radim Roudný, CSc.
Univerzita Pardubice, Fakulta ekonomicko – správní
Pardubice, Studentská 95, PSČ 532 10
radim.roudny@upce.cz

ABSTRAKT

V úvodu je diskutován pojem riziko a možnosti využití tzv. behaviorální ekonomie a principu černá labuť při jeho hodnocení. Dále je kategorizováno myšlení ve vztahu k rozhodování a je doporučen postup hodnocení rizika ve vztahu k rozhodování o prevenci v praxi.

KLÍČOVÁ SLOVA

Riziko, prevence, hodnocení, myšlení, behaviorální ekonomie, černá labuť, rozhodování.

ABSTRACT

In the introduction, the concept of risk and the use of so-called behavioral economics and the principle of black swan is discussed. Furthermore, the decision-making thinking is categorized and a risk assessment process is recommended in relation to decision-making on prevention in practice.

KEY WORDS

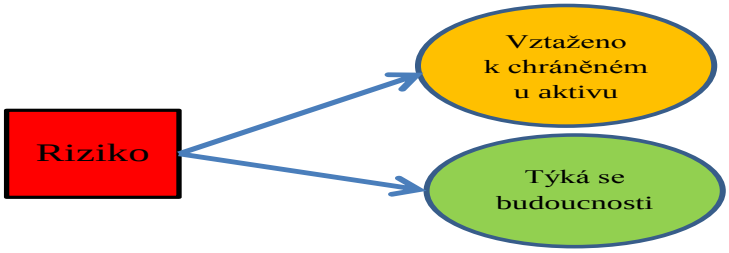
Risk, prevention, evaluation, thinking, behavioral economics, black swan, decision making.

ÚVOD

Toto pojednání navazuje na přednášky na minulých konferencích Krizové řízení a řešení krizových situací v Uherském Hradišti k problematice subjektivního hodnocení rizika. Aktuální inspirací byly poznatky z oponovaných akademických prací a dalších publikací, které svědčí o jistém **nepochopení vztahu teorie a subjektivních vlivů**. Další inspirací byly poněkud diskutabilní publikace v relativně mladém oboru **behaviorální ekonomie** (viz [4], [9] a [8]). Domnívám se, že i v období pokročilé elektroniky a nástrojů rozhodování je a bude nezbytné **respektovat** realitu „matky přírody“ do které zahrnujeme i **neurčitosti jevů a zejména subjektivní vlivy** v rozhodování.

Bezpečnostní rozhodování se týká všech sekvencí bezpečnosti a to:

- **před událostí**, hodnocení rizik a realizace prevence (viz. [9]),
- nežádoucí **událost**, záchrana a snížení účinku, likvidace,
- **revitalizace**, uvedení do nového stavu (nikoliv původního, tzv. obnova).



Obr. 1 Pojetí rizika Zdroj: vlastní

Hodnocení rizik velmi často v životě opomíjíme, v běžném životě i v podnikání. V zásadnějších rozhodnutích[1] je **zanedbání** vědomí **rizika** jednoznačně **chybou**. Hodnocení rizika jako každá lidská činnost vyžaduje určité náklady, není samoúčelné, jeho **smysl je v rozhodnutí o prevenci**, která může být i nulová. Zásadní skutečností je, že **riziko se týká budoucnosti** a škod, **ztrát na aktivu**, viz schéma na obr.1. Prevence a následně bezpečnost aktiv nemůže být absolutní, ale přijatelná vzhledem k prostředkům na ochranu (podrobněji v [7]).

Zajímavé je, že se vžil pojem řízení rizika, který je použit i v převzaté normě ČSN EN 31010:2011 (viz [11]). **Riziko** je potenciální, **fiktivní**, je **odhadem budoucnosti**, jeho hodnocení je významné, ale co v reálném čase neexistuje, nemůžeme řídit, pouze odhadnout. Řídit můžeme proces hodnocení rizika, realizaci prevence a další sekvence bezpečnostního prostředí. Jedná se sice o formální terminologickou otázku, ale v publikacích se často zmatečně zaměňují rizika a reálné mimořádné události. Důležité je srovnávání reality s předpokládanými riziky.

V pojednání jsou velmi zkráceně diskutovány problémy neurčitosti, informací, modelů a subjektivních vlivů na rozhodování. Dále jsou zmíněni hlavní autoři behaviorálního směru v rozhodování.

1. NEURČITOST

Celý proces **bezpečnostního rozhodování** má **značnou míru neurčitosti.** Definice a popis neurčitosti však má různý praktický smysl. O záležitosti např. pojednává velice zajímavá publikace Magdaleny Hykšové Filozofické pojetí pravděpodobnosti v pracích českých myslitelů[2][3]. **Neurčitost** nacházíme **v popisu minulosti** a zejména **předpokládané budoucnosti** (včetně rizika) což je základem veškerého rozhodování. Teorie o neurčitosti se zabývají popisem množin, reálné události se však odehrávají jednotlivě na jednotlivých objektech[3]. Prakticky se jedná o:

- modely a jejich neurčitost (zjednodušený a někdy i chybný popis reality),
- matematickou statistiku, která popisuje reálnou množinu četností určité veličiny x různými ukazateli (pro praxi je významná distribuční funkce),
- statistiku subjektivní, ke které patří významná Bayesovská statistika,
- fuzzy metody, které hodnotí příslušnost k množině,

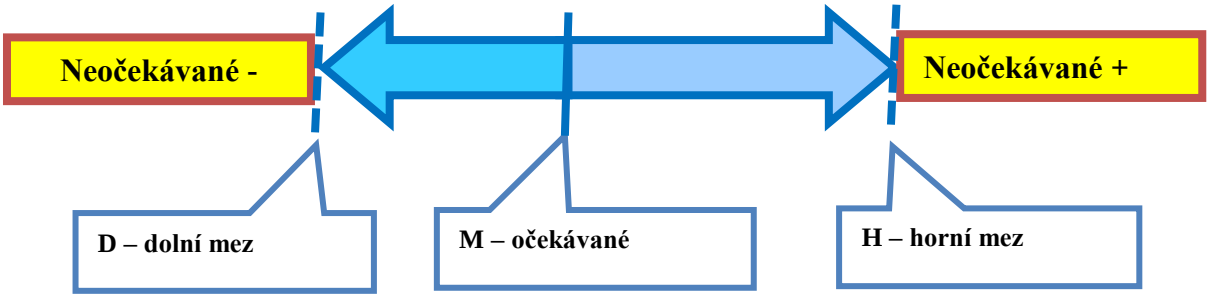
[1] V banálních rozhodovacích situacích, např. kterou nohou vykročím, kam si sednu, co sim dám k jídlu a podobně se riziky odděleně nezabýváme, ale intuitivně je vnímáme.

[2] JE málo známé, že pojetím pravděpodobnosti se zabýval i Tomáš Garrigue Masaryk (str. 127 až 140 v [3]), který na toto téma měl i svoji inaugurační přednášku v roce 1882.

[3] Objektem zde rozumíme obecně statický fyzikální objekt, systém, proces, prostě předmět našeho řešení.

- spolehlivost (důvěryhodnost) jednotlivých informací,

Neurčitost je ve svém popisu **vícekriteriální**, vícehodnotová, což platí pro četnosti i příslušnost množiny. Zásadní význam mají očekávané hodnoty (např. průměr, medián, modus) a mezní hodnoty. Obojí má svůj praktický význam, ale odlišný smysl. V zajímavé publikaci Taleba Černí labuť se hovoří o průměrově a extrémově ([8] str. 54, 61) a dokonce Gaussova křivka je označena za intelektuální podvod (str. 18). Samozřejmě události se odehrávají v konkrétní poloze předpokládaného rozložení neurčitosti, ale závěry Taleba jsou mylné, nejedná se o chybné metody (např. Gaussova křivka vychází z ověřitelného binárního rozložení s pravděpodobností p=0,5, které je i fyzikálně demonstrovatelné – Římská fontána či Galtonovo prkno), ale o jejich chybné či správné použití, interpretaci. Pravdou je, že autoři se značně věnují ukazatelům polohy (průměrov), je to však významný ukazatel, který nemůžeme opomenout[4]. Pro řešení prevence jsou významné především předpokládané mezní hodnoty znázorněné na obr.2. kde tzv. neočekávané jevy (podle Taleba [8] černé labutě) sice nemůžeme kvantifikovat, ale zohledníme je prevencí pro obecné přežití, např. paralelní systémy dodávky elektřiny do územních celků.



Obr. 2 Diskrétní popis množiny Zdroj: vlastní

Popis rozložení je, v zásadě, důležitý pouze při překryvu množin (známé chyby α a β), **obecně** je **důležitá vzdálenost množin**, která vyjadřuje jejich rozdílnost.

Při použití vícekriteriálního hodnocení s j=3 diskrétními charakteristikami D, M a H jsou, pro harmonické funkce kriteriálních hodnot jednoznačné mezní agregace pro m kritérií. Zajímavé a využitelné je hodnocení **kombinací hodnot kritérií** k∈ $(1; m)$ a počtu ukazatelů - kritérií, např. pro m=5 kritérií a hodnocení j=2 podle D a H je 32 kombinací c, podle vzorce

$$c = \sum_{k=0}^{5} \binom{5}{k} = 2^m = 32 \qquad (1)$$

Z toho 2 kombinace jsou mezní, maximální a minimální.

Neurčitost v jednotlivých **sekvencích** managementu **bezpečnosti** je schematizovaná v tab. 1.

Sekvence	Stupeň neurčitosti
Hodnocení rizika a návrh prevence	Vysoký
Realizace prevence	Nízký
Hodnocení výsledné reality	Nízký

Tab. 1 Stupeň neurčitostiZdroj: vlastní

[4] Zajímavá je problematika tzv. defuzzifikace, která více parametricky popsané fuzzy množiny převádí na jeden ukazatel.

2. INFORMACE

Veličiny, které sledujeme, vyjadřují množství (velikost) objektů, např. ztrátu Z v [Kč] a četnost výskytů v množině či v čase p, což je vlastně frekvence. Každá veličina má svůj smysl, např. četnost závad v reklamačním období je hlavní faktor pro spotřebitele, náklady na odstranění jsou hlavním přímým faktorem pro dodavatele (nepřímým faktorem pro dodavatele je i četnost). Významná je i agregace. Pro agregaci je běžně používán jednoduchý vzorec pro riziko R, který je vlastně deterministický předpoklad

$$R = Z * p \tag{2}$$

z hlediska neurčitosti by vyžadoval úpravu o neurčitost ztráty Z a časového výskytu p, např. charakteristiky j=2 (maxima a minima). Je možno použít i agregaci metrickou, která však vyžaduje převod na jednotný rozměr, např. body či bezrozměrnou stupnici.

Informace členíme:

- **vstupní** získané,
- **vytvořené** řešiteli, experimentem či abstraktně,
- **způsobu** řešení,
- **hodnocení** rizika a **návrhu prevence**,
- **rozhodnutí** o prevenci.

Mimo klasické **hodnocení informací** dané datovou velikostí a pravděpodobností získání (a odpovídající cena) má **zásadní význam**:

- **využitelnost** informace pro rozhodnutí o prevenci,
- **přijatelnost** pro zpracovatele (podle odborné dispozice),
- **srozumitelnost** pro rozhodovatele,
- **transparentnost** pro uživatele a občany[5].

V mnoha případech musíme používat subjektivní informace, pokud jiná možnost není (např. estetické vlastnosti), nebo objektivní informace nahrazujeme. O záležitosti existuje rozsáhlá, dostupná literatura, uveďme Hayesová [2], Nakonečný [6] či mnoho informací na internetu, např. [10]. Kvantifikaci subjektivních informací se zabývala přednáška na táto konferenci v roce 2017, připomeňme, že reálných je maximálně 9 až 12 stupňů. Za připomenutí stojí Weberův – Fechnerův zákon (viz. [1] str. 113) o relativním vnímání.

Specifickou oblastí je **náhrada** nedostupných, ale potřebných **informací.**

3. MODELY

Model obecně, popisu řešení, je vždy zjednodušením reality. **Neurčitost** použitých **modelů**, která je **dána zjednodušením** ve vztahu **k realitě.** Forma a **struktura modelů** by měly odpovídat:

- **disponibilním informacím,**

[5] Úplná transparentnost vyžaduje informace o užitku a nákladech řešení (tzv. politické, ekologické či moderní hodnocení nic konkrétního nevyjadřuje), metodách zpracování, řešitelích, rozhodovatelích a rozhodnutím dotčených.

- **praktickým smyslem,**
- znalostní úrovni a **možnostem zpracovatelů,**
- **charakteristice rozhodovatele a uživatelů** (důležitá je srozumitelnost a transparentnost)**.**

Optimální model by měl být **co nejjednodušší** při splnění přijatelné neurčitosti. Setkal jsem se s návrhem modelu o 130 kritériích, což je na prvý pohled nesmyslné.

Pokud si uvědomíme **možné neurčitosti při stanovení rizika**, staneme se velkými **pesimisty.** Realita nás však nutí k rozhodnutí, musíme disponibilní informace ohodnotit a snažit se chyby hodnocení a rozhodnutí minimalizovat. Vždy musíme počítat s tím, že se můžeme dopustit chyb a důležité je připravovat i náhradní řešení. **Jak** můžeme **hodnotit riziko?**

Možnosti jsou:

- **na základě minul**osti, extrapolace,
- **modelování budoucnosti**.

Zdroje pro **modelování** a následné rozhodnutí jsou:

- subjektivní **intuitivn**í (nesdělitelné),
- subjektivní, **myšlenkovými pochody** (mentální),
- modelováním **na základě teorie** (abstraktní),
- modelování **na reálných objektech** (fyzikálních i biologických),
- **kombinace.**

Připomeňme, že u modelování je subjektivní volba metod i použitých informací. Volíme také nástroje řešení modelů, např. počítačové, grafické atd.

Rozdílné přístupy volíme u modelů 1 objektu a u modelů území což je zasvěceně popsáno v publikaci Krömer a kol. [5].

Modely analýzy rizika jsou obecně uvedeny v normě ČSN 31010 [11], která je rozsáhlá – 79 stran, ale poněkud problematická, těžko si můžeme představit její použití praktiky.

4. SUBJEKTIVNÍ VLIVY

Současný pokrok elektroniky a informačních technologií ohromně urychluje a zkvalitňuje odbornou práci i obecně život. Mnoho lidí je však možnostmi moderních technologií až slepě zaujato, žijí v představě jejich nadřazenosti a zapomínají na přirozené zákonitosti světa. Příkladů je možno uvést ohromné množství, např. představa nadřazenosti umělé inteligence. Důležitá je však skutečnost, že tyto technologie a jejich použití je dílo lidí s výsledky pozitivními, ale i negativními. Proto je nutno věnovat primární pozornost realitě a zejména myšlení lidí.

Pohled na stav poznání v psychologii nalezneme v souhrnné publikaci R. Atkinson Psychologie [1]. Zkoumání myšlenkových procesů je možné mnoha způsoby, v podstatě se jedná o zkoumání vlastního myšlení a návazného chování, tzv. behaviorismus, který je rozvíjen již od roku 1920 (viz. [1] str. 7). O myšlení bylo stručně pojednáno na minulé konferenci 2017. Připomeňme si, že **myšlení** je ve výsledku:

- **intuitivní,** jehož hlavní vlastnosti jsou rychlost a nesdělitelnost,

- **racionální**, promýšlíme důvody pro a proti, je sdělitelné.

Kahneman [4] používá pojmy – myšlení pomalé a rychlé, což však vyjadřuje pouze jednu charakteristiku. Příkladem intuitivního myšlení a chování je např. rozhodování hasiče, zda do hořícího objektu vstoupí či nikoliv, zná výsledek, ale není schopen sdělit, proč se tak choval. Racionální myšlení může být časově krátké (rychlé), ale někdy i velmi dlouhé. Typy rozhodování jsou znázorněny na obr. 3. Pokud postačuje, nebo není možné jiné, čistě subjektivní rozhodování (intuitivní či subjektivní racionální) nemusíme hledat nic dalšího. Platí zásada co nejjednoduššího rozhodování pro předpokládaný výsledek. Od nepaměti si lidé uvědomovali, že **čisté subjektivní rozhodování nestačí** a hledali možnosti **podpory myšlení**, které spočívá ve vyhledávání postupů, většinou říkáme teorií, ačkoliv se může jednat o vysoce praktické záležitosti. Např. každý tesař ví, že pravý úhel lze vytvořit v trojúhelníku o odvěsnách 3 a 4 a přeponě 5, což ovšem nevzniklo samovolně, ale je výsledkem bádání minulosti. Respektujme tedy poznatky minulosti, ale vyhledávejme další.

Obr. 3 Typy rozhodování Zdroj: vlastní

Podpora rozhodování nespočívá pouze v teoretické podpoře, ale i v **technické podpoře**, což je v současnosti především počítačová podpora. Důležitá je i podpora interpretace, kde pro lidské vnímání je vhodná hlavně grafická forma[6].

Musíme konstatovat, že **celé rozhodování je subjektivně ovlivněné**. Jak je to však se subjektivním vlivem a reálným výsledkem? Rozhodování je o budoucnosti, ale posléze známe výsledek. **Spolehlivost rozhodování** je **v opakovatelnosti pozitivních výsledků**. Pokud Pythagorova věta byla opakovatelně ověřena nesčíslněkrát, tak o ní nepochybujeme. Neurčitost ale je v realizaci, tj. v nepřesnosti měření stran trojúhelníka.

V praxi ale řešíme např. i spolehlivost expertů, pokud dali opakovaně správnou radu, tak je považujeme za spolehlivé. Vždy ale musíme být vědomi nečekaného vývoje, to je tzv. Talebova Černá labuť.

[6] Říká se, že obrázek či graf je hodina pravdy. V verbálních textech lze skrýt mnoho nepřesností.

5. BEHAVIORÁLNÍ BADATELÉ

Za moderní se považuje tzv. behaviorální ekonomie, nás zajímá jak jsou její poznatky využitelné pro obor bezpečnosti. Jak již bylo uvedeno, nejedná se novou metodu, ale výsledky jsou zajímavé. Za hlavní reprezentanty je možno uvést Daniela Kahnemana [4], Richard Thaler [9] (tzv. Nobelova cena 2017) a Nicolas Taleb, jehož zásadní prací je intelektuálně velice silná Černá labuť [8] (žádná Nobelova cena). Všichni autoři zajímavě popisují řadu situací[7] a shodují se na tom, že slepá aplikace teorií ne zcestná a musíme vycházet z konkrétního chování lidí. S tím nutno souhlasit, zásadní použitelné výsledky pro praxi v jejich je však těžko nalézt. Např. jedním výstupem Thalerova bádání je princip tzv. šťouchu – postrčení (nudge), což je dávno známá marketingová metoda. Talebův princip černé labutě je zcela reálný, nemůže však řešit nebezpečí které neznáme, reálný je princip širší připravenosti, obecné řešení přežití („nic nás nezaskočí“).

ZÁVĚR

V jakémkoliv **rozhodování** včetně bezpečnostního nutno považovat princip, že se jedná o **budoucnost se silnou neurčitostí**. Ve všech fázích a metodách bezpečnostního rozhodování má vliv **člověk** s jeho **subjektivními přístupy**. Teorie a elektronika dosáhly téměř neuvěřitelné úrovně, která někdy vede k opojení a nekritické důvěře a z toho vyplývajících chyb. Vždy musíme dění **posuzovat** tzv. „**zdravým selským rozumem**“ s pokorným přístupem a **respektování přírody**. Vždy bychom měli používat **co nejednoduší metody** srozumitelné pro řešitele i uživatele. Pokud postačí čistě subjektivní metody, nic jiného nehledejme. **Podpora bezpečnostního rozhodování** je většinou nezbytná, ale musí mít **přirozenou logiku**, nikoliv formalizované používání metod. **Absolutní spolehlivost** metod rozhodování **neexistuje**, reálnou spolehlivost nutno **ověřovat na principu opakovatelnosti. Nečekané** mimořádné **události** typu „černá labuť“ nemohou mít konkrétní prevenci (mezní události ano), **řešíme** však problém **přežití**.

Pojednání není a nemohlo být **úplným popisem** vztahu **člověk - bezpečnostního rozhodování**, navazuje na zde v minulých letech publikovaná pojednání a je pouze připomenutím některých problémů.

Literatura

[1] Atkinson, R. Psychologie. Praha: Portál s.r.o., 2003. ISBN 80-7178-640-3

[2] Hayesová, N. Základy sociální psychologie. Praha: Portál, 2007. ISBN 978-80-7367-283-6

[3] Hykšová, M. Filozofická pojetí pravděpodobnosti v pracích českých myslitelů. Praha: MATFYZPRES, 2011. ISBN 978-80-7378-192-8

[4] Kahneman, D., Myšlení rychlé a pomalé. Brno: Jan Melvil Publishing, s.r.o., 2012. ISBN978-80-87270-42-4

[5] Krömer, A. a kol. Mapování rizik. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2010. ISBN 978-80-7385-086-9

[6] Nakonečný, M. Sociální psychologie. Praha: Academia, 1999. ISBN 80-200-0690-7

[7] Seznámení s pracemi uvedených autorů je nejenom zajímavé, ale i užitečné.

[7] Roudný, R. Soušek, R. Management bezpečnosti. Pardubice: Univerzita Pardubice, 2014. ISBN 978- 80-7395-864-0

[8] Taleb, N. Černá labuť. Praha, Litomyšl: PASEKA, 2011. ISBN 978-80-7432-128-3

[9] Thaler. R. Neočekávané chování. Praha: Agro, 2017. ISBN 978-80-257-2121-6

[10] Senzorické procesy a vnímání. *Studium psychologie* [online]. WebyGo.cz, ©2016 [cit. 2017-06-30]. Dostupné z: https://www.studium-psychologie.cz/obecna-psychologie/6-senzoricke-procesy-a-vnimani.html

[11] ČSN – EN 31010 : IEC/ISO 31010:2009. Praha: ÚNMZ, 2011.

RIZIKA A BEZPEČNOST SMART CITIES

RISK AND SAFETY OF SMART CIITIES

Ing. Barbora Schüllerová, Ph.D.
doc. Ing. Vladimír Adamec, CSc.
Ing. et Ing. Kristýna Hrabová
Vysoké učení technické v Brně, Ústav soudního inženýrství,
Purkyňova 464/118
barbora.schullerova@usi.vutbr.cz
vladimir.adamec@usi.vutbr.cz
kristyna.hrabova@usi.vutbr.cz

ABSTRAKT

V současné době, je možné setkat se s konceptem tzv. Smart Cities téměř ve všech zemích světa, vč. České republiky. Rozvoj nových technologií vytváří zcela nový prostor pro ekonomiku, sociální stránku života, zvyšování její kvality a zároveň s sebou přináší i hrozby v podobě doposud neznámých rizik, které mohou významně ovlivnit bezpečnost obyvatel v různých oblastech (zdraví, životy, soukromí apod.). Příspěvek se proto těmito riziky zabývá, společně se stávajícími bezpečnostními opatřeními, která je mají především formou prevence minimalizovat na přijatelnou míru. Cílem je zdůraznit význam rizik, která mohou úměrně narůstat s rozvojem nových technologií zejména v případech, kdy nejsou řádně analyzována a ošetřena.

KLÍČOVÁ SLOVA

inteligentní města, technologie, management, rizika, bezpečnost

ABSTRACT

Currently, it is possible to meet the concept of Smart Cities in almost all countries of the world include Czech Republic. The development of new technologies creates a completely new space in economy, social side of life and improving its quality. However, it brings the threats in the form of hitherto unknown risks that could significantly affect the safety and security of the population in different areas (health, life, privacy, etc.). Therefore, the paper is focused to these risks together with existing security measures, primarily in the form of prevention measures. The aim of the paper is to highlight the significance of the risks, which can proportionally increase with the development of new technologies, especially when they are not properly analyzed and treated.

KEY WORDS

Smart City, technology, management, risk, safety

ÚVOD

Problematika Smart Cities je v současné době oblastí, která vyžaduje pozornost mnoha vyspělých zemí. Tato koncepce je často součástí plánů rozvoje měst do roku 2050. S ohledem na poslání Smart Cities je kladen důraz na vytvoření prostředí, které využívá jednotlivé toky a interakce ve městech (financování, energie, materiály, služby apod.). Tyto procesy se stávají chytrými prostřednictvím strategického využívání informačních a komunikačních infrastruktur a služeb v procesu transparentního územního plánování a řízení, citlivého vůči sociálním a ekonomickým potřebám [1]. Řešení a zavedení těchto chytrých systémů,

je významné v první řadě ve městech, které jsou již v současné době na hranici technické způsobilosti a nejsou schopny již dostatečně plnit služby ve vztahu k zajištění bezpečného zásobování energií, dopravní obslužnosti, bezpečnosti apod. Tyto problémy již není možné řešit běžnými prostředky, jako je zvyšování kapacity nebo například výstavba nových silnic [2]. Aby mohl být zaveden koncept Smart Cities, je důležité držet základních klíčových oblastí, jako je:

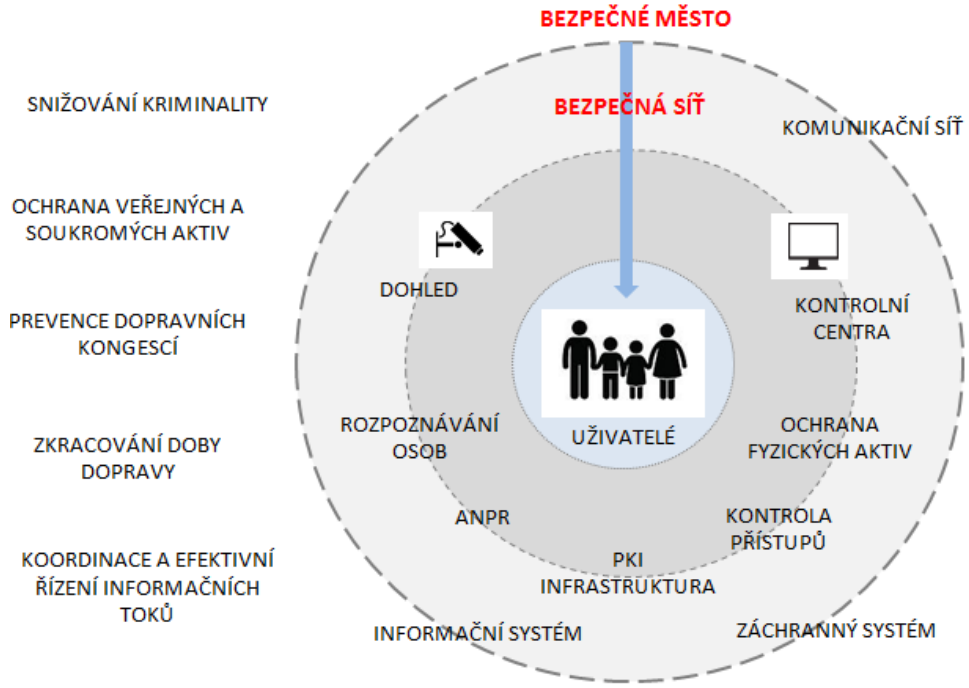
- tvorba partnerství s klíčovými městskými podniky,
- dobrá datová základna s informacemi o každodenním provozu a procesy pro dlouhodobé plánování,
- použití digitálního modelování pro dodávky fyzického prostředí zaměřeného na občany,
- zavádění digitální a komunikační infrastruktury,
- vývoj a testování nových obchodních modelů a procesů [3].

1. VÝZNAM BEZPEČNOSTI KONCEPTU SMART CITY

Současné technologie v souladu s konceptem Smart Cities zahrnují tzv. chytrá řešení, jako je Internet of Things (IoT), cloud, umělá inteligence, big data, automatizace, robotizace apod. Tato řešení se na jednu stranu mohou projevovat jako velmi účinná, vytvářející funkční prostředí. Cílem měst je zjednodušovat chod města a interakci jednotlivých procesů. Jejich cílem je mimo jiné řízení rizik, snižování pravděpodobnosti jejich projevu a to prostřednictvím efektivních a dostupných služeb a informací. Na druhou stranu může na základě implementace těchto technologií docházet ke zvýšení zranitelnosti a vzniku hrozeb. Jedná se především o rizika ohrožující městskou infrastrukturu, nedostatečnou bezpečnost služeb a možnostmi jejich úmyslného zneužití.

Každé město, volí zavádění jednotlivých opatření individuálně a v různém měřítku. Ať se jedná o oblast dopravy, energie, bezpečnosti apod. Obecně, patří mezi základní prvky systému konceptu Smart City doprava, energie, technologie, bydlení, životní prostředí, vzdělávání, ekonomie, politika a bezpečnost. Právě bezpečnost je významnou složkou celého konceptu [5]. Myšlenka bezpečného města (Safe City) je vysvětlována jako " město, kde s integrací technologií a prostředí narůstá efektivita procesů v oblasti bezpečnosti, vede k redukci kriminálních a teroristických hrozeb, nabízí obyvatelům, život ve zdravém prostředí a zjednodušuje přístup zdravotní péče a rychlost jejího poskytnutí" [4, 5]. Systém bezpečného města se tak zaměřuje především na oblasti:

- zdravotní péče,
- chytré dopravy,
- chytrého bezpečnostního systému (odpovědnost, detekce a identifikace),
- chytrého systému krizového managementu podporujícího rozhodování, včasné varování, monitoring a predikci hrozeb a mimořádných událostí,
- Integrovaný záchranný systém,
- apod.



Obr. 1 Systém bezpečného města [6]

1.1 Kritická místa Smart Cities

Městské zástavby se liší nejenom z pohledu architektury, ale i hustoty osídlení, intenzity dopravy apod. Proto je i v tomto ohledu míra rizika proměnná a zdůrazňuje význam aplikace analýzy rizika, na jejímž základě jsou provedena preventivní, represivní a nápravná opatření.

Z pohledu ochrany obyvatel a možnostmi výskytu společenského rizika, jsou zvláště zranitelnými ve městech místa, kde se vyskytuje vysoký počet osob ať už trvale (centra měst, podniky, přestupní stanice dopravních uzlů, nemocnice, školy apod.) nebo přechodně (např. dopravní kongesce na městských okruzích a v centrech měst) [7]. Kritická místa mohou vycházet z kritérií, jako jsou:

- význam konkrétních objektů, oblastí (např. dopravních úseků) a jejich zastupitelnost,
- v případě vzniku mimořádné události, náročnost navrácení zpět do provozu,
- propojenost s dalšími strategickými objekty, oblastmi apod.

Na rozdíl od současné doby fungujících systémů, zde však převládá i další oblast, která z pohledu bezpečnosti může být kritickým místem. Jedná se o kybernetický prostor, který vytváří propojení celé infrastruktury a jeho hranice dosahují nejenom lokální, ale také mezinárodní úrovně, například prostřednictvím bankovního sektoru a obchodních operací s ním spojených. V případě, že tak dojde k selhání v rámci tohoto prostoru, může dojít k narušení celé infrastruktury s dopadem nejenom na jednotlivce, ale celou společnost. K těmto událostem může dojít úmyslně (např. hackerské útoky), tak i neúmyslně např. při implementaci nových technologií, jejich aktualizaci nebo propojení s dalšími systémy [8]. Zranitelnost a hrozby s ním spojené, jsou tak v tomto ohledu spojeny především s dynamicky se vyvíjející oblastí, které je tak nezbytné zabezpečit již v samotném procesu plánování. Proto je důležitá implementace systému řízení rizik, jak je vysvětleno v následující kapitole.

2. ŘÍZENÍ RIZIK A SMART CITIES

Koncepce tzv. chytrých měst patří mezi poměrně nové oblasti, kde jsou vyvíjeny a aplikovány nové technologie prostřednictvím mezinárodních, národních i regionálních projektů. S tím souvisí i potřeba vytváření a udržování bezpečné a odolné infrastruktury. Nárůst těchto projektů vytváří příležitost pro začlenění zásad řízení rizik, které ke snížení zranitelnosti a zvýšení odolnosti měst povedou. Obecně mezi základní hrozby a rizika spojených s oblastí Smart Cities, patří [15]:

- přírodní pohromy,
- technologické havárie,
- kriminální činy a teroristické úroky,
- chyba lidského činitele,
- selhání systému řízení.

V případě ochrany Smart City, jako celku, je nezbytné v první řadě vytvoření bezpečnostní strategie. Ta obsahuje nejenom identifikaci, ale také priorizaci v rámci celé kritické infrastruktury. Následně jsou identifikována a odstraňována zranitelná místa, bezpečnostní nedostatky, škodlivé faktory, zastaralé prvky systému apod. Celý koncept inteligentních měst nabízí mnoho příležitostí, zejména u rychle rostoucích měst vyspělých zemí, které se však musí zároveň vyrovnávat s populačním růstem a zvyšováním nároků na infrastrukturu města jako celku. Bezpečnost se tak stává prioritou. Je důležité říci, že nezbytnou součástí se tak musí stát i vzdělávání a informovanost obyvatel v této oblasti, tak aby byli schopni správně a bezpečně využívat nabízené technologie a zároveň být schopni reagovat na vznik případných rizik. Na vzdělávání se mohou podílet nejenom města samotná, ale v soukromé sféra a dodavatelé jednotlivých služeb a technologií, kteří budou své zaměstnance i zákazníky informovat o případných hrozbách a jejich prevenci [8].

2.1 Přístupy k řízení rizik

Identifikace, analýza a vyhodnocení rizika jsou významným krokem při snaze o jeho eliminaci. Obecně je riziko definováno, jako pravděpodobnost vzniku nežádoucí události společně se vznikem často negativních důsledků [9]. Detailněji je pak riziko popisováno třemi hlavními komponenty, kterými jsou pravděpodobnost vzniku nežádoucího jevu, zranitelnost daného prostředí vůči působení nežádoucího jevu a nakonec i samotné působení nebezpečí, jehož míra je proměnná [10]. V analýze rizika jsou pro rozhodování využívány prvky odhadu pravděpodobnosti (P) vzniku nežádoucí události a jejich důsledků (D) [9]. Při rozhodování o riziku, se pak jedná o odhad pravděpodobnosti a pravděpodobnosti realizace scénáře nebezpečí [10].

Při výběru vhodné metodiky řízení rizik, je nezbytné zvolit takovou kombinaci metod, které zohledňují charakteristiku posuzované entity. Příkladem je rozdíl při hodnocení stacionárních nebo mobilních zdrojů rizik. Společným cílem analýzy rizika je pak získání relevantních informací popisujících zjištěná rizika a jejich význam pro danou oblast.

Již při samotné identifikaci hrozeb a z nich plynoucích rizik by neměla být podceňována a měla by být brány v úvahu i vysoce nepravděpodobné jevy tzv. černé labutě [11]. Ty jsou především v oblasti Smart Cities spojovány s typem tzv. neznámého neznáma nebo také neznámé známo. V prvním případě se jedná o hrozby a rizika, která souvisí s doposud nepoznanými negativními jevy, které mohou mít příčinu v poměrně krátkodobém využívání nových technologií. Ve druhém případě se pak jedná o úmyslné zneužití chytrých technologií

s cílem způsobit poškození v co nejširší míře. Příkladem jsou úmyslné kybernetické útoky a zneužití dat. Přestože je složité predikovat tato rizika, jejich výskyt a rozsah, je nezbytné se zaměřit na jejich minimalizaci. Součástí je i udržování povědomí o možnostech vzniku těchto hrozeb a rizik. Zároveň je nezbytné zavedení dalších opatření, jako [13]:

- založení kvalitní komunikační sítě v případě hrozby vzniku mimořádné událost,
- plánování primárních a sekundárních opatření,
- analýza již uskutečněných událostí, jejich řešení,
- zahrnutí externích hodnocení pro minimalizaci subjektivit.

Tato opatření odráží i stávající volený holistický přístup, založený na analýze, hodnocení, ale také vytváření partnerství (mezi jednotlivými subjekty, systémy apod.) a sdílením informací, budování kapacit a situačního povědomí:

- prostřednictvím interdisciplinárních posouzení a analýz, například mezi jednotlivými sektory, je možné se zaměřit jak na jednotlivá aktiva, tak na systémy jako celek,
- sdílením informací mezi jednotlivými sektory a vytvářením kapacit mezi nimi, je následně možné získávat relevantní data pro hodnocení situace a vytváření preventivních i včasných opatření pro snížení míry dopadu v případě vzniku mimořádné události,
- vytváření partnerství a spolupráce slouží především jako preventivní opatření před vznikem mimořádné události, zároveň v případě jejího vzniku může zajistit lepší koordinaci situace a snížit rozsah dopadu.

Začleněním procesu řízení rizik je možné zajistit dlouhodobou odolnost již při plánování, implementaci i aplikaci a následném užívání chytrých technologií. Pomáhá tak vytvořit komplexní situační povědomí o nových technologiích, jejich účelu, schopnostech a zároveň s nimi souvisejících hrozbách a rizicích. Systém řízení rizik umožňuje budování odolného Smart City jako celku, jeho subsystémů a jednotlivých entit [14].

ZÁVĚR

S rychlým rozvojem technologií i společnosti, je možné konstatovat, že požadavky na vznik inteligentních měst, budou stále narůstat. V tomto dynamicky se rozvíjejícím prostředí ovšem nesmí být zapomenuto na případné hrozby a rizika, které každý takový proces provázejí a to jak při jeho implementaci, tak i užívání. S ohledem na poměrně krátkou dobu užívání některých chytrých technologií se tak oblast řízení rizik a bezpečnost dostává mezi priority, které by neměly být podceňovány. Stejně jako jiná města, jsou i Smart Cities ohrožena běžnými hrozbami, jako jsou přírodní jevy, technické havárie nebo vliv lidského činitele. Zranitelnými oblastmi se zde ovšem stávají i kybernetický prostor a tzv. IoT, které jsou zde běžně využívány, zároveň také znalost populace, schopnost přizpůsobit se a její povědomí o případných rizicích a jednotlivých krocích v oblasti prevence. Cílem příspěvku bylo upozornit na rizika a význam implementace systému řízení rizik v oblasti inteligentních měst a zdůraznit potřebu řešení jejich bezpečnosti. Jedná se o velkou výzvu, kdy musí být kladen důraz na minimalizaci rizik nejenom technologií a jejich případného úmyslného zneužití, ale také v oblasti běžných uživatelů a dopadů rizik na jednotlivce i společnost.

Literatura

[1] European Commission – Digital Agenda for Europe: Smart Cities [online]. 2017 [cit. 2018-08-10]. Dostupné z: https://ec.europa.eu/digital-agenda/en/smart-cities

[2] MATĚJKA, P., JIZBA, T., TVRDÝ, K. Člověk a globální komunikace (Human and Global Comunication). In Sborník 11. konference Prezentace projektů, pp. 23 -- 28. CTU in Prague, Faculty of Transportation Science, Prague (2013).

[3] European Innovation Partnership on Smart Cities and Communities, Strategic Implementation Plan, pp. 2 – 22. European Comission (2013).

[4] LACINÁK, M.; RISTVEJ, J. Smart vity, Safety and Security. In TRANSCOM 2017: Internatiinal scientific conference on sustainable, moder nand safe transport. Proceedia Engineering 192, pp. 522-527.

[5] A. CARAGLIU, CH. DEL BO, P. NIJKAMP, Smart cities in Europe, (2011). In J. Coelho, N. Cacho, F. Lopes, E. Loiola, T. Tayrony, T. Andrade, M. Mendon¸ca, M. Oliveira, D. Estaregue, B. Moura, ROTA: A Smart City Platform to Improve Public Safety, (2016).

[6] *HFCL:* Safe & Smart cities [online]. 2017 [cit. 2018-08-10]. Dostupné z: http://www.hfcl.com/safe-and-smart-cities/

[7] SCHULLEROVA, B., ADAMEC, V., BALOG, K.: The Risk of Transport and Possibility of their Assessment. In: Proceedings of the 2nd International Conference on Traffic and Transport Engineering (ICTTE), Nov 27 – 28, pp.384—391. Scientific Research Center Ltd. Belgrade (2014).

[8] LEIVESLEY, S. 2017. Smart Cities [online]. New Risk [cit. 2018-02-02]. Available from: http://www.newrisk.com/smartcities.html

[9] BRANDER, M. 2017. The Security risk within Smart Cities [online]. Infosec Island [cit. 2018-02-15]. Available from: http://www.infosecisland.com/blogview/24951-The-Security-Risk-Within-Smart-Cities.html

[10] AVEN, T. Uncertainty in Risk Assessment – The Representation and Treatment of Uncertainties by Probabilistic and Non-Probabilistic Method. John Wiley & Sons Ltd., Chichester, UK (2014).

[11] MANNAN, S.: Lees' Loss Prevention in the Process Industries: Hazard Identification Assessment and Control. Elsevier, Oxford (2012).

[12] TALEB, N. N.: Black Swan: The Impact of the Highly Improbable. 2nd edition. Random House Trade Paperbacks, Westminster (2010).

[13] HANSON, D.; WARD, T.; IVES, N. 2013. Responding to a Black Swan: Principles and protocols for responding to unexpected catastrophic events. Ernst & Young. 8 p. http://www.ey.com/Publication/vwLUAssets/Responding_to_a_Black_Swan/$FILE/Responding_to_a_Black_Swan-5_Insights.pdf

[14] GORDON, L. W., MCALEESE, G. 2017. Resilience and Risk Management in Smart Cities [online]. George Mason University, 2017 [cit. 2018-08-04]. Available from: https://cip.gmu.edu/2017/07/06/resilience-risk-management-smart-cities/

[15] PROCHÁZKOVÁ, Dana. Bezpečná Smart cities [online]. 2016 [cit. 2018-08-10]. Dostupné z: http://www.bezpecnostnimanagementvregionech.cz/sites/bezpecnostnimanagementvregionech.cz/files/prochazkova_prochazka_bezpecna_smart_cities.pdf

BEZPEČNÁ AUTENTIZACE UŽIVATELŮ V SYSTÉMECH KRITICKÉ INFORMAČNÍ INFRASTRUKTURY

SECURE USER AUTHENTICATION IN CRITICAL INFORMATION INFRASTRUCTURE

Ing. Vladimír Šulc, Ph.D.
Policejní akademie České republiky v Praze
Lhotecká 559/7, 143 01 Praha 4
sulc@polac.cz

ABSTRAKT

Praktická studie zaměřená na problémy spojené s implementací požadavků na bezpečnou autentizaci uživatelů a administrátorů v systémech kritické informační infrastruktury uvedených v Zákoně o kybernetické bezpečnosti a konkrétně pak ve vyhlášce o kybernetické bezpečnosti. Studie se zabývá smysluplností požadavků na délku a komplexnost hesla, dobou jeho platnosti, použitý algoritmus, způsob uložení hesla, a možných vektorů útoku.

KLÍČOVÁ SLOVA

Autentizace, délka hesla, komplexita hesla, doba platnosti hesla, entropie hesla, lámání hesel, passphrase, VoKB, ZoKB

ABSTRACT

This study is focused on issues connected with implementation of security requirements on user authentication in systems of critical infrastructure stated in Cyber security law. The main aim of this whitepaper is to evaluate relevance of requirements regarding the complexity of password, password length, password age, used algorithm, and possible vectors of attack.

KEY WORDS

Authentication, password length, password complexity, password max age, pasword entropy, password cracking, passphrase, VoKB, ZoKB

ÚVOD

V souvislosti s novelizací Vyhlášky o kybernetické bezpečnosti, zkr. VoKB upřesňující požadavky Zákona o kybernetické bezpečnosti, zkr. ZoKB, jsem si položil otázku, zdali není jednofaktorová autentizace přežitek a stejně tak i bezpečnostními experty roky propagované požadavky na délku hesla, komplexitu, jeho pravidelnou změnu apod., z nichž se některé objevily právě i v nově vydané VoKB, která doznala v poslední úpravě podstatných změn.

V následující kapitole je představen teoretický rámec, aktuálně platná legislativa, její požadavky, možné vektory útoku a předmět dalšího zkoumání. Ve druhé kapitole je pak proveden vlastní výpočet doby potřebné k prolomení hesel a passphrase o různé délce a komplexitě. V závěru je pak formulováno doporučení ohledně bezpečnostní politiky hesel v systémech kritické informační infrastruktury.

1. TEORETICKÝ RÁMEC

Důvody, které bezpečnostní experty vedou nebo vedly k definici určitých bezpečnostních zásad, jsou zřejmé, jejich snahou bylo ochránit subjekty, které se do systému přihlašují prostým zadáním jména a hesla před zcizením jeho identity a zabránit tomu, aby se do systému pod jejich identitou nemohla přihlásit neoprávněná osoba, které se nějakým způsobem podařilo její heslo získat.

Subjektem může být uživatel anebo stroj, v takovém případě se jedná o účet, pod kterým zpravidla běží nějaká služba systému, webový, mailový nebo třeba aplikační server. My se dále budeme zabývat výhradně účty, které jsou používány lidskými operátory.

Samotný proces přihlášení se do systému pomocí jména a hesla se skládá ze dvou kroků, v prvním uživatel zadává své uživatelské jméno, tzv. identifikátor, který mu byl přidělen systémem, nebo které si zvolil sám a říkáme, že se identifikuje. Ve druhém kroku pak uživatel zadává heslo a říkáme, že se autentizuje. V reálné praxi uživatele zadává oba tyto údaje najednou do příslušných polí v přihlašovacím formuláři a ty jsou i v jednom požadavku odesílány na server.

Heslo se někdy též označuje jako sdílené tajemství, protože je skutečně určitým způsobem sdíleno mezi uživatelem a serverem, vůči kterému autentizace probíhá. Dvojice uživatelské jméno a heslo se pak také označuje jako credentials.

Případný útočník musí znát jak identifikátor, tak i heslo. Identifikátor nemusí být veřejně známý, ale zpravidla je znám určitému okruhu osob, minimálně těm, co se rovněž do systému přihlašují anebo je poměrně snadno predikovatelný, neboť je znám způsob jeho tvorby (část jména a příjmení uživatele, e-mailová adresa, číselná řada či sekvence znaků).

Identifikátory pak mohou být významové a bezvýznamové. Významové identifikátory určují účel použití účtu. Takovým identifikátorem je např. účet root v systémech UNIX anebo účet administrátor v systému MS Windows a bývají často sdíleny více osobami.

Bezvýznamové identifikátory pak bývají používány běžnými uživateli systému. Identifikátory mohou být přejmenovány, ale ne vždy je to možné a pouhé přejmenování mnohdy stejně nestačí k tomu, aby se zabránilo útoku na konkrétního uživatele resp. jeho účet v systému.

Účet pak obsahuje kromě identifikátoru a hesla uloženého bezpečným způsobem další atributy, jako datum posledního přihlášení, datum změny hesla, omezení účtu, tj. zda třeba není možné se přihlásit z určitého stroje, v určitou denní dobu, a případně zda není účet uzamčen či zakázán.

K útoku na účet uživatele pak může dojít několika různými způsoby. Zcela ignorovat budeme v této práci ty vektory útoku, při kterých délka hesla a jeho komplexita nehraje žádnou roli. Takovým vektorem je např.:

- **Odchycení hesla** pomocí HW nebo SW keylogeru. Ty bývají nainstalovány na koncovém zařízení buď v operačním systému, nebo přímo v prohlížeči, např. ve formě javascriptu. Zachytávají stisk kláves anebo jsou připojeny na USB sběrnici a zachytávají pak signály vysílané po této sběrnici mezi externí klávesnicí a počítačem.
- **MITM attack**, kdy je útočník schopen zachytávat a číst obsah paketů procházející po síti mezi autentizujícím se subjektem a serverem, ať už proto, že je použit slabý šifrovací algoritmus (např. SSL) anebo proto, že je schopen provést SSL offloading[1],

[1] Comodo (2018) [online] [cit. 2018-8-24]. Dostupné na WWW: <https://securebox.comodo.com/ssl-sniffing/ssl-offloading/>

má pod kontrolou HTTPS-to-HTTPS bridge či jinou část sítě, kde již provoz není šifrován, neboť již byl dříve terminován.

- **Kompromitace aplikace** a začlenění vlastního kódu do aplikace, která provádí dotazy vůči autentizačnímu serveru a může hesla zachytávat. A to jak na klientské, tak i serverové části, kdy může být např. útočníkem modifikován přihlašovací dialog a pak ani stisk kláves CTRL+ALT+DEL nemusí být zárukou, že je volán onen skutečný.
- **Kompromitace databáze**, pokud jsou hesla v databázi uložena v otevřeném tvaru anebo za použití reversibilní šifrovací funkce, např. jsou šifrována pomocí symetrického AES klíče, místo aby byla uložena jako hash.
- **Phishing, vishing, SMShing** a vůbec jakékoliv formy útoku zneužívající technik sociálního inženýrství, kdy oběť své credentials útočníkovi poskytne dobrovolně.
- **Rubber-hose cryptanalysis**, oběť útoku je k prozrazení hesla donucena za užití násilí[2].
- **Útoky postranními kanály**[3], kam patří např. měření odběru proudu, zachycení elektromagnetického vyzařování, nahrání zvuku stisknutých kláves pomocí mikrofonu, využití gyroskopu na mobilních zařízeních, až po vibrace okenních tabulí fungujících jako membrána reproduktoru apod.

Ve všech těchto případech platí, že ať už je délka hesla a jeho komplexita jakákoliv a stejně tak i doba jeho platnosti, tak heslo bude zachyceno prakticky ihned po jeho zadání a zpřístupněno útočníkovi. Specifické postavení pak mají **on-line útoky vůči autentizační autoritě**, kde zpravidla dochází k zablokování účtu po několika neúspěšných pokusech o přihlášení anebo je rostoucí počet neúspěšných pokusů monitorován, včas detekován a je na něj odpovídajícím způsobem reagováno, takže útočník má možnost vyzkoušet jen velice omezenou sadu hesel[4].

Zaměříme se proto dále jen na ty případy, kdy bylo použito bezpečné autentizační schéma, dostatečně odolné kryptografické protokoly a algoritmy a ty byly i implementovány správně. Za těchto podmínek je délka hesla a jeho komplexita relevantní, má smysl se jí zabývat, neboť je na sdílené tajemství možné vést následující útoky:

- **Slovníkové útoky**, tj. útoky založené na zkoušení všech možných slov obsažených ve slovníku, zpravidla již uniklých hesel z DB nejrůznějších organizací, které jsou přístupné ke stažení na internetu a čítající kolem 1,4 miliardy hesel[5].
- **Útoky vedené hrubou silou**, tzv. brute force attack, kdy útočník zkouší všechna možná hesla vůči autentizační autoritě (tzv. on-line útoky) anebo kdy útočník zkouší generovat hashe a porovnává je proti hashům uloženým v databázi (tzv. off-line útoky). Oba tyto útoky dále popíšeme.
- **Útoky založené na odpozorování hesla při jeho zadávání.** Jedná se o tzv. shoulder surfer attack, který může být proveden z bezprostřední blízkosti anebo i z poměrně

---

[2] Wikipedia (2018) [cit. 2018-8-24]. Dostupné na WWW: <https://en.wikipedia.org/wiki/Rubber-hose_cryptanalysis/>

[3] Techdesignforums (2018) [cit. 2018-8-24]. Dostupné na WWW: <http://www.techdesignforums.com/practice/guides/side-channel-analysis-attacks/>

[4] Cleverandsmart (2011) [cit. 2018-8-24]. Dostupné na WWW: <https://www.cleverandsmart.cz/lamani-hesel-on-line-utok/>

[5] Thehackernews (2017)[cit. 2018-8-24]. Dostupné na WWW: <https://thehackernews.com/2017/12/data-breach-password-list.html/>

velké vzdálenosti[6], za použití kamery, dalekohledu, kdy útočníkovi může pomoci i skutečnost, že uživatel zadává heslo během dne opakovaně, může si uživatelovu seanci nahrát a poté i zpomaleně přehrát a vzhledem k pevnému umístění kláves na klávesnici a leckdy i jejich podsvícení, mu postačí i pozice jednotlivých prstů nad klávesnicí určených k tomu, aby zjistil, jaká klávesa byla stisknuta.

Pokud jde o útoky hrubou silou, tak **zde délka a komplexita hesla jednoznačně hraje podstatnou roli a určuje, za jak dlouho může být heslo hrubou silou prolomeno**. Zde je třeba uvést, že vzhledem k masivním únikům miliónů hesel z databází po celém světě mají útočníci výhodu v podobě slovníku reálně používaných hesel, takže mohou nejprve vyzkoušet, zda daný uživatel nepoužívá některé z těchto hesel anebo jejich drobnou modifikaci.

Jako efektivní obrana před útoky hrubou silou a hádáním hesel se obecně doporučuje dodržovat určité zásady, které jsou často zohledněny v tzv. politice hesel[7], která je následně vynucena systémem. V praxi se jedná o vynucení:

- Minimální délky hesla, kdy heslo by mělo být dlouhé minimálně X znaků (toto doporučení se postupně mění a trend je jednoznačně rostoucí).
- Komplexity hesla, kdy heslo by mělo obsahovat znaky minimálně z tří množin, tedy mělo by obsahovat velká písmena, malá písmena, čísla a speciální znaky.
- Heslo by mělo být pravidelně měněno.

V posledních letech se však od dvou výše uvedených požadavků, tedy komplexity a periodické obměny hesla, upouští ve prospěch tzv. passphrase. Toto doporučení se objevuje např. v publikaci NIST SP-800-63B[8] a rovněž i ve VoKB, která byla v tomto roce novelizována a jejíž autoři se tímto standardem, jak sami přiznávají, inspirovali. VoKB v § 19 odstavci 5 požaduje, aby v případech, kdy není možné zavést vícefaktorovou autentizaci, tak aby byla nastavena taková politika hesel, která zajistí, že:

- minimální délka hesla uživatele bude 12 znaků, u administrátora a aplikací 17 znaků,
- toto heslo musí být změněno nejpozději po 18 měsících,
- nesmí být omezováno použití malých a velkých písmen, číslic a speciálních znaků,
- nesmí být umožněno zvolit si nejčastěji používaná hesla, tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému atd.

Všimněme si, že **oproti minulé vyhlášce není požadováno, aby heslo obsahovalo velká a malá písmena, čísla a speciální znaky, jen musí být umožněno je zadat**. Vývoj požadavků na délku a komplexitu hesla za poslední 3 roky zachycuje následující tabulka.

[6] Polimi (2010) [cit. 2018-8-24]. Dostupné na WWW: <http://home.dei.polimi.it/fmaggi/downloads/publications/2010_maggi_volpatto_gasparini_boracchi_zanero_clearshot.pdf>

[7] Cleverandsmart (2010) [cit. 2018-8-24]. Dostupné na WWW: <https://www.cleverandsmart.cz/autentizace-politika-uctu-a-hesel/>

[8] NIST (2017) [cit. 2018-8-24]. Dostupné na WWW: <https://pages.nist.gov/800-63-3/sp800-63b.html/>

Verze VoKB	Délka hesla uživatele	Délka hesla administrátora	Komplexita	Doba platnosti
Účinná od 1.1.2015 do 27.05.2018	8	15	ANO	100 dnů
DRAFT z dubna 2018	14	17	NE	
Aktuálně platná z května 2018	12	17	NE	18 měsíců

Tab. 1 - VoKB a politika hesel

Co vedlo NUKIB ke změně délky hesla z navrhovaných 14 znaků na 12 znaků není nikde v důvodové zprávě ani v připomínkovém meziresortním a mezioborovém řízení, kdy se k návrhu novelizace vyjadřovaly dotčené subjekty, tedy především provozovatelé kritické informační infrastruktury a významných informačních systémů, uvedeno.

Dle zveřejněných informací došlo ke zmírnění těchto požadavků údajně proto, že i komplexní hesla tvořená velkými a malými písmeny, čísly a speciálními znaky byla prolomena a jako příklad lze uvést např. heslo „P4$$w0rd“. Toto heslo vytvořené pomocí tzv. leetspeak[9] techniky splňovalo sice požadavky VoKB, ale nacházelo se v uniklých databázích hesel, takže pokud ho uživatel použil, tak bylo velice rychle prolomeno právě s použitím slovníkového útoku.

Podstatné je, že tato délka nemusí být v některých případech skutečně dostatečná, a pokud u administrátorů existovala reálná obava z lámání LM hashů pomocí rainbow tabulek[10] a bylo proto již v roce 2015 požadováno heslo o minimální délce 15 znaků, mělo být takto dlouhé heslo požadováno ze stejných důvodů i u uživatelů, neboť většina APT útoků[11] není vedena na administrátory, ale na uživatele a manažery.

Budeme-li předpokládat, že LM hashe již nejsou v kritických ani významných systémech provozovány, což by dobu prolomení podstatně zkrátilo, **budeme se zabývat pouze výpočtem doby potřebné k prolomení hesla, které splňuje požadavky uvedené v aktuálně platné VoKB a dokážeme, že uvedené požadavky jsou nedostatečné, neboť prolomení hesla splňujícího tyto požadavky je možné v reálném čase**.

2. JAK RYCHLE LZE PROLOMIT HESLA DO KII A VIS NASTAVENÁ V SOULADU S VOKB

Praktickým pozorováním v rámci jedné nejmenované organizace bylo ověřeno, že pokud uživatel opakovaně zadává heslo, resp. passphrase obsahující pouze malá písmena, tak lze toto heslo snáze odpozorovat a domyslet. Muselo by se však jednat spíše o útok ze strany blízkého spolupracovníka, který je takový útok schopen realizovat. Ještě o něco horší je situace v tzv. openspace, které jsou právě v organizacích provozující kritické informační systémy používány a kde je možné uživatele při zadávání hesla nahrávat a následně si poměrně snadno nahranou sekvenci přehrát a zjistit, jaké bylo zadávané heslo. Zde se ukazuje, že komplexita a délka hesla nehraje příliš roli. Dále byla pozornost věnována

[9] Wikipedia (2018) [cit. 2018-8-24]. Dostupné na WWW: <https://en.wikipedia.org/wiki/Leet/>

[10] Sourceforge (2018) [cit. 2018-8-24]. Dostupné na WWW: <http://ophcrack.sourceforge.net/tables.php/>

[11] IEEE (2018) [cit. 2018-8-24]. Dostupné na WWW: <https://ieeexplore.ieee.org/document/7550947/>

jedinému případu, kdy má délka a komplexita hesla, jako bezpečnostní opatření, smysl a to vůči lámání hesel hrubou silou.

Zde bylo vycházeno z předpokladu, že i kdyby byl použit bezpečný protokol pro uložení hesel, tak již v roce 2012 byla publikována informace o možnostech lámání komplexních 9 znakových hesel v řádu jednotek dnů[12]. V případě špatné bezpečnostní osvěty a tvorby hesla postaveném na slově ze slovníku pak může být i 14 znakové heslo[13] nebo dokonce i 256 znakové heslo[14] prolomeno během pár hodin.

V případě 8 znakového hesla by tato doba byla ještě kratší, záleží jen na výkonu stroje, resp. strojů, které budou použity pro lámání hesla a tedy i nákladech, které by na lámání hesel musel útočník vynaložit. Dále bude proto předpokládáno, že v dané organizaci proběhla bezpečnostní osvěta a uživatelé byli poučeni, jak vytvářet bezpečná hesla. Pří výpočtu doby potřebné k prolomení hesla hrubou silou použijeme následující vzorec:

$$T=K^L/S \quad (1)$$

Kde T je čas potřebný k prolomení hesla, K je množina znaků, L je délka hesla, S je rychlost lámání, ta může být ovlivněna počtem strojů a použitou architekturou. Pokud máme určit znaky K, které mohou být v hesle použity, vyjdeme z ASCII tabulky a znaky si rozdělíme do skupin:

- 10 číslic: 0123456789 (Digits, zkr. D).
- 26 malých písmen: abcdefghijklmnopqrstuvwxyz (Lower Case, zkr. LC).
- 26 velkých písmen: ABCDEFGHIJKLMNOPQRSTUVWXYZ (Upper Case, zkr. UC).
- 33 speciálních symbolů: !”#$%&’()*+,-./:;<=>?@[\]^_`{|}~ (Special chars, zkr. S).
- 33 netisknutelných kódů: pozice 0 až 31 a 127.
- 128 znaků z rozšířené sady: pozice 128 až 255.

Budeme-li předpokládat, že uživatel bude volit znaky z prvních čtyř skupin, musíme se ptát, jaké jsou jejich možné kombinace. To zachycuje následující tabulka.

Množina	LC	UC	D	S	N
A	X	X	X	X	95
B	X	X		X	85
C		X	X	X	69
D	X		X	X	69
E	X	X	X		62
F		X		X	59
G	X			X	59
H	X	X			52

[12] Uio (2018) [cit. 2018-8-24]. Dostupné na WWW: <http://passwords12.at.ifi.uio.no/Jeremi_Gosney_Password_Cracking_HPC_Passwords12.pdf/>

[13] Securityintelligence (2018) [cit. 2018-8-24]. Dostupné na WWW: <https://securityintelligence.com/the-cracken-the-evolution-of-password-cracking/>

[14] Cyberarms [cit. 2018-8-24]. Dostupné na WWW: <https://cyberarms.wordpress.com/2018/04/03/cracking-passwords-up-to-256-characters-with-hashcat/>

I			X	X	43
K	X		X		36
J		X	X		36
L				X	33
N	X				26
M		X			26
O			X		10

Tab. 2 - Množiny znaků a jejich kombinace

Uživatel, pokud není v tvorbě hesla nijak omezen, může zvolit znaky z libovolné množiny. Z jedné, ze dvou, ze tří nebo také ze všech čtyř. V zásadě se jedná o kombinace bez opakování, kdy se uživatel rozhoduje mezi 4 množinami, což nám dává 15 kombinací prvků z množin, z jakých může být heslo sestaveno. Na první pohled vidíme, že nejvíce prvků má množina A s 95 prvky, která se skládá LC + UC + D + S a nejméně pak množina O s pouhými 10 prvky.

Hodnota K je pak v tomto případě rovna 95. V reálné praxi bude tato hodnota mnohem menší, neboť některé znaky uživatel nejspíš zadávat nebude, ale budeme se nicméně držet našeho optimistického předpokladu. Pokud by si uživatel nastavil heslo o minimální délce požadované VoKB, pak by proměnná L byla rovna 8. Počet všech možných variací je v tomto případě 95^8.

Pokud bychom předpokládali rychlost lámání hesel od 10^6 pps, což lze v dnešní době považovat průměrný výkon stroje v hodnotě několika desítek tisíc, tak by doba prolomení takového hesla trvala útočníkovi přibližně jeden rok. Jenže útočník, který by chtěl prolomit heslo do kritického nebo významného systému, bude zcela jistě disponovat větší výpočetní kapacitou. Už při zapojení 10 strojů se doba prolomení zkracuje cca na 1 měsíc a při 100 strojích pak na pouhých několik dnů. Tento počet strojů není pro útočníka problém získat, neboť uvedeným počtem strojů disponuje každá menší firma, případně si útočník může za pár dolarů[15] pronajmout cloud nebo botnet čítající až několik desítek ne-li stovek tisíc strojů[16]. Výše uvedeným výpočtem lze doložit, že požadovaná délka hesla je nedostatečná.

Otázka však je, zda se něco změnilo s novelizací vyhlášky, kdy byla délka hesla prodloužena na 12 znaků. Pokud by byla zachována komplexita hesla, tak by se doba prolomení podstatně prodloužila, neboť by útočník musel vyzkoušet 95^{12} různých hesel. Ovšem v okamžiku, kdy není komplexita vyžadována, tak můžeme předpokládat, že si uživatelé zvolí spíše nějakou jednoduchou passphrase a počet kombinací tak může dramaticky klesnout na pouhých 26^{12}. Ostatně i NIST standard, který je teď hojně citován v nejrůznějších odborných článcích[17], k tomu uživatele sám navádí a používání passphrase doporučuje. Passphrase tak může být

[15] Arstechnica (2018) [cit. 2018-8-24]. Dostupné na WWW: <https://arstechnica.com/information-technology/2018/02/for-sale-ddoses-guaranteed-to-take-down-gaming-servers-just-20/>

[16] Wikipedia (2018) [cit. 2018-8-24]. Dostupné na WWW: <https://en.wikipedia.org/wiki/Botnet/>

[17] Securityboulevard (2018) [cit. 2018-8-24]. Dostupné na WWW <https://securityboulevard.com/2018/05/10-best-practices-to-secure-and-protect-passwords/>

Carleton [cit. 2018-8-24]. Dostupné na WWW: <http://people.scs.carleton.ca/~paulv/papers/expiration-authorcopy.pdf/>

Fedtechmagazine (2018) [cit. 2018-8-24]. Dostupné na WWW: <https://fedtechmagazine.com/article/2018/02/its-time-question-longstanding-password-security-best-practices/>

tvořena jen malými nebo velkými písmeny, případně čísly. V případě passphrase, tak jak je obecně vnímána laickou i odbornou veřejností, se však jedná spíše o spojení několika málo slov, zpravidla tří a více. Abychom mohli porovnat odolnost klasického hesla o dané délce a passphrase, tak musíme místo výše uvedeného vzorce použít entropii hesla vyjádřenou v bitech. Tu spočteme pomocí následujícího vzorce:

$$\mathbf{En = \log_2(S^L)} \quad (2)$$

Kde S je množina znaků a L je délka hesla. Informační entropii passphrase pak budeme odvíjet od počtu použitých slov, přičemž běžný slovník, který zdaleka většina populace nepoužívá, čítá maximálně několik desítek tisíc slov[18]. Budeme ale počítat jak s teoretickým maximem cca 250 000 slov, tak i s 10 000 slovy, což je maximum, tak i s průměrem kolem 5 000 slov, které skutečně aktivně používá rodilý mluvčí[19]. To bude představovat množinu znaků S v případě passphrase a počet slov použitých v passphrase pak bude celkem logicky představovat onu délku L. Dobu potřebnou k prolomení hesla o určité entropii můžeme spočítat jako:

$$\mathbf{T=2^{En}/pps} \quad (3)$$

Kde T je čas nutný k prolomení, En je entropie sdíleného tajemství bitech a pps je rychlost lámání hesel za jednotku času. V následující tabulce je uvedena doba potřebná k prolomení sdíleného tajemství o určité entropii.

Entropie v bitech	Malá písmena 26 znaků	Písmena a čísla a speciální znaky 95 znaků	Passphrase 5000 slov	Přibližná doba prolomení
53		8 znaků		týdny
56	12 znaků			měsíce
59		9 znaků		rok
61	13 znaků		5 slov	roky
66	14 znaků	10 znaků		desítky let
71	15 znaků			stovky let
72		11 znaků		tisíc let
74			6 slov	tisíce let
75	16 znaků			desítky tisíc let
79		12 znaků		sto tisíc let

Tab. 3 – Doba potřebná k prolomení hesla a passphrase.

[18] Frontiersin (2016) [cit. 2018-8-24]. Dostupné na WWW: <https://www.frontiersin.org/articles/10.3389/fpsyg.2016.01116/full/>

[19] CT24 (2018) [cit. 2018-8-24]. Dostupné na WWW: https://ct24.ceskatelevize.cz/veda/1878980-prumerny-american-zna-podle-nove-studie-42-000-slov-a-co-prumerny-cech

ZÁVĚR

Požadavky ve VoKB na délku hesla byly nedostatečné již v roce 2015. S novelizací VoKB v květnu tohoto roku došlo de-facto i de-jure k dalšímu zmírnění požadavků na komplexitu a dobu platnosti hesla uživatelů a tudíž i ke zvýšení rizika prolomení hesel do systémů organizací provozujících kritické a významné informační systémy, což bylo doloženo výše uvedeným výpočtem, který může kdokoliv ověřit.

Z výše uvedeného důvodu doporučuji, aby v případě, že není použita vícefaktorová autentizace a autentizace je založena výhradně na zadání credentials v podobě jména a hesla, tak aby i nadále politika hesel v systémech spadající pod působnost VoKB byla nastavena tak, aby po uživateli bylo požadováno zadání znaků hesla ze tří množin, aby byly akceptovány pouze hesla o minimální délce 12 znaků a aby doba platnosti tohoto hesla byla kratší než 18 měsíců. Anebo pokud nebude komplexita vyžadována, tak aby byla požadována hesla o délce minimálně 15 znaků, kde je výrazně delší doba prolomení.

Toto nastavení nebude v rozporu s požadavkem uvedeným ve VoKB, neboť tam se jasně píše, že nesmí být omezováno použití malých a velkých písmen, číslic a speciálních znaků, což nutně neznamená, že nemůže být vynucováno a tedy že systém nemůže být nastaven restriktivněji.

Při používání dlouhých passphrase pak doporučuji používat takové passpharse, kterými nejsou fráze běžně používané a známé, a to ani ne proto, že při pokusu o jejich odpozorování si nebude moci útočník tak snadno chybějící písmena domyslet, ale proto, že v okamžiku, kdy dojde k prvnímu velkému úniku passfrází, tak bude zřejmé, jaké pasfráze jsou nejpoužívanější a již nebude nutné je lámat hrubou silou, jen dojde o obohacení stávajících slovníků hesel.

V souvislosti s doporučením na přechod na passphrase je nutné připomenout, že uživatelé zadávají slabá hesla, což opakovaně potvrzují každoroční úniky hesel. V okamžiku, kdy nebudou uživatelé dostatečně proškolení, a nebude vyžadována komplexita hesla, tak hrozí, že místo skutečných passphrase složených z více jak tří slov budou zadávat jen 12 znakové řetězce malých písmen, mimo jiné i proto, že se jim nebude chtít několikrát denně zadávat několik desítek znaků dlouhé passphrase.

Literatura

[1] Arstechnica (2018) [cit. 2018-8-24]. Dostupné na WWW: <https://arstechnica.com/information-technology/2018/02/for-sale-ddoses-guaranteed-to-take-down-gaming-servers-just-20/>

[2] Carleton [cit. 2018-8-24]. Dostupné na WWW: <http://people.scs.carleton.ca/~paulv/papers/expiration-authorcopy.pdf/>

[3] Cleverandsmart (2010) [cit. 2018-8-24]. Dostupné na WWW: <https://www.cleverandsmart.cz/autentizace-politika-uctu-a-hesel/>

[4] Cleverandsmart (2011) [cit. 2018-8-24]. Dostupné na WWW: <https://www.cleverandsmart.cz/lamani-hesel-on-line-utok/>

[5] Comodo (2018) [online] [cit. 2018-8-24]. Dostupné na WWW: <https://securebox.comodo.com/ssl-sniffing/ssl-offloading/>

[6] CT24 (2018) [cit. 2018-8-24]. Dostupné na WWW: https://ct24.ceskatelevize.cz/veda/1878980-prumerny-american-zna-podle-nove-studie-42-000-slov-a-co-prumerny-cech

[7] Cyberarms [cit. 2018-8-24]. Dostupné na WWW: <https://cyberarms.wordpress.com/2018/04/03/cracking-passwords-up-to-256-characters-with-hashcat/>

[8] Fedtechmagazine (2018) [cit. 2018-8-24]. Dostupné na WWW: <https://fedtechmagazine.com/article/2018/02/its-time-question-longstanding-password-security-best-practices/>

[9] Frontiersin (2016) [cit. 2018-8-24]. Dostupné na WWW: <https://www.frontiersin.org/articles/10.3389/fpsyg.2016.01116/full/>

[10] IEEE (2018) [cit. 2018-8-24]. Dostupné na WWW: <https://ieeexplore.ieee.org/document/7550947/>

[11] NIST (2017) [cit. 2018-8-24]. Dostupné na WWW: <https://pages.nist.gov/800-63-3/sp800-63b.html/>

[12] Polimi (2010) [cit. 2018-8-24]. Dostupné na WWW: <http://home.dei.polimi.it/fmaggi/downloads/publications/2010_maggi_volpatto_gasparini_boracchi_zanero_clearshot.pdf>

[13] Securityboulevard (2018) [cit. 2018-8-24]. Dostupné na WWW <https://securityboulevard.com/2018/05/10-best-practices-to-secure-and-protect-passwords/>

[14] Securityintelligence (2018) [cit. 2018-8-24]. Dostupné na WWW: <https://securityintelligence.com/the-cracken-the-evolution-of-password-cracking/>

[15] Sourceforge (2018) [cit. 2018-8-24]. Dostupné na WWW: <http://ophcrack.sourceforge.net/tables.php/>

[16] Techdesignforums (2018) [cit. 2018-8-24]. Dostupné na WWW: <http://www.techdesignforums.com/practice/guides/side-channel-analysis-attacks/>

[17] Thehackernews (2017)[cit. 2018-8-24]. Dostupné na WWW: <https://thehackernews.com/2017/12/data-breach-password-list.html/>

[18] Uio (2018) [cit. 2018-8-24]. Dostupné na WWW: <http://passwords12.at.ifi.uio.no/Jeremi_Gosney_Password_Cracking_HPC_Passwords12.pdf/>

[19] Wikipedia (2018) [cit. 2018-8-24]. Dostupné na WWW: <https://en.wikipedia.org/wiki/Rubber-hose_cryptanalysis/>

[20] Wikipedia (2018) [cit. 2018-8-24]. Dostupné na WWW: <https://en.wikipedia.org/wiki/Leet/>

[21] Wikipedia (2018) [cit. 2018-8-24]. Dostupné na WWW: <https://en.wikipedia.org/wiki/Botnet/>

NOVÝ VÝVOJ V PROBLEMATICE VLASTNÍHO KRAJSKÉHO DOPRAVCE V ČESKÉ REPUBLICE

NEW DEVELOPMENT IN THE CASE OF THE OWN REGIONAL BUS TRANSPORT COMPANY IN THE CZECH REPUBLIC

Ing. Martin Šustr [1], Ing. Pavel Viskup, Ph.D. [2]
[1]Univerzita Pardubice, Dopravní Fakulta Jana Pernera
Katedra dopravního managementu, marketingu a logistiky
Studentská 95, 532 10 Pardubice
martin.sustr@upce.cz

[2]Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení
Ústav krizového řízení
Studentské náměstí 1532, 686 01 Uherské Hradiště
viskup@utb.cz

ABSTRAKT

V minulosti byla veřejná autobusová doprava zajišťována státními podniky. Po politických změnách, po roce 1989, byly tyto podniky privatizovány a staly se soukromými. Stále však zůstával požadavek na zajišťování dopravní obslužnosti v regionech. Dnes si kraje na svém území zajišťují celý systém dopravní obsluhy za podpory operátora integrovaného dopravního systému samostatně. V ČR však vznikají problémy mezi krajem dopravcem a řidiči dopravce. Krajské úřady soutěží ve výběrových řízeních dopravce. Dopravci, pro výhru v daném tendru nabízejí co nejnižší cenu, která je hlavním rozhodovacím kritériem. Nešťastným fenoménem však je, že dopravní podniky ve výběrových řízeních nabízejí častokrát podnákladovou cenu a provoz vysoutěžené dopravní obslužnosti je následně neudržitelný. Díky tomu dopravci nabízejí i neadekvátní mzdy svým zaměstnancům (řidičům). Vzhledem ke všem těmto komplikacím je logické zvažovat vytvoření vlastního dopravního podniku. Článek prezentující klady a zápory vlastního dopravce byl prezentován již v roce 2017 na konferenci Transport Means 2017 pořádanou Technickou Universitou v Kaunasu. Tento článek rozšiřuje výzkum realizovaný na Dopravní fakultě Jana Pernera o nové poznatky a o vývoj v dané problematice.

KLÍČOVÁ SLOVA

Základní dopravní obslužnost, autobusová dopravní společnost, integrovaný dopravní systém

ABSTRACT

Public bus transport was previously provided by state-owned enterprises. After the political changes, after 1989, these companies were privatized. However, there was still a need to ensure transport services in the regions. Nowadays the regions in their territory provide the entire transport system with the support of the integrated transport system operator separately. In the Czech Republic problems arise between the region, the carrier and the driver like a employee of the carrier. The regional authorities in the tenders choose the bus carrier. Carriers offer the lowest price, which is the main decision-making criterion, for winning in a given tender. However, the unfortunate phenomenon is that transport companies often offer a sub-cost price in tenders. Running on the definated area (tendred area) is financially unsustainable. As a result of this system, carriers pay inadequate (low) wages to their employees (drivers). Thanks to the all of these complications, it is logical to consider creating own transport company. The article presenting the advantiges and disadvantigies of

the carrier was presented at the Sicentific conference Transport Means 2017 organized by the Kaunas Technical University. This article extends the research realized at the Jan Perner Transport Faculty on new developments in the field.

KEY WORDS

Basic transport service, bus transport company, integrated transport system

ÚVOD

Doporučení vyplývající ze zkušenosti se zajištěním dopravní obslužnosti pomocí vnitřního provozovatele v zemích EU vychází z porovnání způsobů a systému provozování autobusové dopravy vybranými subjekty působících v EU a z poznatků fungování systému městské hromadné dopravy (MHD). Posledně jmenované jsou v ČR zřizovány magistráty, popř. městy, takže pro případnou podobnost návrhu systému zřízení a fungování autobusové dopravní společnosti (ADS) lze vycházet z těchto zjištění, i když se jedná o rozdílnou dopravní obslužnost.

Je však nutné zdůraznit, že v případě fungování MHD a dopravní obslužnosti území kraje se sice nejedná o stejnou činnost, ale struktura navrhovaného krajského autobusového dopravce vychází ze stejného, i když upraveného základu.

Rozsah plánovaných služeb vychází z aktuálního stavu ve veřejné linkové autobusové dopravě na území kraje. Uzemní velikost kraje si můžeme představit jako statistickou územní jednotku na úrovni NUTS 3 (statistická klasifikace je ztotožněna s územním vyjádřením prvku Kraj). Krajem je chápáno území o dané rozloze a velikosti. Toto území se pak člení na okresy (NUTS 4).

Kompenzace za provedený dopravní výkon je hrazena z rozpočtu kraje ve výdajích na dopravní obslužnost. Kompenzace související se zajištěním provozu veřejné linkové dopravy je rozdílem mezi oprávněnými náklady a tržbami z jízdného. Například kompenzace v Královehradeckém kraji ČR činila v roce 2015 ve výši 289 mil. Kč. V tomtéž roce byly tržby z jízdného jen 186 mil. Kč. Rozdíl byl placen právě z rozpočtu kraje. Vzhledem k tomu, že článek hovoří o zřízení jen jednoho dopravce, je zřejmé, že údaje z výběrového řízení (zejména pak celkové náklady a rozsah služby) nemohou být přesně dodrženy. Je však také zřejmé, že se diametrálně nerozcházejí.

Článek také pracuje s jinou technologií z důvodu potencionálního vzniku dopravní společnosti kraje a bere do úvahy také jiné technické zázemí. Variant zpracování existuje více, které lze vytvářet v realizační fázi dle konkrétních představ a možností kraje a situace, která se kolem vzniku dopravce bude vyvíjet.

Přesto se autoři snažili navrhnout přijatelný a nejvhodnější model, který může být funkční. Dále článek řeší i současný vývoj v oblasti vlastní autobusové firmy, kterou v současné době zřizuje Ústecký Kraj.

Cílem článku je zhodnotit situaci, poukázat na možné problémy a přínosy, včetně možnosti které jsou potřebné ke zřízení krajské dopravní společnosti v rozumné variantě a v neposlední řadě hodnotí vývoj v Ústeckém kraji.

1. MANAŽERSKÉ SHRNUTÍ

Výsledky souhrnné kalkulace poukazují na základní problematiku v řešené oblasti a rovněž vyjadřují stanovisko k zásadním okruhům obsahující řešení veřejné linkové dopravy (dále VLD).

Detailní řešení jednotlivých doporučení je součástí dalšího stupně přípravy vytvoření krajského dopravce, tzn. realizační dokumentace. Realizační dokumentace je dle [zdroj: Doprava Ústeckého kraje] v případě Ústeckého kraje již zpracována. Tato dokumentace by měla dodat ucelený konkretizovaný obraz celého řešení problematiky vytvoření a dalšího působení krajského dopravce.

Stručné shrnutí zkušeností se zajištěním autobusové dopravní obslužnosti pomocí vnitřního provozovatele v zemích EU

Mezi kladné zkušenosti v zemích EU lze zařadit zejména:

- jeden vnitřní provozovatel je z časového hlediska stabilním prvkem,
- nejedná se o novinku, v zahraničí jsou s tímto dlouhodobé zkušenosti,
- odpadá dle evropské legislativy právní povinnost konání výběrových řízení na zajišťování dopravních výkonů dopravní obslužnosti v rámci závazku veřejné služby (dále i otázka držení licencí linek),
- investice mají dlouhodobý charakter (především v případě pořizování vozidel a modernizace technické infrastruktury),
- podle ohlasů je pozitivní zkušenost ze strany zřizovatele v tom, že může lépe ovlivňovat chování a činnost právě vnitřního provozovatele,
- snazší jednotnost systému dopravní obslužnosti, než je tomu v případě více smluvních provozovatelů (myšleno například jednotnost u smluvních přepravních podmínek),
- zaměstnanost a operativnost využití provozních zaměstnanců (nejsou vázáni na jednoho smluvního provozovatele),
- v případě komunálních podniků je možná materiální a personální „výpomoc“ v případě mimořádnosti,
- obecná jednotnost tarifu, protože se nevyužívají různé komerční nabídky jednotlivých smluvních dopravců,
- komplexnost při tvorbě jízdních řádů či oběhů, což u více smluvních dopravců je náročnější,
- není problém s dělením dopravců na dominantní a minoritní,
- v případě právní formy odpovídající příspěvkové organizaci není primárně cílem vytváření zisku, jako je tomu u smluvních dopravců,
- operativnější kontrolní systém vnitřního provozovatele ze strany objednatele dopravní obslužnosti,
- eliminace zúčtovacího centra dopravního svazu (někteří smluvní dopravci mohou být podle přerozdělovacího klíče zvýhodněni, jiní naopak – smluvní dopravci mohou poukazovat na nespravedlnost přerozdělovacího klíče).

Mezi záporné zkušenosti v zemích EU lze zařadit především toto:

- závislost na jednom provozovateli je rizikem v případě předem nepředvídatelných skutečností, např. myšlena změna politického zastoupení,

  zde je možné snad uvést příklad v historii z České republiky, konkrétně problémy právě s Dopravním podnikem Ústeckého kraje, zde se však přímo nejednalo o vnitřního provozovatele, proto krajskému úřadu nebyli problémy před nastáním krize indikovány,

- neuskutečňuje se soutěžení dopravních výkonů, tedy výsledná cena může být vyšší než v případě soutěže (současně se ale musí připomenout riziko návrhu dumpingových cen),

- problém s detailními znalostmi regionu, protože v případě vnitřního provozovatele se může jednat o částečnou povrchnost (rozhodování „od stolu“) – v případě nového vnitřního provozovatele existuje na začátku handicap v detailu znalosti místní dopravně přepravní situace oproti místním dopravcům,

- v případě přesahu systému do jiného kraje se musí akceptovat jiné podmínky (včetně standardů), které se pak musí implementovat pro celé kmenové území pokryté vnitřním provozovatelem,

- riziko častých změn v systému dopravní obslužnosti ze strany objednatele (hlavně některá nevyvážená politická rozhodnutí),

- větší „odpovědnost“ objednatele, odpovídající za majetek (vozidla, technická infrastruktura, atd.) a lidské zdroje než u smluvních dopravců,

- různé představy o zajišťování dopravní obslužnosti mezi regiony a městy (otázka příspěvků na kompenzaci prokazatelné ztráty z provozu z jejich rozpočtů),

- u vnitřního provozovatele se nepočítá, že by významnou část zajišťování dopravní obslužnosti řešil formou subdodávky (problém u mimořádností),

- u nově vzniklých vnitřních provozovatelů bývá problém u odborného personálního zajištění, a to nejen řidičů, ale i dopravně provozních pracovníků.

2. CENOTVORBA NÁKLADŮ NA 1 KM NOVÉ AUTOBUSOVÉ DOPRAVNÍ SPOLEČNOSTI

Nově zřízená společnost musí být schopna za stejných finančních prostředků určených na provoz zajišťovat dopravní obslužnost v kraji.

Je třeba na tomto místě také uvést nejspíše nepopulární fakt, že k existenci kvalitní a ekonomicky zdravé firmy je třeba se do budoucna spíše přiklonit k vyšší ceně dopravních výkonů (DV) než je tomu doposud, tzn. v krákodobém horizontu se vlastní dopravní společnost může jevit jako nevýhodná. Výpočty uvedené dále vypovídají o nemožnosti udržet stávající cenu DV v případě, že se budou nasazovat pouze nová vozidla.

V následující tabulce je z výzkumu [1] uvedena rozvaha ceny 1 km, při koupi celého vozového parku novými autobusy s leasingem a odpisy v různých variantách.

Ukazatel		řádek	Vnitrostátní doprava ve veřejném zájmu					
Odpisy (roky)			5	10	14	15	20	20
Leasing (roky)			5	5	10	15	15	20
Pohonné hmoty		11	4,47 Kč	4,47 Kč	4,47 Kč	4,47 Kč	4,47 Kč	4,47 Kč
Přímý materiál a energie		12	1,42 Kč	1,42 Kč	1,42 Kč	1,42 Kč	1,42 Kč	1,42 Kč
Opravy a udržování		13	2,35 Kč	2,35 Kč	2,35 Kč	2,35 Kč	2,35 Kč	2,35 Kč
Odpisy		14	10,77 Kč	5,38 Kč	3,85 Kč	3,59 Kč	2,69 Kč	2,69 Kč
Leasing (pronájem)		15	12,05 Kč	12,05 Kč	6,54 Kč	4,78 Kč	4,78 Kč	3,91 Kč
Přímé mzdy		16	7,70 Kč	7,55 Kč	7,70 Kč	7,70 Kč	7,70 Kč	7,70 Kč
Sociální a zdravotní pojištění		17	2,69 Kč	2,64 Kč	2,69 Kč	2,69 Kč	2,69 Kč	2,69 Kč
Cestovné		18	0,81 Kč	0,80 Kč	0,81 Kč	0,81 Kč	0,81 Kč	0,81 Kč
Úhrada z použití infrastruktury		19	0,44 Kč	0,44 Kč	0,44 Kč	0,44 Kč	0,44 Kč	0,44 Kč
Silniční daň		20	0,00 Kč	0,00 Kč	0,00 Kč	0,00 Kč	0,00 Kč	0,00 Kč
Elektronické mýtné		21	0,00 Kč	0,00 Kč	0,00 Kč	0,00 Kč	0,00 Kč	0,00 Kč
Pojištění zákonné odpovědnosti		22	0,35 Kč	0,35 Kč	0,35 Kč	0,35 Kč	0,35 Kč	0,35 Kč
Ostatní přímé náklady		23	0,52 Kč	0,52 Kč	0,52 Kč	0,52 Kč	0,52 Kč	0,52 Kč
Ostatní služby		24	0,41 Kč	0,41 Kč	0,41 Kč	0,41 Kč	0,41 Kč	0,41 Kč
Režijní náklady		25	1,84 Kč	1,84 Kč	1,84 Kč	1,84 Kč	1,84 Kč	1,84 Kč
Náklady celkem (ř.11 až23)		26	**43,56 Kč**	**37,97 Kč**	**31,13 Kč**	**29,12 Kč**	**28,22 Kč**	**27,36 Kč**
+zisk, -ztráta		27	0	0	0	0	0	0
Součet (ř.28+ř.33)		28	33,26 Kč	27,67 Kč	20,83 Kč	18,82 Kč	17,92 Kč	17,06 Kč
Tržby a výnosy	celkem (ř.30+31+32)	29	*10,30 Kč*	*10,30 Kč*	*10,30 Kč*	*10,30 Kč*	*10,30 Kč*	*10,30 Kč*
	jízdné	30	*10,30 Kč*	*10,30 Kč*	*10,30 Kč*	*10,30 Kč*	*10,30 Kč*	*10,30 Kč*
	jiné tržby	31	*0*	*0*	*0*	*0*	*0*	*0*
	výnosy aut.nádraží	32	*0*	*0*	*0*	*0*	*0*	*0*
Dotace do tržeb	celkem (ř.34+35+36)	33	*33,26 Kč*	27,67 Kč	20,83 Kč	18,82 Kč	17,92 Kč	17,06 Kč
	od obcí a měst	34	0	0	0	0	0	0
	od krajů	35	33,26 Kč	27,67 Kč	20,83 Kč	18,82 Kč	17,92 Kč	17,06 Kč
	slevy	36	0	0	0	0	0	0
Jízdné (vč. DPH) (tis. Kč)		37	186 000 Kč	186 000 Kč	186 000 Kč	186 000 Kč	186 000 Kč	186 000 Kč
Výše poskytnuté slevy dle CVMF celkem (v tis. Kč)		38						
z ř. 37	jízdné I (50% sleva)	39						
	jízdné II (75%˘sleva)	40						
	jízdné V(100% sleva)	41						
Dotace na pořízení DIM		42						

Ukazatel		řádek	Vnitrostátní doprava ve veřejném zájmu					
Odpisy (roky)			5	10	14	15	20	20
Leasing (roky)			5	5	10	15	15	20
z řádku 42	dotace do MD (obnova autobusů)	43	0	0	0	0	0	0
z řádku 24	náklady autobusových nádraží	44	7 944 772 Kč	7 944 772 Kč	7 944 772 Kč	7 944 722 Kč	7 944 772 Kč	7 944 772 Kč

Tab. 1 Náklady a tržby z přepravní činnosti na km (při nastavení odpisech a leasingu) [1]

3. DEFINOVÁNÍ FINANČNÍCH TOKŮ, KTERÝMI KRAJ ZAJIŠTUJE DOPRAVNÍ OBSLUŽNOST

Systém veřejné dopravy je zpravidla tvořen několika subjekty. Na jedné straně je to objednavatel veřejné dopravy a na straně druhé jsou to dopravci, jejichž úloha v systému je poskytnutí dopravních služeb, za což očekávají tvorbu zisku. Dále se v systému objevuje tzv. regulátor, což je stát zastoupený svým ministerstvem dopravy a financí. Posledním článkem jsou vlastní uživatelé veřejné dopravy tedy cestující, kteří za využití veřejné dopravy hradí stanovené jízdné.

Je nutno uvést, že veřejná doprava poskytuje i sociální službu především pro uživatele, kteří si nemohou dovolit plně využívat individuální dopravu.

Veřejná doprava může zastupovat i regulátora individuální dopravy, což vede ke negativních vlivů silniční dopravy (snížení škodlivých emisí, počtu nehod, záboru půdy, apod.).

Financování dopravní obslužnosti veřejné autobusové dopravy probíhá na základě uzavřených smluvních vztahů mezi dopravci a objednatelem veřejné dopravy, tzn. krajem. Smluvní vztah je uzavírán ve smyslu ustanovení zákona č. 194/2010 Sb. o veřejných službách v přepravě cestujících.

4. ZHODNOCENÍ TECHNICKÝCH A KVALITATIVNÍCH PŘÍNOSŮ PRO KRAJ A CESTUJÍCÍ

Jednotlivé oblasti (současný stav v Ústeckém kraji), kde jeden dopravce, zajišťuje dopravní obslužnost dle platných smluv, navrhují autoři zachovat. Nový dopravce, který bude zaštiťovat dopravní obslužnost celého území kraje je zárukou toho, že odpadne dnešní různorodost vozového parku. Již dnes je objednavatelem určen jednotný standard technických parametrů použitých vozidel. Část dopravců však z důvody úspory nákladů nedodržuje standardy (např. klimatizaci nechává vypnutou, na linkách s garantovanou přepravou jízdních kol používá jiná řešení než kapacitní přívěsy na jízdní kola, apod.).

Stejně tak autoři navrhují, aby vozidla pro krajského dopravce byla pořízena centrálně postupně v závislosti na jednotlivém přebírání oblastí od vysoutěžených dopravců. Nezbytným prvkem je včasné objednání vozidel.

Kontrolní orgány objednavatele budou mít možnost bez problémů měřit nastavené hodnoty uvedených ve standardech veřejné dopravy. Odpadá nutnost tolerance provozu starších vozidel, v případě, že dopravce nestihl vozidla v požadované kvalitě zajistit, čímž komplikují nejenom tvorbu oběhů vozidel pro jízdní řády (JŘ), ale i záměry na nasazení určitého typu vozidla pro zájmovou oblast.

U jednoho dopravce odpadá i nekoordinované nastavení parametrů kvality. V praxi to znamená, že nelze předpokládat, že dopravce bude uměle navyšovat zisk nestandardními způsoby, jako je nezabezpečení temperování vozidel, pravidelného úklidu, včetně čištění čalounění sedadel nebo již zmíněné neudžování a nepoužívání klimatizace. Lze předpokládat i zvýšení spolehlivosti a lepší provázanosti mezi řidiči. U různých dopravců je riziko, že i nedodržují čekací doby na zpožděné spoje jiných dopravců z důvodu neznalosti. Tento fenomén by měl být odstraněn.

Hlavní přínos pro kraj však bude přímá kontrola nad vynaloženými dotačními prostředky a nad všemi procesy, které u dopravce budou probíhat. Za pomocí organizací zřízených krajem bude kontrola nad výstupy, které budou pro krajského dopravce tyto organizace zajišťovat. V praxi to bude znamenat, že bude násobný přehled např. o objednávkách a spotřebě pohonných a provozních hmot, náhradních dílů, ad.

Z důvodu nutné spolupráce ve všech oblastech s organizátorem IDS odpadá nutná investice do odbavovacího zařízení a souvisejících periferií u různých dopravců. Opačně bude mít kraj přehled o nutnosti investování organizátora IDS do nových odbavovacích zařízení a centrálního řídícího systému IDS.

S ohledem na doporučenou strukturu krajského dopravce lze očekávat nižší náklady na pokrytí personálních potřeb v porovnání se současným stavem. Důvodem je jednotné vedení společnosti a maximální pokrytí návazných činností organizacemi zřízenými krajem.

V neposlední řadě odpadá problém s rozporováním zadávacího řízení na dopravce a řešení problémů s Úřadem pro ochranu hospodářské soutěže.

5. ZHODNOCENÍ SYNERGICKÉHO EFEKTU ZAJIŠTĚNÍ DOPRAVNÍCH SLUŽEB POMOCÍ KRAJSKÉHO AUTOBUSOVÉHO DOPRAVCE A VYUŽITÍ TECHNICKÝCH KAPACIT SPOLEČNOSTÍ ZŘÍZENÝCH KRAJEM

5.1 Technické zázemí

Pro dosažení požadovaného synergického efektu je zapotřebí především naleznout potřebné kapacity u společností zřízených krajem. V tomto případě je uvažováno s využitím kapacit Správy a údržby silnic (SÚS), resp. zázemí jednotlivých cestmistrovství.

SÚS působí na celém území kraje, hlavní sídlo má v krajském městě a dále je organizačně členěna na několik středisek a větší počty cestmistrovství.

Dislokace jednotlivých cestmistrovství z větší části kopíruje stávající rozmístění provozoven a garáží stávajících dopravců v kraji. Tento stav je využitelný pro zajištění běžných činností souvisejících např. se zajištěním odvodů tržeb z jízdného, atd.

Problematickým bodem se však jeví nedostatečná kapacita v místech s předpokládanou poptávkou po odstavných plochách (garážových stání), mycích linkách, údržbových a opravárenských prostorách (délka autobusů je možným vznikem problému v použitelnosti vybavení dílen).

Jelikož SÚS provozuje velké množství nákladních vozidel, tak musí zajišťovat nákup pneumatik, pohonných a provozních hmot a náhradních dílů. Pro snížení ceny objednávaných dílů a pneumatik navrhují autoři převedení centrálního nákupu náhradních dílů a pneumatik z SÚS na oddělení, která se zabývají nákupem pro potřeby SÚS a nově i autobusového dopravce. Zároveň nákup pohonných hmot a provozních kapalin by mohl být na SÚS povýšen o potřeby veřejné dopravy s tím, že autobusy budou zbrojeny u čerpadel, kde jsou zbrojeny vozidla SÚS.

Při využití vybavení dílen SÚS by bylo vhodné zajištění výměny pneumatik v dílnách SÚS, tak jako další běžná údržba pro výměnu provozních kapalin. Další opravné práce by byly proveditelné pouze v prostorách, které umožní provedení požadovaných operací bez omezení běžného provozu SÚS.

Důležitým krokem je využití SÚS pro instalaci a údržbu označníků zastávek pro dopravce v rámci výkonu pracovních činností běžné údržby. Možným dalším využitím je pomoc zaměstnanců SÚS pro výlepy jízdních řádů zejména při celostátních změnách jízdních řádů vyhlášených Ministerstvem dopravy.

Lze dosáhnout synergického efektu propojení dispečinku organizátora veřejné dopravy s dispečinkem SÚS kraje v oblasti informací o aktuálním stavu pozemních komunikací. Jednalo by se o velmi dobrý přínos efektivního propojení dispečinku organizátora IDS s dispečinkem SÚS.

5.2 Zastávky

Pro zajištění synergického efektu dopravce kraje se SÚS v oblasti zastávek by bylo vhodné smluvně zajistit přímou údržbu zastávek autobusové dopravy. V praxi by to znamenalo zajištění údržby zálivů a vodorovného značení SÚS. Zároveň by bylo vhodné, s ohledem na technické vybavení SÚS, přenést úlohu správce označníků zastávek veřejné dopravy na místně příslušná cestmistrovství. Tímto bude zaručena jednotnost vhledu označníků, nižší pořizovací náklady (vzhledem k množství objednaných označníků v případě plošné výměny). Správce označníků by zajišťoval požadovaný technický stav označníků. Může také zajišťovat výlepu jízdních řádů a tarifních map.

Výlep tarifních map, jízdních řádů a dalších informací by mohl také zajistit organizátor IDS, který v současné době zajišťuje pro dopravce tvorbu tarifních map pro jednotlivé zastávky. Využití zaměstnanců SÚS je možné v případě hromadného výlepu změněných JŘ. Individuální opravy poškozených JŘ je vhodnější řešit dopravcem nebo organizací zřízenou krajem.

Jelikož vývoj informačních technologií zaznamenává neustálý pokrok, tak organizátor IDS by měl provádět místní šetření v přestupních uzlech s registrovanou vyšší poptávkou po veřejné dopravě. Tyto body by pak mohly být pro zpřehlednění vybaveny elektronickým informačním zařízením, tzn. elektronickými označníky.

5.3 Posouzení a porovnání běžného a operativního řízení dopravy za předpokladu vzniku ADS v územní působnosti kraje

Jelikož jsou dnes funkční dispečinky IDS je předpoklad, že ADS má již v současnosti velmi dobré podmínky pro řízení dispečerské práce.

Vzhledem k tomu jak je navržen management společnosti pro řízení a běžné řízení společnosti, rozmístění provozoven a vozoven na teritoriu kraje neočekávají se zásadní problémy také v operativním řízení v jednotlivých oblastech kraje. Rozmístění provozoven respektuje geografické podmínky kraje a to i vzhledem na technologii, operativní řízení, případně běžnou údržbu vozidel vzhledem k oběhům vozidel.

5.4 Varianta realizace tvorby autobusového dopravce postupně v jednotlivých oblastech kraje

Po zvážení všech postupů autoři, dle [článek transport means], nedoporučují zvažovat a případně realizovat model vytvoření dopravní společnosti kraje, která by působila jen na určité části kraje a postupně by se rozšiřovala i do dalších částí. Tento model by pravděpodobně znedůvěryhodnil a zničil celou myšlenku existence jednoho dopravce provozující veřejnou linkovou autobusovou dopravu v kraji a nedošlo by nejspíše k plné realizaci na teritoriu kraje. Bohužel právě tento model chce v současné době Ústecký kraj realizovat.

6. JEDONTNÝ PŘÍSTUP K VEŘEJNÉ DOPRAVĚ OBJEDNÁVANÉ KRAJEM

Dle autorů je nejzasadnější jednotný přístup k veřejné dopravě. V ČR neexistuje jednotný koordinační orgán, který by spolupracoval s krajskými úřady navytváření jednotného dopravního systému pro cestují. Přitom v případě zájmu o rozvoj veřejné dopravy je tato otázka zásadní. Z toho důvodu koordinace probíhá pouze na území jednotlivých krajů.

V Ústeckém kraji, dle [3], z důvodu špatných zkušeností s vysouteženými dopravci v autobusové dopravě, probíhá snaha o vlastního autobusového dopravce. Pro autory je však velmi zvláštní fakt, že ve stejné době Ústecký kraj privatizuje systém krajské regionální železniční dopravy. krajský úřad tedy v případě železniční dopravy dělá přesně to, co se v současné době snaží v autobusové dopravě eliminovat. Nabízí se zde otázka, zda u železničních dopravců nehrozí podobná rizika, vůči kraji, jako u autobusových dopravců. Toto je, dle autorů, jasný signál nekoncepčního a nekoordinovaného přístupu k veřejné dopravě (na jediném krajském úřadě). Díky těmto indikacím, se autoři se obávají poškození dobrého jména veřejné dopravy jako celku.

ZÁVĚR

V článku byly shrnuty základní myšlenky ke vzniku vlastní autobusové dopravní společnosti kraje. Stejně tak bylo upozorněno na současný vývoj v ČR, zejména pak v Ústeckém kraji, který v současné době již podniká kroky k uskutečnění vlastního Autobusového dopravce. Bylo poukázáno na možnosti zapojení již existujících technických zázemí kraje do nové společnosti. Toto zapojení přináší úspory a zvyšuje efektivitu vynakládaných veřejných prostředků do nové autobusové dopravní společnosti.

Je samozřejmé, že pokud má být nová společnost prosperující společností založenou na zdravých ekonomických základech, což by v případě existence ADS mělo být rozhodující z pohledu kraje, je důležité, aby byla řízena kvalifikovaným managementem a je třeba také, že cena výkonu za jeden km by měla být vyšší než v současnosti a umožní tak existenci ekonomicky zdravé a prosperující společnosti s kvalitním vozovým parkem.

Zároveň však článek poukazuje na skutečnost, že právě v Ústeckém kraji se veřejná doprava neřeší komplexně jako celek. Rozdíli je možné pozorovat především mezi veřejnou autobusovou dopravou a regionální železniční dopravou. Zcela odlišný přístup kraje v těchto otázkách je pro autory minimálně zarážející a ukazuje zjevnou nejdnotnost a nekoncepčnost celého systému veřejné dopravy, i přes fungující IDS na území kraje.

Literatura

[1] Cempírek Václav, Soušek Radovan, Drdla Pavel, Průša Petr; Výzkum podmínek k založení vlastního autobusového dopravce v Královéhradeckém kraji, 123s, Institut Jana Pernera, Pardubice 2016

[2] *zDopravy.cz*: Ústecký kraj rozjíždí svého dopravce, už vybírá 49 autobusů pro Děčínsko a Ústecko , [12-08-18], Dostupné na WWW: <https://zdopravy.cz/ustecky-kraj-rozjizdi-sveho-dopravce-uz-vybira-49-autobusu-pro-decinsko-a-ustecko-6316/>

[3] *zDopravy.cz*: Autobusová krize na severu. Polovinu provozu může kvůli Busline převzít krajská firma, [12-08-18]. Dostupné na WWW: <https://zdopravy.cz/autobusova-krize-na-severu-polovinu-provozu-muze-kvuli-busline-prevzit-krajska-firma-13902/>

[4] *zDopravy.cz*: RegioJet poprvé uspěl v regionech, má provozovat vlaky v Ústeckém kraji, [14-08-18]. Dostupné na WWW: <https://zdopravy.cz/regiojet-poprve-uspel-v-regionech-bude-provozovat-vlaky-v-usteckem-kraji-14023/>

[5] *Ústecký kraj*: Doprava Ústeckého kraje – současný stav, [16-08-18]. Dostupné na WWW: <https://www.kr-ustecky.cz/doprava-usteckeho-kraje.asp>

DOPAD ROZŠÍŘENÉ REALITY NA BEZPEČNOSTNÍ OPATŘENÍ PŘI POŘÁDÁNÍ EVENTŮ

IMPACT OF AUGMENTED REALITY TO SECURITY PRECAUTIONS DURING THE EVENTS

Bc. Eva Trojanová[1], RNDr. Jakub Trojan, MSc, MBA, Ph.D.[1,2]
[1]Fakulta logistiky a krizového řízení, Univerzita Tomáše Bati ve Zlíně
Studentské náměstí 1535, 686 01 Uherské Hradiště
gebaeurovae@gmail.com, trojan@utb.cz
[2]Akademie věd České republiky, Ústav geoniky, oddělení environmentální geografie
Drobného 28, 602 00 Brno
jakub.trojan@ugn.cas.cz

ABSTRAKT

Tento příspěvek se z teoretického hlediska zabývá vlivem a dopadem rozšířené reality na pořádaní eventů. Ty už samy o sobě ve své přípravě i ve svém průběhu vždy přinášejí nejrůznější rizika, která je potřeba předem analyzovat a připravit se na ně, případně aplikovat preventivní opatření. Jedním z rizik byla vždy i rozšířená realita, které se nevěnovala dostatečná pozornost. Nyní dochází k masivnímu vlivu rozšířené reality na běžné uživatele chytrých telefonů pomocí různých aplikací. Nastává tak čím dál častější konfrontace pořádané akce s vlivem rozšířené reality jako jednoho z možných faktorů rizik.

KLÍČOVÁ SLOVA

Event, rozšířená realita, Pokémon Go

ABSTRACT

This paper theoretically examines the influence and impact of augmented reality to organizing events. Events have always brought a variety of risks during their all phases that need to be analyzed and prepare for them, or apply preventive measures. One risk has always been in augmented reality, which is not given sufficient attention. Now there is a massive influence on the current state of augmented reality via smartphone users using different applications. Thus it tends to frequent confrontations among organized events with an impact of augmented reality as one of the possible risk factor.

KEY WORDS

Event, augmented reality, Pokémon Go

ÚVOD

Díky tvůrcům a vývojářům nových her, aplikací atp. dochází k robustnímu šíření rozšířené reality mezi uživatele. Posledním z nejvíce propagovaných prvků rozšíření reality je hra „Pokémon Go“. Během pár dní se z ní stala nejstahovanější hra. Vlivem tohoto rozšíření se dá tvrdit, že pokud uživatel hře propadne, je schopen hnát se za jejími účely téměř kamkoliv. Podle vyjádření nejednoho z odborníků, který se zabývá moderními technologiemi, byl kdysi takto velký povyk spojený s geocachingem (Pouchlý, 2016). V příspěvku budeme demonstrovat modelovou situaci eventového koncertu a mobilní hry Pokémon Go.

1. SPECIFIKACE EVENTŮ

Pod pojmem *event* si můžeme představit plesy, svatby, konference atp. Obecně lze event považovat za předem organizovanou akci, která je svým způsobem jedinečná (Kotíková, Schwartzhoffová, 2008). Eventy lze rozdělovat podle nejrůznějších typů a specifických znaků. Postupně se mohou akce blíže specifikovat a zaměřovat. Jako první je třeba si určit o jaký typ eventu se jedná. Pak upřesnit zaměření eventu (na jakou bude cílit věkovou skupinu, zda bude pořádán jen pro „rodinu a přátele“ nebo se jedná o pracovní záležitosti, atp.). Nejvhodnější je začít správnou specifikaci eventu, čímž je jeho typ.

Nelze opomenout i neformální tzv. „rodinné“ akce, jako jsou narozeninové oslavy, svatby, Dalším příkladem specifického eventu je koncert, festival atp. Všechny eventy se dají vzájemně propojovat a kombinovat. Ale i s kombinacemi je potřeba manipulovat velmi obezřetně, ne všechny eventy k sobě typově sedí a musí se do programu zakomponovat velmi šetrně. Ideální ukázkou kvalitního konceptu je koncert (zástupce zábavné části programu) a benefiční akce (dobročinnost). Díky těmto kombinacím se stávají celkové eventy atraktivnější a mohou přinášet hlubší zážitek. Avšak s tím souvisí i vyšší výskyt rizik s tím spojených. Každý typ eventů má svá rizika. Jiná rizika budou na svatbě a jiná rizika při pořádání workshopu. Byť obsahují společné prvky, u obou je potřeba vykonávat jiné přípravy a s těmito rozdíly souvisí i jiná ohrožení.

2. RIZIKOVÉ FAKTORY POTENCIÁLNĚ OVLIVŇUJÍCÍ POŘÁDANÝ EVENT

Každé akci hrozí velké množství faktorů, které mohou ovlivnit její úspěšný průběh. Mohou to být rizika ekonomická, finanční, projektová, tržní, technická, sociální, provozní, bezpečnostní

a další (Managementmania, 2016). Mezi první fázi plánování akce je zapotřebí si sestavit seznam možných rizik (doporučuje se využít k tomu rozdělení do skupin).

Nově by se měl začít klást větší důraz na možnost technických rizik, která jsou často opomíjená a přitom mohou napáchat velké množství škod. Některým technickým rizikům se bohužel nedá předejít, měl by ale být připraven náhradní plán, který nijak zvláště nezasáhne průběh eventu a minimalizuje tak škody.

Novým trendem na trhu je vyšší povědomí uživatelů moderní techniky o rozšířené realitě. Jedná se o riziko zařazující se právě mezi rizika technická. Opravdové ohrožení samotné rozšířené reality není relevantní, ale pokud se (v našem modelovém případě) hra Pokémon zkombinuje s jinými rizikovými faktory, jedná se o nový rizikový faktor. Kombinace rizik, jako je lidská závislost na hře, touha po plnění úkolů, které hra nabízí, alkohol, nespokojenost s akcí,… může vést k ovlivnění pořádání eventu.

3. ROZŠÍŘENÁ REALITA

Teoretická konceptualizace rozšířené reality se přirozeně opírá o poznatky recentního výzkumu kyberprostoru, který patří mezi diskutovaná témata již v minulém miléniu (za všechny např. poznatky Dodge a Kitchina, 2001 nebo Kitchina a Dodge, 2002). V souvislosti s nástupem moderních technologií a zejména kontextově dostupných služeb (tzv. *Location-based services*) se rozšířená realita (*augmented reality*) dostává do masového využití běžnými uživateli. Rozšířená, někdy též augmentovaná, realita je pak spojením mezi světem virtuálním a materiálním (Maad, 2010). Materiální (fyzický, reálný) svět je podle Hynka s Vávrou (2007) typickým příkladem prostoru, v němž se odehrávají naše běžné aktivity. Opakem je svět virtuální, který je tvořen výhradně atributy kyberprostoru. V případě, že se entity světa virtuálního protkávají s prvky světa materiálního, hovoříme o rozšířené realitě (Maad, 2010) a tomu i odpovídající typologii virtuálních míst (viz tab. 1).

Konfigurace/počet uživatelů	**Asynchronní interakce**	**Synchronní interakce**
One-to-one (jeden k jednomu)	E-mail	Instant messaging (ICQ, AOL ...)
		Uzavřené chatovací místnosti
		„šeptání“ v multidimenzionálním virtuálním světě (hra)
		Internetová telefonie
		Videokonference
One-to-many (jeden k mnoha)	Webové stránky	Web kamery
	FTP archivy, cloud	Podcasty / videocasty
	Blogy	
	Newslettery	
Many-to-many (více k mnoha)	Mailinglisty / listservery	Chatovací místnosti
	Diskusní skupiny (Usenet)	Síťové hry

	Peer-to-peer sdílení	Grafické virtuální světy

Tab. 9: Typologický přehled virtuálních míst (Zdroj: Trojan, 2014; upraveno dle Dodge, Kitchin 2007)

Ve světě ubikvitních mobilních technologií s prakticky neustálou internetovou konektivitou je pak dosažení prvků rozšířené reality velmi snadné. Klasickými příklady využití jsou nástroje fungující v cestovním ruchu – mobilní průvodci, kteří s využitím konceptu rozšířené reality provází uživatele (ne)známým prostorem. K tomu, aby mohla rozšířená realita spolehlivě fungovat, je nezbytné splnit minimální prerekvizity. Mezi ně patří chytrý mobilní telefon/tablet s fotoaparátem, GPS/GLONASS čipem pro určení polohy, připojením k internetu a vhodnou aplikací rozšířené reality. Typickými příklady, kdy jsou tyto parametry promítnuty do návrhu univerzálních mobilních aplikací, jsou programy Layar a Wikitude (obě portovány pro mobilní operační systémy Android, iOS a Windows). Komercializace nástrojů rozšířené reality je sice typická v cestovním ruchu, z hlediska počtu uživatelů však dominuje herní průmysl. Zde tvoří leadery ve vývoji společnost Niantic, která představila nejprve hru Ingress, později velmi známou hru Pokémon GO figurující jako modelový příklad tohoto příspěvku.

4. ROZŠÍŘENÁ REALITA V RUKOU BĚŽNÉHO UŽIVATELE

Aplikace, které využívají rozšířenou realitu, si pomalu nacházely cestu k uživatelům po dlouhá léta. Mezi aplikace pracující s rozšířenou realitou pro Android, iOS a Windows Phone patří například Sun Surveyor (předpovídání pozice Slunce a Měsíce), Anatomy 4D (v podstatě učebnice lidského těla), Sky Map (aktuální rozložení hvězd), 3D Compass+ (promítání trojrozměrného kompasu), iOnRoad Lite (aplikace, která počítá bezpečnou vzdálenost při řízení, rychlost automobilu, atp.), dále to jsou již parciálně zmiňované aplikace Augment, Wikitude, Layar, Ingress, Google Goggles,… (Jiříková, 2014). Jedním z největších průkopníků v masivním rozvoji rozšířené reality mezi běžné uživatele je novinka na trhu – hra Pokémon Go. Jedná se o mobilní aplikací, která nabízí pohled na svět přes rozšířenou realitu. Pokémoni (postavičky, které se uživatelé snaží přes svůj mobilní telefon odchytit) se objevují podle svého přirozeného prostředí. Aplikace využívá data z Google Maps a Ingress, které jim umožňují do hry umísťovat další bonusy, jak uvádí např. Eurogamer (2016). Typy odlovitelných Pokémonů představuje následující výčet.

- normální pokémoni (Normal Pokemon)
  - dostupní jsou všude
- kamenní pokémoni (Rock Pokemon)
  - skály, lomy, dálnice,…
- oceloví pokémoni (Steel Pokemon)
  - moderní budovy, nádraží,…
- travní pokémoni (Grass Pokemon)
  - louky, farmy, lesy, zahrádky,…
- zemní pokémoni (Ground Pokemon)
  - letiště, příkopy, nebetonová parkoviště,…
- dračí pokémoni (Dragon Pokemon)
  - významná místa ve městech nebo na venkově,…
- vílí pokémoni (Fairy Pokemon)
  - hřbitovy, kostely,…
- vodní pokémoni (Water Pokemon)
  - řeky, jezera, moře,…

- duchoví pokémoni (Ghost Pokemon)
  - hřbitovy, obytné oblasti,…
- hmyzí a létací pokémoni (Flying / Bugs Pokemon)
  - venkovy, statky, velké parky,…
- ledoví pokémoni (Ice Pokemon)
  - tráva, ledovce, sjezdovky,…
- psychičtí pokémoni (Psychic Pokemon)
  - okolí nemocnic
- električtí pokémoni (Electric Pokemon)
  - průmyslové parky, elektrárny,…
- ohniví pokémoni (Fire Pokemon)
  - čerpací stanice
- bojoví pokémoni (Fighting Pokemon)
  - stadiony, arény,…
- jedoví pokémoni (Poison Pokemon)
  - bažiny, močály

Podle zdrojů se dají některé typy odlovit i na jiných, než výše uváděných místech. Přestože jsou uživatelé upozorňováni, že mají vnímat okolí, když „loví“ pokémony, často dochází k ignorování reálného světa. Některá pietní místa už zakazují, aby tam lidé lovili pokémony, protože tím ruší pietní památku a neumějí se chovat podle daných pravidel. Často také nedodržují potřebné zákazy vstupu (např. na nádraží na koleje, na dálnici atp.) (Eurogamer, 2016).

Někteří pokémoni jsou již přístupni jen na určitých místech, což může ovlivnit i cestovní ruch, protože uživatelé, kteří si hru velmi oblíbí, budou ochotni cestovat do jiných zemí jen pro to, aby si odlovili pokémona, který má v zemi ojedinělý výskyt. Podobné to je i s hrou Geocaching, díky které lidé poznávají nová místa a každé umístění schránky i schránka samotná mohou být originální a přinášet tak obohacení a potěšení. Geocaching se ale odkazuje na realitu a uživatel hledá podle daných souřadnic v reálném světě (ve většině případů fyzickou schránku, do které provádí zápis). S aplikací Pokémon Go v realitě nejde nic najít, uživatel je spokojen jen s rozšířenou realitou a dá se říci, že vlivem dostačujícího obrazu na displeji začíná ignorovat okolní svět (Pouchlý, 2016).

Samotná hra Pokémon Go nepřináší jen fyzická rizika při lovení pokémonů, ale představuje také technické riziko. Díky povolení přístupu umožňují tvůrcům přístup do jejich Google účtu nezbytného pro hraní hry (Novinky.cz, 2016). Takto získává Google další detailní informace o pohybu svých uživatelů, o vytíženosti některých cest atp. (Pouchlý, 2016).

Tato hra ihned po svém spuštění oslovila miliony lidí. První představení hry proběhlo v Japonsku 10. září 2015. Hra byla vytvořená silou tří velkých korporací. Jsou jimi Nintendo, The Pokémon Company a Niantic (tato společnost v roce 2013 vytvořila hru Ingress, která využívá rovněž rozšířenou realitu (Hrapokemongo, 2015). Tato fakta ukazují, že hra umí uživatele vtáhnout do rozšířené reality a to může vést k závislosti, což je samo o sobě rizikovým faktorem. Závislý člověk na nějaké hře, aplikaci atp. se může snadněji stát rizikem pro pořádání eventu (Koutský, 2016).

5. MODELOVÁ APLIKACE

Názornou ukázkou může být pořádání koncertu jedné kapely. I zde je nutné připravit analýzu rizika. Pro základní náčrt možných rizik využijeme nejdříve postup pro identifikaci problému (brainstorming), identifikaci rizika (WHAT-IF) a závěrečné zpětné ověření splnění úprav a předcházení nalezených potenciálních rizik (CHECK- LIST) (Gebauerová, Trojan, 2015).

Vzhledem k moderním trendům je třeba do všech oblastí klást větší důraz na kyberbezpečnost a možnost vlivu rozšířené reality. První krok předběžné analýzy tak může vypadat následovně.

Identifikace problémů:

- může být využita forma brainstormingu, kde je předem připraven scénář, podle kterého sestavený tým vytváří seznam možných rizik a vlivů. (Gebauerová, Trojan, 2015)

Identifikace rizika:

- vytváření nového seznamu rizik, ale z jiného úhlu pohledu. Pokládá se otázka „Co se stane, když." (Gebauerová, Trojan, 2015)

Zpětná kontrola

- nejrychlejším způsobem lze ověřit pomocí tzv. Check-listu, ten slouží k závěrečné kontrole bezchybnosti a opatření rizik na akci. (Gebauerová, Trojan, 2015)

Po každé aplikaci a jištění možného rizika je nutné uvádět možnost řešení.

5.1 Konkrétní modelové aplikování při přípravě koncertu

V následující tabulce je ukázkový příklad jen u pár identifikovaných rizikových faktorů. Ve skutečnosti je možné jich objevit mnohem více, záleží na hloubce analyzování. Pro vystižení účelu tohoto příspěvku je důležité upozornit na poslední řádek tabulky, který aplikuje do rovnocenné pozice k ostatním rizikům i rozšířenou realitu. Ta s sebou vždy nesla určitá rizika, ale nyní, když je masivně šířená mezi běžné uživatele, je možné se s ní častěji setkat a měl by na ni být brán větší zřetel i při pořádání eventů. Je zapotřebí učinit předběžné kroky. Důležité je všechny informovat a připravit je preventivně na reakci, která je adekvátní k nastalé situaci. Uživatel, který se účastní eventu, musí přijmout pravidla, která s ním souvisí. Proto je nutné, aby respektoval zákaz vstupu na určitá místa, jak z důvodu ochrany soukromí vystupujících, zabezpečení věcí, atp. tak i z důvodu svého vlastního bezpečí. Některým rizikům lze předejít kvalitní přípravou, jsou však taková, která samotní organizátoři nemohou ovlivnit (počasí, terorismus, kybernetická bezpečnost, vliv rozšířené reality), pouze mohou věnovat více pozornosti prevenci a přípravě akce.

MOŽNÁ RIZIKA	NÁVRH ŘEŠENÍ BRAINSTORMING	WHAT – IF	CHECK - LIST	ODPOVĚDNOST
		(co se stane, když...)	*(je vyřešená situace, když…? Jak je situace vyřešená?)*	
právní aspekty	kontrola u odborného pracovníka	kontaktovat odborného poradce pro právnickou problematiku a dodržet právní postupy; zaměřit se hlavně na prevenci a předem se poradit o přesných postupech	ano *(připraveny veškeré podklady a zákony potřebné ke konání akce)*	právní oddělení
finanční zabezpečení akce	přesné sestavení předběžného rozpočtu (případné omezení některých aktivit na koncertě, možnost sehnání sponzora,…)	mít zajištěný náhradní zdroj financí (záloha)	ano *(zajištění zálohy)*	finanční oddělení
environmentální vlivy	stanovení možnosti ztrát (hlavně finančních z důvodu menší návštěvnosti) při pořádání venkovní akce a nepřízně počasí. Případné přesunutí akce na jiný termín.	mít připravenou „suchou variantu“; vymyslet program, který bude pro návštěvníky dost atraktivní v kryté části	ne (nepředvídatelný jev) *(suchá varianta vhledem k velkému množství účastníku nelze aplikovat)*	organizační tým
dopad na životní prostředí (např. rušení nočního klidu)	prodiskutování problematiky s příslušnými orgány	soustředit se na prevenci a předem domluvit podmínky konání koncertu s příslušnými úřady	ano *(potřebná domluva s úřady)*	organizační tým

prostorové podmínky (malá kapacita prostoru, poškození poskytnutých prostor,…)	úprava vztahu mezi pronajímatelem a nájemníkem smlouvou či jiným dokumentem; ověření kapacity prostoru	předem avizovat omezenou kapacitu míst na koncertu	ano *(uzavřená smlouva, kde je přímo uvedena kapacitní možnost areálu)*	organizační tým a právní oddělení
teroristická rizika	posílení ochranky a případná kontrola (pravidelná u vstupu, namátková během akce)	je povinností informovat Policii ČR o pořádání akce, s tou se pak doporučuje domluvit si zvýšené hlídky; na akci musí být přítomno hasiči a zdravotníci, kteří mohou v případě ohrožení ihned zasáhnout	ne (nepředvídatelný jev) *(zvýšený počet ochranky, informování Policie, zajištěná přítomnost HZS a záchranné služby)*	bezpečnostní oddělení
kybernetická bezpečnost (zabezpečení dat)	bezpečné zacházení s interními a citlivými daty v PC, šifrování, heslování, porada s odborníkem	mít vytvořenou zálohu všech důležitých dokumentů, případně mít důležitá data u zástupce hlavního organizátora	ne (nepředvídatelný jev) *(preventivní nainstalování antivirových programů, pravidelné kontroly PC)*	technické oddělení
rozšířená realita	informování týmu o novinkách v této oblasti a možnosti vlivu lidského chování na průběh celé akce	vysvětlení, že místo není přístupné a může se tam vydat až po skončení akce; Je nutný zásah ochranky, která je předem informována o možnosti této situace a je předem již připravena na reakci. Pokud návštěvník stále trvá na porušení pravidel dané na koncertě, může zasáhnout pracovník ostrahy, popřípadě je možné zavolat Policii ČR.	ne (nepředvídatelný jev) *(preventivně předány informace o možnosti vzniku tohoto rizika příslušným složkám)*	bezpečnostní oddělení

Tab. 10: Modelový příklad vybraných rizik se začleněním rozšířené reality

ZÁVĚR

Účelem tohoto příspěvku bylo upozornit na aktuální zvýšení rizik vyplývajících z masifikace rozšířené reality mezi běžnými uživateli s možností dopadu na pořádání eventů. Příspěvek na modelovém příkladu pořádání eventu (koncertu) s vlivem rozšířené reality (hra Pokémon Go) reflektoval možné vlivy. V textu je rozšířená realita vnímána rovnocenně stejně jako všechna dosavadní rizika, která jsou pro účely tohoto příspěvku zestručněna a je zařazen jen jejich výběr.

PODĚKOVÁNÍ

Příspěvek čerpá z výstupů projektu Webová aplikace pro dynamizaci prostorových dat industriálních památek formou location-based services (TD03000079) Programu na podporu aplikovaného společenskovědního výzkumu a experimentálního vývoje OMEGA kofinancovaného Technologickou agenturou České republiky (TAČR).

Literatura

[1] Co už víme? Pokémon Go Funpage CZ/SK [online]. 2015 [cit. 2016-08-20]. Dostupné z: https://www.hrapokemongo.cz/2015/10/17/co-uz-vime/

[2] DODGE, M., KITCHIN, R. (2013). Crowdsourced cartography: mapping experience and knowledge. Environment and Planning A, 45, č. 1, 19-36.

[3] DODGE, M., KITCHIN, R. (2001): Mapping cyberspace. Routledge, London, 293 s.

[4] DODGE, M., KITCHIN, R. (2007) Virtual places. In: Douglas, I., Huggett, R., Perkins, C. (ed.): A Companion Encyclopaedia to Geography. Routledge, London, s. 519-536.

[5] GEBAUEROVÁ, E., TROJAN, J. (2015). Rizikové faktory a návrhy na jejich řešení u vybrané společenské akce. In Jiří Konečný, Vladimír Adamec. Sborník příspěvků z konference Krizové řízení a řešení krizových situací 2015. Vydání I. Uherské Hradiště: Univerzita Tomáše Bati ve Zlíně, 2015. s. 103-108, 6 s. ISBN 978-80-7454-573-3.

[6] Hra Pokémon Go představuje bezpečnostní riziko. Tvůrci se mohou zmocnit cizích účtů. In:Novinky.cz [online]. 2016 [cit. 2016-08-21]. Dostupné z: https://www.novinky.cz/internet-a-pc/hry-a-herni-systemy/409014-hra-pokemon-go-predstavuje-bezpecnostni-riziko-tvurci-se-mohou-zmocnit-cizich-uctu.html

[7] HYNEK, A., VÁVRA J. (2007): (Přinejmenším) čtyři prostorovosti krajiny. In: Herber, V. (ed.): Fyzickogeografický sborník 5: Fyzická geografie- výzkum, vzdělávání, aplikace: příspěvky z 24. výroční konference fyzickogeografické sekce České geografické společnosti konané 13. a 14.února 2007 v Brně. Masarykova Univerzita, Brno, 2007, s. 7-14.

[8] JIŘÍKOVÁ, L. (2014): APLIKACE S ROZŠÍŘENOU REALITOU PRO ANDROID, IOS A WP. Tyden.cz [online]. 2014 [cit. 2016-08-08]. Dostupné z: http://svetaplikaci.tyden.cz/aplikace-s-rozsirenou-realitou-pro-android-ios-a-windows-phone/

[9] KITCHIN, R., DODGE, M. (2002): The Emerging Geographies of Cyberspace. In: Johnston, R. J. (ed.): Geographies of Global Change: Remapping the World. Blackwell Publishing, Malden, s. 340-354.

[10] KOTÍKOVÁ, H, SCHWARTZHOFFOVÁ, E. (2008) Nové trendy v pořádání akcí a událostí (events) v cestovním ruchu. Praha: Ministerstvo pro místní rozvoj ČR, 2008. ISBN 978-80-87147-05-4.

[11] KOUTSKÝ, Z. (2016) Pokémon GO překonal rekord v počtu stažení, je nejpopulárnější. In: Appliště [online]. 2016 [cit. 2016-08-05]. Dostupné z: http://www.appliste.cz/pokemon-go/

[12] LATTENBERG, V. (2010) Event, aneb, Úspěšná akce krok za krokem: příručka pro organizátory. Brno: Computer Press, 2010. ISBN 978-80-251-2397-3.

[13] MAAD, S. (2010): Augmented Reality. InTech, 230 s.

[14] Místa výskytu v Pokémon Go podle druhů - kde hledat ohnivé, vodní a jiné pokémony. In:Eurogamer [online]. 2016 [cit. 2016-09-01]. Dostupné z: http://www.eurogamer.cz/articles/kde-hledat-pokemony-podle-jejich-druhu

[15] POUCHLÝ, P. (2016) Pokémon Go? Ruce si mne hlavně Google, všechna data jdou právě tam, tvrdí expert [video]. DVTV [online]. Aktualne.tv, 2016. [30.8.2016]. Dostupné z: https://video.aktualne.cz/dvtv/pokemon-go-ruce-si-mne-hlavne-google-vsechna-data-jdou-prave/r~af1f0d6e4cfe11e68d00002590604f2e/

[16] Řízení rizik (Risk Management). In: Managementmania [online]. 2016 [cit. 2016-08-28]. Dostupné z: https://managementmania.com/cs/rizeni-rizik

[17] TROJAN, J. (2014) Virtuální prostor. In Roman Matoušek, Robert Osman. Prostor(y) geografie. 1. vyd. Praha: Karolinum, 2014. s. 19-31, 12 s. ISBN 978-80-246-2733-5.

MINIMALIZACE BEZPEČNOSTNÍCH RIZIK PŘI PRODUKCI, DISTRIBUCI A SPOTŘEBĚ ZMRAZENÝCH POTRAVIN

MINIMALIZATION OF SAFETY HAZARDS DURING FROZEN FOOD PRODUCTION, DISTRIBUTION, AND CONSUMPTION

doc. Ing. Pavel Valášek, CSc. [1,2], JUDr. Pavel Mauer[1], JUDr. Jaromír Maňásek[1]
1Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení, Ústav environmentální bezpečnosti
Studentské nám. 1532, 686 01 Uherské Hradiště, Česká republika
2Univerzita Tomáše Bati ve Zlíně, Fakulta technologická, Ústav analýzy a chemie potravin
Vavrečkova 275, 760 01 Zlín, Česká republika
valasek@flkr.utb.cz, mauer@flkr.utb.cz, manasek@flkr.utb.cz

ABSTRAKT

Zmrazené potraviny mají při stravování obyvatelstva za mimořádných událostí a krizových situací své významné místo. Většinou se uplatňují následně po kompletovaných potravinových dávkách a tepelně sterilovaných konzervách. Při jejich výrobě se uplatňuje řada specifických fyzikálněchemických procesů, které v konečném důsledku rozhodují o jejich kvalitě a bezpečnosti pro konzumenta. Správné zvládnutí a kontrola technologických procesů jsou pak nezbytnými předpoklady úspěšného dosažení zamýšlených vlastností a užitné hodnoty finálních produktů. V příspěvku jsou rozebrány některé základní aspekty, které se na vlastnostech uvedených potravin podílí.

KLÍČOVÁ SLOVA

Konzervace potravin, zmrazování, zdroje technologických rizik rizik, minimalizace rizik.

ABSTRACT

Frozen foods are irreplaceable as a mean of population food supply during emergency events and crisis situations. They are commonly used after utilization of assembled food rations and thermally sterilized cans. During their production, a number of specific physicochemical processes is applied, consequently influencing their quality and consumer safety. Appropriate management and supervision of technological processes are essential prerequisites of intended attributes and usable value achievement concerning final products. In this article selected basic contributing aspects of listed food attributes are discussed.

KEY WORDS

Food preservation, freezing, sources of technological hazards, hazards minimisation.

ÚVOD

Snižováním teploty prostředí se postupně zpomaluje životní činnost mikroorganismů a enzymové reakce. Zchlazením potravin lze prodloužit jejich skladovatelnost.

Citlivost mikroorganismů na nízké teploty je různá podle druhu mikrobů. Kyzlink uvádí, že Clostridium botulinum, Escherichia coli a Proetus vulgaris se přestávají množit při teplotách +2 °C, kdežto psychofilní mikroorganismy s optimální teplotou 20 °C vegetují i při teplotách 0 °C, stejně jako plísně rodu Penicillinum, Cladosporium a Mucor. Smrtící účinek nízkých teplot není tak jednoznačný jako denaturační účinek teplot vyšších. Spory mikroorganismů přežívají i velmi nízké teploty a teplotami běžně dosažitelnými v praxi

(-40 °C) se nedají vzhledem k malému obsahu vody inaktivovat. Životní projevy a množení většiny mikroorganismů ustává při vychlazení potraviny na teplotu -10 °C.

Enzymy se neničí ani nízkými teplotami a zpomalení enzymové činnosti nízkými teplotami je vratné. Enzymové reakce zvolna působí i při mrazírenských teplotách (- 18 °C) a pokud nejsou enzymy inaktivovány před zmrazením, omezují dobu skladování potravin v mrazírnách.

Podle skladovacích teplot se rozlišují dva způsoby konzervování potravin:

1. konzervace chlazením, kdy se potraviny uchovávají při teplotách kolem 0 °C (nad teplotou zmrznutí),
2. konzervace zmrazováním, (pod teplotou mrznutí), je dlouhodobá reakce potravin hluboko zmrazených [1-4, 6].

1. ZMRAZENÉ POTRAVINY JEJICH HISTORIE A VLASTNOSTI

Uchovávání potravin při nízkých teplotách (potravin hluboko zmrazených) patří k moderním a novodobým způsobům konzervace. První mrazírenské sklady v Evropě byly postaveny v Londýně v roce 1871 pro skladování masa. Ovoce se začíná zmrazovat od roku 1909, zelenina a vaječné obsahy v roce 1929, hotová jídla a polotovary až po druhé světové válce. V Českých zemích byl mrazírenský průmysl vybudován až v období po druhé světové válce a spotřeba zmrazených potravin (mimo masa) činila v roce 1965 2 kg na obyvatele za rok. V současné době je poměr mezi mrazenou zeleninou, hotovými jídly a ovocem přibližně 4:2:1 [1, 4, 6]

Průměrná roční spotřeba zmrazených výrobků v dnešní době je **v celé Evropě 25,5 kg/osobu**, přičemž ve Švédsku 51,6 kg, Irsku 49,6 kg, Norsku 48,3 kg. Z nových zemí je na prvním místě Maďarsko (16,5 kg), zatímco v Polsku je spotřeba jen 8,2 kg, v ČR 5,6 kg a v Rumunsku 2,3 kg [7].

1.1 Vliv nízkých teplot na rozvoj mikroorganismů

Mrazírenské teploty (od -10 do -18 °C) zabraňují rozvoji mikroorganismů spolupůsobením tří činitelů:

- nízké teploty omezují a zastavují životní projevy mikroorganismů
- vymrznutím vody z potravin ve formě ledových krystalů se ve zbylém roztoku zvětší osmotický tlak
- ledové krystaly vlivem zvětšeného objemu působí nepříznivě mechanickým tlakem na mikrobiální buňky, současně však způsobují mechanické poškození rostlinných pletiv a živočišných tkání [4, 6].

Snižováním teploty se postupně zpomalují až zastavují životní projevy mikroorganismů. Citlivost Mikroorganismů je různá podle druhů, vývojového stádia a rychlosti zmrazování. Baktérie nejvíce hynou v rozmezí teplot -1 až -5 °C, psychrofilní baktérie hynou až při teplotách -18 °C. Velmi odolné jsou spory plísní. Hrubý uvádí, že při -10 °C bylo inaktivováno 35%, při -20 °C až 90% přítomných spor. Pomalé zmrazování a zvláště střídání teplot zvyšuje smrtící účinek nízkých teplot na mikroorganismy.

V potravinách zmrazených na teploty nižší než -7 °C je většina vody přeměna v led. Zvýšený osmotický tlak ve zbylém tekutém prostředí zabraňuje rozvoji především baktérií. Koloidní systémy potravin, tzv. hydrofilní koloidy, si však při běžných mrazírenských teplotách udržují

část nezmrzlé vody v tekutém stavu, což umožňuje zvláště sporám zachování životaschopnosti. Mrazené potraviny nejsou sterilní a konzervační zákrok trvá pouze po dobu působení nízkých teplot. Po rozmrazení vlivem mechanického poškození tkání a pletiv ledovými krystaly se kazí rychleji než stejné potraviny nezmrazené [1, 4, 6].

Každé teplotě přísluší rovnovážné procento zmrzlé vody v potravině. Led má asi o 1/11 větší objem než voda, což způsobuje jak mechanické poškození, tak odvodnění koloidních systémů mikroorganismů. Rovnovážné procento zmrzlé vody v hovězím mase a dále v ovoci, zelenině a je uvedeno v tab. 1 a 2.

Teplota (°C)	-2,5	-5,9	-7,5	-10,0	-12,5	-15,0	-17,5	-20	-32,5
Zmrzlá voda (%)	63,5	75,6	80,5	83,7	86,0	87,5	88,5	89,4	91,5

Tabulka 1 Procento zmrzlé vody v hovězím mase při různých teplotách [4]

Teplota (°C)	**Rajčata**	**Fazolové lusky, mrkev**	**Jablka, hrušky, švestky**	**Pomeranče, citróny**	**Višně**
-1	30	0	0	0	0
-2	60	28	0	0	0
-3	70	50	20	20	0
-4	76	58	32	32	20
-5	80	64,5	41	41	32
-6	82	68	48	48	45
-7	84	71	54	54	47
-8	85,5	73	58,5	58,5	52
-9	87	75	62,5	62,5	55,5
-10	88	77	65,5	65,5	58
-12,5	89	80,5	69	69	63
-15	90	83	72	72	67
-18	91	84	75	75	71

Tabulka 2 Procento zmrzlé vody v ovoci a zelenině při různých teplotách [4]

Kryohydratický bod (eutektická teplota (teplota zmrznutí posledního zbytku tkáňové vody v potravině)) je u většiny potravin při teplotě -55 až -65 °C. V dosažitelných zmrazovacích zařízeních nelze na takovou teplotu potraviny zmrazit [1-4, 6].

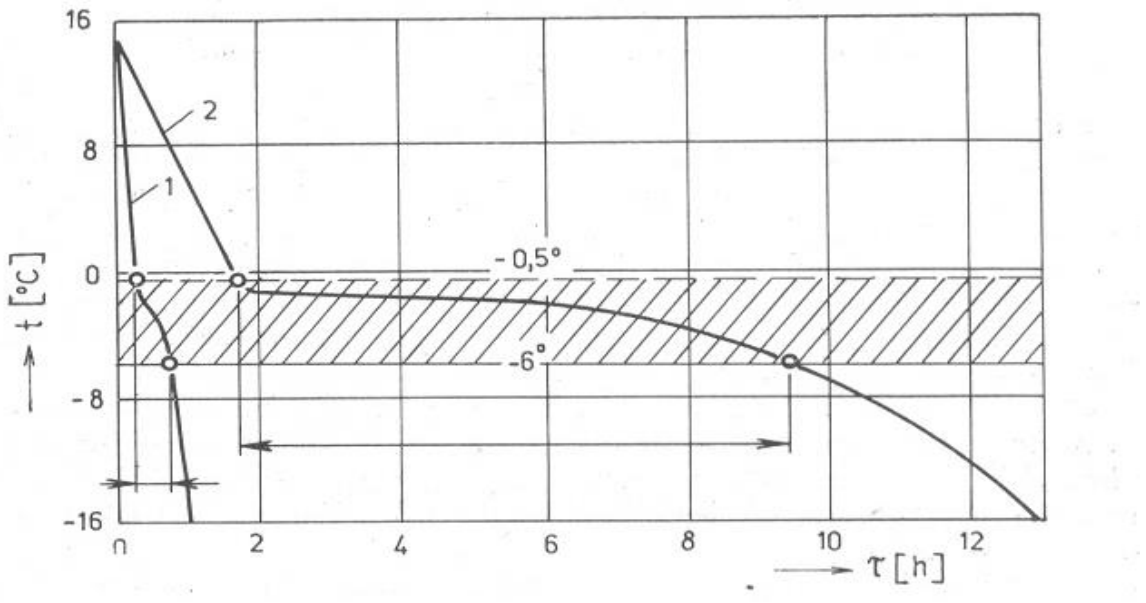
1.2 Vliv nízkých teplot na aktivitu enzymových reakcí

Aktivita enzymů je výrazně ovlivněna teplotou. Zahříváním do teplot 50 °C vzrůstá, dalším zvyšováním teploty se zmenšuje a při dosažení denaturační teploty bílkovin (kolem 65 °C) se enzymy ničí. Nízké teploty nemají jednoznačný denaturační účinek na bílkoviny, snižováním teploty se enzymové reakce zpomalují, aktivita enzymů je úměrná teplotě zchlazení podílu vymrzlé vody. Pozvolna probíhající enzymové reakce mohou ovlivnit jakost zmrazených potravin i při teplotách, při kterých mikrobiální činnost úplně ustala. Teprve při velmi nízkých teplotách (kolem -30 °C), kdy je téměř všechna voda přeměněna v led a enzymy nemají vhodné reakční prostředí, jejich činnost ustává. Hydrolytické enzymy /např. lipasy) jsou při stejně nízkých teplotách aktivnější než oxidasy. V potravinách rostlinného původu je v důsledku většího podílu volné vody aktivita enzymů větší než u masa. Libové maso je za stejných podmínek déle skladovatelné než maso tučné.

Běžně používané mrazírenské teploty -18 až -20 °C nezastavují enzymovou činnost a je-li požadována úplná inaktivace, musí být protienzymový zákrok proveden před zmrazením. Zelenina se proto blanšíruje, ovoce se zmrazuje s cukrem apod. Inaktivace enzymů i hlubokými teplotami je reverzibilní a po rozmrazení je rychlost enzymových reakcí v důsledku mechanického poškození a změny složení tkáňových tekutin rychlejší než v potravinách čerstvých.

1.3 Grafické znázornění průběhu teploty a tvorby ledových krystalů

Z každého zmrazovacího zařízení se odvádí za jednotku času konstantní množství tepla. Závislost mezi teplotou zmrazované potraviny a časem za uvedených podmínek lze vyjádřit křivkou. (Její obecný průběh je znázorněn na obr. 1.)



Obrázek 1 Grafický průběh rychlosti zmrazování potravin [1]
1 – rychlé zmrazování, 2 – pomalé zmrazování

Křivku lze charakterizovat třemi časově odlišnými úseky:

1. časový úsek potřebný ke zchlazení potraviny na teplotu mrznutí (τ_1)
2. časový úsek charakterizovaný největší tvorbou ledových krystalů v potravině (τ_2)

3. časový úsek potřebný k dochlazení potraviny na teplotu skladování (τ_3)

První časový úsek, potřebný ke chlazení potraviny na teplotu mrznutí, je časově krátký. Při zchlazování se odvádí měrné teplo potraviny nad teplotou mrznutí, které je hodnotově menší než 4,186 kJ kg^{-1} K^{-1}. Teploty mrznutí potravin jsou uvedeny v tab. 3.

Druh	**Teplota mrznutí (°C)**	**Druh**	**Teplota mrznutí (°C)**
Brambory	-1,71	Maliny	-0,88
Broskve	-1,45	Okurky	-0,84
Cibule	-1,66	Ostružiny	-1,60
Citróny	-2,16	Pomeranče	-2,23
Hrášek	-1,09	Rajčata	-0,90
Hrušky	-2,2	Rybíz	-1,0
Jablka	-2,0	Ryby	-0,9 až -2,0
Jahody	-1,16	Špenát	-0,75
Kapusta	-0,42	Švestky	-1,95
Karotka	-1,35	Třešně	-2,35
Květák	-1,06	Vejce obsah	-05
Maso	-1,0	Zelí	-0,42

Tabulka 3 Teploty mrznutí potravin [4]

V druhém časovém úseku se snižování teploty v potravině zpomalí, protože se většina přítomné vody v potravině mění v led a uvolňuje se velké množství skupenského tepla. Hodnota skupenského tepla je podstatně vyšší než hodnota tepla měrného (u vody je 334,9 kJ kg^{-1}). Převážná většina ledu se v potravinách tvoří v teplotním rozmezí teploty mrznutí (kolem -1 °C) a teploty -6 až -8 °C. Rozmezí stanovených teplot se nazývá pásmo maximální tvorby ledových krystalů. Skupenská a měrná tepla potravin jsou uvedena v tab. 4.

V této fázi dochází i k řadě nepříznivých změn. Tvořící se ledové krystaly vlivem zvětšeného objemu mechanicky poškozují živočišnou tkáň a rostlinné pletivo. Vymrzáním vody se současně koncentrují rozpuštěné látky v tekutinách a teplota mrznutí klesá. Vymrzání vody může působit až nevratnou dehydrataci koloidů. U potravin bohatých na bílkoviny (koloidy), jako je maso a některá zelenina, se zmenšuje vařivost a vzniká slámovitá chuť zeleniny v důsledku zmenšené bobtnací schopnosti.

Potravina	Obsah vody (%)	Měrné teplo nad zmrzlým stavem	kJ kg^{-1} K^{-1} pod zmrzlým stavem	Teplo mrznutí kJ^{-1} K^{-1}
Drůbež	74	3,35	1,76	246,9
Husa vykrmená	41	3,01	1,72	138,1
Kuře	72	3,43	1,88	242,79
Krocan	55	3,18	7,76	184,2
Hovězí tučné	51	2,55	1,50	171,6
Hovězí libové	72	3,26	7,76	234,4
Telecí	63	2,97	1,67	209,3
Vepřové tučné	39 – 46	2,13	1,39	167,4
Vepřové libové	72	3,47	1,84	234,4

Tabulka 4 Měrná a skupenská tepla potravin živočišného původu [1]

Na rozsah nepříznivých změn má vliv velikost vznikajících krystalů. Při pomalém zmrazování se tvoří velké ledové krystaly, voda potřebná k vytvoření krystalů se odebírá ze vzdálených míst. Mechanické poškození je větší, mění se složení tkáňových tekutin po rozmrazení a odvodnění koloidních systémů je hlubší. Takto zmrazené potraviny mají po rozmrazení nepevnou konzistenci, vytéká z nich nadměrné množství šťávy, rychle mění barvu a podléhají oxidačním reakcím.

Malé ledové krystaly, vznikající při rychlém zmrazování, mají nežádoucí vedlejší účinky menší. Při rozmrazování se stačí většina vody vznikající táním krystalů vázat zpět na koloidy a vytékání tekutin je menší. Malé ledové krystaly se tvoří rychlým zmrazením. Vytvoří se hodně krystalizačních jader a krystaly nemají čas narůst. Teplotní pásmo maximální tvorby krystalů má být při technologicky správném zmrazování časově co nejkratší. Požadavek rychlého zmrazení se musí dodržet především u masa a těch rostlinných surovin, které se zmrazují v čerstvém stavu (bez předchozího blanšírování)

Nežádoucí vliv ledových krystalů lze omezit zmrazováním potravin přehuštěných, zahuštěných cukrem nebo solí. Uvedené úpravy však mění chuť i charakter potravin a v praxi se dají uskutečnit pouze výjimečně. Velmi rychlým poklesem teploty při zmrazování může nastat tzv. nitrifikace. Led se vytvoří bez krystalizačních jader přímo ve vodních obalech koloidů, takže poškození i odvodnění je minimální.

Třetí časový úsek je charakterizován dochlazením potraviny na teplotu skladování. Většina potravin se ve zmrazovacím zařízení mrazí na teplotu skladování. Většina potravin se ve zmrazovacím zařízení mrazí na teplotu -7 °C ve středu (v jádře) a dochlazení na skladovací teplotu -18 °C nastává až ve skladech. Čím nižší je teplota potravin při uložení do skladu, tím méně se vytvoří ledových krystalů pomalým zchlazením. Potraviny nedostatečně vychlazené se nesmějí do mrazírenských skladů uskladňovat. U dostatečně zmrazených potravin je tvorba ledu ve skladech malá. Časově je třetí úsek krátký, protože se odvádí převážně pouze měrné teplo potraviny pod teplotou zmrznutí [1, 4, 7-9].

2. VÝPOČET SPOTŘEBY CHLADU PRO ZMRAZOVÁNÍ POTRAVIN

Spotřeba chladu ke zmrazování se vypočítá tepelnou bilancí zmrazovací křivky nebo orientačně ze změny tepelných obsahů před zmrazením a po zmrazení

2.1 Výpočet spotřeby chladu tepelnou bilancí

$$Q = mc_1(t_1-t_2) + ml + mc_2(t_2-t_3) \quad (1)$$

Kde m je množství tepla (kJ)

G – hmotnost potraviny (kg)

c_1 – měrné teplo potraviny nad teplotou mrznutí (kJ kg^{-1} K^{-1})

t_1 – teplota potraviny před zmrazováním (K)

t_2 – teplota mrznutí potraviny (K)

l – skupenské teplo mrznutí potraviny (kJ kg^{-1})

c_2 – měrné teplo potraviny pod teplotou mrznutí (kJ kg^{-1} K^{-1})

t_3 – teplota zmrazené potraviny (K)

Hodnoty uvedených veličin pro vybrané druhy potravin jsou v tab. 4.

2.2 Výpočet pomocí tepelných obsahů

$$Q = m(i_1-i_2) \quad (2)$$

Kde i_1 je tepelný obsah potraviny před zmrazením (kJ kg^{-1} K^{-1})

i_2 – tepelný obsah potraviny po zmrazení (kJ kg^{-1} K^{-1})

Tepelný obsah potravin je srovnáván s nulovým obsahem při 253 K (-20 °C) a údaje předpokládají, že v potravině neprobíhají reakce spojené s vývinem tepla. U ovoce a zeleniny vlivem dýchání se teplo uvolňuje a při přesných výpočtech se musí připočítat. Tepelné obsahy bývají tabelovány [1, 4, 6].

3. HLAVNÍ ZÁSADY PRO MINIMALIZACI RIZIK A PRO BEZPEČNOST ZMRAZENÝCH POTRAVIN

a) Kvalitní produkt lze vyrobit pouze z kvalitních surovin.

b) Pro dělené zmrazené potraviny je nezbytný vhodný obal, nejlépe nové generace:

- Aktivní materiály - obsahují aktivní složky, které mají udržet nebo zlepšit stav potraviny.
- Inteligentní materiály - mají sledovat stav potraviny, jako je dodržení skladovací teploty, známky kažení apod.

c) Proces zmrazování musí být co nejrychlejší, aby bylo v co nejkratší době překonáno tzv. pásmo maximální tvorby krystalů.

d) Proces rozmrazování musí být co nejpomalejší, aby se stačila koloidně vázaná voda.

e) Jedenkrát již rozmrazené potraviny už znovu nelze zmrazovat.

f) Bezpodmínečně musí být zachován stabilní teplotní řetězec v procesu: výroba-skladování-distribuce-skladování-spotřeba.

g) Uvádění do oběhu musí splňovat následující podmínky [8]:

- Hluboce zmrazené potraviny se přepravují dopravními prostředky, které umožňují zachování teploty hluboce zmrazených potravin minus 18°C nebo nižší. Při přepravě se může teplota výrobku krátkodobě zvýšit nejvýše na minus 15 °C.
- Nebalené hluboce zmrazené potraviny lze uchovávat nebo nabízet k prodeji v mrazicím zařízení pouze odděleně tak, aby nedošlo k jejich vzájemnému ovlivňování.
- Veškerá manipulace při prodeji hluboce zmrazených potravin musí být prováděna za takových podmínek, aby nedošlo ke zvýšení teploty hluboce zmrazené potraviny nad minus 15 °C.

h) Označování hluboce zmrazených potravin musí obsahovat [8]:

Kromě údajů uvedených v zákoně a ve zvláštním právním předpise [9] se obaly značí:

- Slovy, že potravina byla hluboce zmrazena.
- Datem minimální trvanlivosti při teplotě skladování minus 18 °C nebo nižší,
- Teplotou skladování,
- Slovy "po rozmrazení znovu nezmrazujte".

Na obalu pro spotřebitele musí být uvedena informace o době, po kterou má být potravina uchovávána spotřebitelem, a teplota uchování. Informace se uvede slovy "Uchování u spotřebitele".

3.1 Způsoby zmrazování

Podle způsobu odnímání tepla zmrazované potravině se rozlišují tři způsoby zmrazování:

a) zmrazování ponorové (imerzní) - ponoření zmrazované potraviny do kapalného chladiva.

b) zmrazování vzduchem - umístění zmrazované potraviny do proudícího chladného vzduchu,

c) zmrazování dotykové (kontaktní) - umístění zmrazované potraviny do aktivně chlazeného policového prostoru (tepelně izolovaná skříň s nastavitelnými policemi.

3.2 Mrazírenské skladování masa v praxi

Kromě krátkodobého chladírenského skladování při teplotách kolem 0 °C se může maso dále zmrazit a uchovávat zmražené po dlouhou dobu. Libové maso mrzne při -1,5 °C. Při teplotě v mrazírnách -18 °C se skladuje hovězí maso po dobu l roku a vepřové po 1/2 roku. Dochází však ke zhoršení jakosti v důsledku sublimace vody z povrchu, změně barvy v důsledku oxidace hemových barviv a změně aroma při oxidaci tuků (náchylnější je vepřový tuk vzhledem k vyššímu obsahu nenasycených mastných kyselin), nebo jejich odbourání mikrobiální lipázou, která je aktivní až do -30 °C. Tzv. mrazové spálení jsou světlejší skvrny,

které se vytvářejí denaturací bílkovin v důsledku sublimace ledu. Mezi nežádoucí jakostní závady zmrazených výrobků patří také rekrystalizace vody,

Zmrazené výsekové maso a droby smí být uváděny do oběhu pouze balené.

Opětovné zmrazení rozmraženého masa je závažnou chybou jak technologickou tak ekonomickou (zhoršení vaznosti, ztráta exsudátu).

ZÁVĚR

Na správně použitých zmrazovacích teplotách, časech a postupech závisí konečný úspěch výroby kvalitních zmrazených potravin. Proto je nutné věnovat kontrole průběhu zmrazovacího, ale také rozmrazovacího procesu soustavnou pozornost. Před zahájením výroby jednotlivého druhu produktu je třeba stanovit odvod tepla ze zmrazovaného materiálu v závislosti na čase a na teplotě ve zmrazovacím zařízení a na jejich základě následně pak stanovit odpovídající zmrazovací režim. S velmi vysokou pravděpodobností je možná minimalizace bezpečnostních rizik, při důsledném dodržování technologické kázně a s uplatněním moderních kontrolních metod. Kompletně 100% spolehlivá eliminace rizik je zejména při mimořádných událostech a při krizových situacích do značné míry ztížena. Kromě toho je třeba mít důsledně na paměti, že konzervační účinek trvá pouze při působení nízkých, konzervačně účinných teplot a při jejich porušení začnou probíhat rozkladné procesy se zvýšenou intenzitou.

Avšak při dodržování standardních operačních postupů, základních technologických zásad a předepsaných akceptačních hodnot kvalitativních kritérií, lze dosáhnout uspokojivé úrovně jak ve standardnosti výrobků, tak i v jejich bezpečnosti. Je tedy možno přijetí filosofie, že:

Kvalita musí být spolehlivě vyrobena, nikoli následně vyselektována kontrolou!

Literatura

[1] KYZLINK, V. *Principles of food preservation*. KYZLINK, V. P ELSEVIER - Oxford-New York-Tokyo, 1990. ISBN 0-444-98844-0.

[2] ZEUTHEN, P., BOGH-SORENSEN, L. *Food Preservation Techniques*. Woodhead Publishing., 2003. ISBN 978-1-85573.

[3] FRANCIS, FREDERICK, J. *Encyclopedia of Food Science and Technology (2nd Edition) Volumes 1-4. John Wiley & Sons*. John Wiley & Sons, 2003. ISBN 978-1-59124-460-8.

[4] VALÁŠEK, P., ROP, O. *Základy konzervace potravin*. Zlín, 2007. ISBN 978-80-318-587-9.

[5] VALÁŠEK, P., NOVÁK, L., MAUER, P., MAŇÁSEK, J.: Alternativní stravování v krizových situacích, Sborník příspěvků z konference *Krizové řízení a řešení krizových situací 2015, 10. a 11. září 2015v Uherském Hradišti,* Univerzita Tomáše Bati ve Zlíně, pp. 360-368, ISBN: 978-80-7454-573-3

[6] HRABĚ,J., BŘEZINA, P., VALÁŠEK, P.: *Technologie výroby potravin živočišného původu.* Univerzita Tomáše Bati ve Zlíně 2006, ISBN 80 – 7318 – 405 – 2.

[7] SUKOVÁ, I.: Rozdíly ve spotřebě zmrazených potravin, Dostupné z: http://www.agronavigator.cz/default.asp?typ=1&val=95685

[7] Vyhláška č. 326/2001 Sb. Vyhláška Ministerstva zemědělství, kterou se provádí §18 písm. a), d), g), h), i) a j) zákona č. 110/1997 Sb., o potravinách a tabákových výrobcích a o změně a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů, pro maso, masné výrobky, ryby, ostatní vodní živočichy a výrobky z nich, vejce a výrobky z nich

[8] Vyhláška č. 366/2005 Sb. Vyhláška Ministerstva zemědělství, o požadavcích vztahujících se na některé zmrazené potraviny.

[9] Vyhláška č. 113/2005 Sb., o způsobu označování potravin a tabákových výrobků, ve znění vyhlášky č. 368/2005 Sb.

VÝVOJ ČESKÉ BEZPEČNOSTNÍ PROGNOSTIKY

DEVELOPMENT OF CZECH SECURITY PROGNOSTICS

Ing. Jan Valouch, Ph.D.
Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, Ústav bezpečnostního inženýrství
Nad Stráněmi 4511
76005 Zlín
valouch@utb.cz

ABSTRAKT

Prognostika představuje vědní obor, jehož předmět tvoří rozvoj teorií, metod a praxe prognózování. Bezpečnostní prognostika je část futurologie, zabývající se budoucností vývoje bezpečnostního prostředí v objektech, odvětvích, sociálních skupinách, společnosti, státech, regionech, mezinárodním prostředí a vesmíru. Vědecké prognózy je možno využít při přípravě na možné budoucí bezpečnostní hrozby. Cílem následujícího příspěvku je seznámit čtenáře s vývojem bezpečnostní prognostiky (přístupy, pracoviště, autoři, publikace) v České republice.

KLÍČOVÁ SLOVA

Futurologie, prognostika, prognóza, bezpečnost.

ABSTRACT

The futurology is the science, the subject of which is the development of theories, methods and practices of forecasting. A part of futurology is a security prognostics, which deals with the future and development of the security situation in social groups, objects, sectors, companies, regions, states, the universe, etc. Scientific forecasts can be used to prepare for future security threats. This article describes the development of security prognostics (approaches, workplaces, authors, publications) in the Czech Republic.

KEY WORDS

Futurology, prognostics, security, prognosis.

ÚVOD

Futurologie je interdisciplinární věda, která se zabývá studiem a zkoumáním budoucnosti. Jedním ze stěžejních cílů futurologie je tvorba vědecky podložených prognóz, jako výpovědí o budoucnosti objektu nebo stavu a to ve formě futurologických vizi nebo futurologických scénářů.

Bezpečnostní futurologie je nauka o bezpečnostní budoucnosti a představuje součást futurologie, zabývající se budoucností vývoje bezpečnostní situace ve společnosti, státech, regionech, oblastech, ve vesmíru, v objektech, institucích, odvětvích, sociálních skupinách atd. Předmětem vědeckého zkoumání bezpečnostní futurologie je především možný budoucí bezpečnostní vývoj lidstva. Stěžejní činností je tvorba bezpečnostních prognóz společnosti jako celku nebo jejich dílčích částí.

Ve východní Evropě se namísto pojmu futurologie používá pojem **prognostika** [1]. Nicméně prognostika bývá často chápána ne jako synonymum futurologie, ale jako její součást, resp. jako **samostatný vědní obor**, jehož předmět tvoří rozvoj teorií, metod a praxe prognózování.

Její záběr je tedy užší než u futurologie a řeší zejména principy samotné prognostické činnosti a postupy tvorby prognóz a jejich integraci s řídícími procesy. Dále se rovněž zabývá vzájemnými vztahy mezi prognostickou činností a ostatními společenskými vědeckými činnostmi [2].

Bezpečnostní prognostika, jako dílčí část vědního oboru prognostiky, se zabývá možným budoucím vývojem bezpečnostního prostředí referenčních objektů, kterými mohou být např. objekty, odvětví, sociální skupiny, společnost, státy, regiony, mezinárodní prostředí nebo vesmír. Bezpečnostní prognostika je široce komplexní obor, který za účelem tvorby bezpečnostních scénářů a vizí využívá (musí využívat) poznatky (zejména tedy prognózy) z vojenského umění, geopolitiky, kriminalistiky, sociologie, politologie, ekonomie, ekologie, demografie, psychologie, antropologie, statistika atd. Pokud nevíme, jak by se do budoucna mohla vyvíjet politická situace, ekonomika, demografie, nové technologie nebo i ekologické hrozby, nemůžeme vytvořit prognózu vývoje bezpečnostní situace.

Predikování bezpečnostní situace je nezbytnou podmínkou pro zajištění přípravy na možný negativní vývoj v této oblasti. Odborně zpracované bezpečnostní prognózy mají stěžejní význam zejména pro referenční objekty typu stát, Evropská unie, OSN, NATO atd. Nicméně jejich tvorba a uplatnění je již od poloviny minulého století spojena významným podílem rovněž se zájmy především velkých nadnárodních výrobních a obchodních společností.

Vývoj prognostiky je od začátku 40. let minulého století spojen s cíleným a systematickým využíváním metodologie, jako vědní disciplíny, zabývající se metodami, jejich tvorbou a aplikací. Využitím vědeckých přístupů se prognostika odlišuje od běžného předvídání, které vychází z pouhého pozorování, hodnocení průvodních jevů, předtuchy či proroctví. Prognostika se snaží o identifikaci objektivní, pravděpodobné budoucnosti, nikoliv budoucnosti utopické (utopie - idealizovaná, fantastická představa nereálné, dokonalé lidské společnosti, obce nebo státu, nereálný plán).

Na začátku 50. let minulého století začíná prognostika pronikat do oblastí politiky, ekonomiky, ekologie, techniky a vojenství [3]. V tomto období sloužila futurologická studia zejména samotným prognostikům (vědecky poznávajícím badatelům a konstruktérům nové techniky) pro odhad budoucích hodnot [1].

V 60. letech minulého století se začínají formovat futurologická hnutí a futurologie je již považována za samostatný vědní obor. V těchto letech byly založeny významné futurologické organizace, jako např.:

- Peace Research Institute (Oslo, 1959),
- Mankind 2000 (Londýn, 1965),
- Institut für Zukunftsfragen (Vídeň, 1964),
- World Future Society (Světová futurologická společnost, 1966, Washington, Edward Cornish).

60. léta minulého století se rovněž vyznačuji zvýšeným zájmen o zpracování technologických prognóz ze strany velkých výrobních a obchodních společností. V USA mělo více než 600 firem své vlastní prognostické oddělení, které byly financovány cca 1 % podílem z prostředků na výzkumné činnosti, tj. 60 – 100 milionů USD ročně. Vlády jednotlivých států si nechávali zpracovávat bezpečnostní prognózy v oblasti národní bezpečnosti, např. Hudson Institut (Herman Kahn) zpracoval vládní zakázku v oblasti následků termojaderné války. Prognózy jsou chápány jako katalyzátor vývoje (např. cena za prognózu cca 10 000 USD - zisk z následné investice do technologie nebo výrobku stamilióny). Dochází k rozvoji placených

služeb (předplatné prognóz 5 – 20 000 USD / rok) a tím i vzniku nových a rozvoji činnosti významných prognostických pracovišť:

- RAND Corporation, dr. Helmer, metoda Delphi, 1964 (např. zapojení 100 vědců - otázky typu: Které vynálezy budou učiněny během příštích 50 let?),
- Arthur D. Litlle Inc., Chicago,
- SEDEIS, Paříž, Bertrand de Jouvenel, publikace, časopisy,
- Hudson Institut, Herman Kahn, vládní zakázky, následky termojaderné války, národní bezpečnost,
- Battelle Memoirial Institute, Ohio, prognózy pro Úřad kosmického výzkumu, cena až 500 000 USD,
- Samson Science Corporation - prognózy v elektronice,
- TEMPO (General Electric Co.) - aplikace vojenských metod v ekonomice, zákazníci např. vláda Alžíru.

1. ČESKOSLOVENSKÁ PROGNOSTIKA

Nárůst zájmu o prognostiku je možno v rámci ČSSR datovat do 60. let minulého století. První organizací, která se podrobněji a cíleně zabývala prognózováním, byla v ČSSR **Futurologická společnost**, která byla založena v r. 1968. Mezi její členy patřili např. Miloš Zeman, Gustav Bareš, Pavel Hrubý nebo Jaromír Kálal [1]. Stálý pracovní tým Futurologické společnosti zpracoval řadu futurologických studií. Mezi první materiály patřila studie „Československo 1985- 2000“, která byla zpracována pro první celostátní seminář českých a slovenských futurologů (Kroměříž, 13- 15. prosince 1968). Dalším výstupem byla kolektivní studie „Teoretické základy komplexních společenských projektů“, která představovala futurologické simulační modely, a na které spolupracovala Futurologická společnost, **Výzkumný ústav ekonomiky, průmyslu a stavebnictví** a Ministerstvo techniky. Simulační modely byly v té době považovány za metodologický základ futurologie a nejperspektivnější směr jejího vývoje [4].

Po období normalizace je možno sledovat známky liberalizace poměrů a obnovení prognostických aktivit v 80. letech. Prognostická činnost byla v tomto období zaštítěná **Československou vědeckotechnickou společností** (CSVTS) [11]. CSVTS působila v letech 1955- 1990, nejdříve v rámci československé akademie věd, od r. 1959 jako samostatná celostátní organizace pri ROH.

Prognostické aktivity byly realizovány v 80. letech i na dalších pracovištích, např. na **Oddělení komplexního modelování**, (působící v rámci agentury Technosport 1971- 1973, později v rámci Sportpropagu 1973- 1983) [11]. Vedoucím oddělení byl prognostik a současný prezident Miloš Zeman.

V roce 1984 vznikl v ČSSR **Prognostický ústav ČSAV** (Československá akademie věd). Náplní činnost Prognostického ústavu, jehož činnost se datuje do let 1984- 1992, byl výzkum v oblasti identifikace a návrhu řešení zhoršující se ekonomické a společenské situace a to s využitím prognostických nástrojů. Mezi výstupy ústavu patří např. publikace Valtra Komárka a kol. s titulem: „Souhrnná prognóza ČSSR do roku 2010", vydaná v r. 1988.

Úkolem zaměstnanců ústavu (prognostiků) bylo formulovat prognózy, ve formě matematicky podložených odhadů budoucího vývoje společnosti a především ekonomiky. Mezi známé osobnosti, které v ústavu pracovaly, patřili např. Valtr Komárek, Miloš Zeman, Václav Klaus,

Vladimír Dlouhý, Jiří Dolejš, Tomáš Ježek, Jan Mládek, Miroslav Ransdord a další). Prognostický ústav ČSAV zanikl v roce 1993 a to bez pokračovatele v České republice.

Na Slovensku byl v roce 1989 založen **Prognostický ústav Slovenské akademie věd** (PÚ SAV). Náplní činnosti ústavu je interdisciplinární základní a aplikovaný výzkum v následujících oblastech:

- teorie, metodologie a koncepce prognózování vývoje slovenské společnosti v národním i světovém kontextu,
- sociální a ekonomické dimenze globálních environmentálních změn,
- koevoluce (společný evoluční vývoj dvou a více druhů) institucionálních a technologických změn.

Pozn. od r. 2015 je Prognostický ústav SAV organizační součástí Centra společenských a psychologických věd SAV (CSPV SAV) [7].

Do r. 1989 v rámci ČSSR stát centrálně řídil hospodářství, centrální moc vylučovala otevřenou soutěž politických sil a stát kontroloval značnou část života obyvatel.

Po roce 1989 dochází k rozpadu centrálně plánovaného řídicího systému a projevuje se odpor ke všem metodám vládnutí připomínajícím centrální plánování.

V roce 1990 byla zrušena **Státní plánovací komise** a zřízeno **Federální ministerstvo pro národohospodářskou strategii**, které bylo určeno pro řešení koncepčních otázek dlouhodobé strategie hospodářského a sociálního rozvoje [1].

Pozn. Později bylo přejmenováno na **Federální ministerstvo pro strategické plánování** (1990-1992), které tak představovalo ústřední orgán státní správy tehdejší ČSFR pro dlouhodobou strategii hospodářského a sociálního rozvoje [1]. Mezi jeho hlavní náplň činnosti patřilo zejména:

- koordinace přípravy strategie hospodářského a sociálního rozvoje ČSFR,
- vypracování návrhů strategie a její předkládání je vládě ČSFR,
- vyhodnocování uskutečňování strategie,
- vyhodnocování opatření přijatých k realizaci strategie a jejich účinnosti,
- vypracování návrhů:
    - základních směrů, věcných a systémových podmínek hospodářského a sociálního rozvoje a státní politiky strukturálních změn,
    - koncepcí rozvoje vědy a vědeckotechnické politiky,
    - koncepce ekonomického zabezpečení obranyschopnosti a bezpečnosti státu,
    - dlouhodobých koncepcí zapojení československé ekonomiky do světové ekonomiky,
    - hlavních záměrů v oblasti životních podmínek a životní úrovně obyvatelstva.

Od doby zrušení Federálního ministerstva pro strategické plánování neexistuje v ČR v rámci státní správy orgán, který by byl schopen administrativně sladit postupy více resortů, podílejících se na fungování českého bezpečnostního systému, nezávisle na střídání politických stran a jednotlivých ministrů [5].

2. PROGNOSTIKA V ČESKÉ REPUBLICE

Léta 1992- 1997 je možno z hlediska prognostiky charakterizovat jako období bez potřeby strategického plánování. Česká republika se orientovala na neoliberalistický směr, kde budoucnost představuje projekci samovolných sil a nemá smysl zasahovat do řádu věcí a chtít vytvářet koncepce budoucího vývoje [1]. Politický reprezentace se zaměřila zejména na ekonomické cíle. Ekonomové spoléhali na spontánní vyřešení problémů- proto nebyly potřeba žádné instituce produkující ideje strategického vládnutí.

V období 1998-2002 se situace v rámci prognózování budoucího vývoje změnila k lepšímu a to s nástupem bývalého prognostika Miloše Zemana do funkce premiéra vlády. Vláda vyhlásila strategické cíle a k jejich realizaci ustanovila v roce 1999 **Radu vlády České republiky pro sociální a ekonomickou strategii** (poradní vládní orgán). Cílem byla tvorba prognostických a analytických idejí, jako prostředku informační podpory vládního strategického rozhodování a strategického řízení. Od roku 2000 Rada delegovala a zadávala práce nově vzniklému **Centru pro sociální a ekonomické strategie** (CESES).

V roce 2003 byla Rada vlády České republiky pro sociální a ekonomickou strategii zrušena a vznikla Rada vlády pro udržitelný rozvoj (RVUR), která se doposud zabývá zejména oblastí strategie udržitelného rozvoje (aktivity spojené se strategickým řízením jsou utlumeny).

Rada vlády pro udržitelný rozvoj:

- iniciuje, koncipuje, koordinuje, sleduje, vyhodnocuje a podporuje strategické dimenze v řízení státu,
- navrhuje opatření ke sladění dlouhodobých záměrů a cílů se střednědobými a krátkodobými cíli a programy v souladu s principy udržitelného rozvoje,
- sleduje a vyhodnocuje globální jevy a rozvojové příležitosti a navrhuje včasné a odpovídající reakce státu na ně,
- rozpracovává, koordinuje a sleduje uplatnění principů udržitelného rozvoje při dosažení dynamické rovnováhy jeho složky ekonomické, sociální a environmentální,
- zpracovává Strategii udržitelného rozvoje ČR a její aktualizace,
- zpracovává situační zprávy s vyhodnoceným souborem indikátorů udržitelného rozvoje,
- metodicky koordinuje tvorbu koncepčních dokumentů [6].

V loňském roce (2017) byl vydán strategický dokument Česká republika 2030, který stanovuje nové dlouhodobé priority rozvoje České republiky (Úřad vlády České republiky, Odbor pro udržitelný rozvoj).

2.1 České prognostické organizace a pracoviště

Pokusy o vytvoření ústředních strategických jednotek na úrovni centrální vlády nebyly po roce 1989 nikdy příliš úspěšné [1]. Pohled na prognostiku a plánování, tvorbu strategií a vizí se postupně od 90 let minulého století měnil z hlediska tvorby i uplatňování. Prognózy se začaly využívat zejména:

- ve veřejné správě i územní samosprávě,
- v podnikatelském prostředí,
- při tvorbě koncepčních dokumentů a strategií,

- v rámci strategického a územního plánování na regionální i státní úrovni.

Mezi organizace a pracoviště v oblasti futurologie a prognostiky je možné v období po roce 1989 zařadit například:

- Občanská futurologická společnost (1990-),
- Futurologická spoločnosť na Slovensku (1993-),
- Československá asociace Římského klubu (1991-1993),
- Česká asociace Římského klubu a Slovenská asociace Římského klubu (1993-)
- Technologické centrum Akademie věd České republiky (1994-),
- Centrum pro sociální a ekonomické strategie (2000-),
- Středisko bezpečnostní politiky (2005-),
- Ústav strategických studií (1999-2008),
- Centrum bezpečnostních a vojensko-strategických studií (2013-),
- Kabinet pro studium vědy, techniky a společnosti Filosofického ústavu AV ČR,
- Centrum globálních studií, Filosofický ústav Akademie věd ČR,
- Centrum pro teoretická studia (společná pracoviště AV ČR a Univerzity Karlovy),
- Společnost pro trvale udržitelný život a další.

V roce 1990 zahájila svoji činnost **Občanské futurologické společnosti (OFS).** Hlavním iniciátorem jejího vzniku a následně jejím předsedou byl František Petrášek (1934- 2014), český prognostik a futurolog (Katedra hospodářské a sociální politiky, Národohospodářská fakulta, VŠE v Praze). OFS je nezávislou, neziskovou a dobrovolnou organizací s cílem kultivovat předvídavé myšlení, koncipovat a předkládat řešení problémů budoucnosti. OFS pořádá rozpravy věnované dlouhodoběji probíhajícím civilizačním procesům a jejich vlivu na aktuální jednání člověka a společnost [8]. Mezi témata patřily např.:

- Evropa 2038- Alternativní scénáře ekonomického, politického a společenského vývoje,
- Spory o globální budoucnost- transformace nebo revoluce,
- Možné strategie zabezpečení optimálního sociálního a ekonomického vývoje SR a ČR atd.

V roce 1991 byla na základě iniciativy Václava Havla založena **Československá asociace Římského klubu.** Od roku 1993 (po rozdělení ČSFR) působí již jako **Česká asociace Římského klubu.** Asociace organizuje přednášky nebo besedy, podílí se na organizaci konferencí a to ve spolupráci s Centrem pro sociální a akademické strategie. Nicméně v současné době je činnost asociace utlumena.

V České republice patří v současnosti mezi významná pracoviště v oblasti prognózování např. Centrum pro sociální a ekonomické strategie Fakulty sociálních věd Univerzity Karlovy v Praze (CESES) a Středisko bezpečnostní politiky (Fakulta sociálních věd Univerzity Karlovy v Praze).

Centrum pro sociální a ekonomické strategie představuje interdisciplinární výzkumné a výukové pracoviště, která rozvíjejí teorii, metodologii a praxi zkoumání možných

budoucností. Zároveň s tím se věnuje problematice uplatnění analýz a prognóz v řídící praxi. V rámci své činnosti:

- identifikuje klíčové problémy a rozvojové priority ČR,
- zpracovává analýzy, scénáře, vize a strategie sociálního, ekonomického, environmentálního a politického vývoje ČR v evropském a globálním kontextu,
- vytváří platformu pro spolupráci odborníků, politiků, představitelů veřejné správy, občanského sektoru a občanů,
- zabývá se tvorbou metodických předpokladů pro zkvalitňování strategického řízení země [9].

Středisko bezpečnostní politiky (SBP) bylo založeno v roce 2005 jako pracovní skupina CESES. Od roku 2015 působí jako součást Institutu politologických studií FSV UK. Cílem činnosti střediska je snaha o zkvalitnění bezpečnostní politiky České republiky, a to prostřednictvím:

- vědecko-výzkumné činností- tvorba analytických, koncepčních a prognostických prací s důrazem na aplikovatelnost v praxi,
- vzdělávacích aktivit- výuka bezpečnostní politiky pro studenty FSV UK, organizace seminářů atd.
- rozvoje dialogu mezi součástmi bezpečnostní komunity, odbornou veřejností, představiteli veřejné a státní správy, politických stran a nevládních organizací [10].

V letech 1999 - 2008 byl součástí Vojenské akademie v Brně (od r. 2004 Univerzity obrany) **Ústav strategických studií** (ÚSS), jehož činnost byla zaměřena především na oblast vojenské strategie v kontextu výzkumu vojenské bezpečnosti. ÚSS zajišťoval rozvoj strategických studií, jako jedné ze základních cest k rozvoji poznání zákonů a zákonitostí vývoje v oblasti obrany a bezpečnosti státu. Výstupem jeho činnosti byla řada prognostických studií v horizontu let 2020 – 2030 v oblastech vývoje bezpečnostního prostředí, ozbrojených sil, obranných zdrojů, vojenských schopností, vedení vojenských operací atd.

Následovníkem ÚSS je od roku 2013 **Centrum bezpečnostních a vojensko-strategických studií** (CBVSS), jako součást Univerzity obrany. CBVSS zajišťuje vzdělávací a vědeckovýzkumnou činnost zejména v oborech bezpečnostních studií, vojenské strategie, strategického řízení a leadershipu.

2.2 Publikace v oblasti prognostiky v České republice

V rámci prognostických publikačních aktivit (prognóz, vizí, scénářů, dlouhodobých výhledů atd.) je možno hledat zejména v odborných článcích, samostatných publikacích, výstupech vědeckovýzkumných projektů a částečně i v koncepčních a strategických dokumentech vlády nebo jednotlivých resortů. Následující tabulka představuje výběr prognostických publikací národních autorů.

Autor	Název	Pozn.	Rok vydání
POTŮČEK, Martin	Průvodce krajinou priorit pro Českou republiku	Praha, CESES FSV UK	2002
POTŮČEK, Martin a kol.	Putování českou budoucností	Praha, CESES FSV UK	2003

ŠTĚDROŇ, Bohumír a kol.	Svět 2050	Nakladatelství sdělovací technika	2003
Kolektiv autorů	Bezpečnostní budoucnost České republiky: Otázky, výzvy, problémy	Sborník konference	2004
RAŠEK, Antonín (ed.)	Strategické tahy pro Českou republiku (strategickými tahy přiblížíme budoucnost)	Nakladatelství VPK	2004
VALOUCH, Jan.	Vyzbrojování ozbrojených sil vybraných evropských zemí - vývoj a perspektivy.	Vojenské rozhledy, Praha: MO ČR - AVIS	2004
JANOŠEC, J., a kol.	Bezpečnost a obrana České republiky 2015-2025	Ústav strategických studií, Praha:MO ČR-AVIS	2005
RAŠEK, Antonín	Bezpečnostní prognózy a realita	Pražské sociálně vědní studie, Praha: FSV UK	2006
BALABÁN, M. STEJSKAL, L.	Hlavní aktéři vývoje bezpečnostní situace ve světě v horizontu 2020 s výhledem 2050	Sborník workshopu	2006
PROCHÁZKA, J., VALOUCH, J., GALATÍK, V., MAZALOVÁ, V.	Obranné zdroje České republiky. Vývoj, perspektivy, rizika.	Ústav strategických studií, Univerzita obrany	2006
BALABÁN, Miloš, RAŠEK, Antonín	Divoké karty v budoucím vývoji světové bezpečnosti	Vojenské rozhledy, Praha: MO ČR - AVIS	2008
GALATÍK, V. (ed.)	Principy obrany České republiky 2030	Ústav strategických studií, Univerzita obrany	2008
POTŮCEK, M., MUSIL, J., MAŠKOVÁ, M.	Strategické volby pro českou společnost. Teoretická východiska	Praha, Sociologické nakladatelství	2008
POTŮCEK, M., MAŠKOVÁ, M.	Česká republika - trendy, ohrožení, příležitosti	Nakladatelství Karolinum	2009
FRIČ, P. VESELÝ, A. (Ed.).	Riziková budoucnost: Devět scénářů vývoje české společnosti	Vydavatelství MATFYZPRESS	2010
BALABÁN, M., RAŠEK, A.	Nezápadní aktéři světové bezpečnosti	Nakladatelství Karolinum	2010
POTŮČEK, Martin	Poznávání budoucnosti jako výzva	Nakladatelství Karolinum	2011
POTŮČEK, Martin	Cesty z krize	Praha, Sociologické nakladatelství	2011
BALABÁN, M., LUDVÍK, J., STEJSKAL, L. (ed.)	Strategické trendy globálního vývoje	Fakulta sociálních věd Univerzity Karlovy	2012
BALABÁN, M., KAŠÍK, J. RAŠEK, A., STEJSKAL, L.	Tři scénáře o budoucnosti světa, EU, ČR	Výzkumný záměr FSV UK „Rozvoj České společnosti v EU: výzvy a rizika“	2012
RAŠEK, Antonín	Budoucnost bezpečnostního systému ČR	Vojenské rozhledy, Praha: MO ČR - AVIS	2013
KUBEŠA, Milan	Evropská armáda – utopie nebo reálná budoucnost?.....aneb společné ozbrojené síly EU „jinak"	Vojenské rozhledy, Praha: MO ČR - AVIS	2013
BALABÁN, Miloš	Bezpečnostní systém ČR: Problémy a výzvy	Nakladatelství Karolinum	2015
BALABÁN, Miloš	The Limits, Dilemmas and Challenges of European Security in Uncertain Times	CEJISS, Metropolitní univerzita Praha	2016
Procházka Josef, Dyčka Lukáš	Česká obranná politika – kritické hodnocení a doporučení	Vojenské rozhledy	2017
Sommer, Jiří	Předpoklady příští války	Vojenské rozhledy	2017
Kolín, Vilém	Česká republika a „nová“ Společná bezpečností a obranná politika EU: Čas zásadních rozhodnutí	Vojenské rozhledy	2017
Vláda ČR	Strategický rámec - Česká republika 2030	Odbor pro udržitelný rozvoj	2017

Tab. 1 Výběr prognostických publikací České republiky

ZÁVĚR

Vývoj novodobé prognostiky spadá do začátku 40. let minulého století, kdy americký politolog a futurolog Karl Ossip Flechtheim (1909 - 1998) poprvé definoval pojem futurologie a navrhl základní charakteristiku a koncept futurologie jako nového vědního oboru. Období po skončení 2. světové války se vyznačovalo především zájmem o predikci možného vývoje v oblasti vojenství (vývoj ozbrojených sil, politická situace, vedení vojenských operací, možné aplikace nových technologií atd.). Tyto prognostické zájmy resp. potřeby států a aliancí se vývojem prognostiky prolínají trvale. V současné době jsou prognózy ve vojenství využívány mimo jiné např. v rámci výstavby ozbrojených sil, kdy bývá aplikován koncept plánování podle scénářů (scenario based planning, SBP).

Poměrně velký nárůst zájmu o prognostiku představovala 60. léta minulého století. V tehdejší ČSSR byla v r. 1968 založena Futurologická společnost. V 70. a 80. letech se prognostikou zabývalo Oddělení komplexního modelování, (působící v rámci agentury Technosport a Sportpropag). V roce 1984 byl založen Prognostický ústav ČSAV. Odbornou komunitu v dané oblasti reprezentovali např. Miloš Zeman, Jiří Kabele, Martin Potůček, Pavel Machonin, Fedor Gál, Bohuslav Blažek, Jan Hutař, Dagmar Harmacová, Miloš Bárta, Josef Alan, Miroslav Flek, František Petrášek a jiní.

Po roce 1989 zájem o tvorbu a využití prognóz upadá a po zrušení Federálního ministerstva pro strategické plánování (1992) již neexistuje v ČR v rámci státní správy žádný orgán, který by zastřešoval a koordinoval postupy více resortů, podílejících se na fungování českého bezpečnostního systému.

Mezi významná pracoviště v oblasti bezpečnostní prognostiky patřil především Ústav strategických studií (Brno, 1999-2008). V současnosti to jsou např. Středisko bezpečnostní politiky (FSV UK) nebo Centrum bezpečnostních a vojensko-strategických studií (Univerzita obrany).

Literatura

[1] POTŮČEK, M. Poznávání budoucnosti jako výzva. Praha: Univerzita Karlova v Praze, Nakladatelství Karolinum, 2011. 154 s. ISBN 978-80-246-1897-5.

[2] VYSTOUPIL, Jiří. Prognózy a modely v regionálním rozvoji. [Pracovní texty] Brno: ESF MU, 2003. 120 s.

[3] HENDRYCH, Stanislav. Pojednání o futurologii. [online]. c. 2008. [cit. 2018-08-23]. Dostupné z < http://www.hendrychst.cz/pojednani.php>.

[4] ZEMAN, Miloš. Futurologie a filosofie. In Filosofický časopis 4/1969. Praha: Filosofický ústav Akademie věd AV ČR, 1969. s. 522- 532. ISSN 0015-1831.

[5] PERNICA, Bohuslav. Rozpočtová politika české vlády ve věcech vnitřní a vnější bezpečnosti po roce 1998. In Vojenské rozhledy 3/2011. Praha: MO ČR, 2011. s. 66 - 75. ISSN 1210-3292.

[6] Rada vlády pro udržitelný rozvoj. Vláda české republiky. [online]. c. 2018. [cit. 2018-08-24]. Dostupné z < http://www.vlada.cz//>.

[7] Prognostický ústav Slovenskej akadémie vied [online]. c. 2018. [cit. 2018-08-24]. Dostupné z < http://www.prog.sav.sk/>.

[8] Občanská futurologická společnost. [online]. c. 2017. [cit. 2018-08-24]. Dostupné z < http://obcanska.futurologicka.spolecnost.sweb.cz/>.

[9] Centrum pro sociální a ekonomické strategie. [online]. c. 2018. [cit. 2018-08-20]. Dostupné z < http://ceses.cuni.cz/CESES-1.html >.

[10] Středisko bezpečnostní politiky. [online]. c. 2018. [cit. 2018-08-20]. Dostupné z < http://sbp.fsv.cuni.cz/SBP-41.html>.

[11] ŠTEDROŇ, B, POTŮČEK, M., KNÁPEK, M., MAZOUCH, P. a kol. Prognostické metody a jejich aplikace. Praha: C.H. Beck 2012. ISBN 978-80-7179-174-4.

POUŽITÍ NOVÉ METODIKY A METOD VÝCVIKU V PROFESNÍ PŘÍPRAVĚ OZBROJENÝCH SLOŽEK ČR PŘI VÝCVIKU VE STŘELBĚ MŮŽE PŘINÁŠET I SNÍŽENÍ EKONOMICKÝCH NÁKLADŮ VÝCVIKU

USING THE NEW METHODOLOGY AND METHODS OF TRAINING IN THE PROFESSIONAL PREPARATION OF CZECH ARMED FORCES IN THE FIELD OF TRAINING SHOOTING CAN PROVIDE THE REDUCTION OF ECONOMIC COSTS FOR TRAINING

pplk. Mgr. Jan Vaňo [1], pplk. Mgr. Vít Svěrák [2], kpt. Mgr. Miroslav Rouč [3], plk. v.v. PaedDr. Ing. Jan Zelinka, PhD [4]

[1]Vedoucí katedry profesní přípravy FBP PA ČR
Praha, Lhotecká 559/7, Praha 4, 143 00,
vano@polac.cz,

[2]Ajemník katedry profesní přípravy FBP PA ČR
Praha, Lhotecká 559/7, Praha 4, 143 00,
sverak@polac.cz

[3]Střelecký instruktor katedry profesní přípravy FBP PA ČR,
Lhotecká 559/7, Praha 4, 143 00,
rouc@polac.cz

[4]Odborný asistent katedry profesní přípravy FBP PA ČR,
Lhotecká 559/7, Praha 4, 143 00,
zelinka@polac.cz

ANOTACE:

Autoři uvedené úvahy předkládají návrh na modernizaci metodiky střelecké přípravy v ozbrojených sborech České republiky s využitím nových metod, které kromě úspěšnosti ve výcviku a v jeho usnadnění, mohou přinést i snížení ekonomických nákladů na takový výcvik.

KLÍČOVÁ SLOVA:

Střelecký výcvik, metodika výcviku, střelecké dovednosti, ekonomické náklady, ozbrojené sbory ČR

ANNOTATION:

The authors put forward a proposal to modernize the shooting training methodology in the Czech Republic's armed corps using new methods, which, in addition to their success in training and their facilitation, can also reduce the economic costs of such training.

KEYWORDS:

Shooting training, training methodology, shooting skills, economic costs, armed forces of the Czech Republic

ÚVODEM:

Střelecká příprava a výcvik k použití služební zbraně je nedílnou součástí profesní přípravy všech ozbrojených složek. Profesní příprava řeší konkrétní způsoby řešení krizových a mimořádných událostí příslušnými složkami v daném místě. Vzhledem k stávajícím

bezpečnostním rizikům kvalita a intenzita tohoto výcviku, zejména střelecké přípravy, nabývá v rámci profesní přípravy na aktuálnosti.

Střelecká příprava a výcvik k použití zbraně v podmínkách ozbrojených bezpečnostních sborů je záležitostí zcela specifickou. Ve většině případů k základnímu výcviku nastupují nestřelci – tedy osoby, které nemají znalosti o konstrukci a mechanice zbraní a zpravidla ani elementární střelecké dovednosti.

Cílem střelecké přípravy v podmínkách ozbrojených složek přitom není jen ovládání zbraně na elementární úrovni, dostačující např. k získání zbrojního průkazu (tedy mířená střelba v nerušeném prostředí s dostatečnou časovou dotací), nýbrž zvládnutí bojové střelby – tedy schopnost okamžitě reagovat zbraní na vnější podněty v podmínkách často výrazně ztížených (snížená viditelnost, nepřehledný prostor, ozbrojený pachatel, nezúčastněné osoby).

Má-li být příslušník ozbrojeného bezpečnostního sboru schopen adekvátně použít služební zbraň v podmínkách, kombinujících často i více stresorů, je nutno výcvik směřovat k vytvoření psychomotorických dovedností na bázi automatismů.

Takovéto úrovně lze dosáhnout pouze intenzivním výcvikem, kontinuálně zdokonalujícím komplexní spektrum střeleckých dovedností.

Zásadním problémem se ve výcviku tohoto typu jeví primárně faktory časové a ekonomické náročnosti, jako problém sekundární pak problém adekvátních výcvikových prostor (střelnice).

Pracovníci Katedry profesní přípravy Policejní akademie ČR v Praze dlouhodobě pracují na koncepci modulu střelecké přípravy, který by byl s minimálními úpravami aplikovatelný pro většinu vzdělávacích středisek ozbrojených bezpečnostních sborů, s cílem minimalizace dopadů již uvedených problémů.

1. MODUL STŘELECKÉ PŘÍPRAVY

Na tvořený modul byla aplikována následující kritéria primární a sekundární:

1.1 Primární kritéria

1.1.1 Minimalizace finančních nákladů při zachování efektivity výcviku

Finanční úspory cestou např. snížení střelecké dotace nelze akceptovat, je žádoucí nalézt způsob, jak náklady snížit při zachování, ideálně navýšení dotací reálné střelby. Cílem tohoto kritéria je předejít kontraproduktivním metodám typu úspor formou finančních škrtů na úkor rozsahu vlastního výcviku. Primárním požadavkem je snížení nákladů bez negativních sekundárních dopadů.

1.1.2 Materiální dostupnost

Nebudou používány obtížně dostupné či na zakázku vyrobené pomůcky či prototypy. Za ideální stav je považováno využívání standardního materiálu obchodně běžně dostupného. Cílem tohoto kritéria je eliminovat komplikace při získávání technických prostředků, minimalizovat obtíže se servisem a obnovitelností opotřebovaných komponentů, včetně zajištění případného servisu.

1.1.3 Snížení nároků na speciální pracoviště

Část praktického výcviku koncipovat tak, aby mohla být realizována bez nároků na specializovaná pracoviště (střelnice). Mnoho útvarů, jejichž příslušníci mají řízený střelecký výcvik, nedisponuje certifikovanými střelnicemi, na nichž lze tento výcvik provádět. Z tohoto důvodu jsou při výcviku na střelnice dojíždět.

To s sebou nutně nese jak další náklady finanční (dopravní prostředky, pohonné hmoty případně pronájmy střelnic), tak časová omezení (doba přesunu na střelnici nemůže být nijak efektivně využita, z hlediska výcviku je „ztrátová“).

1.2 Sekundární kritéria

1.2.1 Minimalizace vstupních investic a jejich rychlá návratnost

Vzhledem ke skutečnosti, že většina ozbrojených bezpečnostních sborů funguje jako rozpočtové organizace, je žádoucí, aby vynaložené náklady zatěžovaly rozpočet pro daný výcvikový rok co nejméně, nejlépe jednorázově a jejich návratnost byla co nejrychlejší, tak, aby se úspornost systému začala projevovat v co nejkratším časovém horizontu.

1.2.2 Zvýšení bezpečnosti výcviku

Manipulace se střelnou zbraní a ostrá střelba může v začátečnících vyvolávat nežádoucí emoční stavy (stres, nejistota, problémy s koncentrací apod.), v jejichž důsledku může dojít během činnosti se zbraní k nesprávné manipulaci, nechtěnému výstřelu a případnému zranění či usmrcení osoby. Těmto situacím lze částečně předejít důslednou organizací a dodržováním zásad bezpečnosti, nicméně stoprocentní predikce selhání lidského faktoru v tomto případě nelze dosáhnout. Je tudíž nejvýše žádoucí využití technických pomůcek a pedagogických metod, napomáhajících v úvodní části výcviku, kdy se u cvičících vytváří mechanický stereotyp, k potlačení stresorů, což jednak tuto fázi výcviku urychlí, jednak výrazně přispěje k prevenci rizikových situací.

1.2.3 Univerzálnost

Jakkoliv bude koncepce směřovat primárně k základnímu střeleckému výcviku Policie ČR, je žádoucí, aby vzniklý modul byl aplikovatelný i u dalších bezpečnostních sborů, jak již bylo výše předznamenáno. Vlastní koncepce pak má směřovat k základnímu výcviku (tedy k výcviku policistů rámci Základní odborné přípravy, obdobně i u dalších sborů), případně k dalšímu výcviku policistů základních útvarů apod.

2. PRAKTICKÉ ŘEŠENÍ FINANČNÍ ÚSPORY

Při výpočtu reálných nákladů, investic, jejich návratnosti a následných úspor bylo vycházeno z následujících údajů:

Výuka střelecké přípravy na PA ČR

- 4 skupiny po 20 studentech – **celkem studentů 80**
- délka výuky **- 12 týdnů výuky**

Průměrná spotřeba střeliva na jednoho studenta:

- **25 ks nábojů/1 střelby** 80 x 25 = **2000 výstřelů na 1 týden výuky**

- **Celkem** - 2 000 x 12 = **24 000 výstřelů za semestr**

Finanční hodnota při použití střeliva 9 mm Luger, cena 5,- Kč náboj, činí

24 000 x 5 = **120.000 Kč za semestr**

3. ZAKOUPENÉ VYBAVENÍ

- 6 ks vzduchová replika služební zbraně CZ 75 D Compact – pořizovací cena cca 1.900,- Kč/ks – celková částka **11.400,- Kč**
- 6 ks adaptér Kadet na CZ 75 D – pořizovací cena 11.990,- Kč – celková částka **71.940,- Kč**

Výsledná investice – 83.340,- Kč

4. REÁLNÁ ÚSPORA

Vzduchová replika služební zbraně CZ 75 D Compact je identická se služební pistolí policistů, včetně rozměrů a ovládacích prvků, zacházení s touto zbraní je totožné jako se služební zbraní, střílí ocelovými broky, hnacím médiem je CO2 v bombičce. Pořizovací cena 1 500 ks broků je cca 105,- Kč jeden náboj vychází cca na 0.07 Kč. 1 ks bombičky cca 13 Kč – jedna bombička je na 60 výstřelů

Náklady na jeden výstřel činí cca 0.30,- Kč

Adaptér Kadet na CZ 75 D. Aplikace adaptéru do zbraně CZ 75 D Compact (jednoduchá vratná montáž), umožňuje použití střeliva 22 LR (5,6 mm).

Pořizovací cena náboje a **náklady na jeden výstřel činí 1,- Kč.**

Finanční náklady na 1 výcvikový blok počet výstřelů x cena 1 výstřel

Služební zbraň CZ 75 D Compact - použití ostrého střeliva 9 mm Lugger,

Pořizovací cena a finanční náklady na jeden výstřel 5,- Kč

4.1 Shrnutí:

- služební zbraň CZ 75 D Compact - **2000 x 5 = 10.000, -Kč**
- zbraň CZ 75 D Compact s Adaptérem Kadet - **2000 x 1 = 2.000,- Kč**
- vzduchová pistole CZ 75 D Compact - **2000 x 0,30 = 600,- Kč**

Za předpokladu rozdělení 12týdenního výcvikového cyklu na třetiny, kdy 4 výcvikové bloky bude využívána vzduchová replika služební zbraně CZ 75 D Compact, 4 výcvikové bloky zbraň s Adaptérem Kadet a 4 výcvikové bloky služební zbraň CZ 75 D Compact dojdeme k následné úspoře:

- 4 x 600 = 2.400,- Kč
- 4 x 2.000 = 8.000,- Kč
- 4 x 10.000 = 40.000,- Kč

Celkem 50.400,- Kč

Při vedení výcviku pouze služební zbraní CZ 75 D Compact činí náklady na střelivo za semestr, jak již bylo uvedeno **120.000,- Kč**

Úspora tedy činí 120000–**50400 = 69.600 Kč, - za 1 semestr výuky**, při jednorázové vstupní investici 83.**340,- Kč.**

5. SPLNĚNÍ STANOVENÝCH KRITÉRIÍ

Jak vyplývá z výše uvedeného, kritéria uvedená v úvodu statě se podařilo zcela jednoznačně splnit.

Vycházíme-li z rozdílu nákladů při použití jednotlivých zbraní, uvedený systém bude (ve srovnání s výcvikem vedeným pouze služební zbraní CZ 75 D Compact) i při navýšení střelecké dotace stále vykazovat úspory v řádech desítek tisíc Kč za semestr. Vložené náklady jsou jednorázové, s návratností během necelých dvou semestrů, tedy jednoho kalendářního roku.

Použité vzduchové zbraně i adaptéry jsou standardně dostupné v maloobchodní nebo velkoobchodní síti, s bezproblémovým servisem. Vzduchová replika pistole CZ 75 D Compact je zbraní kategorie D, nácvik střelby z této zbraně tudíž nemusí být prováděn na certifikované střelnici. V podmínkách útvarů ozbrojených složek stačí jakýkoliv bezpečný prostor (tělocvična, nevyužívané místnosti typu suterénů, skladovacích prostor apod.).

Při výuce na střelecké přípravy Policejní akademie ČR v Praze je její využití výhodné zejména na Letním výcvikovém kurzu na Přední Labské. Hlavní výhodou je skutečnost, že odpadají náklady na dojíždění a úhradu střelnice. Mobilní střelnici si postavíme na bezpečném místě v dosahu našeho zázemí. Dále můžeme realizovat střelecké cvičení v terénu (kros) a zapojit do cvičení i fyzickou zátěž a narušit střelci i psychickou pohodu. Zbraň lze použít i k simulovanému vyhledávání a zajišťování pachatele, je totiž plně kompatibilní se služebním pouzdrem.

6. VÝHODY MODULU V RÁMCI PRIMÁRNÍHO VÝCVIKU – STŘELECKÁ PŘÍPRAVA NA PA ČR

V prvním semestru převažuje teoretická výuka, která je proložena laserovou střelnicí. Student se dozví základní informace ohledně střeliva, zbraní, balistiky, činnosti na střelnici atd. Na laserové střelnici se učí získat základní návyky v držení zbraně, postoji, dýchání, míření a spouštění. Dalším krokem na laserové střelnici je rychlé vyhodnocení střelecké situace a přenášení záměrného bodu. Na studenta se nahlíží jako by byl na ostré střelnici a tím směrem je také vedena výuka. V rámci semestru student píše 2 postupové testy z problematiky historie zbraní a konstrukce zbraní, konstrukce střeliva a balistika. Semestr se zakončuje písemným testem z celé probrané látky.

Druhý semestr student absolvoval již na ostré střelnici PA se zbraní CZ 75 v provedení s malorážkovou hlavní (ráže 22LR). Hlavní náplň tvoří zacházení se zbraní, nabíjení a střelba na stanovený cíl ze vzdálenosti 10–15 metrů, za současného zvládání povelové techniky a stálého zdokonalování se v držení zbraně. Semestr se zakončuje zápočtem, kde hodnotíme činnost střelce na palebné čáře a úspěšnost zásahů v terči, kde musí střelec dosáhnout minimálně 80 bodů ze 100 na vzdálenost 15 metrů do pistolového terče (50/20).

Cílem střeleckého výcviku příslušníků bezpečnostních sborů je však dosáhnout střelecké připravenosti zejména v oblasti tzv. combat střelby – tedy střelby instinktivní, pudové, vedené na relativně blízké cíle (2,0 – 7,0m), avšak v intenzivním stresu a v minimálním časovém úseku – tedy střelba probíhá prakticky bez míření.

Dalším požadavkem je osvojení si schopnosti okamžitého tasení zbraně a rychlého nabití s případnou následnou střelbou. V obou je pro úspěšné zasažení cíle zásadní tzv. „nahmátnutí“ zbraně. Jedná se o pevný, střelecky správný úchop, při kterém je osa zbraně v přímém prodloužení ruky. Pouze bezpečné zvládnutí tohoto úchopu umožňuje vést spolehlivě střelbu bez možnosti přesného zacílení pomocí mířidel.

Jakkoliv se tato motorická dovednost jeví jako jednoduchá, přesto její zvládnutí v praxi zpravidla představuje zásadní problém. Vlastní úchop i držení musí být vyprecizováno k maximální přesnosti. Rovněž promáčknutí spouště musí být plynulé, bez nežádoucích doprovodných pohybů zápěstí. Již odchylky v řádu milimetrů výrazně ovlivňují přesnost zásahu.

Tato úvodní část střeleckého výcviku je v praxi zpravidla řešena tzv. „suchým nácvikem“, kdy začínající střelci nacvičují nahmátnutí a úchop, případně nabití (natažení závěru zbraně) s následným promáčknutím spouště bez munice. Přes svou prokazatelnou účinnost není tzv. suchý nácvik u začínajících střelců příliš oblíben, a to proto, že má monotónní, dosti stereotypní průběh. Dalším jeho negativem je z pohledu nacvičujících začátečníků, absence zpětné vazby – kontroly, zda v tomto případě pouze hypotetické výstřely zasahují cíl. Zkušený instruktor střelby je schopen z pohledu na nacvičujícího, vyhodnocení jeho postoje, držení zbraně a plynulosti spouštění vyhodnotit přesnost zásahu v případě ostré střelby, avšak sám začínající střelec nikoliv. Pro některé jedince může být tudíž takovýto nácvik výrazně demotivující.

Jako další problém začínajících střelců se jeví až přehnaný respekt ze zbraně, projevující se zejména celkovou tenzí, sklonem k nesoustředěnosti či přehnané opatrnosti, která je paradoxně příčinou chybné manipulace se zbraní, což může mít během výcviku s ostrou municí fatální následky.

Využití vzduchové repliky zbraně CZ 75 D Compact uvedené problémy do značné míry eliminuje. Jak již bylo předznamenáno, zbraň, včetně ovládacích prvků, je identická se standardní služební zbraní. Vzhledem k výši nákladů na střelivo umožňuje intenzivní výcvik, sám střelec má možnost vyhodnocovat si úspěšnost zásahů, individuální kvalitativní posun či stagnace jsou jasně patrné. Vzhledem k účinnosti střeliva, kdy pravděpodobnost případného letálního zranění je minimální a zároveň odpadají vizuální a akustické projevy výstřelu (zášleh, hluk), dochází u cvičenců ke zklidnění, vyšší koncentraci na ovládnutí zbraně a tím i k výrazně vyšší kvalitě výcviku a rychlejší tvorbě žádoucích psychomotorických stereotypů.

Ve druhé fázi výcviku již je využívána služební pistole CZ 75 D Compact, avšak s adaptérem Kadet, umožňujícím střelbu nábojem 22 long rifle. V této fázi již během střelby dochází k vedlejším „efektům“ výstřelu, cvičenci je však vzhledem k předchozímu výcviku a bezpečné manipulaci se zbraní nevnímají jako zásadně rušivý prvek. Tato fáze výcviku je výrazně motivační – cvičenci již provádějí výcvik s reálnou zbraní, zpravidla dosahují solidních výsledků, upevňují si získané návyky a u většiny se projevuje zvýšený zájem o přechod na standardní ráži 9 mm Lugger.

ZÁVĚR

Z uvedené prezentace možností využití nových metod výcviku bezpečnostních sborů ve střeleckém výcviku formou navrhovaného modulu je očividné v tom, že kromě snadnějšího a efektivnějšího výcviku ve střelbě přináší tyto metody i značné ekonomické úspory v nákladech na výcvik, včetně nákladů na provoz střelnic, které tady nebyly sice vyčísleny, ale které by se díky tomu zkrátily (snížily) nejméně o jednu třetinu.

INTEGRATION OF EUROPEAN IT SECURITY ENSURING FEATURES TO RUSSIAN BUSINESS SYSTEM

Daria Vasilenko[1], Jakub Trojan[2], Peter Chrastina[3]
[1]Ufa State Aviation Technical University
Ul. K. Marxa 12, Ufa, 450008, The Republic of Bashkortostan, Volga Federal District, Russian Federation
vdaria96@mail.ru
[2]Faculy of Logistics and Crisis Management, Tomas Bata University
Studentské náměstí 1535, 686 01 Uherské Hradiště, Czech Republic
trojan@utb.cz
[3]Faculty of Arts, University of Ss. Cyril and Methodius in Trnava
Nám. J. Herdu 2, 917 01 Trnava, Slovak Republic
peter.chrastina@ucm.sk

ABSTRACT

Nowadays not every company's management department but even every usual man knows about priority meaning of security of his data and other computer files. Especially it is so relevant because there is the main power like knowledge in the modern world. If you have some information you can reach any goals, be a useful worker or a successful businessperson and whatever else. The main thing is having this information. Moreover, it cannot be such invaluable one without reliable protect of its confidentiality, integrity and availability. So, this work is devoted to considering of this highly important issue.

KEY WORDS

IT security, cyber-attacks, IT security breaches, antivirus software

INTRODUCTION

There is a quite wide list of diverse cyber-attacks and crimes in the world. Nowadays it becomes bigger and bigger every year. So that the question of ensuring of IT security in modern business system is so relevant [8]. For instance, in August 2010, the Privacy Rights Clearinghouse published its latest Chronology of Data Breaches, which showed that since 2005 more than a half-billion sensitive records have been breached. Of those breached records which contained such sensitive data as customer credit card or social security numbers approximately one-fifth came from retailers, merchants and other types of non-financial, non-insurance-related businesses, the majority of which were small to midsized [8].

An equally scary statistic: approximately 80 percent of small businesses that experience a data breach go bankrupt or suffer severe financial losses within two years of a security breach, according to John Sileo, a professional identity theft consultant and speaker, who knows first hand about the havoc a security breach can wreak on a small business [8]. As another example, in 2010, the international non-profit journalistic website Wikileaks began publishing a batch of leaked US diplomatic cables. The scale of the leak was unprecedented; over 260 million words of data was involved, and the publication created headlines across the world over successive weeks. This was the largest disclosure of classified government information in history. It was just the beginning of a new form of political activism reliant on our growing dependency on information technology and on the architecture and infrastructure of the information age [8]. Also in 2013, the computer professional Edward Snowdan leaked about 9000 documents originating from the US National Security Agency. The documents not only in themselves highlighted the vulnerability of digital information to disclosure but also

detailed the degree to which security agencies were engaged in systematic surveillance of digital communications globally [8].

As a result, each year, there are countless cases of extortion and blackmail based on data breaches, many of which go unreported. Each case creates untold anxiety among the organizations' customer bases and did untold damage to the reputations of the organizations involved [8]. If the kinds of incidents described above seem to be becoming more and more common in the 21st century, which is because they are. They testify to a fundamental change in the global information and communications infrastructure. Information itself has become integral to every part of our lives. Individuals, business and governments now generate vastly more information each day than even in the relatively recent past. All commercial operations are now to some degree in the business of managing, manipulating and selling information in one form or another. In a very real sense, information is value in the digital economy. However, information has also become a kind of currency; we exchange information about our interests and identity in order to access services online. If information has greater value, then it becomes more susceptible to criminal or political intervention [8].

While it has become over recent years a matter of widespread public concern and media interest, the problem of information security has been with us for over 30 years, and growing steadily throughout that time [2]. Summing up, one thing is clear: without IT security companies soon run into existential problems. Hundreds of thousands of new viruses, worms and Trojans are created every day. It is common knowledge that the attackers are becoming increasingly professional and their methods increasingly sophisticated. At the same time, the potential targets for attacks are increasing as well: the number of machines, systems, devices and products with Internet access is rising fast. As is the use of mobile devices. In the future companies will have to do more to protect their data and networks [9].

1. THE MAIN CAUSES OF CYBER ATTACKS

According to the Privacy Rights Clearinghouse (and other sources), security breaches typically result from one of the following seven causes.

1. Unintended Disclosure: Someone in or affiliated with your organization inadvertently posts private or sensitive company or customer information on a website (e.g., Facebook or a blog) or in an email, fax or letter.
2. Hacking or Malware: Unauthorized individuals gain access to your computers or servers (often due to inadequate firewalls or weak passwords) and steal or corrupt data by using malicious software programs known as malware.
3. Payment Card Fraud: Information is stolen from a point-of-service credit card or payment terminal.
4. Bad Employees: Someone who works for you intentionally steals or leaks sensitive information.
5. Lost, Discarded or Stolen Paper Documents.
6. Lost, Discarded, or Stolen Mobile Devices (e.g., laptops, smart phones, flash drives, CDs, etc.).
7. Stolen Computers or Servers [8].

Obviously, almost without exception, the real information security weak-spots in any system or process are not technological vulnerabilities but human operators. Humans have a habit of behaving in unpredictable and sometimes inexplicable ways. Hackers have a name for

exploiting the human problem in information security. It is called social engineering. Social engineering is the process of tricking someone into disclosing passwords, access details or confidential information often by masquerading as someone who is or should be entitled to access [2]. The fact that humans are the real weak spot in many information security processes highlights that information security should not be considered primarily as a technological issue. The technology has altered the scale and intensity of communication and information practices, but the underlying principles of human socialization remain the same. Information security is at its heart a problem with people, and their messy, unpredictable, organic nature. The way to address information security is to understand how information slots into the work processes within an organization, and where the vulnerabilities lie [2].

2. SELECTED STATISTICS ABOUT CYBER ATTACKS IN EUROPE AND IN THE WORLD

It is necessary to explore some statistics information to realize indeed the great point of the high importance of ensuring Information security in both contemporary business world and private people life. The statistic shows the amount of damages caused by cyber-crime reported to the IC3 from 2001 to 2016. In the last reported period, the annual loss of complaints referred to the IC3 amounted to 1.33 billion U.S. dollars, up from 781.84 million U.S. dollars in 2013. The most costly cyber-attack consequences for global companies in 2016 were losses suffered through business disruption and information loss. That year, the majority of data breach incidents were related to identity theft, followed by financial and account access [12]. This statistic presents a selection of the biggest online data breaches worldwide as of October 2017, ranked by number of records stolen. In August 2016, a 2014 hack of online platform Yahoo was uncovered, affecting at least 500 million users' accounts. In December 2016, the company revealed another hack dating back to 2013, which affected 1 billion user records. The impact of the second reported Yahoo hack was updated in October 2017, when the company revealed that 3 billion accounts had been affected, making it the largest data breach in history. In 2011, Sony's PlayStation Network and Qriocity music service were attacked by hacking collective Lulzsec. The PSN was offline for more than 43 days and 77 million data records were stolen. With the increasing use of digital files and reliance on digital data by many corporations, data breaches have become common in the last decade or so. For example, the number of data breaches in the U.S. increased from 157 million in 2005 to 781 million in 2015, while the number of exposed records jumped from around 67 million to 169 million during the same period. The largest data breach of all time, as of September 2016, was an allegedly state-sponsored hack of Yahoo, which dates to late 2014 but it was only uncovered in 2016. The company advised all its users to change their passwords and take further measures to secure their accounts.

Identity theft is the most common type of data breach incident in the world. In 2015, identity theft accounted for more than 50 percent of all global data breaches, and about 40 percent of all compromised records that year. The services sector had the highest number of identities exposed that year – nearly 260 million. This figure accounted for just over 60 percent of all identities were exposed through data breaches in 2015. The financial sector is also highly affected by cyber-crimes. Financial access data theft is the second most common type of data breach, accounting for 22 percent of all data breaches. In 2015, this sector had 120 million identities exposed. The costs of cyber-crimes are rather high for the financial services sector. Global cyber-crimes caused, on average, a 13.5 million U.S. dollars annual loss for the financial services industry, the highest average amongst all industries [12].

Summing up, it is necessary to say that the global IT security statistics points to increasing of cybercrime all over the world. However, distribution of ransomware mainly detections in the United States (29%). Besides, number of ransomware attacks has grown 167 times since 2015 to 2016. That year amounts of monetary damage equalled 1,330 billions of US dollars. Yahoo - 3 billions of US dollars, made the most significant loss in the current 2017. It is not a secret youth and middle-aged men use the Internet a lot, that is why especially these people are the most exposed to be harmed by cyber-attacks (38% - 18-30 years old and 30% - 31-40 years old). It is noticed that the identification of vulnerabilities was the most pressure-filled security responsibility for IT security professionals. It is imperative to consider some capabilities for coping with this huge problem.

3. METHODS OF AVOIDING IT SECURITY BREACHES

There are some the simple and actionable ways to protect against data security threats, which could be used by giant corporations with hundreds of employees and small companies and individual business as well. Protecting business from a security breach is not just about practicing safe tech. It is about hiring the right people, having a good security policy in place and employing common sense. Overall, IT security needs to be ensured from end-to-end, involving not only the protection of data but also of communication channels.

The first thing is threat monitoring. We are currently working in the realm of the advanced persistent threat (APT) and until cyber criminals let up on their relentless attacks, chances are that your company is going to be a victim at some point. The best way to prevent this from occurring is to implement IT security automation into the monitoring process.

The second one is incident response. Today's technology facilitates the tracking of a security incident from beginning to end. This addresses both the need to quickly and effectively take action against said threat as well as the importance of documenting that incident process [10].

The third one is remediation and recovery. Modern IT security automation is designed to accommodate this reality by helping IT teams to identify and address successful incidents as quickly and effectively as possible [10].

4. THE MOST POPULAR IT SECURITY SOFTWARE IN EUROPE

Ensuring of Information Security can be provided with many diverse defences. However, the simplest and widespread way is antivirus software. World TOP antivirus software of 2017 is presented in the table 1.

Place	Name	Headquarters
1	Norton Security	Mountain View, California, U.S.
2	ESET	Bratislava, Slovakia
3	Kaspersky Lab	Moscow, Russia
4	Bitdefender	Bucharest, Romania
5	Panda Security	Bilbao and Madrid, Spain
6	Avast Software	Prague, Czech Republic
7	Max Secure Software	India

8	Trend Micro	Tokyo, Japan
9	Avira Operations GmbH & Co. KG	Tettnang, Germany
10	Bullguard	London, United Kingdom

Tab. 1 The most common and usable antivirus software of 2017 [11]

As we can see from the table 1, there is no one leading country producing application security. Within European countries, there are Czech Republic, Slovakia, Romania, Spain and Germany. According to some sources, the most popular antivirus software in Europe is Avast, ESET, Avira, Kaspersky, Panda and Trend Micro. European companies and usual users prefer European software.

5. FINDINGS AND RECOMMENDATIONS FOR RUSSIAN COMPANIES BASED ON EUROPEAN EXPERIENCE

The goal of a modern organization's security strategy is to create harmony between the security strategy, IT environment and business and operational priorities. This is difficult because the IT environment and the organization itself are constantly in the process of transformation; therefore, the organization's risk and security posture is also dynamic. Organizations can take proactive steps to operate more securely - for instance, taking measures to inventory the cloud applications that are in use, understanding how mobile devices (organization owned and personal) are used for professional interaction, assessing the security of devices that transmit information over the internet, and better managing the lifecycle of identities including the identities of third parties and the Internet of things devices.

A rapidly expanding and increasingly complex IT infrastructure cannot be secured purely through more technology. Organizations must drive success by including people and processes in their security strategy. In part, security teams should collaborate with operational leaders to identify the level of security various information assets require and integrate security into every phase of an organization's initiatives.

According to our filed research, there are some clear points of IT security philosophy appeared. First of all it should be known that ensuring of IT security in Russia and in the European countries is similar, but European one has a few important features that is absent in Russia. The basic distinction between them is a view on the causes of cyber-attacks. For example, as a rule, management department at Russian companies pays less attention to the stuff and work with them than European one. Usually there is no deep and painstaking activity to train employees, to teach them for correct using of corporate computer system and then to monitor their daily work. However, especially humans as a company's stuff are the foundation of any business system or activity. That is why HR-management has a paramount performance at every company and enterprise to minimize cyber-attack level and to increase the general capacity. Besides there are some other weaknesses of Russian IT security departments like poor or outdated company hardware and software infrastructure. Moreover, sometimes there could not be known some notable and simple tasks for protecting that are commonly used at European enterprises.

As a result of this entire research it is reasonable to notice that there are countless quantity of diverse software and recommendations how to protect corporate IT system, but the main and the first thing is realizing its significance by everyone at the company and taking personal responsibility for one's work. In addition, these simple rules should be applied both at Russian and European companies.

CONCLUSION

There were considered some of the important dimensions of IT security in this research. Especially high relevance and importance of ensuring IT security in modern business system, the main causes of cyber-attacks, statistics information about cyber-attacks and some methods of avoiding IT security breaches. We also discussed the most popular IT security software in Europe and we did a few recommendations for Russian companies based on European experience.

In summary, modern organizations must understand security risk in the context of impact to operations. With a business-driven security strategy, organizations can connect security risk to business risk that is contextual and specific to the organization. Modern organizations can achieve consistently high levels of organizational efficiency and security even as their attack surfaces continue to expand with every added device, identity and system.

ACKNOWLEDGEMENT

We would like to express our very great appreciation for various IT security experts for their valuable and constructive suggestions during the planning and development of this research work. Their willingness to give their time so generously has been very much appreciated.

References

[1] O. M. Fal' «Standardization in Information Technology Security», Cybernetics and Systems Analysis. January 2017, Volume 53, Issue 1, pp 78–82.

[2] Claire Laybats, Luke Tredinnick «Information security», Business Information Review, volume 33 issue 2 (31 May 2016), pages 76-80.

[3] Mark Stamp «Information Security: Principles and Practice» (2nd Edition), Hoboken, N.J: Wiley, 2011.

[4] Atif Ahmad; Sean Maynard «Information Management & Computer Security», Information Management & Computer Security, volume 22 issue 5 (10 November 2014), pages 513-536.

[5] Nadinia A Davis ; Melissa LaCour « Foundations of Health Information Management », St. Louis: Elsevier, 2017.

[6] Nir Kshetri «Cybercrime and Cybersecurity Issues in the BRICS Economies», Journal of Global Information Technology Management, volume 18 issue 4 (2 October 2015), pages 245-249.

[7] «The Cost of Cybercrime», Network Security, volume 2015 issue 10 (30 September 2015), page 2.

[8] Jennifer Schiff «15 Data Security Tips to Protect Your Small Business», 2010, Small Business [Web source], URL: https://www.smallbusinesscomputing.com.

[9] «Targeted cyber attack prevention with IT security» T-Systems [Web source], URL: https://www.t-systems.com.

[10] «Three Critical Elements of Modern IT Security Automation», 2016, Ayehu [Web source], URL: https://ayehu.com.

[11] «Top 10 Best Antivirus Software of 2017» [Web source], URL: https://www.top10antiviruslist.com.

[12] Cyberbullying Research Center, United States, 2016 [Web source], URL: https://www.statista.com.

[13] Josh Abraham, Practice Manager, Praetorian «How to Dramatically Improve Corporate IT Security without Spending Millions».

TRESTNĚPRÁVNÍ ASPEKTY KYBERKRIMINALITY A PREDIKCE JEJÍHO VÝVOJE

CRIMINAL LAW ASPECTS OF CYBER CRIMINALITY AND PREDICTION OF ITS DEVELOPMENT

JUDr. Radomíra Veselá, PhD. [1], doc. Pavel Kovařík, CSc. [2]
[1]Odborná asistentka Fakulty logistiky a krizového řízení
Univerzity Tomáše Bati ve Zlíně
rvesela@utb.cz

[2]Odborný asistent EPI s.r.o. Kunovice
PavelKovarik@seznam.cz

ABSTRAKT

Cílem příspěvku je charakterizovat kybernetickou kriminalitu, provést její kategorizaci, rozebrat právní úpravu kybernetické kriminality na úrovni mezinárodní, unijní i republikové. Dále se příspěvek zabývá opatřeními, která směřují k prevenci kybernetické trestné činnosti a na základě četnosti nápadu této trestné činnosti v letech 2011 – 2017 byla provedena predikce vývoje kybernetické kriminality na léta 2018 a 2019.

KLÍČOVÁ SLOVA

Kybernetická kriminalita, kyberprostor, počítač, počítačová kriminalita, trestní zákoník, trestný čin, prevence, kybernetická bezpečnost, kriminalita

ABSTRACT

The aim of the paper is to characterize cybercrime, to categorize it, to break the cybercrime legislation at international, EU and republic level. Furthermore, the contribution deals with measures aimed at the prevention of cybercrime and on the basis of the frequency of the idea of this crime between 2011 and 2017 an estimate of cybercrime development was made for the years 2018 and 2019.

KEY WORDS

Cybercrime, cyberspace, computer, komputer crime, criminal code, crime, prevention, victim of cybercrime, kriminality

ÚVOD

Kriminalita patří k nejzávažnějším negativním společenským jevům, a proto je zapotřebí kriminalitě předcházet. Kriminalita se přizpůsobuje vývoji společnosti. S příchodem globalizace se sbližují nejen životní podmínky lidí přes hranice různých států, ale dochází i k internacionalizaci kriminality.

Nejdynamičtěji se rozvíjející kriminalitou je **kybernetická trestná činnost**. Je typickou trestnou činností, u níž dochází k potírání geografických a státně teritoriálních omezení.

1. CHARAKTERISTIKA KYBERKRIMINALITY

Kybernetická kriminalita nebo také kyberkriminalita je relativně nový interdisciplinární obor (v porovnání s obory jinými), zabývající se nelegálními a škodlivými aktivitami v kyberprostoru, které jsou založeny na použití nebo zneužití počítačové technologie.

Pojem kyberkriminalita nahradil dříve používané pojmy jako počítačová kriminalita nebo kriminalita v informační vědě. Počítačová kriminalita byla nejčastěji charakterizována jako „*páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení data nevyjímaje, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako movité věci, nebo jako nástroj trestné činnosti.“*[1]

V USA byl první počítačový trestný čin zaznamenán již v roce 1958[2], ale samotný pojem „počítačová kriminalita“ („computer crime“) se jako obecně přijímaný pojem objevuje v právní a kriminologické terminologii vyspělých zemí až v sedmdesátých letech. Tehdy se odehrál i první čistě počítačový zločin v ČR, který spočíval v tom, že nespokojený pracovník Úřadu důchodového zabezpečení poškozoval magnetem záznamy na magnetických páskách.[3]

Vývoj kybernetické kriminality lze rozdělit na následující etapy:

1. Etapa sólových, nedostupných počítačů.
2. Etapa nástupu osobních počítačů.
3. Etapa propojování počítačů do sítě.[4]

Kybernetická kriminalita je obvykle charakterizován jako souhrn takových trestných činů, které jsou páchány v kyberprostoru. „*Těžištěm útoku již není počítač, ale kyberprostor tvořený počítačovými sítěmi a jejich jednotlivými prvky, ve kterém spolu komunikují veškerá zařízení ovládající protokol TCP/IP“*.[5]

V současné době nemá kybernetická kriminalita žádný oficiálně definovaný obsah. **Jednotná definice neexistuje v teorii ani legislativě.**

Dle dostupné odborné literatury jde v případě kybernetické kriminality, o taková kriminální jednání, při nichž bylo užito výpočetní techniky, informačních či komunikačních systémů:

a) jako předmět této trestné činnosti, tzn. cíl útoku pachatele, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité anebo
b) jako nástroj ke spáchání trestného činu.[6]

---

[1] SMEJKAL, V. a kol. *Počítačové právo*. Praha: C.H.Beck,1995, 264 s. ISBN: 80-7049-101-9. s. 99.

[2] VLČEK, M. *Počítače a kriminalita (trestněprávní a kriminologické aspekty*), Praha, Academia, 1989, ISBN 8020001395.

[3] Viz SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. ISBN 978-80-7380-501-2. s. 73.

[4] Viz SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. ISBN 978-80-7380-501-2. s. 74-75.

[5] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. ISBN 978-80-7380-501-2. s. 15.

[6] SMEJKAL, V. a kol. *Počítačové právo*. Praha: C.H.Beck,1995, 264 s. ISBN: 80-7049-101-9. s. 220.

Pojem kybernetické kriminality tedy nestaví do centra pozornosti počítač, nýbrž klade důraz na využívání komunikačních a informačních technologií a především na virtuální prostor, tedy kyberprostor, v jehož rámci se delikt uskutečňuje. Odráží tak technologický vývoj počítačových systémů a jejich funkcí. Z uvedeného je tedy zřejmé, že **těžištěm útoku** již není počítač, ale **kyberprostor.**

Kybernetický prostor pak věcný záměr zákona o kybernetické bezpečnosti vykládá jako *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními a komunikačními technologiemi, zahrnující připojení k veřejné síti (internet)“*[7]

Kyberprostor tedy vzniká díky počítačovým systémům. Bez počítačů není ani kyberprostoru. Z tohoto úhlu pohledu bude v kybernetické kriminalitě vždy figurovat i počítač a každý případ kybernetické kriminality lze tedy označit i za počítačovou kriminalitu. Dalšími stavebními kameny kyberkriminality jsou kromě počítačů, informace a sítě. Takový přístup k definování kybernetických trestných činů nebude do budoucna udržitelný. S dalším rozvojem počítačových technologií se jejich využívání v každodenním životě natolik rozšíří, že bude možné podřadit pod takto široce pojatou definici kyberkriminality téměř vše. Tím okamžikem však uvedená definice ztratí svůj význam.

Dalším nedostatkem výše uvedené definice kyberkriminality je její navázání na výskyt počítače ve formě nástroje. Pak by každý trestný čin, v jehož rámci je počítač nějakým způsobem využit jako nástroj, bylo možné považovat za projev kyberkriminality, a tím by se pod kyberkriminalitu dostala obsáhlá množina trestných činů. Navíc není zvykem v právní teorii specifikovat kategorii trestných činů podle použitých prostředků.

Kyberkriminalitu definují tři hlavní novinky:

1. uskutečňuje se v novém „virtuálním“ prostoru,
2. obsahuje nová deviantní chování (podle eliminačního testu je „pravou“ kyberkriminalitou taková kriminalita, která by neexistovala bez internetu),
3. novinky v trestněprávních reakcích.[8]

Mezi další nejvýraznější **specifika kyberkriminality**[9] patří:

1. anonymita - znamená, že pachatel kyberkriminality se nemusí do kontaktu s obětí dostat, protože může trestnou činnost páchat z pohodlí domova. Každá interakce však zanechává v prostředí tzv. digitální stopu, a tudíž se jedná o znak zdánlivý.
2. globálnost neboli dosažitelnost - znamená, že internet je celosvětovou sítí, a tudíž interakce mají mezinárodní charakter.*„Kyberprostor existuje nezávisle na vůli jednotlivce 24 hodin 7 dní v týdnu“.* [10]
3. síťovost,
4. informativnost,
5. distribuovanost - rozptýlenost,
6. automatizovanost – umožnění vzniku individuálních malých, na kumulované úrovni však velkých škod.

[7] Věcný záměr zákona o kybernetické bezpečnosti, 2012, s. 56.

[8] ZAVRŠNIK, A. *Kyberkriminalita.* Praha: Wolters Kluwer, 2017, 148 s. ISBN 97880-7552-755-5. s. 4.

[9] Viz ZAVRŠNIK, A. *Kyberkriminalita.* Praha: Wolters Kluwer, 2017, 148 s. ISBN 97880-7552-755-5. s. 4.

[10] GŘIVNA, T. a kol. *Kriminologie*. Praha: Wolters Kluwer, 2014. 530 s. ISBN 97880-7478-614-3. s. 336.

Evropské centrum pro boj proti kyberkriminalitě v EC3 First Year Report identifikoval z hlediska trestněprávních reakcí tyto nové charakteristiky kyberkriminality, které ve svém důsledku ztěžují jejich trestní postih. Jedná se o:

1. přeshraniční povahu internetu,
2. zvyšování počtu trestných činů na masovou úroveň,
3. větší možnost skrývání kyberkriminality (latence) – některé výzkumy uvádějí až 95% latentnosti,
4. široce rozvětvenou zločineckou síť vzniklou spoluprací zločineckých skupin na internetu.

2. KATEGORIZACE KYBERKRIMINALITY

Kybernetickou kriminalitu můžeme dělit dle různých hledisek. Jedním z dělení je klasifikace **podle iniciativy v rámci Lisabonské strategie** na:

1. zločiny porušující soukromí,
2. zločiny se vztahem k obsahu počítače,
3. ekonomické zločiny,
4. zločiny se vztahem k duševnímu vlastnictví.

Další možností je členění **podle Budapešťské Úmluvy** (Úmluva Rady Evropy o kyberkriminalitě – mezinárodní dohoda z roku 2001 pro harmonizaci národních právních systémů v oblasti počítačové a internetové kriminality) na:

1. trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů,
2. trestné činy související s počítači,
3. trestné činy související s obsahem, zejména s dětskou pornografií,
4. trestné činy související s porušením autorského práva a práv příbuzných autorskému právu

Tento výčet v sobě zahrnuje pouze ta jednání, v nichž počítač vystupuje jako přímý či nepřímý prostředek páchání trestné činnosti. Zcela logicky sem nespadají jednání, při kterých sice bylo využito počítače nebo jemu podobných zařízení, avšak tato nebyla pro dokonání trestného činu nezbytná, nicméně přispěla určitou měrou k zefektivnění a ulehčení postupu pachatelů.

Závršník[11] tuto klasifikaci velmi zdařile dále modifikuje pro účely kybernetické kriminality. Tímto způsobem vymezil tři kategorie kybernetické kriminality, a to:

1. kyberkriminalitu spojenou s integritou informačního systému a dat,
2. kyberkriminalitu spojenou s obsahem a
3. kyberkriminalitu spojenou s počítači.

Dalším v dostupné literatuře uváděným členěním je členění kyberkriminality **podle Samuela C. McQuade** (řídícího profesora a koordinátora programu pro bezpečnost podnikání RIT) na:

1. Zločin s využitím počítače – protiprávní jednání, pro jehož spáchání byl užitečný

[11] ZÁVRŠNÍK. A. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017.148 s. ISBN 97880-7552-755-5. s. 16

jeden nebo více počítačů, avšak tyto počítače nebyly pro dokonání nezbytné.

2. Počítačový zločin – protiprávní jednání, pro jehož spáchání a dokonání bylo zapotřebí použít jednoho nebo více počítačů.
3. Zneužití počítače – použití počítače takovým způsobem, který je schopen přivodit újmu jednotlivci, skupině či organizaci, a který může současně narušovat zavedená pravidla nebo procedury. Při zneužití počítače nicméně nemusí nastat taková míra společenské škodlivosti, která by vedla k porušení trestních předpisů.
4. Počítač jako nástroj deviace – tím je myšleno takové chování, které využívá počítačová nebo telekomunikační zařízení jako nástroj k porušování sociálních norem, mnohdy až s trestněprávním přesahem.[12]

3. PRÁVNÍ ÚPRAVA KYBERKRIMINALITYY

Příchod kybernetické kriminality vyžadoval legislativní změny. Trestněprávní úprava se však ukázala obtížnou, protože v případě kybernetické kriminality je třeba navíc vzít v úvahu, že ochrana tradičními právními prostředky nepostačuje, neboť

- nové jevy nejsou ve většině případů postižitelné starými normami,
- působnost trestněprávních norem je omezena, neboť trestní právo je projevem státní suverenity,
- dochází k překrývání jurisdikcí jednotlivých států.

V současné době není právní úprava v oblasti kybernetické kriminality koncepční ani v rámci evropské legislativy, a jinak tomu není ani v České republice.

Nekoncepčnost je způsobena více příčinami, zejména však

1. **Problémy s vlastní definicí kybekriminality** - právní normy nejsou schopny taxativně vyjmenovat všechny druhy nezákonného jednání.
2. **Nedostatkem vůle a kvalifikace zákonodárce –** problém, jak pojmenovat a definovat jednotlivá jednání, a jakým způsobem má být ta či ona problematika upravena. Nestačí jen vůle zákonodárců, ale je třeba i jejich odpovídající vzdělání a schopnost porozumět problému, který se zákonem snaží regulovat, což není v tak specifické oblasti jednoduché.
3. **Rychlostí legislativního procesu,** který nestačí dynamickému vývoji kyberkriminality. V takto dynamickém prostředí je aplikace trestněprávních předpisů přinejmenším obtížná.

3.1 Mezinárodní právní úprava

První reakcí na kyberkriminalitu byl **Manuál OSN o prevenci a kontrole trestných činů spojených s počítači** z roku 1990**,** který upozornil na legislativní nepřipravenost států vůči novým technologiím a vyzval státy k mezinárodní spolupráci. Jako přední orgány zabývající se touto problematikou Manuál označil OECD[13], Radu Evropy a právě OSN.

[12] McQUADE, Samuel C. *Encyclopedia of cybercrime*. Westport, Conn.: Greenwood Press, 2009. ISBN 0313339740. s. 43.
[13] Organizace pro hospodářskou spolupráci a rozvoj

V oblasti mezinárodního práva souvisejícího s kybernetickou kriminalitou je v současné době stále nejvýznamnějším dokumentem **Úmluva o kybernetické kriminalitě.** Úmluva byla schválena Výborem ministrů Rady Evropy na jejím 109. zasedání 8. listopadu 2001 a otevřena k podpisu byla v Budapešti dne 23. listopadu 2001. V platnost vstoupila dne 1. července 2004.

Úmluva o kybernetické kriminalitě neboli Budapešťská úmluva se dělí na Preambuli a čtyři kapitoly, obsahující celkem čtyřicet osm článků. Po úvodních definicích následuje katalog kriminalizovaných činů, které Úmluva dělí do čtyř skupin:

1. Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů
   a) neoprávněný přístup (čl. 2)
   b) neoprávněné zachycení informací (čl. 3)
   c) zásah do dat (čl. 4)
   d) zásah do systému (čl. 5)
   e) zneužití zařízení (čl. 6)
2. Trestné činy související s počítači
   a) falšování údajů souvisejících s počítači (čl. 7)
   b) podvod související s počítači (čl. 8)
3. Trestné činy související s obsahem, zejména s dětskou pornografií (čl. 9)
4. Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu (čl. 10)

Tyto skutkové podstaty se staly základem nových skutkových podstat v současném trestním zákoníku. Dále zakotvuje požadavek na úpravu trestní odpovědnosti právnických osob v rámci právních úprav jednotlivých států, které k Úmluvě přistoupily.

Úmluva představuje nejvýznamnější právní dokument týkající se kyberkriminality a jeho cílem je vytvořit mezinárodní právní rámec pro účinné potírání počítačové kriminality prostřednictvím harmonizace prvků skutkových podstat v oblasti počítačové kriminality za účelem zajištění adekvátního postihu pachatelů, stanovení nezbytných vnitrostátních vyšetřovacích pravomocí pro zajišťování důkazů v elektronické formě a vyšetřování počítačové kriminality, jakož i zavedení pohotového a efektivního režimu mezinárodní spolupráce ve vztahu k trestným činům souvisejícím s informačními.[14] Tzn., že tato úmluva stanoví smluvním stranám povinnost zavést do národních právních řádů takové nástroje, pomocí kterých bude možné postihovat definované kybernetické trestné činy, jejichž taxativní výčet uvádí.

Dne 28. 1. 2003 byl přijat **Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě.**[15]Tento dokument definuje okruh trestných činů, kterým se Úmluva o kyberkriminalitě nevěnuje, tj.

[14] Viz Úmluva o počítačové kriminalitě. In: COE [právní informační systém]. Council of Europe Tre-aty office. [cit. 10.09.2018]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

[15] Viz Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. In: COE [právní informační systém]. Council of Europe Treaty office [cit. 10.09.2018]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f

1. šíření rasistických a xenofobních materiálů,
2. rasisticky a xenofobně motivovaná pohrůžka,
3. rasisticky a xenofobně motivovaná urážka,
4. popření, hrubé snižování, schvalování nebo ospravedlnění genocidy nebo zločinů
5. proti lidskosti,
6. návod a pomoc k těmto jednáním.

Dodatkový protokol vstoupil pro Českou republiku v platnost dne 1. 12. 2014.

Dalším významným dokumentem v oblasti kyberkriminality je **tzv. Talinský manuál** mezinárodního práva použitelný na kybernetickou válku**.** Jedná se o dokument, který vydalo Centrum excelence pro spolupráci v oblasti kybernetické obrany NATO v estonském Talinu. Dokument byl publikován v dubnu 2013 a je primárně zaměřen na kybernetickou válku. Mj. řeší otázku uplatnitelnosti norem mezinárodního práva na oblast kybernetické války, když v pravidle č. 6 uvádí: *„stát nese odpovědnost za kybernetické operace, které jsou u přičitatelné, a které představují porušení závazku mezinárodního práva“*.[16]

3.2 Unijní právní úprava

EU[17] se snaží sblížit právní úpravu jednotlivých členských států tak, aby bylo možno účinněji postihovat kyberkriminalitu.

Již v roce 1999 na zasedání v Helsinkách vyhlásila Evropská komise celoevropskou strategickou iniciativu eEurope - Informační společnost pro všechny. Jejím hlavním cílem bylo poskytnutí výhod informační společnosti všem obyvatelům.

Nejširší rámec, kterým se od roku 2010 EU řídí, se pak nazývá Evropa 2020; jedná se o desetiletou strategii, jejímž cílem je dosáhnout hospodářského růstu. Klade si za cíl pět bodů, kterých chce dosáhnout prostřednictvím sedmi iniciativ, přičemž jednou z nich je tzv. Digitální agenda pro Evropu, která sama navrhuje sedm klíčových oblastí, ve kterých je třeba vhodnými nástroji dosáhnout následujících požadovaných cílů:[18]

- vytvoření jednotného digitálního trhu,
- zlepšení rámcových podmínek pro interoperabilitu mezi výrobky a službami v oblasti ICT,
- posílení důvěry v Internet a jeho bezpečnost,
- záruka poskytování výrazně rychlejšího internetového připojení,
- podpora investic do výzkumu a vývoje,
- zvýšení digitální gramotnosti, dovedností a začlenění,
- zavádění IKT k řešení společenských úkolů, jako jsou změna klimatu, zvyšující se náklady na zdravotní péči a stárnoucí populace.

[16] Talinský manuál mezinárodního práva použitelného na kybernetickou válku. [cit. 10.09.2018]. Dostupné z: http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381

[17] ČR podala žádost o vstup 17. ledna 1996, žádosti bylo vyhověno k 1. květnu 2004.

[18] European Commission. *Digitální agenda pro Evropu: klíčové iniciativy* (online) © European Union, 1995-2015. [cit. 10.09.2018]. Dostupné z: http://europa.eu/rapid/press-release_MEMO-10-200_cs.htm?locale=EN

Prostředkem pro sbližování práva jednotlivých členských států jsou především rámcová rozhodnutí, směrnice a další dokumenty EU/ES. Z hlediska boje s kybernetickou kriminalitou se jeví jako nejvýznamnější následující dokumenty:

1. směrnice Rady 91/250/EHS o právní ochraně počítačových programů,
2. rozhodnutí rady 92/242/EHS o bezpečnosti informačních systémů,
3. rámcové rozhodnutí Rady 2000/375/JHA o boji proti dětské pornografii na internetu,
4. nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů a zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů),
5. rámcové rozhodnutí rady EU č. 2002/584/JHA o evropském zatýkacím rozkazu a postupech předávání mezi státy,
6. nařízení Evropského parlamentu a Rady (EU) 2016/794, o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a o zrušení a nahrazení rozhodnutí 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV, ze dne 11. 5. 2016 a další.

Jedná se pouze o demonstrativní výčet dokumentů.

3.3 Právní úprava kyberkriminality v ČR

Nejvýznamnějším vnitrostátním předpisem upravujícím hmotněprávní aspekty internetové kriminality je nepochybně **z. č. 40/2009 Sb., trestní zákoník.**

První trestné činy spojené s počítači se objevily již v 70. a 80. letech minulého století a byly nejčastěji kvalifikovány jako sabotáž podle § 97 zákona č. 140/1961 Sb. Trestní zákon platný v té době neobsahoval skutkovou podstatu, která by stanovila postih za neoprávněný přístup k počítačovému systému. Postupný nárůst trestné činnosti s využitím počítače s sebou přinesl naléhavou potřebu přijmout takovou trestněprávní úpravu, která by byla účinná a umožnila postihnout i tato protiprávní jednání.

První "počítačový" delikt u nás byl obsažen v zákoně č. 140/1961 Sb., trestním zákonu, do kterého byl včleněn od 1. ledna 1992 zákonem č. 557/1991 Sb. Jednalo se o trestný čin poškození a zneužití záznamu na nosiči informací podle § 257 a) trestního zákona, jehož se dopustil ten, kdo získal přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch

a) takových informací neoprávněně užil,
b) informace zničil, poškodil, změnil nebo učinil neupotřebitelnými, nebo
c) učinil zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení,

za což mu hrozil trest odnětí svobody až na jeden rok nebo zákaz činnosti nebo peněžitý trest nebo propadnutí věci nebo jiné majetkové hodnoty.

Zákon č. 40/2009 Sb., trestní zákoník, zohlednil význam informačních technologií při páchání trestné činnosti a mezinárodní charakter kriminality. Právní úprava skutkových podstat počítačové kriminality v zákoně č. 40/2009 Sb. zahrnuje jednak klasické trestné činy, páchané v kyberprostoru, kterými jsou zejména:

- trestný čin neoprávněného nakládání s osobními údaji podle § 180 trestního zákoníku,

- trestný čin poškození cizích práv podle § 181 trestního zákoníku,
- trestný čin porušení tajemství dopravovaných zpráv podle § 182 trestního zákoníku,
- trestný čin porušení tajemství listin a jiných dokumentů uchovávaných v soukromí podle § 183 trestního zákoníku,
- trestný čin pomluvy podle § 184 trestního zákoníku,
- trestný čin šíření pornografie podle § 191 trestního zákoníku,
- trestný čin výroby a jiného nakládání s dětskou pornografií podle § 192 tr. zákoníku,
- trestný čin krádeže podle § 205 trestního zákoníku,
- trestný čin zpronevěry podle § 206 trestního zákoníku,
- trestný čin neoprávněného užívání cizí věci podle § 207 trestního zákoníku,
- trestný čin podvodu podle § 209 trestního zákoníku,
- trestný čin provozování nepoctivých her a sázek podle § 213 trestního zákoníku.[19]

V souvislosti s ratifikací Úmluvy[20] byly do trestního zákoníku zařazeny skutkové podstaty nových trestných činů, a to:

1. trestného činu neoprávněného přístupu k počítačovému systému podle § 230 tr. zákoníku,
2. trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 trestního zákoníku,
3. trestného činu poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti podle § 232 trestního zákoníku.

Trestné činy podle § 230 – § 232 trestního zákoníku jsou specifickou skupinou soudně trestných deliktů. Od ostatních trestných činů proti majetku, jejichž druhovým objektem jsou majetkové zájmy různorodé povahy, se odlišují právě svým primárním objektem, kterým je společenský, parciální či individuální zájem na důvěrnosti, integritě a dostupnosti počítačových systémů, sítí a počítačových dat, jakož i zájem na zamezení zneužití takových systémů, sítí a dat k páchání trestné činnosti různorodé povahy.[21] Nepřímo jsou chráněny i další zájmy, obchodní tajemství, bankovní tajemství, autorská díla, údaje o pacientech, údaje o zaknihovaných cenných papírech, utajované informace, pokud je nosič informací obsahuje. Předmětem útoku je nosič informací, resp. jeho obsahové a technické vybavení.[22]

Trestného činu **neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 trestního zákoníku** se dopustí ten, kdo překoná bezpečnostní opatření, a tím

[19] ŠÁMAL, P. a kol. *Trestní zákoník. Edice velké komentáře*. Praha: C.H.Beck, 2009, ISBN 978-80-7380-501-2. s. 2084.

[20] Úmluva o počítačové kriminalitě. In: COE [právní informační systém]. Council of Europe Tre-aty office. [cit. 10.09.2018]. Dostupné z:

https://www.coe.int/en/web/conventions/full-list/-conventions/rms/0900001680081561

[21] DRAŠTÍK, A. a kol. Trestní zákoník: komentář. Praha: Wolters Kluwer, 2015, ISBN 978-80-7478-790-4. s. 1476.

[22] JELÍNEK, J. a kol. *Trestní právo hmotné*. 1. vydání. Praha: Leges, 2009, 896 s., ISBN 978-80-87212-24-0. s. 626.

neoprávněně získá přístup k počítačovému systému nebo k jeho části, přičemž mu hrozí trest odnětí svobody až na jeden rok, zákaz činnosti nebo propadnutí věci nebo jiné majetkové hodnoty. Pachatel, který získá přístup k počítačovému systému nebo k nosiči informací a

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,
b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,
c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo
d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, může být potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

Ust. § 230 trestního zákoníku tedy obsahují 2 základní skutkové podstaty:

a) v odstavci 1 je chráněna důvěrnost počítačových dat a počítačového systému nebo jejich částí a
b) v odstavci 2 jsou chráněny integrita a dostupnost počítačových dat a systémů.

Podle ustanovení § 230 odst. 3 písm. b) je okolností podmiňující použití vyšší trestní sazby situace, kdy pachatel spáchá trestný čin podle odst. 1 nebo 2 téhož ustanovení v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat. Jelikož ustanovení § 230 odst. 1 kriminalizuje již pouhý neoprávněný přístup k počítačovému systému a nevyžaduje se, aby došlo k omezení funkčnosti (postačí, že k tomu směřoval úmysl pachatele), je úprava v trestním zákoníku nad rámec závazku vyplývajícího z Úmluvy o kybernetické kriminalitě. Z hlediska subjektivní stránky je k naplnění skutkových podstat definovaných v ustanovení § 230 trestního zákoníku vyžadováno zavinění ve formě úmyslu.

S cílem dostát závazkům plynoucím z Úmluvy o počítačové kriminalitě (čl. 6) byla do trestního zákoníku nově zařazena skutková podstata tr. činu **opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat** podle § 231 odst. 1 trestního zákoníku, která kriminalizuje jednání pachatele, jež spočívá již v pouhém držení, výrobě, zpřístupňování nebo jiném nakládání s prostředky, postupy nebo nástroji užívanými ke spáchání vlastních kybernetických útoků, tj. svou povahou přípravné jednání k trestným činům porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b). c) nebo neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, odst. 2 (tzv. předčasně dokonaný trestný čin).

Objektem tohoto trestného činu je zájem na ochraně společnosti a osob před možným ohrožením vyplývajícím z nekontrolovaného opatření a přechovávání zařízení, nástrojů a prostředků, jež primárně slouží ke spáchání trestných činů porušení tajemství dopravovaných zpráv podle ustanovení § 182 odst. 1 písm. b), c) nebo neoprávněného přístupu k počítačovému systému a nosiči informací podle ustanovení § 230 odst. 1, 2.[23]

[23] ŠÁMAL, P. a kol. *Trestní zákoník. Edice velké komentáře*. Praha: C.H.Beck 2009, ISBN 978-80-7380-501-2. s. 2097-98.

Z hlediska subjektivní stránky je k naplnění skutkové podstaty definované v ustanovení § 231 trestního zákoníku vyžadováno zavinění ve formě úmyslu a to tak, že úmysl musí směřovat ke spáchání některého z uvedených trestných činů. To znamená, že opatření a přechovávání přístupového zařízení a hesla samo o sobě bez takového úmyslu trestné není. Neoznámení ani nepřekažení tohoto trestného činu nejsou trestné.

Trestného čin **poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti podle § 232 trestního zákoníku se dopustí ten, k**do z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté

a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo

b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat, a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

Úprava ustanovení § 232 trestního zákoníku jde nad rámec závazků vyplývajících z mezinárodních smluv nebo unijního práva. Objektem je v tomto případě ochrana dat a technického a programového vybavení počítače před nedbalostním poškozovacím jednáním, pokud je těmito zásahy způsobena značná škoda.

Z důvodu, že kriminalizace nedbalostního jednání je v tomto případě i s ohledem na zásadu subsidiarity trestněprávní represe (§ 12 odst. 2 trestního zákoníku) poněkud diskutabilní, tak byla trestní odpovědnost omezena na případy hrubé nedbalosti a zároveň způsobení škody značného rozsahu.

Tabulka č. 1 – Nápad trestných činů podle § 230 – 232 trestního zákoníku

Tr. činy podle § 230 – 232 TZk	
rok	nápad
2011	134
2012	178
2013	301
2014	669
2015	707
2016	635
2017	784

Tab.1 Nápad trestných činů podle § 230-232 TZk v ČR (vlastní zpracování)

Tabulka č. 2 – Predikce nápadu trestných činů podle § 230 – 232 trestního zákoníku na rok 2018

Bodový odhad pro rok 2018	Interval spolehlivosti 95%		Koeficient spolehlivosti R^2
	horní hranice	dolní hranice	
967,679	643,346	1292,010	0,8955

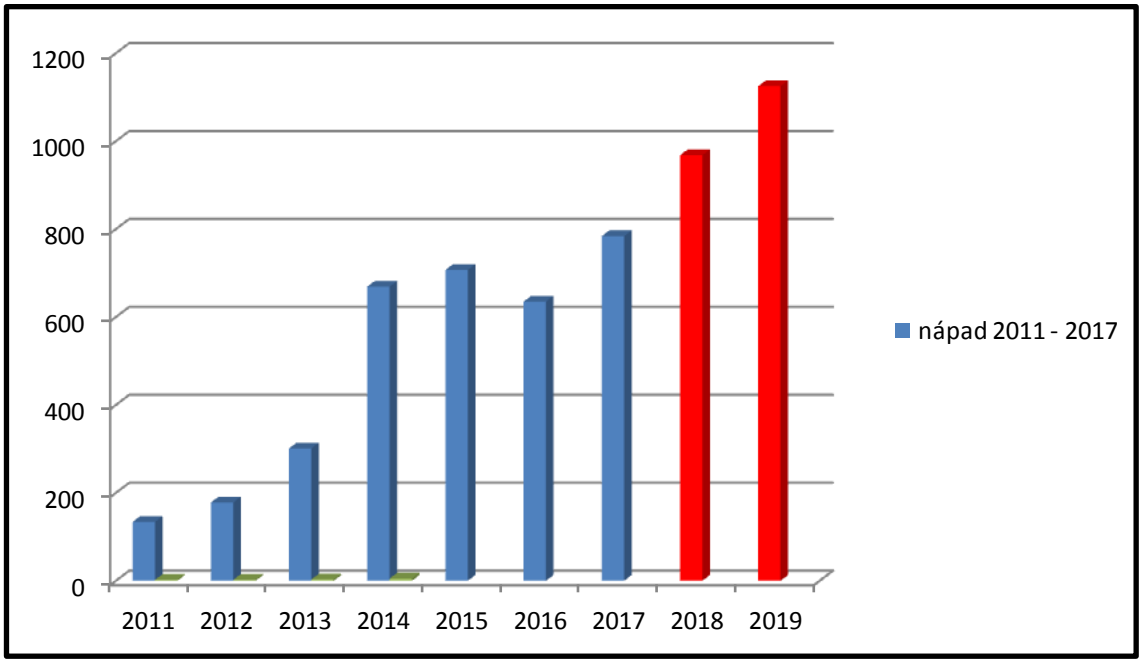
Tab. 2 Predikce nápadu trestných činů kybernetické kriminality v ČR pro rok 2018 (vlastní zpracování)

Tabulka č. 3 – Predikce nápadu trestných činů podle § 230 – 232 trestního zákoníku na rok 2019

Bodový odhad pro rok 2019	Interval spolehlivosti 95%		Koeficient spolehlivosti R^2
	horní hranice	dolní hranice	
1125,130	818,497	1431,763	0,9214

Tab. 3 Predikce nápadu trestných činů kybernetické kriminality v ČR pro rok 2019 (vlastní zpracování)

Graf č. 1 – **Graf nápadu trestných činů podle § 230 – 232 trestního zákoníku s predikcí vývoje na roky 2018 a 2019**



Graf 1 Nápad trestných činů kybernetické kriminality v ČR s predikcí pro roky 2018 a 2019 (vlastní zpracování)

Tabulka č. 4 – Predikce nápadu trestných činů podle § 230 – 232 trestního zákoníku na roky 2018 a 2019

Tr. činy podle § 230 – 232 TZk	
2018	968
2019	1125

Tab.4 Predikce nápadu trestných činů kybernetické kriminality podle § 230-232 TZk na roky 2018 a 2019 (vlastní zpracování)

Jiné, již existující skutkové podstaty trestných činů, byly v trestním zákoníku doplněny tak, aby odpovídaly závazkům plynoucím z Úmluvy. Jedná se o tyto trestné činy:

- **porušení tajemství dopravovaných zpráv podle § 182 a § 183 tr. zákoníku**

Původní úprava tohoto trestného činu v trestním zákoně byla doplněna o postih porušení tajemství při neveřejném přenosu počítačových dat. Důvodem této změny byl především vývoj v oblasti kyberprostoru a dále implementace směrnice Evropského Parlamentu a Rady č. 2002/58/ES. 42 Neveřejným přenosem se rozumí takový přenos, který je chráněný neboli programově zabezpečený. Z hlediska subjektivní stránky se vyžaduje úmyslné zavinění. Pachatelem může být, vyjma skutkové podstaty definované v odstavci 5, kdy pachatelem je zaměstnanec provozovatele, kdokoli.

Ustanovení § 183 tr. zákoníku chrání, stejně jako ustanovení § 182 trestního zákoníku, data. Rozdíl je ale v tom, zda jsou data přenášena (přes internet nebo veřejnou/soukromou síť) nebo zda jde o data uchovávána v počítači (například fotky a videa uložená na pevném disku počítače).

- **trestné činy související s dětskou pornografií podle § 192 a násl. tr. zákoníku**

Kriminalizují jak přechovávání dětské pornografie, tak její výrobu či distribuci, dále jednání spočívající v najímání a lákání dětí k výrobě dětské pornografie nebo účasti na pornografickém představení, jehož se dítě účastní.

Platný trestní zákoník rozlišuje tedy následující trestné činy:

1. výroba a jiné nakládání s dětskou pornografií podle § 192,
2. zneužití dítěte k výrobě pornografie podle § 193,
3. účast na pornografickém představení podle § 193a,
4. navazování nedovolených kontaktů s dítětem podle § 193b.

- **porušení autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 270 tr. zákoníku**

Podle judikatury se za neoprávněný zásah do zákonem chráněných práv ve smyslu § 270 odst. 1 trestního zákoníku rozumí i takové jednání pachatele, který v prostoru vyhrazeném pro své internetové stránky umístí odkazy umožňující neoprávněný přístup k rozmnoženinám děl umístěným na externích serverech tak, že kdokoli k nim může mít prostřednictvím takové stránky přístup, aniž by k tomu měl souhlas nositelů autorských práv, a využije tzv. hostingu

s možností uložení dat na serveru. Pachatel, který takovým jednáním umožní přístup k rozmnožení díla, aniž by k tomu byl oprávněn, poruší autorská práva k jednotlivým dílům a poruší práva na sdělování díla veřejnosti ve smyslu § 18 odst. 1, 2 autorského zákona.[24]

Na základě Úmluvy o kybernetické kriminalitě zavedl **zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim** trestní odpovědnost právnických osob, a tím **stíhat, odsoudit a potrestat právnickou osobu, která spáchala trestný čin.** Pokud zákon nestanoví jinak, použije se na trestní odpovědnost právnických osob trestní zákoník. Odpovědnost za trestný čin právnické osobě vzniká, pokud statutární orgán, jeho člen nebo jiná osoba ve vedoucím postavení, nebo s rozhodujícím vlivem na řízení, nebo zaměstnanec právnické osoby při plnění pracovních povinností páchá protiprávní čin v zájmu právnické osoby nebo v rámci její činnosti. Druhou podmínkou pro vznik trestní odpovědnosti právnické osoby za jednání jejího zaměstnance je, že se musí jednat o čin schválený nebo na pokyn některé z osob ve vedoucím postavení nebo s rozhodujícím vlivem.

Právní úprava, která se týká kybernetické bezpečnosti v ČR, je obsažena zejména v **zákoně č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů**. Přijetím tohoto předpisu došlo s účinností od 1. ledna 2015 ke zvýšení efektivity řešení kybernetických incidentů, a to stanovením podmínek spolupráce mezi veřejnou správou a soukromými osobami. Charakterizuje kybernetický bezpečnostní incident jako narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. Základním cílem zákona o kybernetické bezpečnosti je zvýšit bezpečnost kybernetického prostoru a zejména se snažit ochránit tu část infrastruktury, která je pro fungování státu důležitá a jejíž narušení by vedlo k poškození nebo ohrožení zájmu České republiky.[25]

Na základě zákona o kybernetické bezpečnosti došlo ke zřízení **Národního úřadu pro kybernetickou a informační bezpečnost**, jehož činnost byla zahájena dne 1. srpna 2017. Tento úřad převzal činnost Národního centra kybernetické bezpečnosti, které spadalo pod Národní bezpečnostní úřad. Součástí úřadu je tzv. Vládní CERT (Computer Emergency Response Team), což je specializovaný tým pro prevenci a řešení bezpečnostních incidentů v počítačových sítích.

4. TENDENCE VÝVOJE KYBERNETICKÉ KRIMINALITY

Ve vývoji kybernetické kriminality lze předpokládat:

- že objektem útoku budou v převážné většině nehmotné informace, nikoliv hmotné prostředky informačních systémů a technologií,
- že útoky na technická zařízení se budou odehrávat zejména na mobilní zařízení a zařízení nedostatečně zabezpečená a připojená do sítě zaměstnavatele,
- možnost útoků na průmyslové řídicí systémy (ICS) a systémy dispečerského řízení a sběru dat (SCADA) v kritické infrastruktuře,
- využití všech druhů internetové komunikace, vč. sociálních sítí,
- tupý vandalismus,

[24] Viz Usnesení Nejvyššího soudu sp. zn. 8 Tdo 137/2013 ze dne 27. 2. 2013

[25] Viz SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. ISBN 978-80-7380-501-2. s. 93.

- finanční podvody spojené s kyberprostorem,
- kriminální jednání vlastních zaměstnanců,
- masivní zneužívání Internetu k šíření nepravdivých údajů, a to nejen vůči fyzickým osobám, ale i vůči osobám právnickým,
- prohloubení střetu mezi anonymitou a ochranou soukromí na Internetu,
- porušování autorských práv,
- útoky na kritickou informační a komunikační infrastrukturu ze strany cizích států ale i malých skupin osob.[26]

Aby byl boj s kyberkriminalitou opravdu úspěšný, je třeba řešit všechny problémy jak v oblasti zákonodárství, tak v oblasti organizační a technické současně. Zákony by měly zahrnovat všechny formy trestního jednání a stanovit dostatečné postihy.[27]

Prevence je důležitější než represe. V případě bezpečnostního incidentu je Dle Václava Jirovského by měla prevence spočívat především v následujících činnostech:

1. přijetí opatření, která omezí možnost útoku na počítačový systém,
2. testování přijatých opatření,
3. detekci průniku nebo počátečních aktivit směřujících k průniku do systému a maximální využití nástrojů, které jsou k tomu určeny. Během detekce takové aktivity je možno ve smyslu prvního kroku přijmout okamžitá opatření vedoucí ke zvýšení bezpečnosti ohrožené části systému nebo eliminaci útočníka.
4. vyšetřování průniku, shromažďování důkazů a odstraňování vzniklých škod.[28]

5. PREDIKCE VÝVOJE KYBERKRIMINALITY

Česká policie v roce 2014 zaznamenala 4348 případů kyberkriminality. Vzhledem k enormnímu nárůstu oproti roku 2013, kdy bylo zaznamenáno 3108 případů,[29] zřídila policie on-line formulář *„Hlášení kyberkriminality"*, umístěný přímo na hlavní stránce internetových stránek policie. Kyberkriminalita i nadále narůstala, jak je zřejmé z Tabulky č. 1, která byla zpracovaná na základě údajů ze statisticky sledovaných přehledů kyberkriminality evidovaných v ČR policií, a to v období let 2011 – 2017.[30]

Policie ČR od r. 2011 sleduje počet trestných činů spáchaných v kyberprostoru. V tomto období byl zaznamenán trend setrvalého nárůstu evidovaných případů kybernetické kriminality od 1502 trestných činů v roce 2011 do 5654 trestných činů zaznamenaných v roce 2017. Na základě statistických údajů z let 2011 – 2017 byla zpracována níže uvedená Tabulka č. 5, v níž jsou zachyceny i údaje predikované pro roky 2018 a 2019.

---

[26] Viz SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. ISBN 978-80-7380-501-2. s. 571.

[27] GŘIVNA, T., POLČÁK, R. *Kyberkriminalita a právo*. Praha: nakladatelství Auditorium, 2008. 220 s. ISBN: 978-80-903786-7-4. s. 88.

[28] Viz JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing, 2007.

[29] *Statistické přehledy kriminality za rok 2014 až 2015*. Policie ČR, [cit. 10.09.2018]. Dostupné z: http://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2014.aspx

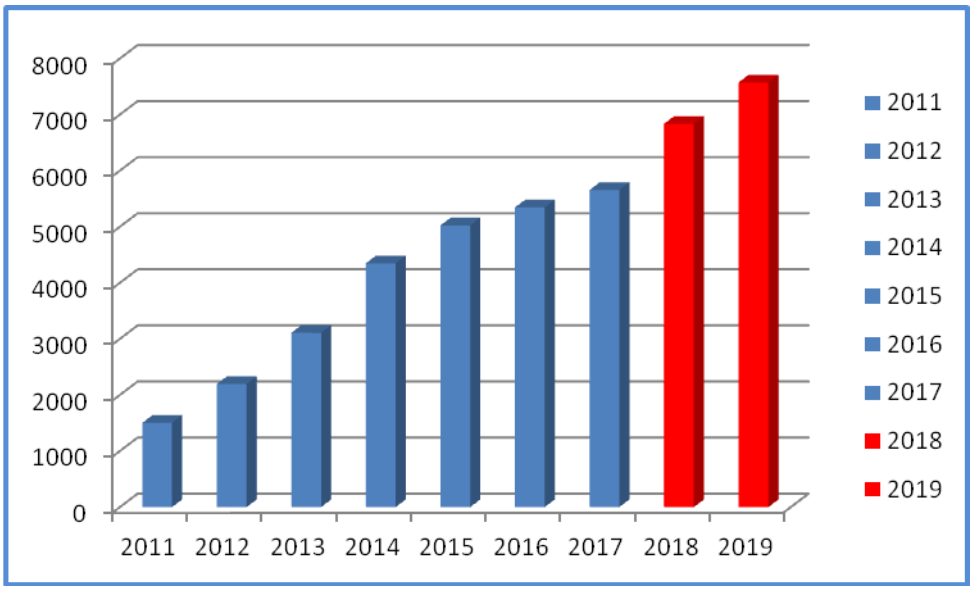
[30] *Statistické přehledy kriminality za roky 2011 až 2017*. Policie ČR. [cit. 10.09.2018]. Dostupné z: http://www.policie.cz/clanek/archiv-statistiky-statisticke-prehledy-kriminality.aspx

Tabulka č. 5 – Tabulka nápadu trestných činů kybernetické kriminality v ČR v letech 2011-2017 s predikcí pro roky 2018 a 2019

Struktura nápadu kyberkriminality	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**
podvodná jednání	917	1303	1863	2478	2932	3235	3140	**3924**	**4339**
hacking	66	112	220	555	578	534	608	**786**	**887**
mravnostní delikty	132	161	261	314	351	344	561	**553**	**770**
autorskoprávní delikty	155	241	181	262	315	237	296	**320**	**339**
násilné projevy	86	111	155	202	230	265	318	**350**	**388**
ostatní	146	267	428	537	617	729	731	**903**	**1006**
Celkový nápad kyberkriminality	**1502**	**2195**	**3108**	**4348**	**5023**	**5344**	**5654**	**6835**	**7573**

Tab. 5 Nápad trestných činů kybernetické kriminality v ČR s predikcí pro roky 2018 a 2019 (vlastní zpracování)

Graf č. 2 **– Graf nápadu trestných činů kybernetické kriminality v ČR v letech 2011-2017 s predikcí pro roky 2018 a 2019**



Graf 2 Nápad trestných činů kybernetické kriminality v ČR s predikcí pro roky 2018 a 2019 (vlastní zpracování)

Tabulka č. 6 - Výpočet nápadu trestných činů kybernetické kriminality v ČR pro rok 2018

Nápad kyberkriminality	Predikce pro rok 2018			Koeficient spolehlivosti R^2
struktura nápadu	bodový odhad	interval spolehlivosti 95%		
		horní hranice	dolní hranice	
podvodná jednání	**3924,286**	4748,231	3100,341	0,94
hacking	**785,857**	1145,407	426,308	0,84
mravnostní delikty	**552,429**	711,104	393,753	0,89
autorskoprávní delikty	**319,429**	451,147	187,710	0,84
násilné projevy	**349,429**	371,558	327,299	0,99
ostatní	**903,286**	1051,239	755,332	0,96
Celkem	**6834,714**	7941,214	5728,215	0,96

Tab. 6 Predikce nápadu trestných činů kybernetické kriminality v ČR pro rok 2018 (vlastní zpracování)

Tabulka č. 7 - Výpočet nápadu trestných činů kybernetické kriminality v ČR pro rok 2019

Nápad kyberkriminality	Predikce pro rok 2019			Koeficient spolehlivosti R^2
struktura nápadu	bodový odhad	interval spolehlivosti 95%		
		horní hranice	dolní hranice	
podvodná jednání	**4338,643**	4903,510	3773,776	0,96
hacking	**886,857**	1133,351	640,363	0,88
mravnostní delikty	**770,143**	1114,739	425,547	0,76
autorskoprávní	**339,036**	450,595	227,477	0,88
násilné projevy	**387,964**	406,707	369,221	0,99
ostatní	**1005,714**	1131,023	880,405	0,88
Celkem	**7572,893**	8510,043	6635,743	0,97

Tab. 7 Predikce nápadu trestných činů kybernetické kriminality v ČR pro rok 2019 (vlastní zpracování)

Při výpočtu predikce vývoje kyberkriminality pro roky 2018 a 2019 byla využita klasická analýza (modelování) časových řad, přičemž výpočet lineárního trendu je založen na metodě nejmenších čtverců. Jiné než lineární trendy dávaly horší výsledky. Spolehlivost prognóz měřená koeficientem R^2 je u všech zkoumaných řad vysoká (>0,84), s výjimkou mravnostních deliktů, kde ovšem koeficient 0,76 je rovněž dost vysoký a zajišťuje validitu. Výpočet je

zachycen v Tabulkách č. 6 a 7, přičemž výsledky výpočtů byly vepsány do sloupců pro roky 2018 a 2019 v Tabulce č. 5.

Ze shora uvedených tabulek je zřejmé, že navzdory poklesu obecné kriminality počet trestných činů kyberkriminality každým rokem roste. Za první tři měsíce tohoto kalendářního roku činil celkový nápad kyberkriminality 1.753 případ, ač celkový nápad v roce 2017 byl 5.329 případů**.**

V roce 2018 by se měl počet případů kyberkriminality v ČR pohybovat **v rozmezí od 5.728 do 7.941 případů** a **v roce 2019 v rozmezí 6.636 – 8.510 případů**. Lze předpokládat, že *„čím více věcí bude připojeno (stane se součástí kyberprostoru), s tím větším rizikem zneužití musíme počítat"*[31].

ZÁVĚR

Kybernetická kriminalita je neoddělitelnou součástí světa tak, jak je kyberprostor nedílnou a dnes již neoddělitelnou součástí našeho světa. Jeho ochrana proti nelegálním aktivitám (kyberkriminalitě) se musí stát rovněž nedílnou součástí ochrany nejen států, ale i fyzických a právnických osob. Proti kybernetickému nebezpečí lze stejně jako proti jakémukoliv jinému nebezpečí bojovat jednak prevencí a a dále represí. Do oblasti prevence zahrnujeme budování zabezpečených ICT, výchovu k bezpečnosti, základní i aplikovaný výzkum a mezinárodní spolupráci.

Trestní právo je sice podstatným nástrojem v boji proti kyberkriminalitě, ale nemělo by být primárním prostředkem ochrany. Podle zásady subsidiarity trestní represe, jak ji vymezila judikatura Ústavního soudu ČR, by měly být nejprve voleny prostředky obrany v řízení ve věcech občanskoprávních, dále v řízení správním a pouze v krajních případech by mělo být přistupováno k trestnímu stíhání. Legislativa bohužel na kriminální jevy spojené s novými technologiemi reaguje s velkým zpožděním.

Pro lepší regulaci kyberprostoru je nutné:

1. pokračovat v harmonizaci právní úpravy kyberprostoru, a to nejen v rámci Evropy, ale celosvětově,
2. zlepšovat spolupráci při vyšetřování kybernetické kriminality mezi státy navzájem a tak zvýšit úspěšnost odhalení pachatelů trestné činnosti v oblasti kyberprostoru,
3. zefektivnit vymáhání práva v kyberprostoru.

„Aby byl boj s počítačovou kriminalitou opravdu úspěšný, je třeba řešit všechny problémy jak v oblasti zákonodárství, tak v oblasti organizační a technické současně. Zákony by měly zahrnovat všechny formy trestního jednání a stanovit dostatečné postihy."[32]

[31] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. ISBN 978-80-7380-501-2. s. 610.

[32] GŘIVNA, T., POLČÁK, R. *Kyberkriminalita a právo*. Praha: nakladatelství Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4. s. 88.

Literatura:

[1] DRAŠTÍK, Antonín a kol., 2015. *Trestní zákoník: komentář*. Praha: Wolters Kluwer, 3264 s. ISBN 978-80-7478-790-4.

[2] JELÍNEK, Jiří a kol., 2009. *Trestní právo hmotné*. 1. vydání. Praha: Leges, 896 s. ISBN 978-80-87212-24-0.

[3] JIROVSKÝ, Václav, 2007. *Kybernetická kriminalita, nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a.s., 288 s. ISBN 978-80-247-1561-2.

[4] GŘIVNA, Tomáš a kol., 2014. *Kriminologie*. Praha: Wolters Kluwer, 530 s. ISBN 97880-7478-614-3.

[5] GŘIVNA, Tomáš a Radim POLČÁK, 2008. *Kyberkriminalita a právo*. Praha: nakladatelství Auditorium, 220 s. ISBN: 978-80-903786-7-4.

[6] SMEJKAL, Vladimír, 2015. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 220 s. ISBN 978-80-903786-7-4. Čeněk. 636 s. ISBN 978-80-7380-501-2.

[7] ŠÁMAL, Pavel a kol., 2009. *Trestní zákoník. Edice velké komentáře*. Praha: C.H.Beck, 2084 s. ISBN 978-80-7380-501-2.

[8] VLČEK, Martin, 1989. *Počítače a kriminalita (trestněprávní a kriminologické aspekty*), Praha, Academia, ISBN 978-80-2000-139-5.

[9] ZAVRŠNIK, Aleš, 2017. *Kyberkriminalita.* Praha: Wolters Kluwer, 148 s. ISBN 97880-7552-755-5.

[10] *Statistické přehledy kriminality za roky 2011 až 2017* [cit. 10. 09. 2018]. Dostupné: http://www.policie.cz/clanek/archiv-statistiky-statisticke-prehledy-kriminality.aspx

[11] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In: ASPI [právní informační systém]. Wolters Kluwer ČR

[12] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů. In: ASPI [právní informační systém]. Wolters Kluwer ČR

[13] Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže), ve znění pozdějších předpisů. In: ASPI [právní informační systém]. Wolters Kluwer ČR

[14] Zákon č. 418/2011 Sb, o trestní odpovědnosti právnických osob a řízení proti nim), ve znění pozdějších předpisů. In: ASPI [právní informační systém].Wolters Kluwer ČR

[15] Manuál OSN pro prevenci a kontrolu počítačového zločinu. [online] OSN ©2001. [cit. 10.09.2018]. Dostupné z: http://216.55.97.163/wpcontent/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf

[16] Úmluva o počítačové kriminalitě. In: COE [právní informační systém]. Councilof Europe Treaty office. [cit. 10.09.2018]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

[17] Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. In: COE [právní

informační systém]. Council of Europe Treaty office [cit. 10.09.2018]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f

[18] Talinský manuál mezinárodního práva použitelného na kybernetickou válku, [cit. 10.09.2018]. Dostupné z: http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381

[19] Věcný záměr zákona o kybernetické bezpečnosti. 2012. [cit. 10.09.2018]. Dostupné z: https://www.govcert.cz/download/legislativa/container-nodeid-926/vecny-zamer-final-vlada.pdf

VYUŽITÍ SOFTWARU PTV VISSIM VE VÝUCE A V PRAXI

USING SOFTWARE PTV VISSIM IN TEACHING AND PRACTICE

Ing. Kateřina Víchová, doc. Ing. Martin Hromada, Ph.D., Ing. Pavel Viskup, Ph.D.
Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky
Nad Stráněmi 4511, 760 05 Zlín
kvichova@utb.cz

ABSTRAKT

Software PTV Vissim dokáže řešit mikroskopické simulace individuální i veřejné hromadné dopravy. Pomocí tohoto softwaru lze simulovat jak městský provoz včetně cyklistů, tak úseky dálnic včetně rozsáhlých mimoúrovňových křižovatek. Rozsáhlé analytické nástroje nashromážděné ve Vissimu z něj činí nástroj pro dopravní plánování a optimalizaci dopravy a dopravních systémů, rovněž tak i pro různé systémy řízení dopravy. Cílem článku je představení možností tohoto softwaru, který je využíván pro účely výuky na Fakultě logistiky a krizového řízení. Součástí článku je představení využití tohoto softwaru přímo na vybrané komunikaci ve Zlínském kraji. Tento software v sobě skrývá velký potenciál pro územní plánování v rámci vybraného území.

KLÍČOVÁ SLOVA

PTV Vissim, mikroskopické simulace, veřejná doprava, dopravní plánování

ABSTRACT

Software PTV Vissim could handle microscopic simulations of both individual and public transport. With this software, you could simulate both urban traffic, including cyclists, and motorway sections, including significant, cross-country intersections. The extensive analytical tools gathered in Vissim make it a tool for traffic planning and optimization of transport and transport systems, as well as for various traffic management systems. The aim of the article is to present the possibilities of this software, which is used for teaching at the Faculty of Logistics and Crisis Management. Part of the article is introducing the use of this software directly on selected communications in the Zlín Region. This software has unique potential for spatial planning within the selected territory.

KEY WORDS

PTV Vissim, microscopic simulations, public transport, traffic planning

ÚVOD

V současné době můžeme pozorovat nárůst intenzity v silniční dopravě. To má za následek nejen zvýšený počet dopravních nehod, ale také dopravní zácpy. Vzhledem na tento fakt je důležité, aby tato situace byla brána zejména v územním plánování dané obce. Cílem územního plánování je dosáhnout optimálního využití území. [1] Pro to, abychom mohli zjistit, zdali by změna územního plánování pomohla při dopravních zácpách, slouží modely a simulační programy. Model představuje zastoupení skutečných nebo plánovaných událostí, objektů nebo systémů. Model ukazuje systém na určité úrovni abstrakce s cílem ho reprezentovat matematicky věrohodným způsobem. [2] Simulace je metoda, ve které hledáte, vypočítáte stav a chování skutečného systému pomocí systému. [3] Jedním z nich může být software PTV Vissim.

Doprava může být rozdělena podle několika hledisek, základní rozdělení podle předmětu dopravy je osobní doprava, nákladní doprava a přenos informací. [4] Mezi základní prostředky, které lze použít, patří: železniční, silniční, letecká doprava, loď, potrubí. [4, 5] V silniční dopravě se jedná o dynamické modely řízení nákladní dopravy [6], hledání optimální cesty vozidel [7], plánování poptávky po dopravě [8] a určení optimální frekvence dopravy. [9]

Jak již bylo zmíněno, software PTV Vissim slouží k provádění mikroskopických simulací individuální i veřejné hromadné dopravy. Cílem tohoto článku je představení tohoto systému a představení jednotlivých funkcí, které lze v tomto systému využít. Fakulta logistiky a krizového řízení vlastní licenci na tento software a využívá jej ve výuce. Dále je možné software využívat při přípravě bakalářských a diplomových prací, případně dalších vědeckých statí.

1. SOFTWARE PTV VISSIM

Software PTV Vissim je jedním ze softwarů skupiny PTV Group umožňující simulaci a řízení silničního provozu. Jedná se o software, který řeší mikroskopické simulace individuální i veřejné hromadné dopravy. Tento program dokáže simulovat jak městský provoz včetně cyklistů, tak úseky dálnic včetně rozsáhlých mimoúrovňových křižovatek. Rozsáhlé analytické nástroje nashromážděné ve Vissimu z něj činí nástroj pro dopravní plánování a optimalizaci dopravy a dopravních systémů, rovněž tak i množství interface pro různé systémy řízení dopravy.

Vissim dokáže simulovat řadu běžných, ale i unikátních geometrických a provozních podmínek, které se vyskytují v dopravní síti. Schopnost Vissimu definovat neomezené množství typů vozidel umožňuje uživateli plný rozsah multimodálních provozů. Typy vozidel zahrnují osobní automobily, nákladní automobily, autobusy, cyklisty, invalidní vozíky, chodce, letadla atd.

Vissim nabízí unikátní schopnost přidělení vozidel na síť za užití jedné nebo kombinací tří metod. Základní metoda předpokládá, že doprava je stochasticky distribuována na pevně dané trasy od uživatelem definovaného počátečního bodu po cílový bod. Definice odbočovacích manévrů umožňuje distribuci dopravy v křižovatce nebo několika křižovatkách. Dynamické trasy umožňují dynamické přidělování dopravy na uživatelem specifikované trasy.

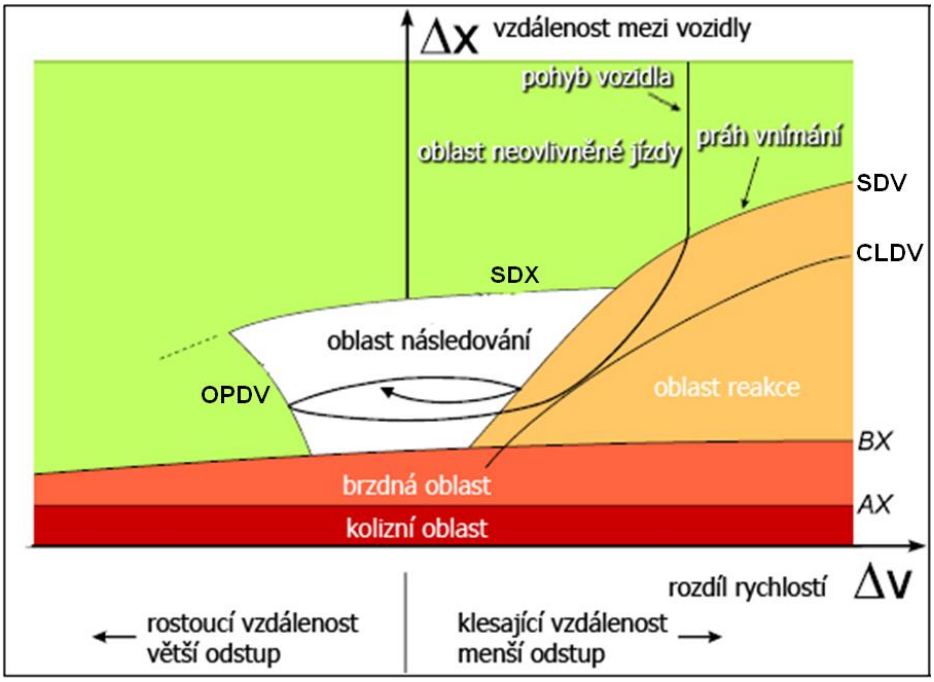
Metoda dynamického zatěžování umožňuje Vissimu přiřadit dopravu na síť matic zdroj/cíl (v závislosti na čase a kategorii vozidel) a stochastických (dopravně-nákladových) zatěžovacích technik.

Software PTV Vissim využívá pohyb vozidel dle Wiedemanna. Základní předpoklad R. Wiedemanna je takový, že vozidlo se může nacházet v jednom ze čtyř jízdních režimů.

- Neovlivněná jízda – řidič není žádným způsobem ovlivněn ve svém pohybu. Pohybuje se tedy určeným směrem a zvolenou rychlostí. Není ovlivněn před ním jedoucími vozidly, ani příkazy podle pravidel silničního provozu. Ve skutečnosti je rychlost, závislá na sešlapávání plynového pedálu, a proto není konstantní. To je jedním z důvodů, proč se ve Vissimu rychlost zadává intervalově (např. 50km/h se zadá intervalem (48-58 km/h)).
- Proces přibližování vozidel – řidič se postupně přibližuje k před ním jedoucímu vozidlu a postupně ubírá rychlost, až do doby, kdy mezi ním a prvním vozidlem bude požadovaná bezpečná vzdálenost.

- Následování vozidla – vozidlo následuje předcházející automobil bez jakékoli změny rychlosti (kromě kolísání rychlosti v zadaném intervalu). Jede tedy shodnou rychlostí, jako vozidlo před ním a stále od něj udržuje bezpečnou vzdálenost.
- Brzdění – pokud řidič nemůže dodržet předepsanou bezpečnou vzdálenost (vozidlo jedoucí před ním stojí), vozidlo postupně snižuje svou rychlost a zastavuje.

Následující obrázek znázorňuje ohraničení stavů interakce dle Wiedemanna, který je využíván v softwaru PTV Vissim.



Obr. 1 Ohraničení stavů interakce dle Wiedemanna [10]

Tento model má stanoveny následující parametry:

- Průměrná vzdálenost zastavení (AX) – definuje průměrnou požadovanou vzdálenost mezi zastavenými auty. Odchylka ± 1 metr.
- Rezervní část požadované bezpečné vzdálenosti (BX_add).
- Fixní část požadované bezpečné vzdálenosti (BX_mult).

Bezpečnou vzdálenost zjistíme na základě následujícího vzorce:

$$BX = (BX_{add} + BX_{mult} * z).\sqrt{v} \quad (1)$$

Kde *v* představuje rychlost vozidla (m/s), *z* představuje hodnotu jízdního dosahu (= 0,5).

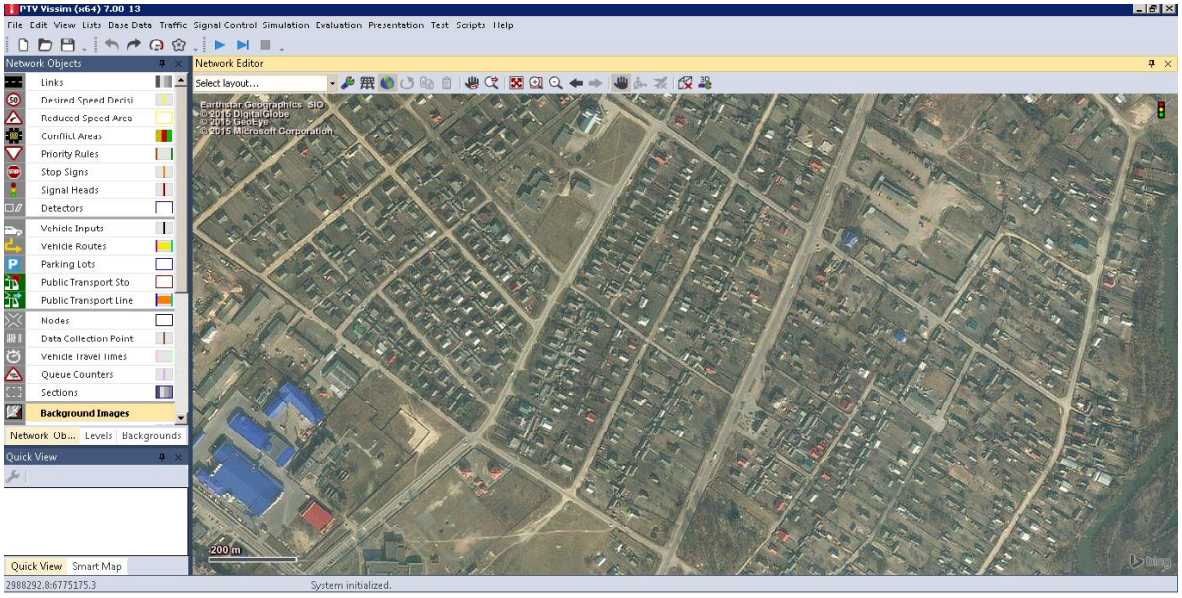
Vzdálenost mezi dvěma vozidly *d* (m) se vypočítá za použití následujícího vzorce:

$$d = AX + BX \quad (2)$$

2. PRÁCE S PTV VISSIM

Pro práci se softwarem PTV Vissim je nezbytná práce s mapou. Software umožňuje pracovat s různým zpracováním map. Může se jednat o formu obrázku, či nákresu, který máme ve formátu png. Tento obrázek lze získat jako grafickou součást projektu či si ji stáhnout, kde jsou mapy volně dostupné a získat z ní obrázek (např. Google Maps, Seznam mapy). Dále je

možné pracovat se softwarovou mapou. Jedná se o mapu celého světa. Není zde ovšem vyhledávač dle adresy, a tudíž pro nalezení konkrétní adresy je vyžadována orientace v mapě a znalost hledaného území. Nakonec je možné pracovat bez mapového podkladu a vytvářet tak nové mapové simulace pouze na základě předem známých vzdáleností.

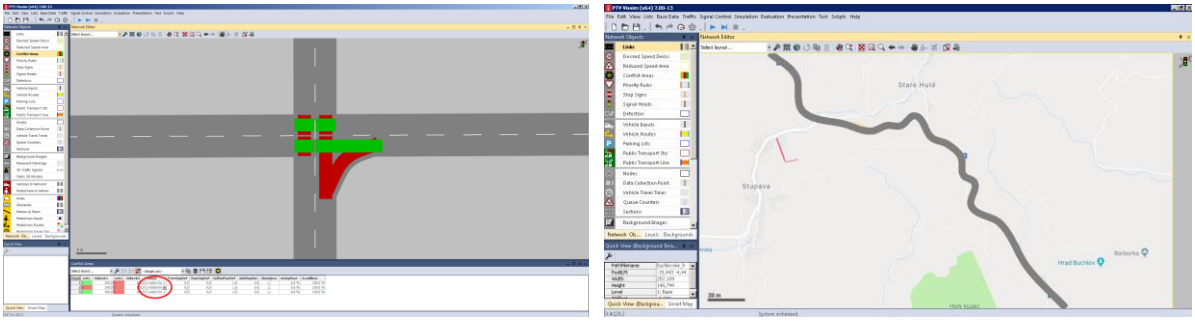


Obr. 2 Softwarová mapa

2.1 Práce s mapovým podkladem

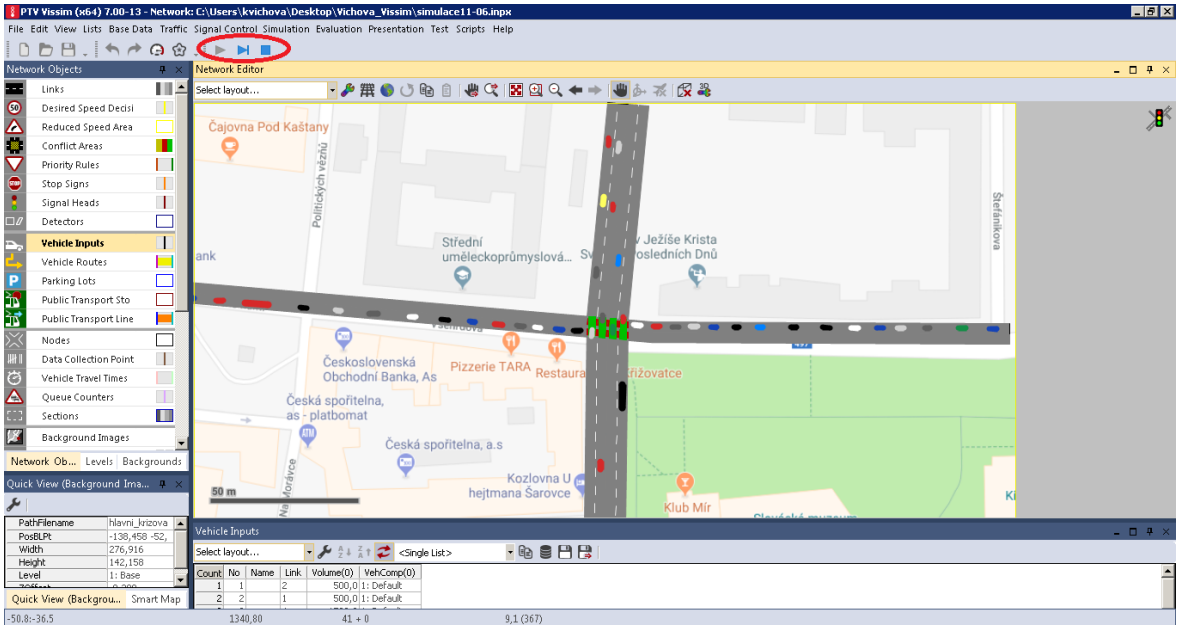
Pokud již má uživatel připraven mapový podklad, ve kterém chce provádět simulaci, tak musí překreslit tento mapový podklad do podoby silnic, křižovatek, dopravního značení dle nabídky softwaru. Software nedokáže rozpoznat z mapového podkladu, kde se jedná o silnici a o křižovatku. Na druhou stranu ovšem software dokáže nakreslit jakoukoliv dopravní situaci. V softwaru je tedy nezbytné, aby ovládal kreslit kruhové objezdy, silnice, které nejsou kolmé, víceproudé silnice či odbočovací pruhy.

Pro tyto účely jsou níže zobrazeny možnosti, jak lze tyto situace překreslit do mapy.



Obr. 3, 4 Znázornění silnic v mapě

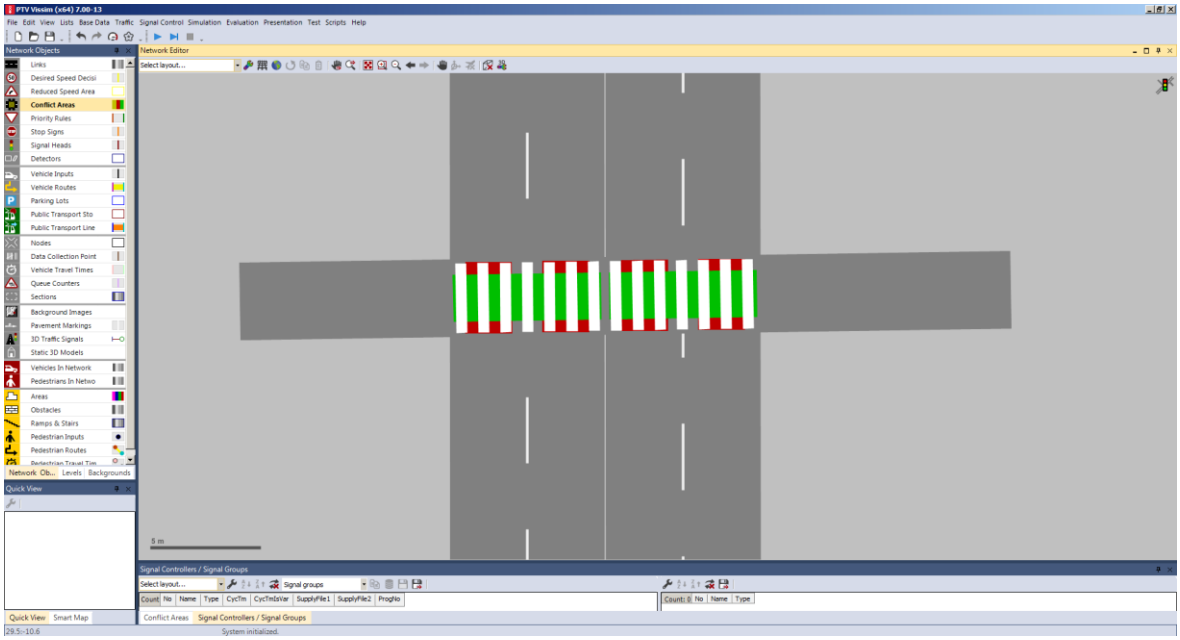
V případě, že máme v softwaru zadány veškeré požadavky, software umožňuje simulaci. Díky této simulaci lze zjistit, zda je současný stav či navrhovaný stav vhodný pro danou situaci. Díky tomuto softwaru, lze zadat parametry současného stavu do křižovatky a poté navrhnout danou křižovatku s novým řešením. Novým řešením je myšleno například nový odbočovací pruh, další jízdní pruh, či časové vyjádření intervalů u semaforů. Následující obrázek znázorňuje simulaci na křižovatce.



Obr. 5 Simulace v PTV Vissim

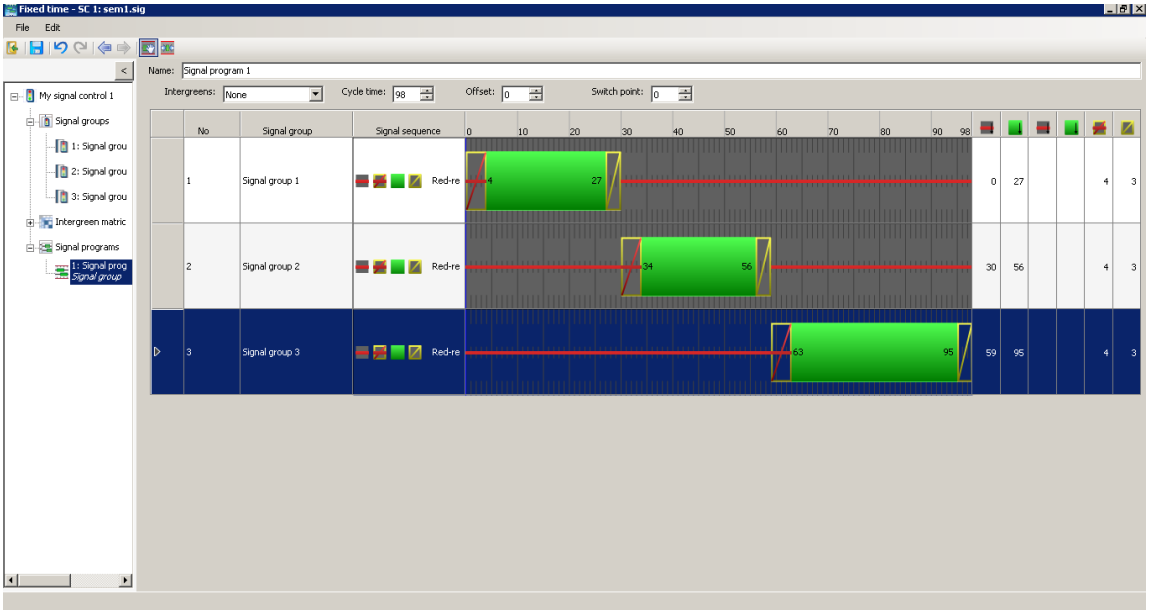
Software umožňuje také pokročilé simulace, a to se zadáním svislého a vodorovného dopravního značení či světelného dopravního značení.

Za vodorovné dopravní značení jsou v tomto softwaru považovány směrové šipky, přechody pro chodce či další značení nezbytné pro provoz na pozemních komunikacích. Na následujícím obrázku je tedy možné vidět, jak lze na silnici nakreslit přechod pro chodce. Aby software zvládal tyto simulace také s chodci, tak je nezbytné, aby byly určeny přednosti v jízdě neboli priority i u přechodu pro chodce. Jak je známo z pravidel silničního provozu v České republice, chodec má přednost (ne vždy absolutní) před jedoucím vozidlem, pokud to není dopravním světelným značením upraveno.



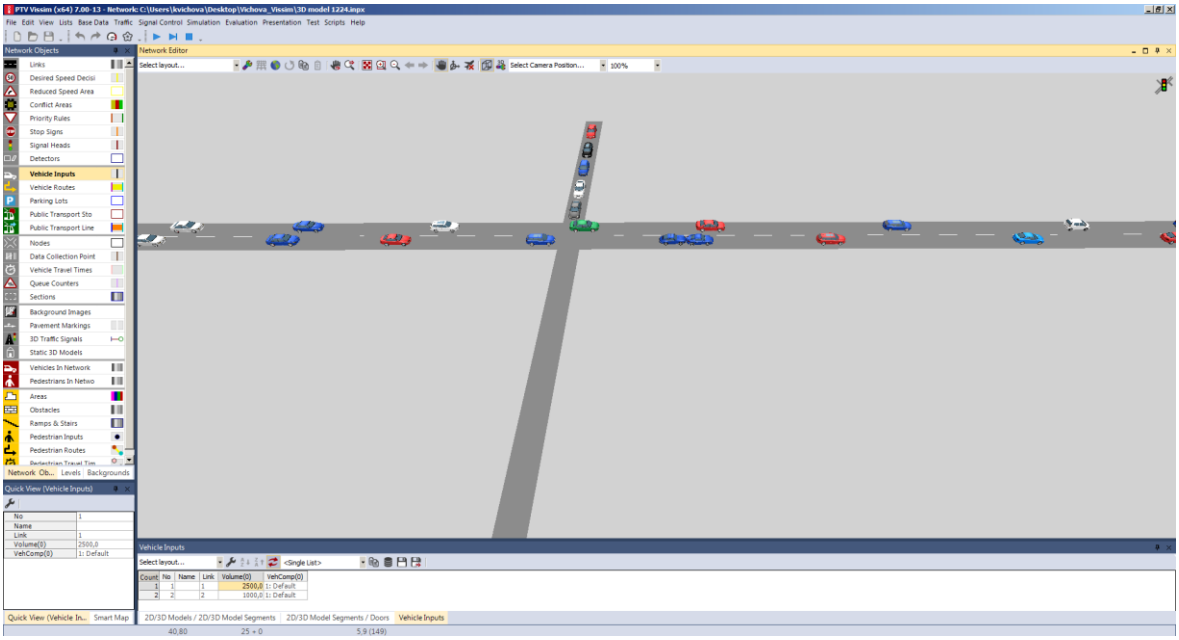
Obr. 6 Znázornění přechodu pro chodce

Pro práci se světelným dopravním značením v softwaru je nutné znát intervaly současného stavu u tohoto značení. Na základě simulace lze pozorovat pohyby přednastavených vozidel.



Obr. 7 Nastavení světelného dopravního značení

Pro ještě lepší představu simulace software umožňuje 3D simulace provozu. Tyto simulace lze využít jak přímo pro provoz, tak pro znázornění světelného dopravního značení.



Obr. 8 3D simulace

ZÁVĚR

Software PTV Vissim umožňuje mikroskopické simulace, které jsou uplatnitelné v oblasti územního plánování. Umožňuje nejen simulovat pohyb vozidel v prostoru, ale také pohyb chodců. Je tedy možné kombinovat pohyb na přechodu pro chodce s pohybem vozidel na silnici. Při těchto simulacích je důležité nastavení přednosti v jízdě neboli priorit jak na silnicích, tak na přechodech pro chodce. Software využívá pohyb vozidel dle Wiedemanna. Mezi další výhodu tohoto simulačního softwaru je možnost nastavení si časového intervalu u světelného dopravního značení. Je tedy možné pozorovat simulaci při změně časových intervalů na této signalizaci a její vliv na dopravu v daném úseku.

Jak již bylo zmíněno v úvodu, tento software je využíván na Fakultě logistiky a krizového řízení při výuce. Dále je software využíván u bakalářských či diplomových prací a dalších vědeckých statí. Software lze využít také pro projektování územního plánování měst a obcí nejen v České republice.

Literatura

[1] LEDVINOVÁ, Michaela. Územní plánování, 2005.

[2] SOKOLOWSKI, J. A. and C. M. BANKS. Principles of modeling and simulation: A multidisciplinaty approach. Hoboken, New Jersey, 2009, ISBN 978-0-470-28943-3.

[3] MALINDŽÁK, D. et al. Modelovanie a simulácia v logistike. Košice: TU Košice, 2009, ISBN 978-80-5530265-2.

[4] STRAKA, M., MALINDŽÁK, D. et al. Distribučná logistika. Košice: TU Košice, 2005, ISBN 80-8073-296-5.

[5] MARASOVÁ, D. et al. Logistika dopravy. Košice: TU Košice, 2007, ISBN 978-80-8073-892-1.

[6] POWEL, W. B. et al. Dynamics Models for Freight Trasportation. In Transportation, Handbooks in Operations Researcg and Management Science, 2007.

[7] CORDEAU, J.-F. et al. Vehicle Routing. In Transportation, Handbooks in Operations Researcg and Management Science, 2007.

[8] CORDEAU, J.-F. et al.Transportation on Demand. In Transportation, Handbooks in Operations Researcg and Management Science, 2007.

[9] BERTAZZI, L. et al. Minimalization of logistic costs with given frequencies. In Treansportation Research Part B: Methodological, 1997, ISSN 0191-2615.

[10] HOFHANSL, Petr. Aplikace mikroskopických simulačních nástrojů k evaluaci a optimalizaci dopravně-inženýrských řešení silniční infrastruktury – validace nástrojů a stanovení standardů. In Rešerše k průběžné zprávě o postupu řešení projektu TA01031193, 2011.

KOMPARAČNÍ ANALÝZA KRIZOVÉ PŘIPRAVENOSTI NEMOCNIC VE ZLÍNSKÉM KRAJI

THE COMPARATIVE ANALYSIS OF CRISIS PREPAREDNESS OF THE HOSPITAL IN THE ZLÍN REGION

Ing. Kateřina Víchová, doc. Ing. Martin Hromada, Ph.D.
Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky
Nad Stráněmi 4511, 760 05 Zlín
kvichova@utb.cz

ABSTRAKT

Celý svět se potýká s nárůstem mimořádných událostí a krizových situací. Tyto události ohrožují také krizovou infrastrukturu, do které spadá také zdravotnický segment. Ten zajišťuje základní, existenčně nezbytné funkce systému poskytování zdravotních služeb a zdravotní péče v podmínkách nouzových až kritických situací. Je tedy nezbytné, aby každé zdravotnické zařízení mělo tzv. krizovou připravenost a zvládalo řešit i krizové situace. Cílem článku je provedení komparační analýzy krizové připravenosti nemocnic ve Zlínském kraji. Součástí článku je analýza mimořádných událostí a krizových situací, které mohou ohrozit nemocnice. V závěru článku je návrh na hodnocení krizové připravenosti nemocnic a to pomocí modulu informačního systému.

KLÍČOVÁ SLOVA

Krizová připravenost, zdravotnictví, blackout, krizová situace, Zlínský kraj

ABSTRACT

The whole world is struggling with an increase in emergencies and crisis. These events also threaten the crisis infrastructure, which also includes the medical segment. It provides essential, existentially necessary functions of the system of delivering health services and healthcare in conditions of emergency to critical situations. It is, therefore, essential for each healthcare facility to have the so-called crisis preparedness and manage to solve crisis situations as well. The aim of the article is to perform a comparative analysis of the crisis preparedness of hospitals in the Zlín region. Part of the article is an analysis of emergencies and crisis situations that can threaten hospitals. At the end of the article, there is a proposal for evaluating the crisis preparedness of hospitals using an information system module.

KEY WORDS

Crisis preparedness, healthcare, blackout, crisis, Zlín region

ÚVOD

Celý svět se potýká s řadou mimořádných událostí a krizových situací. O těchto situacích můžeme číst každý den a dějí se na celém světě. Dle studií lze poukázat také na vzrůstající počet krizových situací. Podle Řeháka je planeta Země a její obyvatelstvo jsou v současné době vystaveny celé řadě nebezpečí. Přibývá živelních katastrof, průmyslových havárií, sociálních, náboženských a etnických konfliktů často spojených s válkami a eskaluje nebezpečí terorismu, které nezná hranice. [1] Sena uvádí, že přírodní katastrofy způsobené extrémními povětrnostními jevy se v posledních letech zvyšují. [2] Nejčastějšími katastrofami jsou přírodní katastrofy. [3] Podle Cioca člověk žije v prostředí, které je trvale vystaveno

rozmanitosti více či méně nebezpečných situací, které vznikají mnoha faktory. Extrémní přírodní jevy, jako jsou: bouře, povodně, sucho, sesuvy půdy, zemětřesení a další, kromě technologických nehod (například silné znečištění) a konfliktních situací mohou přímo ovlivnit život každého člověka a života společnosti jako celku. [4]

Tyto přírodní katastrofy mají za následek další krizové situace. Může se jednat například o přerušení dodávek vody, potravin či energií. Jelikož si příroda nevybírá, tak tyto situace zasahují obytné zóny, památky, ale také zdravotnická zařízení. Zde je ovšem nezbytné, aby byla poskytována zdravotní péče i v době krizové situace.

Odpovědným orgánem pro oblast krizového řízení ve zdravotnictví je Ministerstvo zdravotnictví České republiky. Listina základních práv a svobod uvádí, že *každý má právo na ochranu zdraví. Občané mají na základě veřejného (zdravotního) pojištění právo na bezplatnou zdravotní péči a na zdravotní pomůcky za podmínek, které stanoví zákon.* [5] Ministerstvo zdravotnictví uvádí, že jeho *úkolem v krizovém řízení je prostřednictvím tvorby a prosazování státní zdravotní politiky zajistit rámcové podmínky pro poskytování zdravotní péče při mimořádných událostech a za krizových stavů.* [6]

Krizová připravenost ve zdravotnictví v České republice je definována jako *schopnost poskytovatelů zdravotnických služeb a zdravotnických zařízení zajistit nezbytnou zdravotní péči obyvatelstvu místně příslušného správního celku za krizových stavů a za mimořádných událostí v kontinuitě medicínských zásad pro poskytování zdravotní péče odborně způsobilými pracovníky.* [6]

Jako jeden z problémů Světové zdravotnické organizace (WHO) je připravenost nemocnic na katastrofy. [7] Stále neexistuje žádný standardní a platný nástroj pro hodnocení nemocnic na katastrofy. [8] Manažeři katastrof potřebují platné a účinné nástroje pro vyhodnocování připravenosti nemocnic na katastrofy. Pro tento účel však neexistuje standardizovaný a komplexní nástroj. [9]

Cílem tohoto článku je komparační analýza krizové připravenosti nemocnic ve Zlínském kraji a následný návrh hodnotícího nástroje pro hodnocení krizové připravenosti nemocnic v oblasti nouzového zásobování energií.

1. PROCESNÍ VYJÁDŘENÍ RIZIK

Každá nemocnice je ohrožována řadou mimořádných událostí a krizových situací. V tomto případě byly brány pouze naturogenní hrozby, které způsobují domino efekt a dále způsobují další a další katastrofy. Byly identifikovány tyto základní hrozby pro nemocnice:

- přívalová povodeň,
- vydatné srážky,
- extrémní vítr,
- povodeň,
- požár velkého rozsahu.

Následující diagram znázorňuje procesní vyjádření vlivu větrné smršti na objekty.

Obr. 1 Procesní vyjádření vlivu větrné smršti

Z historických událostí představují větrné smršti velká rizika pro Českou republiku, které mají za následek blackout. Můžeme brát příklad z orkánu Kyrill v roce 2007, orkánu Emma v roce 2008 či orkánu Herwart v roce 2017. Z diagramu jsou patrné následky takových větrných smrští, které v konečném důsledku mívají často za následek blackout. Pokud tato situace nastane, tak jsou zasaženy také nemocnice, které musí v takových stavech zajišťovat lékařskou pomoc. V případě, že nastane blackout, nemocnice musí využít nouzových zdrojů energie. Každá nemocnice je připravena na nouzové zásobování energií rozdílným způsobem. Následující analýza poukáže na rozdílnost v krizové připravenosti nemocnic.

2. METODA

Pro účely zhodnocení současného stavu krizové připravenosti nemocnic byla použita heuristická analýzy připravenosti. Tato metoda je založena na kvantitativním hodnocení připravenosti nemocnic na nouzové zásobování. Díky tomuto hodnocení získáme přesnou představu o slabých a silných stránkách hodnocených nemocnic. V rámci hodnocení byl použit soubor hodnotících otázek, který byl rozdělen do pěti kategorií.

Nouzové zásobování vodou – tato kategorie má za úkol zhodnotit, zdali je nemocnice připravena na výpadek vody – pitné a užitkové. Je hodnoceno, jak dlouho je nemocnice schopna vydržet z vlastních zásob vody. Dále je hodnoceno, zdali má nemocnice smluvně zajištěny dodavatele pitné vody – balené, v cisterně. Je nutné hodnotit také oblast užitkové vody, která je nutná k chodu zdravotnického zařízení. V poslední části je hodnoceno zajištění suchých toalet v době výpadku užitkové vody. Nouzové zásobování potravinami – tato kategorie hodnotí, zdali je v nemocnici vystavěna vývařovna. V případě, že dojde k výpadku zásobování potravinami, je hodnoceno, zdali má nemocnice zásoby potravin. Dále je hodnoceno, zdali má nemocnice smluvně zajištěny dodavatele teplého jídla, dodávky pokrmů či hotových jídel. Nouzové zásobování energií – tato kategorie hodnotí připravenost nemocnice z hlediska nouzových dodávek energií – vlastnictví agregátů pro nahrazení dodávek energie. Ovšem tyto agregáty jsou závislé na pohonných hmotách, a proto je nutné zhodnotit zásobování nemocnice pohonnými hmotami. Je zde řešena oblast smluvního zajištění pohonných hmot, vlastní benzinové pumpy apod. Další nouzové zásobování – tato kategorie jen okrajově zjišťuje zásobování nemocnice z hlediska dodávek léků, krve, krevní plazmy, zdravotnického materiálu a jejich smluvní zajištění. Kapacita nemocnice – tato kategorie řeší aktuální kapacity nemocnice. Je zde hodnocena dostupnost volných lůžek, lékařského personálu, hospitalizovaných. Dále je u hospitalizovaných důležité řešit jejich rozdělení (děti/dospělí, diety, akutnost). Na základě výše uvedené metody bylo provedeno vyhodnocení za pomocí následujícího vztahu:

$$PZZ = \frac{V + H}{2\ x\ H}\ x\ 100 \quad (1)$$

Kde, „PZZ“ představuje připravenost zdravotnického zařízení, „V“ představuje součet výsledků (získaných bodů) a „H“ představuje počet hodnocených heuristik.

Hodnotící metodika spočívala v přiřazení odpovědi ke každé zodpovězené otázce ve formě ohodnocení z předdefinované množiny hodnot (-1 = nesplňuje; 0 = částečně splňuje, 1 = splňuje; prázdné pole pokud otázka není relevantní).

3. VÝSLEDKY

Tato kapitola se zabývá výsledky hodnocení nemocnic z hlediska jejich krizové připravenosti. Nemocnice mají rozdílné financování a rozdílné vedení nemocnice. Každá nemocnice se k této problematice staví vlastní cestou, jelikož není zákonem přímo dáno, na co musí být nemocnice připravena.

Vzhledem k tomu, že se jedná o citlivé informace, nebudou uváděny přímo názvy nemocnic, ale budou pouze náhodně označeny čísly. Hodnocení probíhalo dle zmíněné metody - heuristické analýzy připravenosti nemocnic.

Nemocnice 1

Kategorie	**Počet otázek**	**Počet odpovědí**	**Získané body**	**Skóre**
Voda	9	6	-2	33,34%
Potraviny	11	9	-2	38,89%
Energie	9	8	1	56,25%
Ostatní	7	7	3	71,43%
Kapacity	8	8	8	100%
Celkem	**44**	**38**	**8**	**59,98%**

Tab. 1 Analýza krizové připravenosti nemocnice 1

Tabulka 1 znázorňuje výsledky analýzy krizové připravenosti nemocnice č. 1. Celková připravenost nemocnice je dle zvolené metody hodnocení 59,98%. Mezi nejlépe hodnocenou kategorii patří online kapacity nemocnice, které jsou na výborné úrovni. Z hlediska nouzového zásobování nemocnice – zbývající čtyři kategorie, byla nejlépe hodnocena oblast ostatní, kde spadá nouzové zásobování krví, krevní plazmou, zdravotnickým materiálem apod. Naopak mezi nejhůře hodnocenou kategorii patří nouzové zásobování vodou.

Nemocnice 2

Kategorie	**Počet otázek**	**Počet odpovědí**	**Získané body**	**Skóre**
Voda	9	6	0	50%
Potraviny	11	5	1	60%
Energie	9	7	1	57,14%
Ostatní	8	6	4	83,34%
Kapacity	8	6	6	100%
Celkem	**45**	**30**	**12**	**70,096%**

Tab. 2 Analýza krizové připravenosti nemocnice 2

Tabulka 2 znázorňuje výsledky analýzy krizové připravenosti nemocnice č. 2. Celková připravenost nemocnice je dle zvolené metody hodnocení 70,096%. Mezi nejlépe hodnocenou kategorii patří opět online kapacity nemocnice. Z hlediska nouzového zásobování nemocnice – zbývající čtyři kategorie, byla nejlépe hodnocena oblast ostatní, kde spadá nouzové zásobování krví, krevní plazmou, zdravotnickým materiálem apod. Naopak nejhůře hodnocenou kategorií je opět nouzové zásobování vodou.

Nemocnice 3

Kategorie	**Počet otázek**	**Počet odpovědí**	**Získané body**	**Skóre**
Voda	9	6	-2	33,34%
Potraviny	11	6	0	50%
Energie	9	7	1	57,14%
Ostatní	8	8	6	87,50%
Kapacity	8	7	-1	42,86%
Celkem	**45**	**34**	**4**	**54,168%**

Tab. 3 Analýza krizové připravenosti nemocnice 3

Tabulka 3 znázorňuje výsledky analýzy krizové připravenosti nemocnice č. 3. Celková připravenost nemocnice je dle zvolené metody hodnocení 54,168%. Mezi nejlépe hodnocenou kategorii patří oblast ostatní, kde spadá nouzové zásobování krví, krevní plazmou, zdravotnickým materiálem apod. Naopak nejhůře hodnocenou kategorií je opět nouzové zásobování vodou. V případě této nemocnice online kapacity získaly méně než 50%.

Nemocnice 4

Kategorie	**Počet otázek**	**Počet odpovědí**	**Získané body**	**Skóre**
Voda	9	6	2	66,67%
Potraviny	11	9	1	55,56%
Energie	9	8	6	87,5%
Ostatní	8	8	2	62,5%
Kapacity	8	8	4	75%
Celkem	**45**	**39**	**15**	**69,45%**

Tab. 4 Analýza krizové připravenosti nemocnice 4

Tabulka 4 znázorňuje výsledky analýzy krizové připravenosti nemocnice č. 4. Celková připravenost nemocnice je dle zvolené metody hodnocení 69,45%. Mezi nejlépe hodnocenou kategorii patří oblast energií, kde spadají kapacity nemocnice z hlediska počtu agregátů, pohonných hmot do těchto agregátů a případně dalších smluvních dodávek. Naopak nejhůře hodnocenou kategorií je nouzové zásobování potravinami. V případě této nemocnice online kapacity získaly 75%.

Nemocnice 5

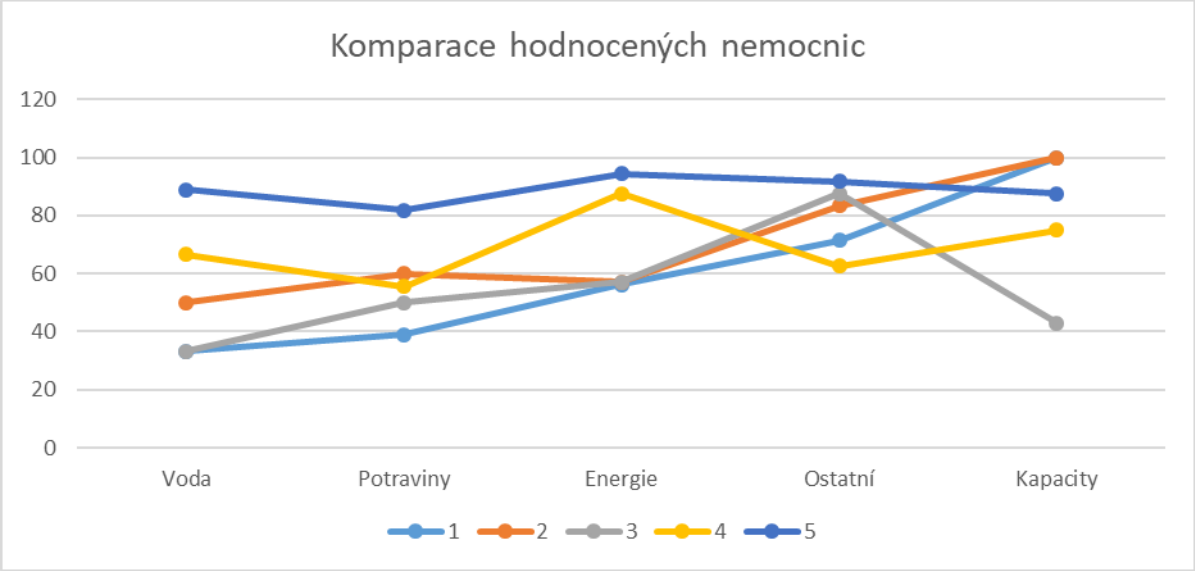
Kategorie	**Počet otázek**	**Počet odpovědí**	**Získané body**	**Skóre**
Voda	9	9	7	88,89%

Potraviny	11	11	7	81,81%
Energie	9	9	8	94,45%
Ostatní	6	6	5	91,67%
Kapacity	8	8	6	87,5%
Celkem	**43**	**43**	**33**	**88,87%**

Tab. 5 Analýza krizové připravenosti nemocnice 5

Tabulka 5 znázorňuje výsledky analýzy krizové připravenosti nemocnice č. 5. Tato nemocnice nespadá do Zlínského kraje, ale byla hodnocena z důvodu vysoké krizové připravenosti. O tom svědčí také celková připravenost nemocnice, která je dle zvolené metody hodnocení 88,87%. Mezi nejlépe hodnocenou kategorii patří oblast energií, kde spadají kapacity nemocnice z hlediska počtu agregátů, pohonných hmot do těchto agregátů a případně dalších smluvních dodávek. Naopak nejhůře hodnocenou kategorií je nouzové zásobování potravinami. V případě této nemocnice online kapacity získaly 87,5%.

Následující graf znázorňuje komparaci hodnocených nemocnic.



Obr. 2 Komparační analýza hodnocených nemocnic

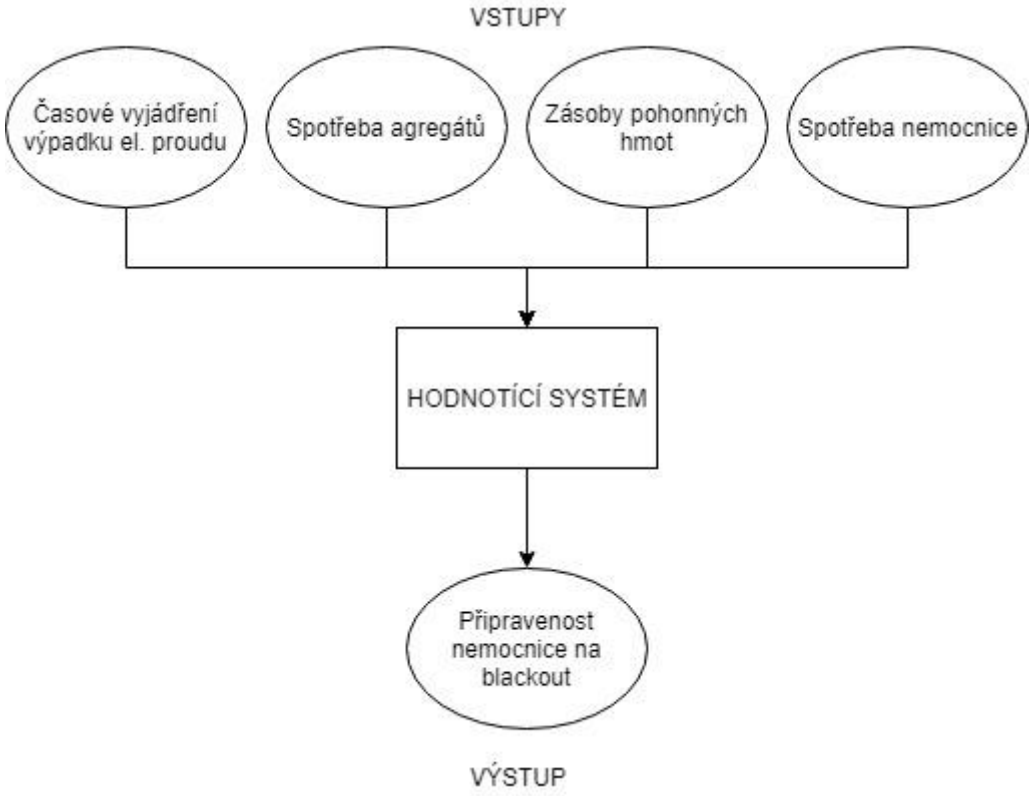
Z grafu je patrné, že celkově mezi nejhůře hodnocenou kategorii patří nouzové zásobování vodou a poté zde spadá nouzové zásobování potravinami. Naopak mezi nejlépe hodnocenou kategorii patří online kapacity nemocnice. Z hlediska nouzového zásobování nemocnice – zbývající čtyři kategorie, byla nejlépe hodnocena oblast ostatní, kde patří nouzové zásobování krví, krevní plazmou, zdravotnickým materiálem apod.

4. DISKUZE

Cílem článku bylo zhodnocení krizové připravenosti nemocnic ve Zlínském kraji. Každá nemocnice je povinna poskytovat lékařkou péči, což bezesporu platí také v době krizové situace. Tyto situace mohou být způsobeny různými faktory. Nemocnice může být zasažena přírodní katastrofou přímo či pouze jako následek krizové situace v okolí. Takovou událostí může být větrná smršť, která může způsobit pády stromů na elektrické vedení. Tato mimořádná událost má poté za následek přerušení dodávek elektrické energie koncovým

uživatelům. Jedním z těchto uživatelů můžou být také nemocnice. Je tedy nezbytné, aby byly na tyto situace připraveny.

V současné době neexistuje hodnotící systém, který by odhalil, zda je nemocnice připravena na nastalou krizovou situaci – výpadek elektrického proudu – blackout. Pro tyto účely bude navržen algoritmus, který bude hodnotit připravenost nemocnice na blackout.



Obr. 3 Návrh hodnotícího systému nemocnic

Obrázek znázorňuje návrh algoritmu, který dokáže určit, zda je nemocnice připravena čelit blackoutu, a na jak dlouho bude mít zásoby. V opačném případě dokáže učit, kolik pohonných hmot, či další agregáty bude potřebovat.

ZÁVĚR

Cílem článku bylo provedení komparační analýzy krizové připravenosti nemocnic ve Zlínském kraji. Byla provedena komparační analýza u čtyř nemocnic ve Zlínském kraji a jedné nemocnice mimo tento kraj. Účelem této analýzy bylo zjištění úrovně krizové připravenosti a zhodnocení současného stavu. Nemocnice mohou být ohroženy řadou mimořádných událostí, které mohou přejít do krizové situace. Je tedy nezbytné, aby byly nemocnice schopny poskytovat lékařskou péči i v těchto situacích. Pro tyto účely byl v závěru článku nastíněn návrh algoritmu pro hodnocení připravenosti nemocnice při blackoutu.

PODĚKOVÁNÍ

Tento výzkum vznikl na základě podpory Interní grantové agentury Univerzity Tomáše Bati ve Zlíně, projektu IGA/FAI/2018/001 a Ústavu bezpečnostního inženýrství, Fakulty aplikované informatiky.

Literatura

[1] ŘEHÁK, David, Bohumír MARTÍNEK a Petra RŮŽIČKOVÁ. Ochrana obyvatelstva v kontextu aktuálních bezpečnostních hrozeb. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2015. SPBI Spektrum. Červená řada. ISBN 978-80-7385-169-9.

[2] SENA, Aderita, Carlos CORVALAN and Kristie EBI. Climate Change, Extreme Weather and Climate Events, and Health Impacts. In: Freedman B. (eds) Global Environmental Change. Handbook of Global Environmental Pollution, vol 1. Springer, Dordrecht, 2014.

[3] Gathering, transmitting or losing defense information [online], 2012. [cit. 2018-07-10]. Dostupné na WWW: http://uscode.house.gov/download/pls/18C37.txt

[4] CIOCA, Marius a Lucian-Ionel CIOCA. Decision support for disaster management. Operations Management Research. 2010, vol. 3, no. 1-2, s. 68-79. ISSN 1936-9735.

[5] Česká republika. Listina základních práv a svobod. In Sbírka zákonů, Česká republika. 1992, roč. 1993, částka 1, Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=22426>. ISSN 1211-1244.

[6] FIŠER, Václav. Krizové řízení v oblasti zdravotnictví, modul J. Praha, 2006.

[7] ARDALAN, Ali et al, Hospitals safety from disasters in I.R.iran: the results from assessment of 224 hospitals, 2014.

[8] JETKINS, JL et al, Review of hospital preparedness instruments for National Incident Management System compliance, 2009.

[9] HEIDARANLU, Esmail et al, Hospital Disaster Preparedness Tools: a Systematic Review, 2015.

Krizové řízení a řešení krizových situací 2018
Sborník příspěvků z konference

Editor:
Ing. et Ing. Jiří Konečný, Ph.D.

Vydavatel:
Univerzita Tomáše Bati ve Zlíně, nám. T. G. Masaryka 5555, 760 01 Zlín

Uherské Hradiště 2018

Vydání I.

Vydáno elektronicky

www.krizoverizeni-uh.cz

ISBN: 978-80-7454-821-5