VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA BEZPEČNOSTNÍHO INŽENÝRSTVÍ

ŽILINSKÁ UNIVERZITA V ŽILINE
Fakulta bezpečnostného inžinierstva

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Vysoká škola báňská – Technická univerzita Ostrava
Fakulta bezpečnostního inženýrství

Žilinská univerzita v Žiline
Fakulta bezpečnostného inžinierstva

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

ve spolupráci se

Sdružením požárního a bezpečnostního inženýrství, z.s.

Sborník přednášek

MLADÁ VĚDA 2026

XXI. ročníku mezinárodní konference mladých vědeckých pracovníků a doktorandů

13. – 14. dubna 2026
Ostrava

VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA BEZPEČNOSTNÍHO INŽENÝRSTVÍ

ŽILINSKÁ UNIVERZITA V ŽILINE
Fakulta bezpečnostného inžinierstva

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Vysoká škola báňská – Technická univerzita Ostrava
Fakulta bezpečnostního inženýrství

Žilinská univerzita v Žiline
Fakulta bezpečnostného inžinierstva

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

ve spolupráci se

Sdružením požárního a bezpečnostního inženýrství, z.s.

Sborník přednášek

MLADÁ VĚDA 2026

XXI. ročníku mezinárodní konference mladých vědeckých pracovníků a doktorandů

13. – 14. dubna 2026
Ostrava

MLADÁ VĚDA 2026
Sborník přednášek XXI. ročníku mezinárodní konference mladých vědeckých pracovníků a doktorandů

Editor: prof. Ing. David Řehák, Ph.D.

Nebyla provedena jazyková korektura
Za věcnou správnost jednotlivých příspěvků odpovídají autoři
ISBN 978-80-7385-286-3

Konference se koná pod záštitou

prof. Dr. Ing. Aleše Bernatíka

děkana Fakulty bezpečnostního inženýrství VŠB – Technické univerzity Ostrava

ODBORNÝ GARANT KONFERENCE:

David ŘEHÁK	VŠB – Technická univerzita Ostrava, Česká republika

VĚDECKÝ VÝBOR KONFERENCE:

Milan ADÁMEK	Univerzita Tomáše Bati ve Zlíně, Česká republika
Karla BARČOVÁ	VŠB – Technická univerzita Ostrava, Česká republika
Aleš BERNATÍK	VŠB – Technická univerzita Ostrava, Česká republika
Jacek DWORZECKI	Jan Dlugosz University in Czestochowa, Polsko
Martin HROMADA	Univerzita Tomáše Bati ve Zlíně, Česká republika
Roman JAŠEK	Univerzita Tomáše Bati ve Zlíně, Česká republika
Petr KUČERA	VŠB – Technická univerzita Ostrava, Česká republika
Marek KULCZYCKI	Uniwersytet Wrocławski, Polsko
Tomáš LOVEČEK	Žilinská univerzita v Žiline, Slovenská republika
Vladimír MÓZER	České vysoké učení technické v Praze, Česká republika
Balázs Vince NAGY	Budapest University of Technology and Economics, Maďarsko
Witalis PELLOWSKI	Wyższa Szkoła Oficerska Wojsk Lądowych, Polsko
Jiří POKORNÝ	VŠB – Technická univerzita Ostrava, Česká republika
Marzena PÓŁKA	Szkoła Główna Służby Pożarniczej, Polsko
Jozef RISTVEJ	Žilinská univerzita v Žiline, Slovenská republika
Marek RYBAKOWSKI	Uniwersytet Zielonogórski, Polsko
Eva SVENTEKOVÁ	Žilinská univerzita v Žiline, Slovenská republika
Katarzyna TOBÓR-OSADNIK	Politechnika Śląska, Polsko
Jiří VOJTĚŠEK	Univerzita Tomáše Bati ve Zlíně, Česká republika
Mike ZEEGERS	Security Risk Watch, Nizozemsko

ORGANIZAČNÍ VÝBOR KONFERENCE:

Lenka ČERNÁ	Sdružení požárního a bezpečnostního inženýrství, z.s.
Stanislava KUBACZKOVÁ	Sdružení požárního a bezpečnostního inženýrství, z.s.
Patricie GAMONOVÁ	VŠB – Technická univerzita Ostrava, Česká republika
Ondřej RYŠKA	VŠB – Technická univerzita Ostrava, Česká republika

Obsah

Sorpcia pohonného agregátu za použitia textilných sorpčných materiálov **7**
Dušan Bóna, Iveta Marková

Využitie a aplikovanie metód krízového manažmentu v cykle krízového riadenia **14**
Ivan Buday

Časoprostorová heterogenita kriminality v rámci samopodněcujících bodových procesů **25**
Karolina Dlouhá, Lukáš Pospíšil, Radomír Ščurek

Vektor narušenia mäkkého cieľa **32**
Martin Flodr

Navržený postup posouzení rizik pro spolupráci člověka s robotem **40**
Kristýna Hamříková

Examining the Dynamics of Youth Crime and Delinquency in the Regions of the Slovak Republic **52**
Samuel Hubočan, Katarína Kampová

SWOT analýza vybraných kultúrnych pamiatok **61**
Michal Huliak, Iveta Marková

Interaktívny AI agent pre prácu s geografickými informačnými systémami **68**
Daniel Chovanec, Jozef Ristvej, Jozef Kubás, Ivan Buday

Hodnocení připravenosti jednotlivce na zvládání násilných incidentů **76**
Lukáš Kotek, Martin Hromada

Návrh hodnocení bezpečnostních opatření měkkých cílů **86**
Pavel Král, Dora Kotková, Martin Hromada

Využitie umelej inteligencie v kriminalistickom objasňovaní – tvorba kriminalistických verzií **97**
Lukáš Lencsés, Veronika Adamová

Skenovanie zraniteľností ako nástroj kybernetickej odolnosti pri ochrane kritickej infraštruktúry v podmienkach SR **106**
Timotej Mačuha, Katarína Kampová

Plošné bezpečnostní vzdělávání prostřednictvím technologie Text to speech **112**
Tereza Mičulková, Martin Hromada, Dora Kotková, Lukáš Kotek

Riziká vyplývajúce z používania pokrokových monitorovacích technológií **120**
Michal Miške

Komunikační vzorce organizovaných teroristických skupin a osamělých aktérů v online prostředí **129**
Jana Neuwirthová, Martin Haváček

Vliv koncentrace vodných roztoků methanolu na teploty vzplanutí **136**
Vojtěch Pelech, Hana Věžníková

Komparatívna analýza súladu vnútroštátnej legislatívy v oblasti kybernetickej bezpečnosti s regulačnými rámcami Európskej únie (NIS2, CER, DORA a AI Act) **144**
Martin Pipíška, Katarína Kampová

Mediálny tréning pre príslušníkov Hasičského a záchranného zboru **155**
Mária Pohanková Zahatlanová

Security Incident Reporting in Hospitals and its Application in the Risk Management Process **162**
Vladimír Pustay

Experimentálne stanovenie teploty vzplanutia a teploty vznietenia jaseňa štíhleho (Fraxinus excelsior) a smreku obyčajného (Picea abies) **169**
Anna Mária Rajnohová, Linda Makovická Osvaldová

Psychosociální rizika ve výrobním prostředí: Případová studie z automobilového průmyslu **179**
Karolína Šablaturová, Hana Halíčková

Ekonomicko-sociální aspekty ergonomie v kontextu české legislativy: rámec pro vyčíslení přínosů ergonomických projektů **185**
Dariusz Trachta

Návrh riešenia rozdelenia poskytovateľov zdravotnej záchrannej služby na Slovensku **193**
Lukáš Valla

Effect of Physical Load on Physiological Parameters of Students During Patient Transport **201**
Tatiana Verešová

Možnosti numerického modelovania indukovaných rázových vĺn vo vybraných softvérových nástrojoch **216**
Sebastián Vojtáš, Miroslav Mynarz, Juraj Sinay

Investície do bezpečnosti železničnej infraštruktúry a ochrana života **226**
Drahoslav Vyšný, Martin Flodr

Manažment rizík technickej kompatibility pri implementácii technologických zmien v priemyselnom procese **239**
Alžbeta Žerebáková

Sorpcia pohonného agregátu za použitia textilných sorpčných materiálov

Dušan Bóna[1], Iveta Marková[2]

[1] Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva,
1. mája 32, 01026 Žilina, dusan.bona@uniza.sk

[2] Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva,
1. mája 32, 01026 Žilina, iveta.markova@uniza.sk

Abstrakt:

Článok sa zameriava na podrobné určenie sorpčnej kapacity textilných sorpčných materiálov pri vystavení vybraným nebezpečným látkam, so špecifickým dôrazom na naftu ako modelový kontaminant. Nafta predstavuje významné environmentálne riziko. Štúdia bola realizovaná v súlade so štandardom ASTM F726-17, ktorý špecifikuje metodiku hodnotenia sorpčnej kapacity sorbentov pre ropné látky a iné kvapaliny. Metodika bola primerane prispôsobená konkrétnym laboratórnym podmienkam, pričom sa zachovala reprodukovateľnosť a porovnateľnosť výsledkov. Experimentálny postup zahŕňal presne definované kroky prípravy vzoriek, kontrolu teploty prostredia a minimalizáciu vonkajších vplyvov, ktoré by mohli ovplyvniť presnosť meraní. V laboratórnych experimentoch bolo testovaných šesť typov textilných sorbentov, rozdelených do troch základných kategórií: hydrofóbne, chemické a univerzálne. Pred samotným testovaním boli vzorky sorbentov kondicionované za štandardizovaných podmienok vlhkosti a teploty, aby sa zabezpečila ich hmotnostná stabilita. Následne boli presne odvážené analytickými váhami s vysokou presnosťou. Každá vzorka bola ponorená do vopred stanoveného a kontrolovaného objemu nafty na dobu 24 hodín, čím sa umožnila maximálna saturácia materiálu. Rozdiel medzi počiatočnou a konečnou hmotnosťou predstavoval množstvo absorbovanej látky. Na základe týchto údajov bola vypočítaná sorpčná kapacita, vyjadrená v gramoch absorbovanej látky na gram sorbentu (g/g) a v mililitroch na gram (ml/g). Výsledky boli štatisticky spracované a porovnané medzi jednotlivými typmi sorbentov. Výsledky štúdie poskytujú dôležité poznatky pre praktickú aplikáciu textilných sorbentov v oblasti environmentálnej ochrany, havarijného manažmentu a priemyselnej bezpečnosti. Zistenia môžu slúžiť ako podklad pre výber vhodného sorpčného materiálu v závislosti od typu kontaminantu a konkrétnych podmienok zásahu, čím prispievajú k efektívnejšiemu a ekologicky zodpovednému riešeniu environmentálnych záťaží.

Kľúčové slova: sorpčná kapacita, nebezpečné látky, textilné sorbenty, ASTM F726-17, nafta.

1 Úvod

Pojem sorbent označuje skupinu prevažne tuhých materiálov, ktoré sú schopné viazať na svojom povrchu plynné alebo kvapalné látky. Ak sa sorbent dostane do kontaktu napríklad s roztokom anorganických solí, môže dôjsť k zníženiu koncentrácie jednej alebo viacerých zložiek roztoku. V niektorých prípadoch je tento jav pozorovateľný aj voľným okom, najmä ak sa oddelená látka zachytí na povrchu sorbentu s vysokou sorpčnou účinnosťou. Hoci každá tuhá látka disponuje určitou sorpčnou schopnosťou, jej intenzita sa môže výrazne líšiť. Táto vlastnosť súvisí s nábojovou a väzbovou nerovnováhou atómov na medzifázovom rozhraní. Snaha systému o vyrovnanie tejto nerovnováhy vedie k hromadeniu molekúl alebo iónov na povrchu pevnej fázy [1].

Termín sorpcia predstavuje súhrnné označenie pre dva rozdielne procesy. Pri zachytávaní molekúl plynu alebo kvapaliny tuhou látkou prebiehajú dva základné deje. Prvým je ich zhromažďovanie na povrchu pevnej látky, čo sa označuje ako adsorpcia. Druhým procesom je prenikanie molekúl do vnútra štruktúry materiálu, ktoré sa nazýva absorpcia. V mnohých prípadoch prebiehajú oba mechanizmy súčasne, a preto sa často používajú pod spoločným názvom sorpcia, aj keď môže ísť prevažne len o jeden z uvedených dejov. Podobná terminologická nepresnosť sa vyskytuje aj pri používaní pojmov adsorbent a sorbent, ktoré sa nie vždy dôsledne rozlišujú [2].

2 Textilné sorpčné materiály

Fungovanie týchto absorbentov je založené na schopnosti rozliatej kvapaliny zachytiť sa a priľnúť na ich povrch. Vyrábajú sa najmä z polypropylénu spracovaného do formy jemných mikrovlákien, pričom tento materiál je zdravotne nezávadný. Vyznačujú sa vysokou nasiakavosťou – dokážu absorbovať kvapaliny v množstve predstavujúcom niekoľkonásobok ich vlastnej hmotnosti. Textilné materiály tohto typu sú určené predovšetkým na zachytávanie organických látok, ako sú ropné produkty či surová ropa [3, 9].

Pri hodnotení ich vlastností sa kladie dôraz najmä na sorpčnú schopnosť, teda mieru, do akej je materiál schopný absorbovať alebo nasať ropnú látku či inú uniknutú kvapalinu. V súčasnosti neexistuje jednotný normatívny postup na posudzovanie sorpčnej účinnosti týchto materiálov. Odborné zdroje však uvádzajú, že textilné sorbenty môžu dosahovať sorpčnú kapacitu až približne pätnásťnásobku svojej vlastnej hmotnosti. Ich objemová hmotnosť sa pohybuje približne v rozmedzí 900 až 920 $kg.m^{-3}$ [4, 8].

Významnou prednosťou týchto sorbentov je možnosť ich opakovaného použitia pri dlhšie trvajúcich zásahoch. Po nasýtení je možné materiál mechanicky vyžmýkať a následne znovu aplikovať, avšak len do momentu, kým nedôjde k prekročeniu jeho maximálnej sorpčnej kapacity. V praxi sa uprednostňujú najmä také sorbenty, ktoré sú ľahké, jednoducho manipulovateľné a konštrukčne nenáročné [5, 8].

Textilné sorbenty sa vyrábajú v rôznych formách, napríklad ako:

- norné steny,
- sorpčné pásy a upchávky,
- sorpčné drviny,
- sorpčné hady,
- sorpčné vankúše,
- stieracie mopy,
- koberce a rohože.

Medzi hlavné výhody textilných sorbentov patrí:

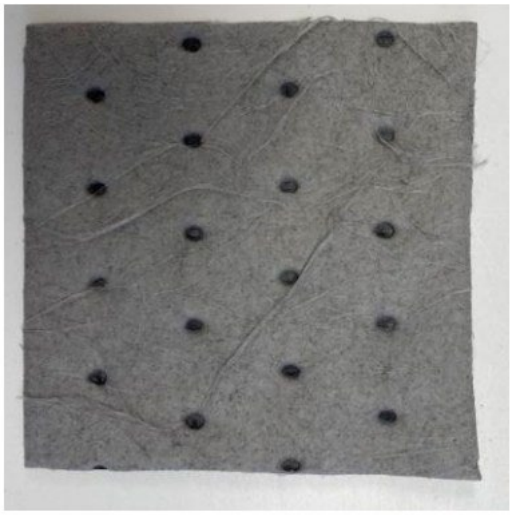
- ich účinnosť nezávislá od hrúbky vrstvy uniknutej látky,
- možnosť opakovaného použitia,
- schopnosť zachytenú látku z materiálu odčerpať a potenciálne znovu využiť,
- relatívna nezávislosť ich aplikácie od poveternostných podmienok [5].

2.1 Experimentálne vzorky

Pre vykonaný experiment bolo použitých celkovo 6 druhov textilných sorpčných materiálov. Použité materiály boli: Hydrofóbny sorpčný perforovaný koberec spevnený HKZP4040, Hydrofóbny sorpčný perforovaný koberec základný HKP2446, Chemický sorpčný koberec spevnený perforovaný CKZP4040, Neznámy sorpčný koberec (v práci označovaný ako žltý chemický koberec), Univerzálny sorpčný ľahký koberec spevnený perforovaný UKZP4040, Univerzálny sorpčný koberec základný UK4450.

Univerzálne sorbenty:

- Univerzálny sorpčný ľahký koberec spevnený perforovaný UKZP4040.
- Univerzálny sorpčný koberec základný UK4450text.



Obrázok 1. UKZP4040 (UA)

Obrázok 2. UK 4450 (UB)

Hydrofóbne sorbenty:

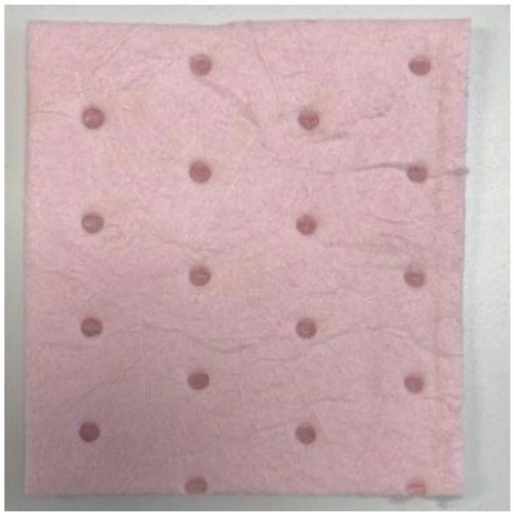
- Hydrofóbny sorpčný perforovaný koberec spevnený HKZP4040.
- Hydrofóbny sorpčný perforovaný koberec základný HKP2446text.

Obrázok 3. HKZP4040 (HA)

Obrázok 4. HKP2446 (HB)

Chemické sorbenty:

- Chemický sorpčný koberec spevnený perforovaný CKZP 4040.
- Žltý chemický koberec (CHB).



Obrázok 5. CKZP4040 (CHA)

Obrázok 6. Žltý chemický koberec (CHB)

3 Experimentálny postup

Pri určovaní sorpčnej kapacity je možné použiť šesť rozdielnych postupov (v našom laboratóriu). Pre konkrétny článok sme zvolili postup podľa normy ASTM F726-17.

Norma definuje postup testovania schopnosti sorpčných materiálov adsorbovať olej. Tento postup umožňuje porovnávať sorpčné kapacity rôznych typov sorbentov pri absorpcii oleja. Vzorky sorpčných materiálov a vybraných nebezpečných látok by mali byť kondicionované pri teplote 23 ± 4 °C [6].

Pomôcky: testovacia nádoba na zvolenú nebezpečnú látku, sieťkový kôš, svorka, pravítko, nožnice, sorpčná podložka, váhy, zberná nádoba a testovacia kvapalina – nebezpečná látka.

Vzorky: Ak je hrúbka sorbentu menšia ako 2,5 cm, hladina testovacej kvapaliny by mala byť 2,5 cm. Ak hrúbka sorbentu presahuje 2,5 cm, hladina kvapaliny musí byť aspoň rovnaká ako hrúbka sorbentu. Textilný sorbent sa nareže na štvorce s rozmermi 13 · 13 cm². Každá testovacia vzorka by mala mať hmotnosť najmenej 4 g [6].

Postup testovania (opakuje sa trikrát pre každú vzorku):

Pripravené vzorky sorbentu sa odvážia a zaznamenajú sa ich hmotnosti. Testovacia nádoba sa naplní požadovaným množstvom testovacej kvapaliny a sorbent sa do nej vloží tak, aby voľne plával. Sorbent zostáva v nádobe 24 hodín ± 30 minút. Po uplynutí tejto doby sa vzorky vyberú, pripevnia svorkou na okraj nádoby a nechajú sa odkvapkať. Následne sa umiestnia nad zbernú nádobu, opäť sa odvážia a namerané hodnoty sa použijú na výpočet.

Výsledky sa vyjadria výpočtom podľa predpísaného vzorca [6]:

$$adsorpcia = \frac{s_s}{s_0} \quad (1)$$

Kde: S_0 je hmotnosť suchej vzorky v gramoch,
S_s je vypočítaná hmotnost sorbovaného oleja,
S_t hmotnosť zmáčanej vzorky v gramoch.

$$s_s = s_t - s_0 \quad (2)$$

Vykonali sme dva pokusy. Do nádoby sme naliali 1,8 litra nafty aby siahala do výšky 2,5 cm. Do nádoby sme následne vložili vzorky sorbentov a zopakovali sme postup stanovený normou, upravený na naše podmienky dvakrát. V Tabuľke 1 môžeme vidieť namerané hodnoty pre sorpciu motorovej nafty podľa ASTM F726-17, hmotnosť suchej vzorky a zmáčanej vzorky, hmotnosť adsorbovanej látky, výslednú adsorpčnú kapacitu a adsorpčnú kapacitu vzoriek v mililitroch na gram skúšobnej vzorky.

Tabuľka 1. Namerané hodnoty pre sorpciu nafty podľa ASTM F726-17

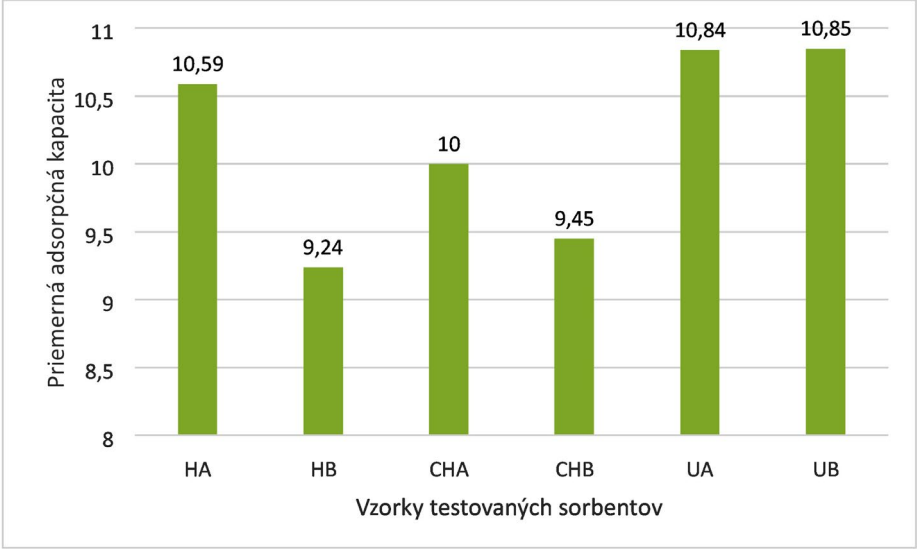
Vzorky	Hmotnosť suchej vzorky [g]	Hmotnosť zmáčanej vzorky [g]	Množstvo nasorbovanej látky [g]	Adsorpčná kapacita	Adsorpčná kapacita [ml/g]
Hydrofóbny sorpčný perforovaný koberec spevnený biely HA					
HA1	6,32	74,05	67,73	10,72	13,02
HA2	6,91	79,22	72,31	10,46	12,72
Hydrofóbny sorpčný perforovaný koberec základný biely HB					
HB1	5,61	60,17	54,56	9,73	11,82
HB2	5,71	55,72	50,01	8,76	10,64
Chemický sorpčný koberec spevnený perforovaný ružový CHA					
CHA1	6,65	72,32	65,67	9,88	12,00
CHA2	6,18	68,78	62,6	10,13	12,31
Chemický žltý sorpčný koberec CHB					
CHB1	6,36	66,29	59,93	9,42	11,45
CHB2	6,32	66,54	60,22	9,48	11,52
Univerzálny sorpčný ľahký koberec spevnený perforovaný šedý UA					
UA1	6,58	77,83	71,25	10,83	13,16
UA2	6,82	80,81	73,99	10,85	13,18
Univerzálny sorpčný koberec základný šedý UB					
UB1	7,18	86,16	78,98	11,00	13,37
UB2	7,44	87,07	79,63	10,70	13,01

Na základe získaných výsledkov sme zistili, že najmenšiu priemernú adsorpčnú kapacitu nafty 9,24 násobku priemernej hmotnosti suchého sorbentu mali vzorky hydrofóbneho sorbentu HB. Druhú najmenšiu priemernú adsorpčnú kapacitu 9,45 mali vzorky chemického sorbentu CHB. Vzorky chemického sorbentu CHA mali priemernú adsorpčnú kapacitu 10,00. Priemerná adsorpčná kapacita vzorky HA bola 10,59 násobku pôvodnej priemernej hmotnosti sorbentu. Najlepšiu priemernú adsorpčnú kapacitu mali vzorky univerzálneho sorbentu UB 10,85 a UA 10,84. Výsledné hodnoty sú uvedené v tabuľke 7.15 Priemerná adsorpčná kapacita motorovej nafty.

Tabuľka 2. Priemerná adsorpčná kapacita motorovej nafty

Priemerná adsorpčná kapacita motorovej nafty					
Textilný sorbent	HA	HB	CHA	CHB	UA
Priemerná adsorpčná kapacita	10,59	9,24	10,00	9,45	10,84

Na Obrázku 7 môžeme vidieť v grafe porovnanie priemernej adsorpčnej kapacity motorovej nafty.



Obrázok 7. Porovnanie priemernej adsorpčnej kapacity

4 Záver

Cieľom príspevku bolo posúdiť sorpčnú kapacitu vybraných textilných sorpčných materiálov pri kontakte s motorovou naftou, ktorá bola použitá ako modelová nebezpečná látka. Experimentálne merania boli realizované podľa metodiky stanovenej normou ASTM F726-17, ktorá umožňuje hodnotenie a vzájomné porovnanie sorpčných vlastností materiálov používaných pri odstraňovaní ropných látok z prostredia. Na základe získaných výsledkov možno konštatovať, že všetky skúmané sorbenty vykazovali relatívne vysokú sorpčnú schopnosť. Namerané hodnoty sa pohybovali približne v intervale od 9 do 11-násobku hmotnosti pôvodne suchého sorbentu. Najvyššiu priemernú sorpčnú kapacitu dosiahli univerzálne sorbenty typu UB a UA, ktoré absorbovali približne 10,84 až 10,85-násobok svojej vlastnej hmotnosti. Naopak najnižšia hodnota bola zaznamenaná pri hydrofóbnom sorbente HB, ktorého priemerná sorpčná kapacita dosiahla hodnotu 9,24. Rozdiely medzi jednotlivými sorpčnými materiálmi poukazujú na význam vhodného výberu sorbentu v závislosti od charakteru kontaminácie a konkrétnych podmienok zásahu.

Referencie

[1] JESENÁK, K., 2001. Biológia, ekológia, chémia. In: Prírodné sorbenty a ich využitie pri ochrane životného prostredia. Roč. 6, č. Mimoriadne číslo, s. 28-33. ISSN 1338-1453

[2] ORINČÁK M., 2016. Overenie účinnosti sorpčných materiálov pri zneškodňovaní chemických látok [online]. Časopis Krízový manažment, dostupné na internete: https://krm.uniza.sk/pdfs/krm/2016/01/05.pdf

[3] MARKOVÁ, I. 2003. Ekologické prostriedky pre likvidáciu unikajúcich látok pri zásahu hasičov. In Riešenie krízových situácií v špecifickom prostredí. Žilina: TU Žilina, 2003. ISBN 80-8070-090-7, s. 311–317

[4] MARKOVÁ, I. 2006. Sorbenty – prostriedky používané pri zachytávaní uniknutej nebezpečnej látky na vodnej hladine. In Riešenie krízových situácií pri úniku nebezpečnej látky na vodných hladinách. Zvolen: TU, 2006. ISBN 80-228-1574-8, s. 41–50

[5] MARKOVÁ, I. 2009. Ekologické prostriedky na zachytávanie nebezpečných látok uniknutých v dôsledku dopravnej nehody. In Súčinnosť záchranných zložiek integrovaného záchranného systému pri dopravných nehodách na pozemných komunikáciách [CD-ROM]. Žilina: Wettrans, 2009. s. 8. ISBN 978-80-85418-67-5

[6] ASTM F726-17 (2024), Standard Test Method for Sorbent Performance of Adsorbents for use on Crude Oil and Related Spills

[7] Hydrophilic Definition [online]. Electronic portal Biology Online, dostupné na internete: https://www.biologyonline.com/dictionary/hydrophilic

[8] Hydrophobic Definition [online]. Electronic portal Biology Online, dostupné na internete: https://www.biologyonline.com/dictionary/hydrophobic

[9] Oleophilic: A Powerful Tool for Environmental and Water Treatment [online]. Electronic portal Simply Explained, dostupné na internete: https://www.tidjma.tn/en/glenv/oleophilic/

Využitie a aplikovanie metód krízového manažmentu v cykle krízového riadenia

Ivan Buday[1]

[1] Žilinská univerzita v Žiline, Katedra krízového manažmentu,
1. mája 32, 010 26 Žilina, buday@uniza.sk

Abstrakt:

Článok sa zaoberá komparáciou vybraných analytických, rozhodovacích a technologických prístupov využívaných v krízovom manažmente, pričom zahŕňa tradičné metodologické postupy aj moderné analytické nástroje. Pozornosť je venovaná významu vhodného výberu metód, keďže ich správna aplikácia výrazne ovplyvňuje efektívnosť rozhodovania, koordináciu činností a priebeh zvládania krízových situácií. Spracovanie vychádza zo systematickej analýzy odbornej literatúry, na základe ktorej sú identifikované vybrané tradičné a moderné metódy krízového manažmentu a ich uplatnenie v jednotlivých fázach cyklu krízového riadenia. Dôraz je kladený najmä na moderné metódy, ktoré v súčasnosti predstavujú významný nástroj podpory hodnotenia rizík, prognózovania a riadenia krízových situácií. Článok poukazuje na skutočnosť, že metódy krízového manažmentu nemožno vnímať izolovane, ale ako súčasť vzájomne prepojeného systému činností, ktorý tvorí ucelený cyklus krízového riadenia. Ich systematické a kombinované využívanie umožňuje objektívnejšie posudzovanie ohrození, zvyšovanie úrovne pripravenosti a efektívnejšie znižovanie negatívnych dopadov mimoriadnych udalostí na obyvateľstvo, majetok a územie. Prínos článku spočíva v systematizácii poznatkov o aplikácii metód krízového manažmentu v rámci cyklu krízového riadenia a vo vytvorení prehľadného metodického rámca využiteľného v teoretickej aj aplikačnej rovine, najmä ako podpora rozhodovania orgánov miestnej samosprávy a východisko pre ďalší výskum v oblasti krízového riadenia.

Klíčová slova: krízový manažment, cyklus krízového riadenia, metódy krízového manažmentu, mimoriadne udalosti, pripravenosť.

1 Úvod

Aktuálna bezpečnostná situácia vo svete prináša pre krízový manažment nové výzvy a situácie, na ktoré je potrebné adekvátne reagovať. V podmienkach rastúcich mimoriadnych udalostí nadobúda význam krízového manažmentu čoraz väčší dôraz na systematickom využívaní metód krízového manažmentu. Tieto metódy umožňujú racionálne rozhodovanie, koordináciu činností a efektívne využívanie zdrojov na vzniknuté udalosti. Vzhľadom na to predstavuje krízový manažment interdisciplinárnu oblasť zameranú na predchádzanie vzniku mimoriadnych udalostí, prípravu na ich zvládanie, efektívnu reakciu počas ich priebehu a zabezpečenie obnovy po ich skončení. Dôležité postavenie v systéme krízového manažmentu má hlavne miestna samospráva, ktorá je základným prvkom pri riešení mimoriadnych udalostí. Úroveň jej pripravenosti závisí od uplatňovania vhodných metód, nástrojov a postupov krízového manažmentu na zvládnutie vzniku a priebehu mimoriadnej udalosti. Riadenie mimoriadnych udalostí sa v praxi najčastejšie opiera o model cyklu krízového riadenia. Krízové riadenie miestnej samosprávy či celkového štátu sa opiera hlavne na využívanie správnych metód, ktoré sa aplikujú počas pôsobenia mimoriadnej udalosti. Ich vhodný výber a využitie sa odzrkadľuje na priebehu riešenia. Tieto metódy predstavujú systematické postupy a nástroje využívané na analýzu rizík, plánovanie, rozhodovanie a hodnotenie pripravenosti rôznych subjektov zapojených do riešenia mimoriadnych udalostí. Ich uplatňovanie umožňuje zvyšovať efektívnosť riadenia krízových situácií a podporuje objektívne hodnotenie úrovne pripravenosti

miestnej samosprávy. Článok sa zameriava na popis, využitie a aplikovanie metód krízového riadenia pri riešení mimoriadnych udalostí v cykle krízového riadenia. Analýza sa zamerala na viaceré metódy a ich výhody, ktoré je možné aplikovať do krízového manažmentu. Súčasťou článku je opis ako možnosti aplikovania moderných metód do krízového manažmentu a ako by tieto metódy pomohli pri systematickom hodnotení pripravenosti, znižovaní zraniteľnosti a posilňovaní odolnosti miest a obcí v kontexte krízového riadenia.

Hlavným cieľom článku je analyzovať a komparovať vybrané metódy krízového manažmentu a poukázať na ich využitie v jednotlivých fázach cyklu krízového riadenia.

2 Podstata a význam krízového manažmentu v cykle krízového riadenia

Zabezpečenie ochrany života, zdravia a majetku obyvateľov při rôznych udalostiach je jednou z najdôležitejších úloh, ktorými sa zaoberá krízový manažment. Práve vznik týchto udalostí a situácií predstavuje veľké ohrozenie nielen pre obce alebo mestá, ale hlavne aj pre celý štát. Na obyvateľstvo ale aj fungovanie štátu pôsobia rôzne mimoriadne udalosti, ktoré ohrozujú fungovanie štátu. Pod pojmom mimoriadna udalosť (MU) sa rozumie príhoda, ktorá je ťažko časovo predvídateľná, priestorovo ohraničená a závažná a je spôsobená živelnou pohromou, technologickými alebo technickými haváriami, prípadne úmyselným konaním a vyvoláva narušenie stability daného systému, jeho dejov a činností. Mimoriadna udalosť ohrozuje zdravie, život, kultúrne a hmotné statky ako aj životné prostredie [1]. Podľa zákona č. 42/1994 Z. z. o civilnej ochrane sa mimoriadnou udalosťou berie živelná pohroma, havária, katastrofa, ohrozenie verejného zdravia II. stupňa, smogová situácia, narušenie dodávok tepla, nežiadúci výskyt medveďa hnedého, hromadný prílev cudzincov na územie Slovenskej republiky či teroristický útok [1]. Chrániť je potrebné aj počas krízových situácií, ktoré definuje zákon č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu je krízová situácia popsiovaná ako obdobie kedy je narušená bezpečnosť štátu a vzniká ohrozenie mimo času vojny a vojnového stavu. Počas tohto obdobia sa môže vyhlásiť výnimočný, núdzový stav alebo mimoriadna situácia [2].

Zákon č. 42/1994 Z. z. o civilnej ochrane pojem okrem definovania mimoriadnej udalosti popisuje aj mimoriadnu situáciu (MS), ktorá sa vyhlasuje v období počas ktorého pôsobia následky z MU na zdravie, život a majetok. Po vyhlásení sa vykonávajú opatrenia určené na záchranu majetku, zdravia a života občanov ako aj na minimalizáciu rizík ohrozenia a zamedzeniu následkov MU. Vyhlasuje sa a odvoláva pomocou informačných prostriedkov (rozhlas, masmédia a iné). Počas vyhlásenia MS sú osoby povinné poskytovať vecné plnenie alebo pracovnú povinnosť ak ich na to vyzve príslušný orgán [1].

V dôsledku vzniku MU je nutné zabezpečiť, aby sa táto udalosť dokázala efektívne riešiť, riadiť a poskytovať pomoc zasiahnutým osobám. Z toho dôvodu je nutne zabezpečiť krízové riadenie, ktoré zabezpečuje činností orgánov krízového riadenia na monitorovanie, analýzu a vyhodnotenie rizík a rôznych ohrození. Úlohou krízového riadenia je aj plánovanie, príprava a prijímanie preventívnych opatrení pri riešení krízových situácií. Zásady krízového riadenia je nevyhnutné uplatňovať vo všetkých sférach verejnej správy [3]. Orgány krízového riadenia sú:

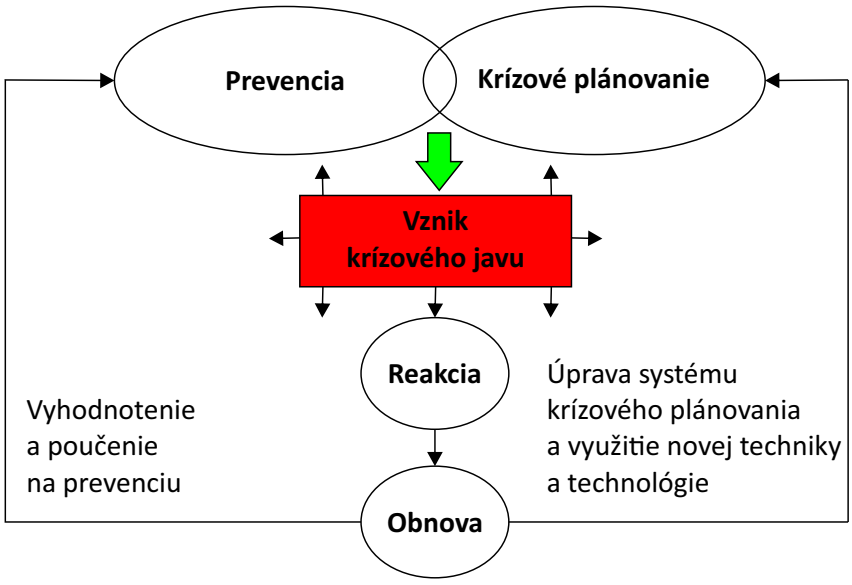
- Vláda Slovenskej republiky,
- bezpečnostná rada,
- ministerstvá,
- Národná banka Slovenska,
- bezpečnostná rada kraja,
- obvodný úrad,
- bezpečnostná rada okresu,

- obec,
- vyšší územný celok [2].

Hlavným pojmom v krízovom riadení je práve krízový manažment. Viacerí autori definujú tento pojem rôzne, avšak základ vychádza z terminologického slovníka krízového riadenia a zásady jeho používania, kde je definovaný ako: „Súhrn činností vecne príslušných inštitúcií určených na analýzu bezpečnostných rizík a ohrození, na monitorovanie rizikových činiteľov, na prevenciu vzniku krízových situácií a na plánovanie, organizovanie, uskutočňovanie a kontrolu činností určených na vytváranie podmienok na riešenie a na samotné riešenie krízových situácií“ [4].

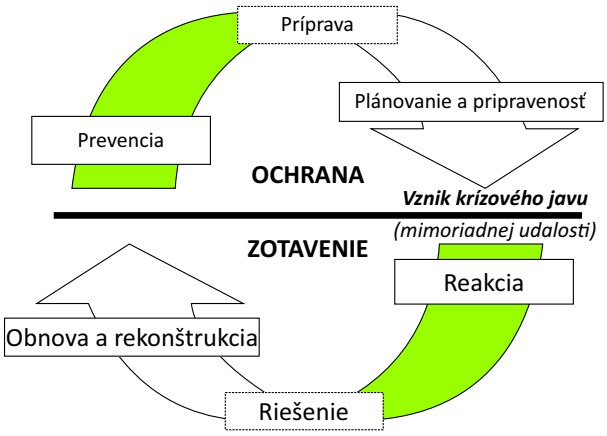
Krízový manažment má za úlohu posudzovať a predvídať vznik aj priebeh krízových javov, odhaľovať riziká, ktoré ohrozujú bezpečnosť dejov a procesov. Medzi jeho hlavné úlohy patrí pripravenosť, zabezpečenie preventívnych opatrení a hlavne predchádzanie vzniku krízových javov. Ďalšími úlohami je vytváranie predpokladu na riadenie krízových javov, adekvátne reagovanie a zabezpečenie obnovy systému do pôvodného stavu [5]. Tým umožňuje vytvoriť účinný systém s preventívnymi opatreniami, ktoré sú určené na predchádzanie vzniku krízových javov. Dôležité je aj vytvorenie vhodných podmienok na okamžitú reakciu v prípade vzniku krízovej situácie. Pri riešení konkrétnych kríz vytvára a používa dostatočné sily, nevyhnutné prostriedky a zdroje. Preto by mal byť krízový manažment nevyhnutnou súčasťou orgánov štátnej správy, samosprávy, vlády a ministerstiev. Pojem krízový manažment sa rozšíril do širšieho spoločenského prostredia a stal sa súčasťou práce manažérov, ktorí využívajú jeho metódy, postupy a nástroje nielen vo verejnej správe ale aj v podnikateľských subjektoch [6]. Hlavným zameraním krízového manažmentu je predovšetkým znižovanie rizík, ktoré súvisia s ohrozením a rovnako sa kladie dôraz na aktivity, ktoré zabezpečujú ochranu a bezpečnosť ľudí, životného prostredia a infraštruktúry. Preto je krízový manažment jeden z najdôležitejších systémov, ktorý dokáže ovplyvniť fungovanie štátu a má vplyv na pocity bezpečia občanov [7].

Na základe definovania úloh a princípov krízového manažmentu je možné charakterizovať model krízového riadenia. Tento model tvoria štyri prepojené fázy (prevencia, plánovanie, reakcia a obnova). Hlavnou podstatou modelu je riešenie vzniknutého krízového javu. Práve pomocou týchto fáz sa má jav riešiť. Obrázok 1 znázorňuje model krízového riadenia podľa Šimáka [6] Tento model vychádza z teoretických poznatkov riešenia javov.



Obrázok 1. Základný model krízového riadenia [6]

Na tento model následne nadviazal Ristvej [8], ktorý popísal model ako cyklus krízového riadenia. Cyklus končí vtedy, keď existuje predpoklad vzniku nového cyklu na riešenie krízového javu. Model cyklu je zobrazený na Obrázku 2.



Obrázok 2. Cyklus krízového riadenia [8]

Každá fáza na seba nadväzuje a prepája sa, čo tvorí celkový cyklus. Fáze plánovania predchádzajú pripravenosť a prevencia. Fáza prevencie zahŕňa tvorbu a prijímanie opatrení na zabránenie vzniku krízového javu. Pri fáze pripravenosti a plánovania je nutné mať pripravené plány, sily a prostriedky určené na vykonanie reakcie na vzniknutý jav. Fáza reakcie má za úlohu znížiť následky vzniknutej udalosti. Po reakcií nastáva fáza riešenia krízového javu a nakoniec nasleduje obnova zasiahnutého územia [8].

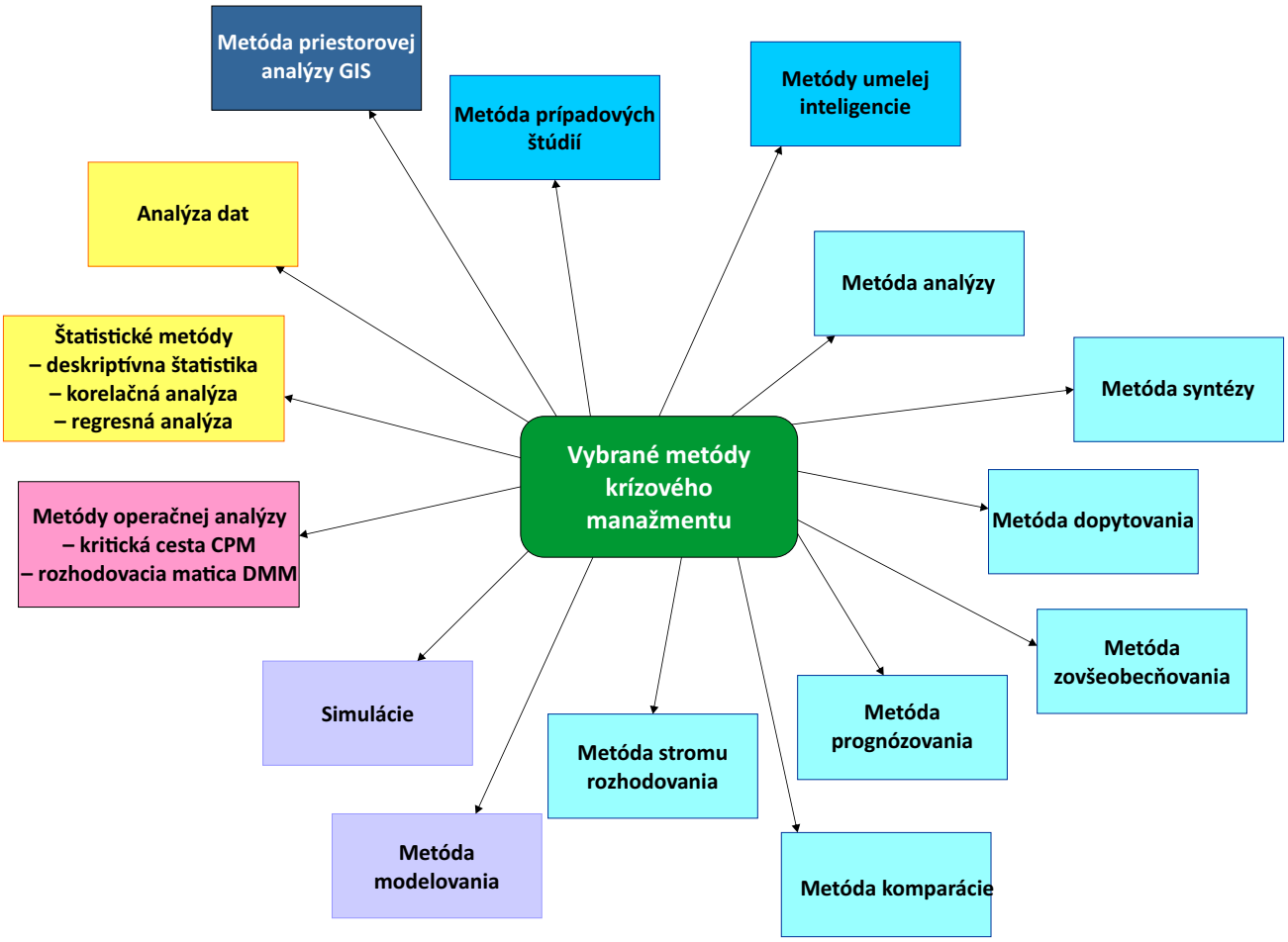
Novší a rozšírenejší model cyklu krízového riadenia predstavili autori [9] vo svojej publikácií „Vulnerability and disaster preparedness"- Zraniteľnosť a pripravenosť na katastrofy. Model je doplnený o viaceré fázy oproti modelu podľa Šimáka a Ristveja. Dôraz kladú autori hlavne na hrozby a zraniteľnosť systému, ktorý sa môže časom meniť a je nutné, aby model bol aplikovateľný aj mimo riešenia krízových javov. Ak nastane krízový jav, je nutné ho riešiť dokedy sa stav nenavráti do obdobia pred krízou. Model obsahuje aj menšie mini cykly, ktoré je nutné vykonať, aby sa celý cyklus mohol naplniť. Cyklus je znázornený na Obrázku 3.

Obrázok 3. Upravený cyklus krízového riadenia [10]

Navrhovaný cyklus krízového riadenia je koncipovaný ako komplexný a vzájomne prepojený proces, ktorý zahŕňa viacero na seba nadväzujúcich fáz. Jednotlivé fázy nie sú vnímané izolovane, ale tvoria kontinuálny systém, v ktorom sa výsledky predchádzajúcich krokov premietajú do ďalších činností. Cyklus je doplnený o rozšírené fázy zamerané nielen na reakciu na krízový jav, ale aj na jeho predchádzanie, systematickú prípravu, riešenie následkov a spätné hodnotenie. Takto koncipovaný prístup umožňuje efektívnejšie riadenie krízových situácií a prispieva k zvyšovaniu celkovej úrovne bezpečnosti a pripravenosti subjektov. [10]

3 Aplikovanie metód krízového manažmentu

Existuje množstvo vedeckých metód, ktoré majú uplatnenie v krízovom manažmente. Na Obrázku 4 sú zobrazené metódy, ktoré sa využívajú najčastejšie, avšak existuje ich viac a každý krízový manažér si môže zvoliť alebo vybrať metódu podľa potreby Tieto metódy často priamo podporujú jednotlivé fázy cyklu krízového riadenia. Vybrané metódy sú zlomkom metód, ktoré sú využívané v krízovom manažmente od posudzovania rizík, cez analyzovanie dát až po priame riešenie krízového javu.



Obrázok 4. Vybrané metódy krízového manažmentu [autor]

Metódy krízového manažmentu nachádzajú uplatnenie najmä pri identifikácii a analýze rizík, prognózovaní možného vývoja krízových situácií, výbere optimálnych variantov riešenia a následnom vyhodnocovaní účinnosti realizovaných opatrení. V praxi ide o kombináciu všeobecných vedeckých metód, operačných a rozhodovacích metód, štatistických postupov, priestorových analýz a moderných informačných technológií, vrátane využitia geografických informačných systémov a umelej inteligencie. Jednotlivé metódy sa v krízovom manažmente

navzájom dopĺňajú a ich využitie závisí od charakteru mimoriadnej udalosti, dostupných informácií a časového tlaku. Výber a aplikácia jednotlivých metód závisí od dostupnosti údajov, časových možností a charakteru mimoriadnej udalosti, pričom žiadna metóda sama o sebe neposkytuje univerzálne riešenie všetkých krízových problémov. Ich využívanie a aplikovanie je možné popísať priamo samotným cyklom krízového riadenia.

Metóda **analýzy** sa v krízovom manažmente aplikuje hlavne v preventívnej fáze a pri posudzovaní rizík. Analýza sa využíva na rozklad mimoriadnej udalosti alebo potenciálneho ohrozenia na časti ako sú zdroje rizika, ohrozené objekty, pravdepodobnosť výskytu a možné následky. Táto metóda dokáže identifikovať kľúčové faktory, ktoré môžu viesť k vzniku krízového javu a vytvára základ pre ďalšie hodnotenie a rozhodovanie. Metóda analýzy je nevyhnutná pri tvorbe krízových plánov a hodnotení pripravenosti územia alebo organizácie. Poukazujú na to aj štúdia, ktoré sa zameriavali práve na tvorbu procesu krízového riadenia, kde pomocou dôkladnej analýzy, myšlienkovej mapy a inými analytickými metódami skúmali ako sa obyvatelia pripravujú na mimoriadne udalosti a ako dokážu chápať tvorbu práve procesu krízového riadenia [11]. **Syntéza** nadväzuje na analytické spracovanie údajov a jej využívanie spočíva v prepájaní čiastkových poznatkov do uceleného celku. Je ju možné aplikovať pri tvorbe krízových plánov, opatrení a koordinácii záchranných zložiek. Syntéza umožňuje zosúladiť informácie z rôznych zdrojov (analýzy rizík, prognózy, štatistických údajov) a vytvoriť komplexný návrh riešenia mimoriadnej udalosti [12]. Poukazuje na aplikovanie práve syntézy v hodnotení hrozieb vplývajúcich na obyvateľstvo, kde odhaľuje medzery v teoretických poznatkoch, a tým aj v zlej pripravenosti obyvateľstva na mimoriadne udalosti. Metóda dopytovania sa využíva hlavne pri získavaní informácií z rôznych údajov ako sú napr. odborníci a obyvateľstvo. Využíva sa pri hodnotení pripravenosti, zisťovaní skúseností z predchádzajúcich mimoriadnych udalostí a pri identifikácii nedostatkov. Výsledky dopytovania slúžia ako podklad pre analýzu rizík, zlepšovanie a tvorbu krízových plánov a optimalizáciu preventívnych opatrení.

Zovšeobecnenie je možné aplikovať v krízovom manažmente pri vyhodnocovaní minulých krízových udalostí. Na základe opakujúcich sa znakov a skúseností je možné formulovať všeobecné závery, odporúčania a pravidlá pre zvládanie vzniku budúcich mimoriadnych udalostí. Aplikovanie metódy prispieva k zvyšovaniu pripravenosti systému krízového riadenia a k neustálemu zlepšovaniu preventívnych a reakčných opatrení [13]. **Prognózovanie** patrí k významným metódam využívaných najmä vo fáze prevencie a pripravenosti, ale aj počas samotnej reakcie na krízový jav. Je možné ho použiť na predvídanie vývoja mimoriadnej udalosti, jej následkov a celkovému priebehu. Rovnako je táto metóda využiteľná pri predpovedi šírenia povodní, požiarov alebo epidémie, čím sa umožňuje prijímanie včasných opatrení vo forme síl, prostriedkov a materiálu. Týmto je možné pripraviť strategické scenáre, odhadnúť pravdepodobnosť výskytu mimoriadnej udalosti a navrhnúť opatrenia na minimalizáciu jeho dopadov ako to popisujú [14].

Metódu **porovnávania** je možné použiť pri hodnotení rôznych variantov riešenia mimoriadnej udalosti alebo pri porovnávaní výsledkov zásahu. Poskytuje možnosť získať najvhodnejšie postupy a vyhodnotiť účinnosť prijatých opatrení. Je významná najmä v rozhodovacích procesoch a v etape obnovy po krízovej udalosti. Metóda **stromu rozhodovania** sa aplikuje predovšetkým vo fáze riadenia mimoriadnej udalosti, keď je nutné čo najskôr vybrať vhodný postup riešenia. Pomáha vizualizovať možné varianty vývoja krízovej situácie a ich dôsledky. Táto metóda podporuje systematické a transparentné rozhodovanie v podmienkach neistoty a časového tlaku [15].

Modelovanie a simulácie sú dôležitými nástrojom pri analýze zložitých mimoriadnych udalostí a poskytovania potrebných informácií na ich zvládanie Sú úzko spojené, čo má za následok, že by nemali samostatne význam z hľadiska krízového riadenia. Používajú sa na simulovanie vývoja mimoriadnych udalostí, testovanie krízových plánov a preverovanie pripravenosti či už jednotiek IZS, ale aj obyvateľstva. Výsledky modelovania poskytujú cenné informácie pre rozhodovanie a optimalizáciu opatrení. Zásadnú pozíciu zohrávajú aj z hľadiska

informačnej podpory krízového riadenia. Pre podporu krízového riadenia sa využíva program ALOHA, ktorý sa zaoberá simuláciou úniku nebezpečnej látky a analýzou možného zásahu oblasti touto látkou. Ďalším využívaním nástrojom je TerEx, ktorý slúži rovnako na úniky nebezpečných látok, ale hlavne na modelovanie a simuláciu možných teroristických útokov s využitím nebezpečných látok. Práva využívanie programov napomáha k lepšiemiu pochopeniu problematiky o únikoch nebezpečných látok. Modelovanie a simulovanie je možné využívať hlavne vo fázach plánovania, prípravy, ale aj v riešení. Výsledky modelov a simulácií poskytujú podklady pre rozhodovanie, lepšie rozdelenie zdrojov a zvýšenie pripravenosti daného systému na MU [16, 17, 18].

Metóda kritickej cesty (CPM) sa v krízovom manažmente využíva pri časovom plánovaní a koordinácii činností počas riešenia krízovej situácie. Umožňuje identifikovať najkritickejšie činnosti, ktorých oneskorenie by mohlo ohroziť úspešné zvládnutie krízy. Je vhodná najmä pri riadení obnovy a logistických procesov. Pri aplikácii metódy CPM sa jednotlivé činnosti krízového riadenia znázorňujú vo forme sieťového grafu. Každej činnosti je priradený čas trvania a väzby na ostatné činnosti, čím sa vytvára ucelený model časového priebehu riešenia mimoriadnej udalosti. Umožňuje určiť kritickú cestu (sled činností), ktoré priamo ovplyvňujú celkový čas zvládnutia MU. Je nutné dbať na zvýšenú pozornosť, pretože pri ich oneskorení môže dôjsť k neefektívnej reakcií na MU. Významným prínosom je pri simulovaní rôznych variantov vývoja MU a overovať reakčný čas systému krízového riadenia. Týmto spôsobom možno identifikovať slabé miesta v systéme, ako sú oneskorená komunikácia, nejasné kompetencie alebo nedostatočné personálne zabezpečenie. Rozhodovacia matica (DMM) sa používa pri viackriteriálnom hodnotení variantov riešenia MU. Poskytuje tak objektívne porovnávanie jednotlivých možnosti na základe stanovených kritérií, ako sú čas, náklady, účinnosť alebo riziko. Metóda podporuje transparentné a racionálne rozhodovanie [19, 20].

Štatistické metódy sú v krízovom manažmente dôležitým nástrojom na kvantitatívne zhodnotenie údajov, identifikáciu vzťahov medzi premennými a podporu rozhodovacích procesov v podmienkach neistoty a komplexnosti. Medzi základné metódy patria deskriptívna štatistika, korelačná analýza a regresná analýza, ktoré poskytujú objektívne podklady pre analýzu, prognózovanie a hodnotenie rizík či dopadov krízových situácií. Deskriptívna štatistika sa používa na opis a sumarizáciu údajov o MU. Je to metóda, ktorá spracováva získané dáta a poskytuje prehľad o ich základných charakteristikách, ako sú priemery, smerodajné odchýlky, rozdelenie alebo frekvencie. Takéto údaje sú kľúčové pri pochopení celkového priebehu MU [21]. Korelačná analýza sa v krízovom manažmente môže využiť na overenie súvislostí medzi intenzitou MU a inými faktormi, ako sú čas odozvy záchranných zložiek, počet zasiahnutých osôb alebo dopad následkov. Táto metóda dáva manažérom podklad pre lepšie pochopenie vzájomných väzieb v systéme krízového riadenia [22]. Regresná analýza sa v krízovom manažmente využíva na prognózovanie a testovanie hypotéz čím prináša poznatky, ako konkrétne faktory ovplyvňujú priebeh MU a následky. Regresné modely slúžia na odhad dopadu preventívnych opatrení na mieru škôd alebo na prognózovanie vývoja [22]. Metóda analýzy dát sa využíva na spracovávanie a vyhodnocovanie získaných údajov o MU, historických záznamoch či iných priestorových a štatistických údajoch. V krízovom manažmente má uplatnenie hlavne vo fázach posudzovania rizík, monitorovaní a hodnotení dopadov. Výsledky poskytujú podklady pre rozhodovanie, prognózovanie či tvorbu opatrení pre vznik nových MU. Analýza dát je súčasťou štatistických metód spomenutých vyššie [23].

Geografické informačné systémy (GIS) predstavujú technologický nástroj podporujúci aplikáciu metód priestorovej analýzy. Tieto systémy predstavujú v krízovom manažmente významný analytický nástroj, používaný n efektívnu prácu s priestorovo viazanými údajmi počas všetkých fáz krízového cyklu. GIS plnia funkciu hlavne na zber, ukladanie, spracovanie, analýzu a vizualizáciu geopriestorových dát, čím sa získavajú informácie o ohrozených územiach, infraštruktúre, obyvateľstve či dostupných zdrojoch. Poskytuje komplexný prehľad o situácii v území, čím zvyšuje situačné povedomie a podporuje kvalifikované rozhodovanie krízových manažérov. V priebehu riešenia krízových situácií slúži GIS na identifikovanie kritickej oblasti, plánovanie evakuačných trás,

či riadenie a zásahu a optimalizovanie síl a prostriedkov. Po krízovej udalosti sa GIS využíva na zhodnotenie rozsahu škôd a podieľa sa na plánovaní obnovy územia. V spojení s modernými analytickými nástrojmi, najmä umelou inteligenciou, sa GIS stáva kľúčovým podporným nástrojom pre efektívne a objektívne riadenie krízových situácií [24].

Prípadové štúdie umožňujú komplexné skúmanie priebehu udalosti, prijatie rozhodnutí či reakciu zodpovedných subjektov na MU. V krízovom manažmente sa využívajú hlavne vo fázach plánovania a pripravenosti vzhľadom na hodnotenie efektívnosti prijatých opatrení, identifikácií postupov a pri odhaľovaní nedostatkov v systéme krízového riadenia. Ich zastúpenie má aj fáza hodnotenia, nakoľko dokážu zbierať údaje z celého cyklu krízového riadenia a predložiť informácie o hodnotení zvládnutia riešenia danej MU. Výstupy prípadových štúdií slúžia ako podklad pre zlepšenie krízových plánov, tvorbu preventívnych opatrení ale aj na vzdelávanie odborníkov [25]. Význam prípadových štúdií a prenosu skúseností z praxe do vzdelávacieho procesu poukazujú aj medzinárodné projekty zamerané na implementáciu skúseností krízového manažmentu z krajín V4 do výučby, čím sa podporuje zvyšovanie pripravenosti budúcich odborníkov [27].

Umelá inteligencia (AI) predstavuje moderný technologický nástroj, ktorý podporuje analýzu dát, prognózovanie a rozhodovanie v krízovom manažmente. Algoritmy strojového učenia analyzujú historické údaje, rozpoznávajú vzory a vytvárajú prediktívne modely na predpovedanie budúcich udalostí a ich dopadov, čím zlepšujú pripravenosť a alokáciu zdrojov. AI sa tiež používa na monitorovanie v reálnom čase a systémy včasného varovania, ktoré detekujú anomálie na základe údajov zo senzorov, satelitov a sociálnych médií. Počas kríz pomáha identifikovať poškodené oblasti a optimalizovať intervencie, zatiaľ čo po udalosti podporuje hodnotenie škôd a plánovanie obnovy infraštruktúry [24]. Pri riešení núdzových situácií zohráva umelá inteligencia dôležitú úlohu v procese ochrany života, zdravia a majetku obyvateľstva, ale aj pri vytváraní plánov a postupov pre ďalšie riešenie MU. Technológie a komponenty používané AI sú kľúčové nástroje pre efektívne riadenie miest, najmä pri riešení a riadení MU a krízových situácií. Ich implementácia prispieva k zvýšeniu bezpečnosti, udržateľnosti a kvality života obyvateľov [26]. Používanie umelej inteligencie v riadení MU je veľmi sľubné. Umelá inteligencia má obrovský potenciál v riadení povodní, metódy založené na údajoch môžu výrazne zlepšiť celý cyklus krízového riadenia. Pomocou modelov strojového učenia trénovaných na historických hydrologických záznamoch, údajoch o zrážkach a topografických informáciách môže umelá inteligencia zlepšiť predpovede povodní a identifikovať oblasti, ktoré sú obzvlášť náchylné na zaplavenie. Podporuje tiež monitorovanie prichádzajúcich udalostí v reálnom čase pomocou senzorových prúdov a údajov diaľkového prieskumu Zeme, čo pomáha úradom skôr rozpoznať nebezpečné situácie a efektívnejšie alokovať zdroje [28].

Na základe uvedených charakteristík možno konštatovať, že jednotlivé metódy majú v krízovom manažmente široké aplikačné možnosti v rôznych fázach krízového cyklu, najmä v oblasti prevencie, plánovania, riadenia a hodnotenia mimoriadnych udalostí.

4 Záver

Vykonaná analýza poukazuje na to, že efektívnosť krízového riadenia je podmienená systematickým a koordinovaným využívaním vhodných metód krízového manažmentu v jednotlivých fázach cyklu krízového riadenia. Jednotlivé metódy majú svoje špecifické uplatnenie v závislosti od fázy, v ktorej sú aplikované, pričom ich význam spočíva najmä vo vzájomnej previazanosti a schopnosti podporovať rozhodovanie v podmienkach neistoty a časového tlaku, ktoré sú pre riešenie mimoriadnych udalostí typické. Analytické, štatistické a prognostické metódy zohrávajú kľúčovú úlohu najmä pri identifikácii rizík, prevencii a plánovaní, zatiaľ čo modelovanie, simulácie a rozhodovacie metódy nachádzajú významné uplatnenie počas reakcie na mimoriadne udalosti a v procese obnovy zasiahnutého systému. Prínos článku spočíva v systematickom prepojení vybraných

metód krízového manažmentu s jednotlivými fázami cyklu krízového riadenia, čím bol vytvorený prehľadný metodický rámec využiteľný nielen v teoretickej rovine, ale aj v aplikačnej praxi. Pozornosť bola venovaná najmä možnostiam praktického využitia metód pri hodnotení pripravenosti, plánovaní opatrení a zvyšovaní odolnosti území voči mimoriadnym udalostiam, najmä na úrovni miestnej samosprávy. Výsledky článku poukazujú na potrebu vnímať krízový manažment ako dynamický a neustále sa rozvíjajúci proces, ktorý si vyžaduje priebežné vyhodnocovanie skúseností a aktualizáciu používaných postupov. Do budúcnosti sa otvára priestor pre empirické overovanie navrhovaného metodického rámca v podmienkach konkrétnych území a typov mimoriadnych udalostí, ako aj pre hlbšie skúmanie možností využitia moderných nástrojov pri podpore rozhodovania v krízovom riadení.

Poděkování

Článok bol spracovaný v rámci projektu KEGA č. 046ŽU-4/2025 „Vzdelávacia online platforma pre prípravu obyvateľov na sebaochranu a vzájomnú pomoc a interaktívna vysokoškolská učebnica zameraná na problematiku civilnej ochrany, zároveň bol podporený Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-24-0153.

Reference

[1] Zákon č. 42/1994 Z. z. Zákon národnej rady Slovenskej republiky o civilnej ochrane obyvateľstva

[2] Zákon č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu

[3] BETUŠ, M. a kol. 2022. Výkladový slovník pojmov civilnej ochrany obyvateľstva, krízového riadenia a integrovaného záchranného systému. 1. vyd. Košice: Technická univerzita v Košiciach – FBERG, 2022. 176 s. ISBN 978-80-553-4049 4

[4] HOFREITER, L. 2004. Bezpečnosť, bezpečnostné riziká a ohrozenia. 1. vydanie. Žilina: EDIS vydavateľstvo UNIZA, 2004. 146 s. ISBN 80-8070-181-4

[5] RISTVEJ, J. – MITAŠOVÁ, V. – KUBÁS, J. 2024. Krízový manažment 2: Časť 1: Medzinárodný krízový manažment. 1. vyd. - Žilina: Žilinská univerzita v Žiline, 236 s., ISBN 978-80-554-2088-2

[6] ŠIMÁK, L. 2016. Krízový manažment vo verejnej správe. 2 vyd. Žilina: Žilinská univerzita v Žiline – EDIS, 2016. 263 s. ISBN 978-80-554-1165-1

[7] PIETREK, G. 2021. The Crisis Management and the Civil Protection in Poland. In: The Journal of Organizational Management Studies [online]. 2021. s. 1–10. [cit. 8-1-2026]. ISSN 2166-0816. Dostupné na: https://ibimapublishing.com/articles/JOMS/2021/847128/

[8] RISTVEJ, J. – ZAGORECKI, A. – RISKA, T. 2015. Krízový manažment II.- časť 2. Aplikačné softvéry v krízovom manažmente. 1. vydanie. Žilina: Žilinská univerzita v Žiline, EDIS. 2015. 272 s. ISBN 978-80-554-1073-9

[9] TITKO, M. – KUBÁS, J. 2023. Vulnerability and disaster preparedness. 1st edition. Lüdenscheid: RAM-Verlag. 2023. 129 p. ISBN 978-3-96595-037-5

[10] KUBÁS, J. 2024. Vplyv civilnej ochrany na dosiahnutie požadovanej úrovne bezpečnosti v miestnej samospráve s ohľadom na krízové javy. 1. vydanie. Žilina: Žilinská univerzita v Žiline: EDIS-vydavateľstvo UNIZA, 2024. 161 strán: Vedecké monografie. ISBN 9788055421612

[11] Avdhesh, J. 2020. Crisis Management: A Way Towards Being Human. Pamukkale Üniversitesi İşletme Araştırmaları Dergisi, 7(2), 288-307. https://doi.org/10.47097/piar.828702

[12] Kalbassi, C. Identifying Crisis Threats: A Partial Synthesis of the Literature on Crisis Threat Assessment with Relevance to Public Administrations. J Risk Anal Crisis Response 6, 110–121 (2016). https://doi.org/10.2991/jrarc.2016.6.3.1

[13] TRNEČKOVÁ, J. 2021 Komparace prognostických metod. InTrilobit. [online] . Zlín (Česko): Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky. [cit. 8-1-2026]. ISSN 1804-1795. Vydanie č. 1. Dostupné na: https://trilobit.fai.utb.cz/komparace-prognostickych-metod

[14] Tarasova, H., Kondrashova, L., Chuvasova, N., Kondrashov, M., & Tsikh, H. (2021). A combination of forecasting internal and external crises in managing the development of educational institution. Amazonia Investiga, 10(47), 35–46. https://doi.org/10.34069/AI/2021.47.11.4

[15] Song YY, Lu Y. Decision tree methods: applications for classification and prediction. Shanghai Arch Psychiatry. 2015 Apr 25;27(2):130-5. 10.11919/j.issn.1002-0829.215044

[16] JÁNOŠÍKOVÁ, M. - LACIŇÁK, M. 2021. VYUŽITIE SIMULÁCIÍ PRI RIEŠENÍ KRÍZOVÝCH JAVOV V DOPRAVE. In: Trilobit. [online]. Zlín (Česko): Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky. [cit. 8-1-2026]. ISSN 1804-1795. Vydanie č. 3. Dostupné na: https://trilobit.fai.utb.cz/Data/Articles/PDF/1d1053e9-0c1e-45f6-8fdf-b4f4e53a6608.pdf

[17] JÁNOŠÍKOVÁ, M. – RISTVEJ, J. 2018. PODPORA ROZHODOVANIA V KRÍZOVOM MANAŽMENTE PROSTREDNÍCTVOM SIMULÁCIÍ. In: Mladá veda. Prešov: UNIVERSUM [online]. 2018. roč. 6. č. 3. s. 71-80. [cit. 8-1-2026]. ISSN 1339-3189

[18] FEHÉR, L. 2012. Využitie modelovania a simulácie v rámci krízového riadenia vybraného subjektu [diplomová práca]. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. 82 s. 2012

[19] SLEMENSKÝ, M. 2020. MOŽNOSTI APLIKÁCIE METÓD OPERAČNEJ ANALÝZY V PROCESOCH KRÍZOVÉHO RIADENIA. In: Mladá veda. Prešov: UNIVERSUM [online]. 2010. roč. 8. č. 1. s. 251-265. [cit. 8-1-2026]. ISSN 1339-3189. Dostupné na: https://www.mladaveda.sk/casopisy/2020/01/01_2020_25.pdf

[20] MÁCA, J., LEITNER, B.: Operačná analýza pre bezpečnostný manažment. FŠI ŽU, Žilina 2002. Skriptá [online]. [cit. 8-1-2026]. Dostupné na: http://fbiw.uniza.sk/ktvi/leitner/2_predmety/OA/00_Priblizne_riesenie_AHP.pdf

[21] Wut TM, Xu JB, Wong SM. Crisis management research (1985-2020) in the hospitality and tourism industry: A review and research agenda. Tour Manag. 2021 ;85: 10.1016/j.tourman.2021.104307

[22] TITKO, M. - NOVÁK, L.- JÁNOŠÍKOVÁ, M. 2021. Praktická štatistika. [online]. Žilina: Žilinská univerzita v Žiline, EDIS – vydavateľstvo UNIZA, 2021. [cit. 8-1-2026]. ISBN 978-80-554-1814-8. Dostupné na: https://ukzu.uniza.sk/wp-content/uploads/2022/04/Skripta-Titko.pdf

[23] MUCHOVÁ, M. – PAĽOVÁ, D. 2020. Implementing a decision support system in the transport process management of small Slovak transport company. In: Journal of Entrepreneurship, Management and Inovation: vol. 6, issue 1, s. 75-106 [online]. Košice: JEMI. [cit. 08-01-2026]. ISSN 2084-4735. https://doi.org/10.7341/20201613

[24] Emami P, Marzban A. The Synergy of Artificial Intelligence (AI) and Geographic Information Systems (GIS) for Enhanced Disaster Management: Opportunities and Challenges. Disaster Med Public Health Prep. 2023. 17: e507. 10.1017/dmp.2023.174

[25] RISTVEJ, J, - KUBÁS, J. – KOLLÁR, B. 2024. METODICKÝ POSTUP RIEŠENIA PRÍPADOVÝCH ŠTÚDIÍ V KRÍZOVOM MANAŽMENTE. In: Mladá veda. Prešov: UNIVERSUM [online]. 2024. roč. 12. č. 3. s. 60-68. [cit. 8-1-2026]. ISSN 1339-3189. Dostupné na: https://www.mladaveda.sk/casopisy/2024/03/03_2024_06.pdf

[26] J. Lyu et al., “Intelligent-Technology-Empowered Active Emergency Command Strategy for Urban Hazardous Chemical Disaster Management,” Sustainability, vol. 15, no. 19, art. 14369, 2023. https://doi.org/10.3390/su151914369

[27] KUBÁS, J.; TITKO, M.; RISTVEJ, J.; STRELCOVÁ, S.; KELÍŠEK, A.; PETRLOVÁ, K. 2025. Implementation of crisis management experience from the V4 countries into the educational process. In: ICERI2025 – 18th Annual International Conference of Education, Research and Innovation. Seville (Spain), 10.–12. November 2025. Seville: IATED Academy, 2025. Dostupné na: https://library.iated.org/view/KUBAS2025IMP?re=downloadnotallowed

[28] RISTVEJ, J. – KUBÁS, J. – BUDAY, I. – CHOVANEC, D. 2025. INTEGRATION OF ARTIFICIAL INTELLIGENCE INTO SMART CITIES FOR ENHANCED EMERGENCY PREPAREDNESS In Proceedings of the 25th International Scientific Conference on Earth and Planetary Sciences SGEM

Časoprostorová heterogenita kriminality v rámci samopodněcujících bodových procesů

Karolina Dlouhá[1], Lukáš Pospíšil[2], Radomír Ščurek[3]

[1] VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství,
Lumírova 13, 700 30 Ostrava, karolina.dlouha@vsb.cz

[2] VŠB – Technická univerzita Ostrava, Fakulta stavební,
Ludvíka Podéště 17, 708 00 Ostrava, lukas.pospisil@vsb.cz

[3] VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství,
Lumírova 13, 700 30 Ostrava, radomir.scurek@vsb.cz

Abstrakt:

Kriminalita představuje dynamický časoprostorový jev, jehož intenzita i mechanismus vzniku se mohou výrazně lišit mezi jednotlivými částmi území. Přesto jsou mnohé analytické přístupy založeny na předpokladu homogenního chování v celém sledovaném prostoru nebo pracují pouze s agregovanými daty, která potlačují lokální rozdíly. Tento článek se zaměřuje na problematiku časoprostorové heterogenity kriminality a diskutuje možnosti jejího zachycení pomocí parametrických samo-podněcujících bodových procesů. Text systematicky shrnuje vývoj metod od deskriptivních přístupů založených na segmentaci prostoru a časovém vyhlazování k procesnímu modelování jednotlivých incidentů. Zvláštní pozornost je věnována limitům globálních modelů a potřebě segmentovaného rámce, v němž jsou dynamické charakteristiky odhadovány odděleně pro strukturálně odlišné oblasti. Studie tak vymezuje metodologický posun od popisu prostorových vzorců k analýze mechanismů, které tyto vzorce vytvářejí, a vytváří teoretický základ pro další rozvoj časoprostorového modelování kriminality.

Klíčová slova: časoprostorová analýza, heterogenita kriminality, bodové procesy, Hawkesův proces, near-repeat efekt, segmentace prostoru.

1 Úvod

Kriminalita je jevem, který se nevyvíjí náhodně ani rovnoměrně. Její výskyt je podmíněn kombinací sociálních, ekonomických a environmentálních faktorů, které se liší nejen mezi regiony, ale často i v rámci jednotlivých městských čtvrtí. Vedle prostorové variability vykazuje kriminalita také výraznou časovou dynamiku – sezónní výkyvy, krátkodobé nárůsty i dlouhodobější trendy. Zachycení těchto souvislostí představuje jednu z klíčových výzev současné bezpečnostní analýzy.

Tradiční přístupy k analýze kriminality se opírají především o agregované statistiky, hustotní mapy nebo regresní modely, které umožňují identifikovat oblasti se zvýšeným rizikem výskytu trestné činnosti [1, 2]. Tyto metody jsou cenné z hlediska vizualizace a základní orientace v datech, jejich interpretace však zůstává převážně deskriptivní. Neodpovídají na otázku, jakým mechanismem jednotlivé incidenty vznikají a zda mezi nimi existuje dynamická vazba.

V reakci na tento limit se v posledních letech prosazují přístupy založené na modelování kriminality jako časoprostorového bodového procesu. Zejména samo-podněcující (Hawkesovy) modely umožňují rozlišit základní intenzitu výskytu trestné činnosti od její reaktivní složky, která je spojována s tzv. near-repeat efektem,

tedy zvýšenou pravděpodobností opakování incidentu v blízkém čase a prostoru [3, 4]. Tento procesní pohled představuje významný metodologický posun od pouhého popisu vzorců k analýze jejich dynamiky.

Současně se však většina aplikací těchto modelů opírá o předpoklad homogenní dynamiky v rámci celého sledovaného území. Takový předpoklad může vést k potlačení lokálních rozdílů a ke zkreslené interpretaci parametrů modelu. Otázka časoprostorové heterogenity kriminality proto zůstává otevřeným problémem, který vyžaduje systematičtější teoretické uchopení.

Cílem tohoto článku je analyzovat problematiku časoprostorové heterogenity kriminality a diskutovat možnosti jejího zachycení pomocí parametrických samo-podněcujících modelů. Text se zaměřuje na vymezení metodologických limitů globálních přístupů a na formulaci koncepčního rámce, který umožňuje oddělené modelování strukturálně odlišných oblastí.

2 Vývoj přístupů k časoprostorové analýze kriminality

2.1 Deskriptivní a hustotní přístupy

První systematické pokusy o prostorovou analýzu kriminality byly založeny na identifikaci tzv. hotspotů, tedy oblastí s nadprůměrnou koncentrací trestné činnosti. Tyto přístupy vycházejí především z práce s bodovými daty o incidentech a jejich transformace do hustotních map pomocí metod kernel density estimation (KDE) nebo jejich prostorově-časových rozšíření [1, 5]. Výsledkem jsou vizuálně přehledné mapy rizika, které umožňují identifikovat lokální koncentrace událostí.

Význam těchto metod spočívá zejména v jejich interpretační srozumitelnosti a praktické využitelnosti pro plánování bezpečnostních opatření. Systematický přehled studií zaměřených na prostorovou predikci kriminality však ukazuje, že většina těchto přístupů zůstává na úrovni popisu prostorových vzorců a pracuje s předem zvolenou prostorovou agregací [2]. Volba velikosti mřížky či šířky vyhlazovacího jádra přitom může významně ovlivnit výslednou strukturu hotspotů.

Vedle čistě prostorových metod se rozvíjely i postupy kombinující prostorové shlukování s časovým vyhlazováním. Tyto přístupy umožňují identifikovat nejen místa zvýšeného výskytu kriminality, ale také rozdílné typy časového vývoje [6]. Přesto zůstávají převážně deskriptivní – jejich cílem je klasifikace či typologie, nikoli modelování samotného generujícího procesu.

2.2 Modelování kriminality na úrovni agregovaných jednotek

Vedle deskriptivního mapování se výzkum kriminality postupně zaměřil na modely, jejichž cílem bylo vysvětlit rozdíly v míře trestné činnosti mezi jednotlivými oblastmi. Tyto přístupy vycházejí z předpokladu, že prostorová distribuce kriminality souvisí s charakteristikami prostředí – například hustotou obyvatelstva, socioekonomickou strukturou nebo urbanistickým uspořádáním [7].

Modely tohoto typu umožňují kvantifikovat vztah mezi intenzitou kriminality a vybranými faktory a identifikovat proměnné, které s výskytem trestné činnosti statisticky souvisejí. V novějších studiích jsou tyto vztahy modelovány i pomocí flexibilnějších datově orientovaných přístupů, které dokážou zachytit složitější závislosti v rozsáhlých datech [8, 9].

Společným rysem těchto modelů je však práce s územními jednotkami definovanými předem – například administrativními celky nebo pravidelnou mřížkou. Kriminalita je zde chápána jako míra či počet incidentů v dané jednotce během určitého období. Dynamika jednotlivých událostí tak ustupuje do pozadí a analytická pozornost se soustředí především na rozdíly mezi oblastmi.

2.3 Přechod k procesnímu modelování

Zásadní metodologický posun nastává ve chvíli, kdy kriminalita přestává být chápána jako agregovaná míra v určité oblasti a období, ale jako posloupnost jednotlivých událostí v čase a prostoru. V tomto rámci je každá událost reprezentována konkrétním časem a polohou a analytickým cílem se stává modelování jejich vzájemné struktury.

Procesní přístup pracuje s pojmem intenzity bodového procesu, která vyjadřuje okamžitou pravděpodobnost výskytu nové události podmíněnou historií předchozích incidentů. Tento pohled umožňuje zkoumat nejen to, kde je kriminalita koncentrována, ale také zda a jak na sebe jednotlivé incidenty navazují.

Zvláštní význam zde mají samo-podněcující procesy, které předpokládají, že výskyt jedné události může krátkodobě zvýšit pravděpodobnost dalších událostí v jejím okolí. Tento mechanismus odpovídá empiricky pozorovanému near-repeat efektu a byl opakovaně potvrzen v městském prostředí [3, 4].

Tímto krokem se analytická pozornost přesouvá od popisu distribuce k modelování dynamiky. Současně se však otevírá otázka, zda lze tuto dynamiku popsat jednotným modelem pro celé území, nebo zda je třeba uvažovat o strukturální heterogenitě v rámci sledovaného prostoru.

3 Samo-podněcující bodové procesy jako teoretický rámec

Procesní perspektiva chápe kriminalitu jako realizaci časoprostorového bodového procesu, tedy jako posloupnost jednotlivých událostí definovaných časem a polohou. Namísto práce s agregovanými počty incidentů v předem daných jednotkách se modeluje mechanismus generování událostí. Klíčovým pojmem se zde stává intenzita procesu, která vyjadřuje okamžitou míru výskytu nové události podmíněnou historií předchozích incidentů.

Základní tvar samo-podněcujícího (Hawkesova) procesu lze zapsat jako:

$$\lambda(t) = \mu + \sum_{t_i<t} g(t - t_i) \tag{1}$$

kde μ představuje základní (exogenní) intenzitu a druhý člen zachycuje vliv minulých událostí prostřednictvím interakční funkce g. Každá minulá událost tak může dočasně zvýšit pravděpodobnost další události. Tento mechanismus odpovídá empiricky pozorovanému near-repeat efektu, kdy například vloupání zvyšuje krátkodobé riziko dalších vloupání v blízkém okolí [3, 4].

V kontextu kriminality je exogenní složka často interpretována jako strukturální riziko dané charakteristikami prostředí, zatímco endogenní složka reprezentuje reaktivní dynamiku, tedy krátkodobé „zesílení“ rizika vyvolané samotnými incidenty. Oproti vysvětlujícím modelům založeným na proměnných prostředí tak Hawkesův proces explicitně pracuje s vazbami mezi událostmi a umožňuje popsat dynamiku jejich časového „navazování“ [4].

3.1 Prostorové rozšíření modelu

Pro aplikace v reálném prostředí je nezbytné rozšířit model o prostorovou složku. Intenzita pak závisí nejen na čase, ale i na poloze:

$$\lambda(t,x) = \mu(x) + \sum_{t_i<t} g(t-t_i, x-x_i) \tag{2}$$

Zde je základní intenzita funkcí prostoru μ(x) a interakční funkce *g* zohledňuje jak časový odstup, tak prostorovou vzdálenost mezi událostmi. Model tak umožňuje zachytit lokální difuzi kriminality a krátkodobé prostorové shlukování incidentů. Aplikace v městském prostředí ukazují, že reaktivní složka může tvořit významnou část celkové intenzity procesu, zejména u vybraných typů majetkové kriminality [3].

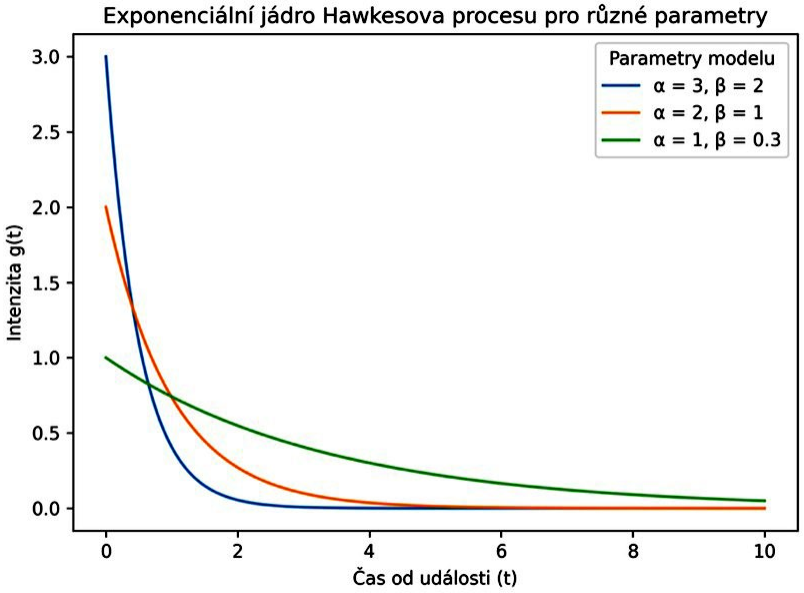
3.2 Parametrizace interakční funkce a interpretace parametrů

V praxi je nutné zvolit konkrétní tvar interakční funkce *g*. Častou volbou je exponenciální časové jádro, které je matematicky jednoduché a dobře interpretovatelné:

$$g(t) = \alpha e^{-\beta t} \tag{3}$$

Parametr α určuje počáteční sílu reaktivního efektu (bezprostředně po události), zatímco β popisuje rychlost jeho odeznívání v čase. Intuitivně tedy platí, že vyšší α znamená výraznější krátkodobé zvýšení rizika, zatímco vyšší β vede k rychlejšímu návratu na základní úroveň.

Vliv kombinací parametrů na tvar exponenciálního jádra je znázorněn na Obrázku 1. Je zřejmé, že některé kombinace vedou k velmi intenzivní, ale rychle mizející odezvě (např. vysoké α a vysoké β), zatímco jiné odpovídají slabšímu, avšak dlouhodobějšímu doznívání zvýšeného rizika (nižší β). Taková parametrizace je sice přehledná, ale zároveň předpokládá předem daný tvar reaktivního mechanismu, což může být v heterogenním prostředí limitující [4].



Obrázek 1. Exponenciální časové jádro Hawkesova procesu pro různé parametry α a β

3.3 Problém homogenity a motivace heterogenního přístupu

Při odhadu parametrů Hawkesova procesu na úrovni celého území se často implicitně předpokládá, že dynamika reaktivity je v prostoru v zásadě homogenní. V reálných podmínkách však může být mechanismus near-repeat efektu výrazně odlišný mezi oblastmi s rozdílnou strukturou prostředí (např. centrum města, sídliště, příměstské zóny). Pokud je celý region popsán jedinou sadou parametrů, může výsledný model „průměrovat" odlišné procesy a tím zkreslit interpretaci reaktivní složky.

Tato skutečnost otevírá potřebu přístupů, které budou schopny pracovat s heterogenitou dynamiky – například prostřednictvím segmentovaného rámce, v němž jsou parametry modelu odhadovány odděleně pro strukturálně odlišné části prostoru. Právě tato problematika tvoří výchozí bod následující kapitoly.

4 Časoprostorová heterogenita a segmentovaný rámec modelování

Prostorová i časová heterogenita kriminality představuje zásadní výzvu při aplikaci bodových procesů v reálném prostředí. Ačkoli samotná formulace Hawkesova procesu umožňuje modelovat dynamiku mezi jednotlivými událostmi, většina empirických aplikací předpokládá jednotnou strukturu parametrů pro celé sledované území [3, 4]. Tento předpoklad implikuje, že síla reaktivity i rychlost jejího odeznívání jsou v různých částech prostoru totožné.

Empirické studie však opakovaně ukazují, že kriminalita je výrazně podmíněna lokálními charakteristikami prostředí a že její dynamika se může mezi oblastmi zásadně lišit [1, 7]. Zatímco základní intenzita μ(x) může reflektovat strukturální rozdíly, samotná forma a síla reaktivní složky bývá často modelována globálně. Pokud jsou parametry α a β odhadovány pro celé území současně, může výsledný model zachytit pouze průměrnou dynamiku, která nereprezentuje žádnou konkrétní část prostoru.

Z metodologického hlediska je proto vhodné rozlišit dva zdroje variability:

- strukturální heterogenitu, související s rozdílnými charakteristikami prostředí [7],
- dynamickou heterogenitu, která se týká odlišné míry a časového průběhu reaktivity mezi událostmi [4].

Zatímco první typ heterogenity lze zahrnout prostřednictvím prostorově proměnlivé základní intenzity, druhý typ vyžaduje hlubší úpravu parametrizace interakční funkce.

4.1 Segmentace jako koncepční řešení

Jedním z možných teoretických řešení je zavedení segmentovaného rámce modelování. V tomto přístupu je sledované území rozděleno na relativně homogenní oblasti, v nichž jsou parametry modelu odhadovány odděleně. Segmentace může vycházet z prostorových charakteristik, typologie časových průběhů nebo kombinace více kritérií [6, 2].

Tento přístup je v souladu s širšími snahami o zohlednění nestacionarity v prostorových datech, kdy jsou parametry modelů uvažovány jako lokálně proměnlivé namísto globálně konstantních [4]. Segmentovaný rámec tak umožňuje zabránit situaci, kdy jeden model „vyvažuje" rozdílné dynamické mechanismy v rámci celého regionu.

Zároveň otevírá možnost komparace parametrů mezi segmenty. Parametry α a β pak nepředstavují pouze technické koeficienty, ale analytické indikátory síly a trvání reaktivního efektu v konkrétních typech prostředí.

4.2 Teoretické implikace heterogenního přístupu

Zavedení heterogenního rámce však přináší nové metodologické otázky. Jednou z nich je volba počtu segmentů a kritéria jejich vymezení. Příliš jemná segmentace může vést k nestabilním odhadům parametrů, zatímco příliš hrubé dělení může opět potlačit skutečnou variabilitu procesu [2].

Dalším aspektem je interpretace rozdílů mezi segmenty. Vyšší hodnota parametru α může indikovat silnější krátkodobou reaktivitu, avšak její význam musí být vždy posuzován ve vztahu k rozsahu dat a kvalitě evidence [3]. Heterogenní přístup tak neznamená pouze technickou modifikaci modelu, ale vyžaduje i opatrnější interpretaci výsledků.

Z teoretického hlediska proto představuje modelování heterogenity posun od předpokladu jednotného generujícího mechanismu k pohledu na kriminalitu jako na soubor lokálně odlišných dynamik. Tento rámec vytváří prostor pro další metodologický rozvoj, aniž by bylo nutné opouštět interpretovatelný parametrický základ.

5 Diskuse

Předložená analýza ukazuje, že vývoj metod časoprostorové analýzy kriminality lze chápat jako postupný posun od deskriptivního mapování vzorců k modelování dynamických mechanismů. Zatímco hotspot analýza a hustotní přístupy umožňují identifikovat koncentrace událostí v prostoru [1], a regresní modely přispívají k vysvětlení rozdílů mezi oblastmi [7], teprve procesní modelování pomocí bodových procesů umožňuje explicitně pracovat s časovou návazností jednotlivých incidentů [3, 4].

Samo-podněcující procesy představují v tomto kontextu významný metodologický nástroj, neboť umožňují oddělit strukturální složku rizika od jeho reaktivní dynamiky. Parametry interakční funkce tak získávají interpretační význam – mohou indikovat sílu a trvání krátkodobého zvýšení rizika v návaznosti na předchozí události. Tento přístup však implicitně předpokládá, že sledované území lze popsat jednotným generujícím mechanismem.

Literatura přitom opakovaně upozorňuje na nestacionaritu a lokální variabilitu prostorových procesů [2]. Pokud je heterogenita ignorována, může globální model produkovat parametry, které představují kompromis mezi rozdílnými dynamikami. Takový výsledek může být matematicky konzistentní, avšak interpretačně problematický.

Segmentovaný rámec modelování, diskutovaný v předchozí kapitole, proto nepředstavuje pouze technickou modifikaci, ale koncepční rozšíření procesního přístupu. Umožňuje nahlížet kriminalitu nikoli jako jednotný proces s proměnlivou intenzitou, ale jako soubor lokálně odlišných dynamik, které se mohou lišit jak strukturálními podmínkami, tak reaktivní odezvou.

Zároveň je však nutné zdůraznit, že zavedení heterogenity zvyšuje nároky na kvalitu dat, rozsah pozorovaného období i stabilitu odhadu parametrů. Interpretace rozdílů mezi segmenty musí být opatrná a opřená o teoretické i empirické souvislosti [4]. Heterogenní model tedy nepředstavuje univerzální řešení, ale nástroj, který vyžaduje metodologickou disciplínu.

Z širší perspektivy lze konstatovat, že procesní modelování kriminality otevírá prostor pro systematické propojení prostorové analýzy, statistického modelování a teorie bezpečnostních rizik. Zachování interpretovatelného parametrického rámce přitom zůstává důležité zejména v kontextu aplikací, kde je transparentnost modelu zásadní.

6 Závěr

Článek se zaměřil na problematiku časoprostorové heterogenity kriminality a na možnosti jejího zachycení v rámci parametrických samo-podněcujících modelů. Bylo ukázáno, že vývoj analytických přístupů k modelování kriminality lze chápat jako postupný přechod od deskriptivního mapování prostorových vzorců k procesnímu modelování dynamiky jednotlivých incidentů. Hawkesovy bodové procesy představují v tomto kontextu významný nástroj, neboť umožňují oddělit strukturální složku rizika od reaktivní dynamiky související s časovou návazností událostí [3, 4].

Současně však bylo poukázáno na limit globálních modelů předpokládajících jednotnou dynamiku v celém sledovaném území. Ignorování heterogenity může vést k průměrování odlišných procesů a ke zkreslené interpretaci parametrů. Segmentovaný rámec modelování proto představuje koncepční rozšíření procesního přístupu, které umožňuje zohlednit lokální rozdíly v intenzitě i reaktivitě kriminality.

Předložená diskuse nevytváří nový algoritmický postup, ale vymezuje teoretický rámec pro systematické uchopení heterogenity v časoprostorových modelech kriminality. Zachování interpretovatelného parametrického základu přitom zůstává klíčové zejména v kontextu bezpečnostní praxe, kde je transparentnost modelu nezbytnou podmínkou jeho využitelnosti. Další výzkum by se měl zaměřit na metodologicky robustní způsoby identifikace homogenních segmentů a na komparaci dynamických charakteristik mezi nimi.

Reference

[1] LEVINE, Ned, 2013. CrimeStat IV: A Spatial Statistics Program for the Analysis of Crime Incident Locations. Houston: Ned Levine & Associates

[2] KOUNADI, Ourania, Dieter DIRKZON a Michael LEITNER, 2020. A systematic review of spatial crime forecasting. ISPRS International Journal of Geo-Information. 2020, 9(7), 1–27

[3] MOHLER, George O., Martin B. SHORT, P. Jeffrey BRANTINGHAM, Frederic P. SCHOENBERG a George E. TITA, 2011. Self-exciting point process modeling of crime. Journal of the American Statistical Association. 2011, 106(493), 100–108

[4] REINHART, Alex, 2018. A review of self-exciting spatio-temporal point processes and their applications. Statistical Science. 2018, 33(3), 299–318

[5] HU, Yujie; WANG, Fahui; GUIN, Cecile; ZHU, Haojie, 2020. A spatio-temporal kernel density estimation framework for predictive crime hotspot mapping and evaluation. ISPRS International Journal of Geo-Information. 2020, 9(7), 1–19

[6] DLOUHÁ, K., POSPÍŠIL, L., ŠČUREK, R. (2025). Spatiotemporal crime analysis for risk management using the non-stationary moving average method. In: Proceedings of the European Safety and Reliability Conference (ESREL 2025)

[7] PERRY, Walter L., Brian McINNIS, Carter C. PRICE, Susan SMITH a John S. HOLLYWOOD, 2013. Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. Santa Monica: RAND Corporation

[8] STALIDIS, Panagiotis; SEMERTZIDIS, Theodoros; DARAS, Petros, 2021. Examining deep learning architectures for crime classification and prediction. Forecasting. 2021, 3(4), 741–762

[9] WANG, Tong, et al., 2019. Deep learning for spatiotemporal crime prediction. IEEE Access. 2019, 7, 1–12

Vektor narušenia mäkkého cieľa

Martin Flodr[1]

[1] QEM s.r.o.,
J.Janošku 3, 031 01 Liptovský Mikuláš, flodr@qem.sk

Abstrakt:

Článok sa venuje klasifikácii útočných vektorov pre mäkké ciele so zameraním na externé a interné útočné vektory. Zdôrazňuje parametrické rozdiely medzi útočnými vektormi s podrobným rozpisom. Autor priraďuje vzorec na výpočet hodnoty útočného vektora ku každému útočnému vektoru a tým určuje jeho klasifikáciu. Okrem toho je prezentovaný aj praktický prípad potenciálneho útočného vektora pre mäkký cieľ. Článok uzatvára zhrnutie zistení s odporúčaniami pre špecifické obmedzenia v skúšobnom tréningu metódy „Uteč-Skry sa-Bojuj“.

Klíčová slova: mäkký cieľ, vonkajšia hrozba, vnútorná hrozba, stresujúca situácia, dôsledky.

1 Úvod

Všeobecne môžeme konštatovať, že mäkké ciele sú primárne charakteristické kumuláciou ľudských aktív, v obmedzenom časo-priestore a s minimálnym stupňom zabezpečenia. [1]

Uvedenú predchádzajúcu stručnú parafrázu definície je možné v rozšírenej forme konkretizovať aj nasledovne: „Mäkké ciele sú objekty (budovy, areály, voľné priestranstvá), v ktorých sa zoskupujú na určitom mieste veľké množstvo osôb. Tieto objekty nemajú aplikované žiadne alebo len mierne špeciálne bezpečnostné opatrenia, koré by bránili násilnému útoku na život osob nachádzajúcich sa v těchto objektech, zabezpečovali by rýchlu reakciu na tento útok, alebo by napomáhali zvládnutiu potenciálneho násilného útoku bez straty na životoch osôb. Násilný útok na tento cieľ by mohlo spôsobiť smrť, alebo zranenie osoby, alebo viacerych osôb, ktoré sa v blýzkosti nachádzajú.“ [2]

Pre konkrétne aplikácie je možné uplatniť aj nasledovnú definíciu: „Mäkké ciele sú miesta s vysokou koncentráciou osôb a minimálnym stupňom zabezpečenia proti násilným útokom, alebo prostredie, ktoré je ľahko dostupné, priťahuje množstvo ľudí a je ľahkým cieľom útoku pomocou dostupných zbraní a pomerne jednoduchou taktikou. Sú to napr. školy, cirkevné objekty, nemocnice, kultúrne centrá/podujatia, športové centrá/podujatia, nočné kluby, divadlá, opery, kiná, kaviarne a reštaurácie, objekty verejnej dopravy, ale aj hromadné dopravné prostriedky.“ [3]

Vytvoriť pre mäkký ciel bezpečné prostredie, ktoré by eliminovalo alebo aspoň minimalizovalo bezpečnostné riziká alebo ohrozenia pri zachovaní podstaty a realistických podmienok, umožňujúcich neobmedzenú kumuláciu ľudských aktív, je prakticky nemožné.

Z uvedeného pohľadu je zrejmé, že už len z pohľadu teórie pravdepodobnosti alebo pravdepodobnostnej logiky, musí krízová situácia za určitých okolností nastať, pričom môže mať potenciál vývinu až do mimoriadnej udalosti.

Z určitého uhľa pohľadu, môže nastať útok na mäkký cieľ z nasledovných vektorov:

- **Externý vektor útoku**, je pri riziku alebo ohrození charakteristický svojou externalitou vzťahu a väzieb voči predmetnému mäkkému cieľu. Jedná sa teda o vzťahovo cudzí zdroj hrozby voči aktívu, ktorý nemá v aktuálnom časo-priestore kumulácie ľudského aktíva, dlhodobú expozíciu na predmetný mäkký cieľ (napr. neznámy útočník).
- **Interný vektor útoku**, je pri riziku alebo ohrození charakteristický svojou internalitou vzťahu a väzieb voči predmetnému mäkkému cieľu. Jedná sa teda o vzťahovo necudzí zdroj hrozby voči aktívu, ktorý má v aktuálnom časo-priestore kumulácie ľudského aktíva, dlhodobú expozíciu na predmetný mäkký cieľ (napr. člen skupiny ľudského aktíva).

Je zaujímavá vzťahová závislosť medzi jednotlivými vektormi útoku, konkrétne pri anonymizovaných mäkkých cieľoch (napr. zhromaždenie na verejnom priestore) sa jedná primárne o externý vektor útoku. Naopak, pri neanonymizovaných mäkkých cieľoch (napr. školský kolektív) sa môže jednať o externý alebo aj interný vektor útoku.

„Výhodou“ interného vektora útoku na mäkký cieľ je, že existuje potenciál tento útok predvídať alebo aj odvrátiť.

Nevýhodou interného vektora útoku na mäkký cieľ, je rutinná kolektívna adaptácia na riziko, ktorá utlmuje prah citlivosti rizikového trendu vrátane paralyzujúceho šoku zo straty dôvery.

2 Externý vektor útoku

Charakteristika externého vektora útoku na mäkký cieľ spočíva v nasledovných kľúčových vlastnostiach a prejavoch:

- Obmedzený vzťah k mäkkému cieľu;
- Obmedzené vplyvy mäkkého cieľa;
- Neobmedzené opatrenia mäkkého cieľa;
- Neobmedzené možnosti výberu mäkkého cieľa.

Na výpočet predpokladaného vektora útoku, použijeme nasledovný vzorec:

Vzorec 1. Vzorec výpočtu (autor)

$$\text{VÚ} = \frac{\text{Vzťah (2 alebo 1)} \cdot \text{Vplyvy (2 alebo 1)}}{\text{Opatrenia (2 alebo 1)} \cdot \text{Možnosti (2 alebo 1)}}$$

- Vz (vzťah) hodnota priameho vzťahu je 2, hodnota nepriameho vzťahu je 1;
- Vp (vplyvy) hodnota veľkých vplyvov je 2, hodnota malých vplyvov je 1;
- Op (opatrenia) hodnota veľkých opatrení je 2, hodnota malých opatrení je 1;
- Mo (možnosti) hodnota veľkých možností je 2, hodnota malých možností je 1;
- VÚ (vektor útoku) vypočítaná hodnota 0,25 alebo 0,5 zodpovedá externému vektoru útoku.

Tabulka 1. Hodnoty vektora útoku (autor)

Hodnota / Vektor	Externý vektor útoku	Interný vektor útoku
Preferovaná hodnota výpočtu	0,25	4
Preferovaná hodnota výpočtu	0,5	2
Hraničná hodnota výpočtu	1	1

2.1 Praktický príklad externého vektora útoku

V nasledovnom príklade z praxe uvedieme hraničnú situáciu, ktorá prerušovanou eskaláciou spĺňala definíciu útoku na mäkký cieľ.

Skupina pracovníkov na stavenisku vykonávala čistiace a upratovacie práce pozemnej komunikácie. Náhodný okoloidúci ich upozornil na neporiadok, pričom došlo k názorovej nezhode. Po silnom verbálnom prejave okoloidúci odišiel z verejného priestranstva, na ktorom sa odohral konflikt.

Po niekoľkých minútach sa vrátil na miesto konfliktu a fyzicky zaútočil rukou na najsilnejšieho názorového oponenta. Tento názorový oponent spontánne sa zahnal lopatou, ktorú držal v ruke. Opätovaná reakcia protistrany bolo vytiahnutie predmetu nadobúdajúceho dojem, že sa jedná o strelnú zbraň. Vzhľadom na agresivitu a sebaistotu protiútoku, pravdepodobne išlo o plynovú pištoľ. Zhluk stavebných robotníkov sa rýchlo, formou behu rozptýlil do bezprostredného okolia v okruhu 10–20 metrov.

Jednalo sa teda o dôvodnú hrozbu, nakoľko ju emocionálne v rovnakom časo-priestore vyhodnotilo viacero ľudí a ostatný sa pod vplyvom davovej psychózy prispôsobili aktuálnej situácií (útek). Nasledoval krátky výhražný verbálny prejav útočníka, ktorý následne opustil miesto konfliktu.

2.2 Simulačná prípadová štúdia externého vektora útoku

Nasledovne vykonám simulačnú prípadovú štúdiu za účelom opakovaného overenia navrhnutého vzorca pre výpočet vektora útoku.

Príklad 1. Simulovaný výpočet (autor)

$$\text{VÚ} = \frac{\text{Vzťah (hodnota 1)} \cdot \text{Vplyvy (hodnota 1)}}{\text{Opatrenia (hodnota 2)} \cdot \text{Možnosti (hodnota 2)}}$$

- Vz (vzťah) hodnota priameho vzťahu je 2, hodnota nepriameho vzťahu je 1;
- Vz = 1 (náhodný okoloidúci je nepriamy vzťah);
- Vp (vplyvy) hodnota veľkých vplyvov je 2, hodnota malých vplyvov je 1;
- Vp = 1 (náhodný a nepredvýdateľný útok);
- Op (opatrenia) hodnota veľkých opatrení je 2, hodnota malých opatrení je 1;
- Op = 2 (možnosť úteku pracovníkov);
- Mo (možnosti) hodnota veľkých možností je 2, hodnota malých možností je 1;
- Mo = 2 (výber cieľa útoku z väčšieho počtu pracovníkov);
- **VÚ (vektor útoku) vypočítaná hodnota 0,25 zodpovedá externému vektoru útoku**.

Zo zistených hodnôt pre uvedený výpočet možem konštatovať, že navrhnutý vzorec je opakovane použitelný s dôveryhodným výstupom.

3 Interný vektor útoku

Charakteristika interného vektora útoku na mäkký cieľ spočíva v nasledovných kľúčových vlastnostiach a prejavoch:

- Neobmedzený vzťah k mäkkému cieľu;
- Neobmedzené vplyvy mäkkého cieľa;
- Obmedzené opatrenia mäkkého cieľa;
- Obmedzené možnosti výberu mäkkého cieľa.

Na výpočet predpokladaného vektora útoku, použijeme nasledovný matematický vzorec:

Vzorec 2. Vzorec výpočtu (autor)

$$\text{VÚ} = \frac{\text{Vzťah (2 alebo 1)} \cdot \text{Vplyvy (2 alebo 1)}}{\text{Opatrenia (1 alebo 2)} \cdot \text{Možnosti (1 alebo 2)}}$$

- Vz (vzťah) hodnota priameho vzťahu je 2, hodnota nepriameho vzťahu je 1;
- Mo (možnosti) hodnota veľkých možností je 2, hodnota malých možností je 1;
- Op (opatrenia) hodnota veľkých opatrení je 2, hodnota malých opatrení je 1;
- Vp (vplyvy) hodnota veľkých vplyvov je 2, hodnota malých vplyvov je 1;
- VÚ (vektor útoku) vypočítaná hodnota 4 alebo 2 zodpovedá internému vektoru útoku.

Tabulka 2. Hodnoty vektora útoku (autor)

Hodnota / Vektor	**Externý vektor útoku**	**Interný vektor útoku**
Preferovaná hodnota výpočtu	0,25	4
Preferovaná hodnota výpočtu	0,5	2
Hraničná hodnota výpočtu	1	1

3.1 Praktický príklad interného vektora útoku

V nasledovnom príklade z praxe uvedieme hraničnú situáciu, ktorá neprerušovanou eskaláciou do hraničnej situácie, mohla spĺňať definíciu útoku na mäkký cieľ.

Skupina študentov na odbornom kurze absolvovala v učebni prednášku. Náhle do miestnosti vstúpil ďalší inštruktor, ktorý direktívnym verbálnym prejavom požadoval od vyučujúceho, aby ukončil aktuálnu prednášku a presunul študijnú skupinu na iný študijný predmet.

Aktuálny vyučujúci oponoval voči predčasnému ukončeniu študijného predmetu, na čo agresívny inštruktor opakovane a stupňujúcim pokrikom vyzýval náhodného študenta, aby zodpovedal odbornú otázku. Študent ju zodpovedal správne, konflikt sa stupňoval nezrozumiteľným pochopením ústnej výpovede formou zámeny odborných slov (popáleniny – poleptaniny) a to stupňovalo agresívny prejav inštruktora v domnienke nesprávnej odpovede.

Agresívny inštruktor bol výrazne vekovo, inštitucionálne a fyzicky vo výhode, čo patrične aj využil (zneužil). Po upozornení zo strany ostatných študentov, že odpoveď bola správna, agresívny inštruktor opustil študijnú miestnosť.

3.2 Simulačná prípadová štúdia interného vektora útoku

Nasledovne vykonám simulačnú prípadovú štúdiu za účelom opakovaného overenia navrhnutého vzorca pre výpočet vektora útoku.

Príklad 2. Simulovaný výpočet (autor)

$$\text{VÚ} = \frac{\text{Vzťah (hodnota 2)} \cdot \text{Vplyvy (hodnota 2)}}{\text{Opatrenia (hodnota 1)} \cdot \text{Možnosti (hodnota1)}}$$

- Vz (vzťah) hodnota priameho vzťahu je 2, hodnota nepriameho vzťahu je 1;
- Vz = 2 (inštruktor je priamy vzťah);
- Vp (vplyvy) hodnota veľkých vplyvov je 2, hodnota malých vplyvov je 1;
- Vp = 2 (stupňujúci pokrik je predvýdateľný útok);
- Op (opatrenia) hodnota veľkých opatrení je 2, hodnota malých opatrení je 1;
- Op = 1 (možnosť úteku pracovníkov);
- Mo (možnosti) hodnota veľkých možností je 2, hodnota malých možností je 1;
- Mo = 1 (výber cieľa útoku z konkrétnej skupiny študentov);
- **VÚ (vektor útoku) vypočítaná hodnota 4 zodpovedá internému vektoru útoku**.

Zo zistených hodnôt pre uvedený výpočet možem konštatovať, že navrhnutý vzorec je opakovane použitelný s dôveryhodným výstupom.

4 Premenné na výpočet interného a externého vektora útoku

Premenné vo vzorci na výpočet vektora útoku, pozostávajú z dvoch skupín:

- Priame vplyvy;
- Nepriame vplyvy.

Pod pojmom „priame vplyvy“ rozumieme premenné „možnosti“ a „opatrenia“. Možnosti predstavujú podmienky, podporujúce alebo obmedzujúce konanie útočníka (napr. možnosť plánovania, realiácie, úniku). Opatrenia predstavujú podmienky súvisiace s úrovňou odolnosti obete útoku voči útočníkovy (napr. schopnosť predvídať útok, schopnost odraziť útok, schopnost vysporiadať sa s útokom).

Pod pojmom „nepriame vplyvy“ rozumieme premenné „vzťah“ a „vplyvy“. Vzťah predstavuje sociálnu väzbu medzi útočníkom a obeťou. Vplyvy predstavujú pôsobenie oboch zainteresovaných strán (útočník aj obeť) na vektor útoku, či už z pozitívneho alebo negatívneho pohľadu.

Špecifikom útoku na mäkký cieľ, na rozdiel od tvrdého cieľa, kde je cieľom útoku neživý objekt (môže nastať príklad, že útok na tvrdý cieľ je plánovaný alebo transformovaný do útoku na mäkký cieľ, pričom je potrebné pre útočníka prekonať samotný tvrdý cieľ, ktorý bol použitý na ochranu mäkkého cieľa), pri útoku na mäkký cieľ, je cieľom útoku samotná ľudská bytosť (jednotlivec alebo skupina).

Je teda zrejmé, že východiskový stav predpokladá pomerové rozdelenie, a to 50 % podielu na útoku majú priame vplyvy a 50 % podielu na útoku majú nepriame vplyvy. Toto pomerové rozdelenie by mohlo predstavovať rozhodovací východiskový bod potenciálního páchateľa, ktorý plánuje vykonať potenciálny útok. Neplánovaný

útok je spontánny, pri ktorom je rozhodovanie páchateľa vopred nepredvídateľné, jedinečné, silno ohraničené aktuálnym situačným stavom, ktoré dôsledky bývajú zväčšia menšie, ako keby bol útok prevedený plánovane.

4.1 Vonkajšie vplyvy – fyzický aspekt

Za fyzický aspekt v kontexte vektora útoku na mäkký cieľ sa dá považovať odolnosť obete útoku voči útočníkovi. V kontexte fyzickej a objektovej bezpečnosti, ide hlavne o modul režimovej, klasickej, technickej a fyzickej ochrany v rozsahu prispôsobenom špecifikám mäkkého cieľa.

V prípade modulu režimovej ochrany, je to súbor pasívnych organizačných opatrení, ktoré minimalizujú vzájomný kontakt útočníka a obete. Typicky sa jedná o vstupno-výstupný režim, návštevný režim a prevádzkový režim.

V prípade modulu klasickej ochrany, je to súbor pasívnych mechanicko-fyzických opatrení, ktoré tvoria pasívnu fyzickú prekážku medzi útočníkom a obeťou. Typicky sa jedná o mechanické zábranné prostriedky (oplotenie chráneného priestoru, stavebné prvky objektu, prostriedky osobnej balistickej ochrany.

V prípade modulu technickej ochrany, je to súbor aktívnych technicko-technologických opatrení, ktoré tvoria detekčnú a dokumentačnú prekážku medzi útočníkom a obeťou. Typicky sa jedná o elektronické detekčné a monitorovacie prostriedky, ako sú prístupový systém, zabezpečovacií systém, protipožiarny systém, kamerový systém.

V prípade modulu fyzickej ochrany, je to súbor aktívnych fyzických opatrení, ktoré tvoria aktívnu fyzickú překážku medzi útočníkom a obeťou. Typicky sa jedná o fyzickú ochranu prostredníctvom strážnej služby, bezpečnostných zborov alebo ozbrojených bezpečnostných zborov.

Reálne, nie je možné za každých okolností dosiahnúť maximálnu ochranu potenciálnej obete, pretože všetky opatrenia zabezpečujúje odolnosť, musia podliehať nasledovným princípom: [4]

- Spoločenskej efektívnosti;
- Ekonomickej efektívnosti;
- Technickej efektívnosti;
- Prevádzkovej efektívnosti.

Uvedené principy efektívnosti v podstate určujú, na akej reálnej úrovni bude realizovaná úroveň ochrany mäkkého cieľa. Tieto obmedzenia nám teda stanovujú priame a nepriame náklady na ochranu mäkkého cieľa úmerne k riadeniu rizík vplývajúcich na mäkký cieľ. Teoreticky to znamená, že môžeme ovplyvňovať 50 % podiel útoku na mäkký cieľ. Z jedného pohľadu to znamená, že v niektorých prípadoch nedokážeme úplne zabrániť útoku, z druhého pohľadu to znamená, že útoku dokážeme úplne zabrániť.

4.2 Vnútorné vplyvy – psychologický aspekt

Za psychologický aspekt v kontexte vektora útoku na mäkký cieľ sa dá považovať riešenie náročných životných situácií. „Spoločným znakom obranných mechanizmov a stratégií zvládania krízových situácií je, že sa vzťahujú na situácie, ktoré sa pre danú osobu zdajú neriešiteľné“ (Křivohlavý). [5]

Šrobárová definuje základnú klasifikáciu krízových situácií z pohľadu krízi jedinca, krízi rodiny, krízi komunity, krízi spoločnosti. Kríza, ako stav psychickej nerovnováhy je zložitý proces, ktorý je subjektívne vnímaný, ako ohrozujúca situácia, v ktorej človek prežíva celý rad emócií a pocitov. [6]

Podľa Vágnerovej a Šrobárovej, obranné reakcie vychádzajú z dvoch základných mechanizmov, ktorými sú únik a útok. Útok, je aktívnou obranou, ktorá znamená všeobecnú tendenciu nejakým spôsobom bojovať s ohrozujúcou a neprijateľnou situáciou. Ďalším typom obrannej reakcie je únik. Je to zmena postoja k situácií, ktorá sa javí ako neriešiteľná. [7]

5 Záver

Rozdelenie vektorov útoku na externý a interný umožní zamerať bezpečnostnú analýzu rizík na kľúčové smery. Taktiež rozdelenie dáva priestor na logické zameranie vytvorenia adresných bezpečnostných postupov. A v neposlednom rade môžeme vykonať účelové cvičenia na identifikáciu počiatočných fáz krízových situácií a následných operatívnych protiopatrení.

Čo sa týka praktických príkladov, z právneho hľadiska zámerne nebudem analyzovať, či sa jednalo o priestupky alebo trestné činy, účelom reálnych príkladov z praxe, bolo zvýrazniť povahu vektora rôznej formy útoku na skupinu ľudských aktív v obmedzenom časo-priestore.

V prípade externého vektora útoku, je jedným z kľúčových zistení, že eskalácia verbálnej komunikácie vysoko pravdepodobne vedie k eskalácií celého priebehu útoku až do extrémnej situácie. Je potrebné použiť nástroje na utlmenie konfliktu, keď aj za cenu krátkodobých ústupkov voči požiadavkám agresora.

V príklade interného vektora útoku, je jedným z kľúčových zistení to, že je neprípustné testovať metódu „UTEČ – SKRY SA – BOJUJ“ vopred neohláseným spôsobom na akomkoľvek ľudskom aktíve. Toto zistenie pramení z poznania, že študenti až do konca odborného kurzu nadobudli strach z konkrétneho inštruktora a nepriamo stratili dôveru k ostatným inštruktorom, pričom sa nemohli plnohodnotne sústrediť na prebiehajúce štúdium.

Pre každého jedinca, je zvládanie krízových situácií jedinečné. Môžeme však definovať podmienky zvládania pre oba možné smery, teda pre únik aj pre útok. Metóda UTEČ – SKRY SA – BOJUJ, v sebe obsahuje obidva základné riešenia, konkrétne UTEČ a BOJUJ. Skutočný problém ale nastane v pípade, keď niektoré z riešení nemôžeme z objektívnych (nemáme možnosť utiecť) alebo subjektívnych (nemáme možnosť bojovať) dôvodov použiť.

V tomto prípade nám v logickej rovnici (bezpečnostnom vzťahu) zostáva možnosť SKRY SA. Je to variant, pri ktorom obeť útoku útočníka predpokladá, že sa nachádza v jeho možnom útočnom dosahu, teda že je bezprostredne ohrozené zdravie alebo život obete. Táto situácia predstavuje pre obeť (ale prípadne aj pre útočníka) vysokorizikový situačný profil, pretože sa nachádza v situácií vysokej neistoty a chýbajúceho bezprostredného situačného povedomia.

Poďakovanie

Tento článok bol pripravený s podporou projektu APPV-23-0437 Stratégia a metodika ochrany mäkkých cieľov so zameraním na základné, stredné a vysoké školy.

Referencie

[1] Nevrkla, J., Lapková, D., Jenčková, K., Šternová, T., Rožek, D., Mrázková, L., Kotek, L. (2019). MĚKKÉ CÍLE: IDENTIFIKACE, OHROŽENOST A JEJICH OCHRANA, Soft Targets Protection Institute, z.ú. Praha 2019, ISBN 978-80-270-7066-4

[2] Apeutauler, T., Dufek, Z., Vangeli, B., Rosenkranz, J., Hromada, M., Mrázková, L., Lapková, D., Kotek, L., Ljubymemko, K., Ochrana měkkých cílů, Praha: Leges 2019, ISBN 978-80-7502-427-5

[3] DVOŘÁK, Z., ŠIMONOVÁ, J., VEĽAS, A., 2024 Minimálny štandard pre audit bezpečnosti a ochrany vysokej školy s. 23

[4] FALISOVÁ, B. 1994 AKADÉMIA POLICAJNÉHO ZBORU SLOVENSKEJ REPUBLIKY 1994. OCHRANA OBJEKTOV s. 239. ISBN 80-88751-26-8

[5] KŘIVOHLAVÝ, J. 1994. Jak zvládat stres. Praha: Grada. 1994. 190 s. ISBN 80-7169-121-6

[6] ŠROBÁROVÁ, S. [Autor, 100%] ; Žiaková, Eva [Recenzent] ; Špatenková, Naděžda [Recenzent]. – 1. vyd. – Ružomberok (Slovensko): ID: 273965 | Krízová intervencia v multicisciplinárnom ponímaní v riešení vybraných akútnych sociálnych problémov [textový dokument (print)] [učebnica pre vysoké školy (do 2021)]: Katolícka univerzita v Ružomberku. VERBUM - vydavateľstvo KU, 2016. 214 s. [tlačená forma]. – ISBN 978-80-561-0375-3

[7] VAGNEROVÁ, M. 1999. Psychopatologie pro pomahající profese: variabilita a patologie lidské psychiky. Vyd. 1. Praha: Portál, 1999. 448 s. ISBN 80-7178-214-9

Navržený postup posouzení rizik pro spolupráci člověka s robotem

Kristýna Hamříková[1]

[1] VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství,
Lumírova 13, 700 30 Ostrava - Výškovice, kristyna.hamrikova@vsb.cz

Abstrakt:

Předkládaný příspěvek se zabývá problematikou posouzení rizik v oblasti spolupráce člověk – robot v kontextu přechodu na principy Průmyslu 5.0. Hlavním cílem práce je prezentace integrovaného postupu posouzení rizik, který kombinuje techniky Hierarchické analýzy úkolů (HTA) pro strukturální dekompozici úkolů a Studii nebezpečí a provozuschopnosti (HAZOP) pro identifikaci procesních odchylek. Jádro návrhu tvoří modifikovaná technika HRC-PFMEA, která umožňuje kvantifikaci identifikovaných rizik s důrazem na separaci dopadů na zdraví operátora a stabilitu výrobního procesu. Navržený postup řeší absenci historických dat u inovativních aplikací a poskytuje integrátorům a bezpečnostním specialistům systematický nástroj pro rozhodování o přijatelnosti rizik. Práce dále nastiňuje plánovanou verifikaci metodiky v digitálním prostředí a následně v reálných podmínkách kolaborativní aplikace.

Klíčová slova: spolupráce člověka s robotem, kolaborativní aplikace, bezpečnost, posouzení rizik.

1 Úvod

Nástup konceptu Průmyslu 4.0 a jeho aktuální evoluce směrem k Průmyslu 5.0 přináší zásadní změnu paradigmatu v průmyslové automatizaci, kde se pozornost přesouvá od izolovaných robotických buněk k úzké spolupráci člověka a stroje. Zatímco tradiční průmyslové roboty byly z bezpečnostních důvodů striktně odděleny fyzickými bariérami, moderní kolaborativní systémy sdílejí s operátorem společný pracovní prostor a čas, což generuje nová, dříve neznámá rizika spojená zejména s chybami v komunikaci a lidským faktorem.

Z legislativního hlediska jsou roboty určené pro kolaborativní aplikace považovány za neúplná strojní zařízení dle Směrnice 2006/42/ES, což přenáší plnou odpovědnost za bezpečnost a finální certifikaci CE na integrátora. Současné standardizované techniky posouzení rizik však často narážejí na své limity, neboť vyžadují rozsáhlá historická data, která pro inovativní kolaborativní aplikace nejsou aktuálně k dispozici. Předkládaný příspěvek se proto zaměřuje na návrh integrovaného hybridního postupu, který kombinuje několik technik, které jsou představeny níže.

2 Teoretické vymezení řešené problematiky

Koncept spolupráce robotů s lidmi má své kořeny v technické literatuře a spekulativních myšlenkách počátku 20. století, kdy Karel Čapek ve své hře R.U.R. v roce 1921 poprvé zavedl termín „robot“ pro popis humanoidních automatů. [1] Výraz robot však nevymyslel on, ale jeho bratr, Josef Čapek, který hledal náhradu za původní označení „laboři“, který chtěl Karel Čapek použít ve své zmíněné hře pro označení umělých dělníků. Na radu svého bratra Josefa nakonec název změnil na roboti, který vychází z českého slova „robota“, označení pro těžkou, nucenou práci. [2]

Skutečný technologický rozvoj interakce člověka s robotem se však začal formovat až v polovině 20. století s nástupem první generace průmyslových robotů. Tradiční průmyslové systémy byly z bezpečnostních důvodů striktně odděleny od lidské obsluhy pevnými bariérami a orientovaly se výhradně na vysokorychlostní, repetitivní úlohy bez možnosti přímého kontaktu s člověkem. Významný posun nastal koncem 90. let 20. století, kdy se objevily první systémy schopné bezpečné práce v těsné blízkosti operátora. Tyto kolaborativní aplikace byly navrženy s cílem eliminovat potřebu fyzických bariér s použitím inteligentních senzorických systémů. [3]

Robotika představuje významný prvek současné průmyslové výroby a její uplatnění se v posledních desetiletích výrazně rozšířilo o čemž vypovídá statistika Mezinárodní federace robotiky o ročních instalacích robotických systémů. V průmyslové praxi se lze setkat jak s tradičními průmyslovými roboty, tak i s roboty určenými pro spolupráci s člověkem. Zatímco tradiční průmyslové robotické systémy byly zpravidla navrhovány pro práci v oddělených prostorech a jejich bezpečnost byla zajišťována především fyzickou separací člověka a robotu pomocí ochranných bariér, oplocení nebo blokovacích prvků [4], u robotů určených pro spolupráci s člověkem je cílem umožnit sdílení pracovního prostoru a využít výhody vzájemné interakce. [3]

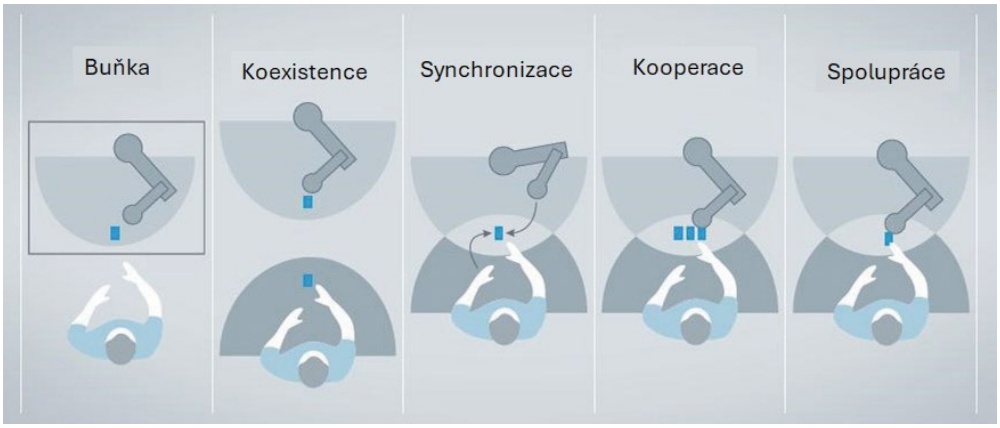
S rozvojem spolupráce člověka s robotem se uplatňují specifické bezpečnostní přístupy, které umožňují bezpečnější provoz ve sdíleném pracovním prostoru. Tyto přístupy jsou dány normou ISO 10218 – 1:2025 [5], která pojednává o požadavcích na bezpečnost aplikace průmyslových robotů a robotických buněk, rovněž také o bezpečnosti kolaborativních aplikací.

Kolaborativní aplikace nepředstavují zvýšené riziko vždy. Pouze v případech vyšší úrovně interakce, při které dochází k přímé fyzické interakci a vzájemné reakci mezi robotem a člověkem v reálném čase za účelem splnění společného úkolu. [3, 4]

Mezi definované úrovně jsou tyto interakce člověka s robotem:

- Buňka – Jedná se o nejnižší, a tedy i nejbezpečnější úroveň interakce. Robot a člověk jsou fyzicky odděleni bezpečnostním oplocením. Neexistuje žádné sdílení prostoru. [6]
- Koexistence – Tato úroveň již představuje princip vykonávání činností ve stejném prostoru člověk – robot, bez bezpečnostních bariér nebo oplocení. Člověk a robot pracují ve stejném prostoru bez fyzických bariér, ale nemají sdílený pracovní úkol a jejich pracovní zóny se nepřekrývají. [7]
- Synchronizace – Tato úroveň již demonstruje práci ve sdíleném pracovním prostoru člověka – robotu, ovšem bez vzájemné spolupráce. Člověk a robot pracují ve sdíleném prostoru, ale jejich aktivity na sebe časově navazují. V daný okamžik se v zóně nachází pouze jeden, buď operátor nebo robot. [8]
- Kooperace – Tato úroveň už představuje pro člověka riziko. Jedná se o situaci, kdy člověk a robot pracují na stejném úkolu ve stejném čase, přičemž robot i člověk vykonávají své operace současně, ale bez nutné fyzické interakce. [9]
- Spolupráce – Tato úroveň představuje nejvyšší riziko pro člověka. Na této úrovni dochází k přímé fyzické interakci a vzájemné reakci mezi robotem a člověkem v reálném čase za účelem splnění společného úkolu. [10]

Všechny zmíněné úrovně jsou zobrazeny na Obrázku 1.



Obrázek 1. Úrovně interakce člověk – robot [11]

Revidovaná norma ISO 10218-2:2025 a technická specifikace ISO/TS 15066:2016 poskytují komplexní pokyny pro kolaborativní aplikace a specifikují, že by tyto aplikace měly zahrnovat jeden nebo více z následujících bezpečnostních režimů [5], které jsou zobrazeny na Obrázku 2.

- Ručně vedené ovládání

Tento režim umožňuje jednotlivcům ručně ovládat pohyby robotu. Roboty mohou pracovat plnou rychlostí, když jsou lidé mimo pracovní prostor robotu. Lidé však mohou vstoupit do tohoto prostoru a provádět úkoly ručního vedení pouze tehdy, když robot dosáhne stavu bezpečného monitorovaného zastavení (MS). Jedná se o bezpečnostní funkci, která se používá v situacích, kdy lidé a roboty pracují v oddělených pracovních prostorech. V této situaci může robot fungovat bez omezení, dokud do jeho oblasti nevstoupí člověk. Člověk smí vstoupit do pracovního prostoru robotu pouze tehdy, když je aktivován systém monitorovaného zastavení, který zajistí dočasné zastavení robotu. Jakmile člověk opustí prostor robotu může robot pokračovat ve svých úkolech. K detekci lidské přítomnosti jsou používána bezpečnostní zařízení jako např. kamery a senzory. Pokud je zařízení určené k ručnímu vedení používáno, bezpečnostní funkce MS se deaktivuje. [3] Jakmile člověk odejde z pracovního prostoru robotu, robot se opět vrátí zpět k činnosti s původní naprogramovanou rychlostí bez omezení.

- Monitorování rychlosti a vzdálenosti

V tomto režimu mohou lidé i roboty sdílet stejný pracovní prostor. Rychlost robotu se upravuje podle blízkosti lidského pracovníkovi vůči němu. Robot musí udržovat bezpečnou vzdálenost od člověka a zastavit se, pokud se k němu člověk příliš přiblíží. [3]

- Omezení síly a výkonu

Tento režim umožňuje fyzický kontakt mezi lidmi a roboty. Provoz v režimu omezení síly a výkonu je navržen pro roboty určené ke spolupráci s lidmi. Roboty jsou vybavené integrovanými senzory síly a momentu. I když je kontakt mezi člověkem a robotem povolen, síly působící na lidské tělo, ať už úmyslné či neúmyslné, musí zůstat pod prahovými hodnotami stanovenými během posouzení rizik. [3] Tyto hodnoty jsou stanoveny v normě ISO 10218-2:2025 a ISO/TS 15066:2016.

Obrázek 2. Režimy kolaborativních aplikací [10]

Současný normativní vývoj zároveň ukazuje posun od označení „kolaborativní robot“ ke konceptu „kolaborativní aplikace“. Bezpečnost není chápána jako vlastnost samotného robotu, ale jako výsledek konkrétního návrhu, integrace a provozu dané aplikace. Právě z tohoto důvodu je nutné věnovat zvýšenou pozornost systematickému postupu posouzení rizik, který bude reflektovat specifika spolupráce člověka s robotem v konkrétním pracovním prostředí. [5]

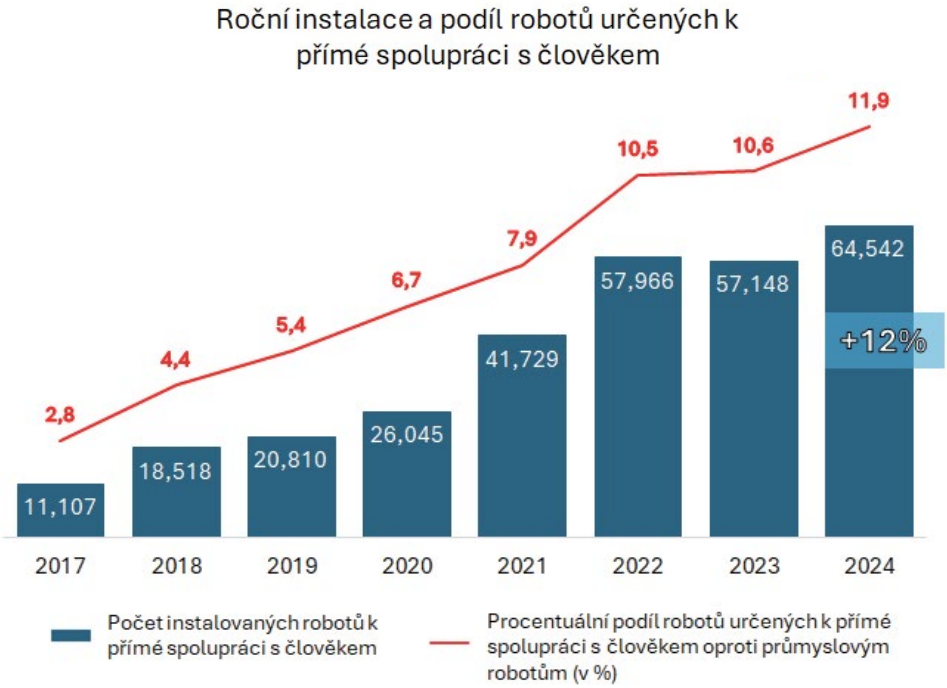
2.1 Vývoj využívání robotů určených ke spolupráci v průmyslu

Kolaborativní aplikace se v posledních letech prosazují v průmyslu stále více díky své flexibilitě a možnosti přímé spolupráce s člověkem [13]. Zatímco u tradičních robotických pracovišť bývá bezpečnost řešena především fyzickou separací, v kolaborativních aplikacích je žádoucí zachovat sdílený pracovní prostor a přínosy spolupráce člověka a robotu [4]. To však klade zvýšené nároky na systematické posouzení rizik vyplývajících z interakcí, provozních scénářů a změny v pracovních postupech [14, 15].

V roce 2024 dosáhla roční globální instalace přibližně 542 tisíc robotických jednotek a celkový počet provozovaných průmyslových robotů překročil hranici 4,6 milionů, což představuje přibližně 7 % meziroční nárůst instalovaných robotů [13].

Strukturální změny v průmyslu se v posledních letech projevují posunem od tradičních velkosériových výrobních odvětví, zejména automobilového průmyslu, směrem k tzv. všeobecnému průmyslu, mezi který patří např. elektrotechnika, strojírenství, logistika nebo potravinářský průmysl. Tento trend se odráží i ve zvyšujícím se zájmu o robotická řešení umožňující přímou spolupráci člověka a robotu. V tomto kontextu dochází k rozvoji oblasti spolupráce člověk – robot tzv. *Human Robot Collaboration* (dále HRC), která umožňuje sdílení pracovního prostoru člověkem a robotem. [12] Podle statistik Mezinárodní Federace robotiky došlo v roce 2024 k celosvětové

instalaci přibližně 64,5 tisíce robotů určených ke kolaborativním aplikacím viz Obrázek 3, což představuje téměř 12 % všech instalovaných robotů [13].



Obrázek 3. Růst instalací robotů určených ke spolupráci s člověkem [13]

HRC je tak stále častěji využívána jako prostředek ke zvýšení flexibility výroby, zlepšení ergonomie práce a efektivního rozdělení úloh mezi člověka a robotický systém. [16] Bezpečnost v HRC nelze zajistit separací robotu od člověka, a proto je nezbytné provádění důkladného posuzování rizik, které je nezbytné k zajištění bezpečnosti operátorů.

2.2 Posuzování rizik v oblasti spolupráce člověk – robot

Posuzování rizik je podle bezpečnostních standardů pro průmyslové robotické systémy požadováno před uvedením do provozu. U průmyslových robotických systémů je tento požadavek spojován zejména s normou ISO 10218-2. [5] V prostředí HRC se uplatňují pokročilejší ochranná opatření (např. detekce kolize, laserové skenery či kamerové systémy pro detekci člověka), která umožňují práci člověka a robotu v blízkosti, případně ve sdíleném prostoru. Tím se posouzení rizik stává klíčovým nástrojem pro návrh a volbu opatření, protože cílem, již typicky není uzavřít robota do bariér, ale řídit rizika vyplývající z interakce člověk – robot [17, 18]

Doporučený postup posuzování a snižování rizik v rámci aktuálních ISO standardů je obecně založen na zkušenosti a expertním úsudku, který bývá podporován pouze intuitivními metodami jednoduchými nástroji. [18] V prostředí HRC se objevují specifické faktory, které posouzení rizik dále komplikují. Těmito faktory jsou:

- Složitost, která je daná množstvím návrhových faktorů (např. uspořádání pracoviště, volba robotu, provozní režimy) a dynamickými efekty (např. doba zastavení robotu, síly při kontaktu). [18]
- Nedostatek zkušeností s HRC aplikacemi. Využívání kolaborativní aplikace se sice zvyšuje, ale stále chybějí zkušenosti a odborné znalost, což představuje jistý problém a určitou výzvu. [18]
- Obtížnost predikce lidského chování a lidské chyby, která je klíčová při posouzení rizik. [18]

- Odhad kritičnosti kontaktu nebo kolize. Predikcí kolizí nedisponují zatím všechny systémy HRC. V některých případech jsou kolize mezi člověkem a robotem přijatelné, pokud síla a tlak při kolizi zůstávají pod určitou prahovou hodnotou, která je stanovena v ISO/TS 15066 [19]. V těchto případech musí posouzení rizik nejen určit, zda ke kolizím může dojít, ale také zda jsou jejich následky pro zdraví a bezpečnost operátorů kritické. [18]

Z uvedených důvodů je účelné pracovat s postupy nebo technikami, které mají jednoznačně definované kroky a návaznosti výstupů tak, aby bylo možné převést výsledky identifikace a analýzy rizik do konkrétních opatření. K řešení této potřeby již byla navržena řada nových technik. Ovšem jejich sloučení do komplexního použitelného nástroje, který by splňoval potřeby praktických uživatelů, je stále výzvou. Mezi identifikované potřeby patří např. srozumitelnější vedení uživatele postupem, katalog vhodných bezpečnostních opatření pro dané nebezpečí, identifikace nebezpečí pomocí simulace nebo AI [18].

2.3 Používané techniky posuzování rizik v interakci člověk – robot

Techniky lze z hlediska jejich role v procesu posuzování rizik rozdělit na techniky zaměřené na identifikaci nebezpečí, techniky pro analýzu a strukturované vyhodnocení identifikovaných scénářů a nástroje pro hodnocení a rozhodování o přijatelnosti rizik a prioritách opatření. [20]

V oblasti HRC se v odborné literatuře objevuje řada přístupů, které pokrývají různé části tohoto procesu, od jednoduchých nástrojů používaných v praxi až po sofistikované techniky využívané ve výzkumu. Zároveň je opakovaně zdůrazňováno, že průmyslová praxe často stojí na zkušenosti, expertním úsudku a snadných nástrojích jako jsou kontrolní seznamy. Nově navrhované techniky a přístupy na rozdíl od těch již využívaných vyžadují vyšší úsilí jako jsou data, časová a expertní náročnost, a proto se do praxe prosazují pomaleji, i navzdory tomu, že mohou být efektivnější než ty dosavadní. [18]

Jako výchozí rámec se v praxi i literatuře opírá posouzení rizik o postupy vycházející z ISO 12100 a robotických norem ISO 10218-2 a ISO/TS 15066, které poskytují strukturu procesu a také přehled typických zdrojů nebezpečí a režimů kolaborativního provozu. [5, 19, 21]

V HRC jsou často používány úkolově orientované přístupy vycházejí z toho, že průmyslová spolupráce mezi člověkem a robotem je často realizována jako opakující se úkoly (např. montáž, manipulace, předávání dílů apod.). Rizika se proto hledají „z pohledu úkolu“ – tj. rozkladem činností a následnou identifikací kritických míst, kde vzniká kontakt člověk – robot, vstup do sdíleného prostoru nebo změna režimu. V literatuře se v této souvislosti objevují různé úkolové šablony a analýzy, které umožňují systematicky zachytit kroky práce a vazby mezi člověkem a robotem. Celý proces se nejprve rozloží na dílčí úkoly a ty se následně analyzují z hlediska nebezpečí. [18, 22]

Na tomto principu stojí i níže představený podpůrný přístup Hierarchická analýzy úkolů tzv. *Hierarchical Task Analysis* (dále HTA). Tento přístup podporuje identifikaci rizik za pomocí hierarchického rozkladu úkolu na dílčí kroky včetně plánu jejich provádění. HTA se v kontextu HRC používá především jako nástroj pro identifikaci kritických interakčních bodů člověk – robot a jako struktura, na kterou lze navázat další kroky procesu posouzení rizik. [23] Dalším přístupem je např. Pracovní rozklad činností tzv. *Work Breakdown Structure*. Podstatou tohoto přístupu je hierarchické rozdělení úkolu na menší celky, až na úroveň, kterou lze snadno posoudit a řídit. Dalším přístupem je např. Procesní mapování tzv. *Flowcharting*, které slouží k identifikaci kritických uzlů, kde je riziko nejvyšší nebo kde závisí jeden krok na druhém. Vizuální podoba často odhalí rizika, která v textu nejsou patrná.

Další přístupem využívaným v HRC je adaptace již zavedených technik. Příkladem je Studie nebezpečí a provozuschopnosti s použitím modelovacího jazyka UML tzv. HAZOP-UML. Tato technika kombinuje klasikou techniku HAZOP a její klíčová slova a modelování pomocí UML diagramů. Tyto diagramy umožní přenést analýzu do modelového prostředí a je mnohem efektivnější. Tento směr ale typicky zvyšuje nároky na vstupní modely a může generovat velké množství odchylek. U této techniky je značná časová náročnost, přičemž kvalita výsledků je silně závislá na kvalitě modelu. Další upravenou technikou je Analýza možných vad a jejich následků v procesu (PFMEA) nebo *Human Robot Collaboration – Process Failure Mode and Effects Analysis* (HRC-PFMEA). [18]

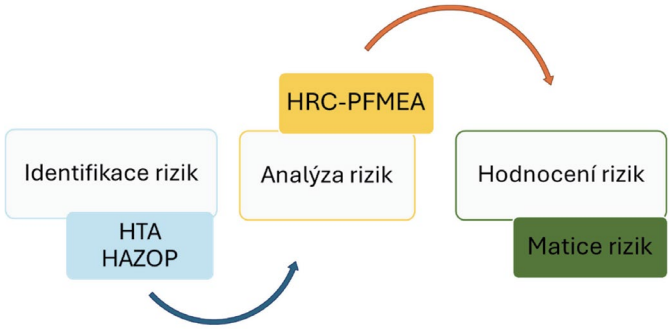
Rovněž využívaným přístupem jsou tzv. odvozené přístupy, kam patří systémově-teoretické techniky typu Systémově-teoretická analýza procesů (STPA), které pracují s hierarchickou řídicí strukturou systému a identifikací nebezpečné kontrolní akce. STPA se v HRC používá hlavně pro systematickou identifikaci nebezpečných systémových chování včetně vazeb mezi člověkem, robotem, softwarem a prostředím. Současně je v literatuře opakovaně uváděno, že STPA bývá náročná na čas a vstupy a že poskytuje primárně kvalitativní výstupy, což komplikuje přímé srovnání a prioritizaci rizik bez doplňkových nástrojů. [18]

Poslední zmíněné jsou přístupy založené na simulaci, které mohou v HRC sloužit k detailnější identifikaci nebezpečí a verifikaci bezpečnostně kritických aspektů, zejména tam, kde už jednoduché metody nebo expertní posouzení nestačí. [18]

3 Návrh nového postupu posuzování rizik v interakci člověk – robot

Cílem nově navrženého postupu je systematicky projít kolaborativní úkol krok za krokem, najít situace, které mohou vést k nehodě nebo úrazu, a rozhodnout, které z nich vyžadují opatření. Postup je sestaven tak, aby byl použitelný i v případě, když hodnotitel nemá k dispozici podrobná měření nebo historická data o poruchách nebo úrazech.

Navrhovaný postup posouzení rizik kombinuje čtyři na sebe navazující techniky viz Obrázek 4.



Obrázek 4. Navržený postup posouzení rizik v HRC

Identifikace rizik bude prováděna technikami HTA a HAZOP. Technika HTA identifikuje kritické situace procesu, tak že rozepíše práci na jednotlivé kroky, které se v procesu provádějí. Vytvoří tzv. „strom úkolů“, který představuje seznam kroků a kritických míst, kde dochází k vzájemné spolupráci člověka a robotu. Na tyto identifikované body bude aplikována technika HAZOP, která tyto interakční body rozšíří o identifikované odchylky a možné nebezpečné situace. Po provedení prvního kroku procesu posouzení rizik, kterým je identifikace rizik, vznikne seznam rizik a nebezpečných situací, s možnými odchylkami, jejich příčinami a následky. Tyto identifikované situace budou dále kvantifikovány technikou HRC-PFMEA.

Analýza rizik bude provedena modifikovanou technikou HRC-PFMEA, která posoudí identifikovaná rizika na základě stanovených parametrů. Z těchto parametrů je následně vypočítán tzv. index rizika, který vypovídá o výsledné hodnotě posuzovaného rizika nebo nežádoucí situace. Index rizika je vypočítán vynásobením hodnot parametrů (dopad x výskyt). Dále budou navržena bezpečnostní opatření.

Posledním krokem je hodnocení rizik, které bude provedeno nástrojem matice rizik, kterou bude rozhodnuto o přijatelnosti nebo nepřijatelnosti rizika a prioritizaci opatření.

Proces posouzení rizik i terminologie je v souladu s normou ISO 31000. [24]

3.1 Postup provádění navrženého postupu posouzení rizik

Návrh tohoto postupu bude testován v laboratorních podmínkách na Fakultě bezpečnostního inženýrství v nově vybudované laboratoři Bezpečné spolupráce člověka s robotem. Tato laboratoř v současné době disponuje dvěma roboty typu GoFa.

První krok postupu – aplikace techniky HTA

Tato technika se používaná především v ergonomii a systémech člověk-stroj k analýze úkolů prováděných lidmi nebo systémy. Jejím cílem je rozložit složitý úkol na menší tzv. dílčí úkoly, hierarchicky uspořádat kroky a identifikovat, kde mohou nastat chyby nebo bezpečnostní rizika. HTA se zaměřuje na „co člověk dělá“, „proč to dělá“ a „v jakém pořadí“.

Cíle HTA jsou následující:

- Porozumět aktivitám operátora a robotu v rámci konkrétního procesu/úkolu.
- Identifikovat kritická místa, která mohou vést k chybám nebo rizikům.
- Vytvořit strukturu, na kterou lze systematicky aplikovat technika HAZOP.

Postup HTA:

1. Definujte hlavní cíl – jasně uveďte, co je konečným cílem činnosti (např. montáž součásti, přesun objektu atd.).
2. Shromážděte informace o úkolu – pozorujte pracovníka, sledujte videa, konzultujte s odborníky, prostudujte pracovní pokyny a postupy.
3. Rozložte úkol na dílčí kroky – identifikujte všechny činnosti nezbytné k dosažení cíle.
4. Určete hierarchii (strom úkolů) – uspořádejte kroky do hierarchické struktury podle závislostí a pořadí činností.
5. Definujte plán: popište pořadí úkolů, podmínek a rozhodovacích bodů (např. kroky 2.1–2.3, které lze provést v libovolném pořadí, poté krok 3).
6. Ověřte hierarchii a plán s pracovníky a odborníky: ověřte správnost rozdělení, zda odpovídá skutečnosti činností.
7. Identifikujte rizik nebo chybové kroky: určete, kritické interakční body, kde může dojít k nesprávným postupům, zpožděním, nesprávným reakcím, nesprávným interakcím apod.
8. Aplikujte techniku HAZOP.

Druhý krok postupu – aplikace techniky HAZOP

Technika HAZOP se provádí za pomocí použití klíčových slov na interakční body a kritické kroky odhalené v prvním kroku pomocí HTA. Díky aplikace klíčových slov jsou systematicky identifikovány možné odchylky od zamýšleného průběhu, jejich potenciální příčiny a důsledky. Klíčová slova pomáhají identifikovat nebezpečné scénáře. Klíčová slova jsou obsahem Tabulky 1.

Tabulka 1. Klíčová slova HAZOP

Klíčová slova	Význam
Žádný	Úplná negace záměru projektu. Situace, kdy se akce nebo podmínka neprovede, přestože by měla.
Více	Kvantitativní nárůst. Situace, kdy je akce nebo podmínka nadměrná (větší, než se očekávalo).
Méně	Kvantitativní pokles. Situace, kdy je akce nebo podmínka nedostatečná (méně, než se očekávalo).
Opačný	Je dosaženo logického opaku zamýšleného návrhu. Situace, ve které se akce nebo stav odehrává v opačném směru, než byl zamýšlen.
Navíc	Všechny konstrukční plány jsou realizovány společně. Situace, kdy k neočekávané události nebo podmínce dochází současně s očekávanou.
Část z	Záměr návrhu je dosažen pouze částečně. Situace, ve které je akce nebo stav neúplný.
Jiný než	Úplná náhrada, kdy není dosaženo původního záměru, ale stane se něco úplně jiného. Situace, ve které dochází k jinému stavu nebo akci, než se očekávalo.
Předčasný	Něco se stane dříve, než se očekávalo z hlediska času (hodin).
Zpožděný	Něco se stane později, než se očekávalo z hlediska času (hodin).
Před	Něco se stane dříve, než se očekávalo, s ohledem na pořadí nebo posloupnost.
Po	Něco se stane později, než se očekávalo, s ohledem na pořadí nebo posloupnost.

Výstupem těchto dvou kroků bude seznam nebezpečných situací a rizik, jeho odchylek, příčin, možných následků a existujících opatření. Na tato identifikovaná rizika a situace (scénáře) se následně aplikuje technika HRC-PFMEA, která přidělí identifikovaným scénářům parametry výskytu, závažnosti a detekce.

Třetí krok postupu – aplikace techniky HRC PFMEA

Technika HRC-PFMEA je modifikovanou technikou FMEA. Tato technika je zaměřená na kolaborativní aplikace. Jejím cílem je systematicky analyzovat potenciální chyby vyplývající ze spolupráce člověka a robotu a vyhodnotit jejich detekci, závažnost a pravděpodobnost výskytu. Následně navrhnout opatření k jejich minimalizaci. Tato technika byla použita i ve studii [25].

Parametry hodnocení rizika:

Dopady (S)

Vyjadřují, jak vážné by byly dopady pro člověka a pro proces, kdyby k nežádoucí situaci došlo. Používá se škála 1–10 (od nejméně závažných až po ty nejzávažnější).

Výskyt (O)

Vyjadřuje, jak pravděpodobné je, že k dané situaci dojde. V prostředí HRC se často stanovuje expertním odhadem stejně jako v této metodice. Používá se škála 1–10 (od velmi nepravděpodobného výskytu až po častý výskyt).

Detekce (D)

Vyjadřuje, jak dobře lze vznik situace odhalit nebo zastavit dříve, než dojde k dopadu. Používaná škála je 1–10 (kde nízké hodnoty znamenají dobrou detekci nebo prevenci vzniku nežádoucí situace a vysoké hodnoty nízkou detekci).

Risk index (RI)

Index rizika je výsledná hodnota posuzovaného rizika nebo nebezpečné situace. Výpočet se provádí pomocí vynásobení stanovených parametrů, kterými jsou S, O, D. Rozsah RI je 1–1000.

Čtvrtý krok postupu – aplikace nástroje MATICE RIZIK

Matice rizik je nástroj, který pomáhá převést výsledky do rozhodnutí. Matice rizik vizualizuje výsledné hodnoty rizik a na základě kritérií se rozhoduje, zda je riziko:

- Nízké (přijatelné),
- Střední (přijatelné jen s podmínkami),
- Vyšší (riziko vyžaduje okamžité nastavení dalších opatření,
- Vysoké (nepřijatelné).

Do matice se promítají výsledná hodnota RI, která je stanovena vynásobením hodnot S, O a D. Výstupem je rozhodnutí o přijatelnosti rizika, priorita opatření.

3.2 Výstupy postupu posouzení rizik

Předpokládanými výstupy tohoto navrženého postupu posouzení rizik je:

- strukturovaný popis úkolu a kritických kroků (z techniky HTA),
- seznam scénářů a odchylek s příčinami a následky (z techniky HAZOP),
- vyhodnocené položky rizik s parametry S, O a D společně s návrhy opatření (z techniky HRC-PFMEA),
- a rozhodnutí o přijatelnosti a prioritě opatření (z matice rizik).

Z těchto výstupů lze následně vytvořit bezpečný pracovní postup, bezpečné uspořádání pracoviště, změna pracovních činností.

Zamýšlený rozsah tohoto navrženého postupu posouzení rizik je pokrytí celé procesní bezpečnost tedy i na integrace robotu do konkrétního pracovního prostředí s navázáním na standardní postupy bezpečnosti a ochrany zdraví při práci.

4 Závěr

Navržený postup představuje komplexní řešení pro posouzení rizik v kolaborativních aplikacích, který se snaží překonat limity izolovaně používaných technik. Hlavním přínosem je vytvoření logické synergie mezi technikami HTA, která definuje strukturu procesu, HAZOP, zaměřenou na identifikaci odchylek, a modifikovanou HRC-PFMEA, jež umožňuje kvantifikovat rizika s ohledem na specifika Průmyslu 5.0. Rozdělení závažnosti následků na oblast zdraví a procesní stabilitu poskytuje integrátorům přesnější podklady pro návrh cílených nápravných opatření.

Snaha tohoto hybridní přístup je i zvýšení transparentnosti bezpečnostní analýzy a usnadnění procesu posouzení shody neúplného strojního zařízení (v tomto případě robot). Další fáze výzkumu se zaměří na verifikaci navrženého postupu v digitálním prostředí a následně na reálné kolaborativní aplikaci.

Reference

[1] Advances in Robot Manipulators. Online. IntechOpen, 2010. ISBN 978-953-307-070-4. Dostupné z: https://doi.org/10.5772/238

[2] MZV. Aktuality. Online. 2021. Dostupné z: https://mzv.gov.cz/ottawa/cz/aktuality/nejslavnejsi_ceske_slovo_robot_slavi_100.html

[3] SAMARATHUNGA, S. M. A. P. B. Advancing Safety in Physical Human-Robot Interaction: A Contribution Towards the Improvement of Testing Transient Contact. Università degli Studi di Brescia. Dostupné z: Tesi Samarathunga corretta.pdf

[4] WEISS, Astrid; WORTMEIER, Ann-Kathrin a KUBICEK, Bettina. Cobots in Industry 4.0: A Roadmap for Future Practice Studies on Human-Robot Collaboration. Online. IEEE Transactions on Human-Machine Systems. 2021, vol. 51, no. 4, s. 335-345. ISSN 2168-2291. Dostupné z: https://doi.org/10.1109/thms.2021.3092684

[5] ČSN EN ISO 10218-2 ed. 2 (186502) Robotická zařízení – Bezpečnostní požadavky – Část 2: Aplikace průmyslových robotů a robotické buňky. Česká agentura pro standardizaci, 2025

[6] E. Magrini, F. Ferraguti, A. J. Ronga, F. Pini, A. De Luca, and F. Leali, Human-robot coexistence and interaction in open industrial cells. Robot Comput Integr Manuf, vol. 61, p. 101846, Feb. 2020. Dostupné z: https://doi.org/10.1016/j.rcim.2019.101846

[7] B. Hans-Jürgen. Human-Robot Collaboration. International Journal of Robotic Engineering, vol. 5, no. 1, Dec. 2020. Dostupné z: 10.35840/2631-5106/4121

[8] R. Gervasi, L. Mastrogiacomo, and F. Franceschini, "A conceptual framework to evaluate human-robot collaboration," The International Journal of Advanced Manufacturing Technology, vol. 108, no. 3, pp. 841–865, May 2020. Dostupné z: https://doi.org/10.1007/s00170-020-05363-1

[9] Y. Liu, M. Habibnezhad, and H. Jebelli, "Brainwave-driven human-robot collaboration in construction," Autom Constr, vol. 124, p. 103556, Apr. 2021. Dostupné z: https://doi.org/10.1016/j.autcon.2021.103556

[10] Y. Ye, H. You, and J. Du, "Improved Trust in Human-Robot Collaboration With ChatGPT," IEEE Access, vol. 11, pp. 55748–55754, 2023. Dostupné z: 10.48550/arXiv.2304.12529

[11] BionicCobot: Robot spolupracující s člověkem. Online. In: Automatizace.hw. Dostupné z: https://automatizace.hw.cz/bioniccobot.html

[12] GUERTLER, Matthias R.; BAUER, Philipp a BURDEN, Alan. A matrix-based approach to step-wise assess the safety of collaborative robots in manufacturing. Proceedings of the Design Society. 2024. Dostupné také z: https://doi.org/10.1017/pds.2024.258

[13] Statistics: World Robotics 2025. Online. In: Ifr.org. Dostupné z: https://ifr.org/downloads/press_docs/PressConference2025_presentation.pdf

[14] KOLBEINSSON, Ari; LAGERSTEDT, Erik a LINDBLOM, Jessica. Foundation for a classification of collaboration levels for human-robot cooperation in manufacturing. Online. Production & Manufacturing Research. 2019, vol. 7, no. 1, s. 448–471. ISSN 2169-3277. Dostupné z: https://doi.org/10.1080/21693277.2019.1645628

[15] JOCELYN, Sabrina; LEDOUX, Élise; ISVIEYSYS ARMAS MARRERO; BURLET-VIENNEY, Damien; CHINNIAH, Yuvin et al. Classification of collaborative applications and key variability factors to support the first step of risk assessment when integrating cobots. Online. Safety Science. 2023, vol. 166, s. 106219-106219. ISSN 0925-7535. Dostupné z: https://doi.org/10.1016/j.ssci.2023.106219

[16] HUCK, T. P.; LEDERMANN, C. a KRÖGER, T. Simulation-based Testing for Early Safety-Validation of Robot Systems. In: 2020 IEEE Symposium on Product Compliance Engineering – (SPCE Portland). 2020, s. 1–6. Dostupné z: https://doi.org/10.1109/SPCE50045.2020.9296157

[17] CHEMWENO, Peter; PINTELON, Liliane a DECRÉ, Wilm. Orienting safety assurance with outcomes of hazard analysis and risk assessment: A review of the ISO 15066 standard for collaborative robot systems. Online. Safety Science. 2020, vol. 129, s. 104832-104832. ISSN 0925-7535. Dostupné z: https://doi.org/10.1016/j.ssci.2020.104832

[18] TOM P. HUCK; MÜNCH, Nadine; HORNUNG, Luisa; LEDERMANN, Christoph a WURLL, Christian. Risk assessment tools for industrial human-robot collaboration: Novel approaches and practical needs. Online. Safety Science. 2021, vol. 141, s. 105288-105288. ISSN 0925-7535. Dostupné z: https://doi.org/10.1016/j.ssci.2021.105288

[19] Technical Specification: ISO/TS 15066: Robots and Robotic Devices: Collaborative Robots. 2016

[20] ČSN EN 31010 (010352) A Management rizik – Techniky posuzování rizik. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011

[21] ČSN EN ISO 12100 Bezpečnost strojních zařízení – Všeobecné zásady pro konstrukci – Posouzení rizika a snižování rizika. Praha: Český normalizační institut, 2011

[22] GOPINATH, Varun; ORE, Fredrik; GRAHN, Sten a JOHANSEN, Kerstin. Safety-Focussed Design of Collaborative Assembly Station with Large Industrial Robots. Procedia Manufacturing. 2018, roč. 25, s. 503-510. ISSN 2351-9789. Dostupné z: https://doi.org/10.1016/j.promfg.2018.06.124

[23] TOO CHUAN TAN, Jeffrey; DUAN, Feng; KATO, Ryu a ARAI, Tamio. Collaboration Planning by Task Analysis in Human-Robot Collaborative Manufacturing System. In: 2010. London: IntechOpen, 2010, s. 113–132. Dostupné z: https://doi.org/10.5772/9543

[24] ČSN ISO 31000 (01 0351) Management rizik – Směrnice. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018

[25] ANTONELLI, D. a STADNICKA, D. Predicting and preventing mistakes in human-robot collaborative assembly. IFAC-PapersOnLine, vol. 52, no. 13, pp. 743–748, 2019. Dostupné z: https://doi.org/10.1016/j.ifacol.2019.11.204

Examining the Dynamics of Youth Crime and Delinquency in the Regions of the Slovak Republic

Samuel Hubočan[1], Katarína Kampová[2]

[1] University of Zilina, Faculty of Security Engineering,
Univerzitná 1, 01026 Žilina, samuel.hubocan@uniza.sk

[2] University of Zilina, Faculty of Security Engineering,
Univerzitná 1, 01026 Žilina, katarina.kampova@uniza.sk

Abstract:

This paper examines regional patterns and temporal trends in youth crime and delinquency in the Slovak Republic over the last decade. Using official police statistics from the Ministry of the Interior of the Slovak Republic and demographic data from the Statistical Office's DataCube, the study calculates indices of minors' delinquency (6–13 years) and juvenile crime (13–17 years) for all NUTS 3 regions for the period 2014–2024. The analysis focuses on both overall prevalence and the structure of offences, as well as the dynamics of these indices across time. The results show that the level of juvenile crime is approximately one order of magnitude higher than the level of delinquency among minors, although both indicators exhibit a predominantly declining trend at national and regional level. Marked regional disparities are identified: the Bratislava region records the lowest rates of both minors' delinquency and juvenile crime, whereas the highest values are concentrated in regions of Košice, Prešov and Banská Bystrica, reflecting the broader socio economic divide between western and eastern Slovakia. Property delinquency is the most prevalent form of offending among minors, while juvenile crime is dominated by moral offences, followed by property crime. A positive association is observed between regional levels of minors' delinquency and juvenile crime, suggesting shared underlying risk factors in more disadvantaged territories. The findings highlight the need for regionally differentiated prevention strategies, with particular emphasis on central and eastern Slovakia and on targeted programmes addressing moral crime among juveniles.

Key words: Juvenile Crime, Delinquency of Minors, Level of Crime, Slovak Republic, Crime Prevention.

1 Introduction

The issue of children's and youth safety has become one of the key topics among security and criminology experts in recent years. This debate is not limited to the Slovak Republic, since developed countries generally recognise that the healthy and safe development of young people is a prerequisite for the future prosperity of society. One of the major phenomena that can disrupt this safe and healthy development is crime and other forms of antisocial behaviour [1, 2].

In general, crime can be understood as conduct that has negative consequences for society, affecting its economy, development and overall security [3]. Under Act No. 583/2008 Coll. on the Prevention of Crime and Other Antisocial Activities, as amended, crime is defined as any conduct that constitutes a criminal offence within the meaning of Act No. 300/2005 Coll. the Criminal Code, as amended. Other antisocial activities are defined by the same legal provisions as behaviour that constitutes an offence, another administrative delict, or any other conduct that society does not tolerate and perceives as negative [4, 5]. When a crime is committed by a person under the age of 14 years, the act is described as a delinquency of minors. When studying the behaviour

of these younger delinquents, the age group of 6–13 is examined and considered as able to understand the antisocial behaviour they are committing. When a crime is committed by a person under 18 years of age but above 14 years of age, the act is described as juvenile crime [1, 3].

Crime and other antisocial activities affecting children do not represent rare or isolated phenomena. When crime is examined specifically as criminal activity, it is possible to draw on statistical data, which can be further analysed [6]. Some authors even try to predict future crime using advanced statistical methods and mathematical models [7, 8, 9]. This paper will further examine crime statistics collected by the Ministry of the Interior of the Slovak Republic, which make it possible to analyse the dynamics of crime both at the level of the entire country – NUTS 1 and within individual regions – NUTS 3 [6].

Various preventive measures can be used to reduce crime. Crime prevention, as a distinct field within criminology, examines measures that can be implemented to prevent offending and to mitigate its negative consequences for society. Within modern approaches to the prevention of juvenile crime and minors' delinquency, young people themselves can be actively involved as important actors in prevention efforts [1, 2]. Within this article, the youth crime and delinquency will be examined, trying to understand current trends in crime of juveniles and delinquency of minors. The focus of the article is to provide answers for research questions (RQ):

1. In which regions are the current highest proportion of juvenile crime and minor´s delinquency recorded?
2. What are the dynamics of delinquency and crime in the individual regions of the Slovak Republic over the last ten years?

2 Youth Crime Dynamics in the Slovak Republic (NUTS1)

Socio-pathological phenomena, most notably crime and other forms of antisocial behaviour (delinquency), represent a dynamic phenomenon that changes and evolves over time. The distinctiveness of youth crime and delinquency lies primarily in the causes and conditions under which it arises, which differ from those typical for adult offenders. Numerous studies indicate that one of the key differences is related to the neurobiological development of the brain, which constitutes an important endogenous criminogenic factor. Juvenile offenders aged 14–18 years have an incompletely developed prefrontal cortex, which continues to mature into the mid-twenties. This brain region is responsible for planning, self-control, impulse regulation and the assessment of consequences, and its immaturity helps explain why adolescents tend to be more impulsive, have greater difficulty regulating emotions and are less able to anticipate the long-term impact of their actions [10, 11].

In terms of exogenous criminogenic factors, young people are, compared with adults, more susceptible to peer pressure, fear of missing out on important social experiences (FOMO), and to the quality of relationships within the family, particularly between parents and children [11].

Open source crime statistics compiled by the Ministry of the Interior of the Slovak Republic allow to examine statistical indicators of crime within criminology. Phenomenology in this context focuses on quantitative and qualitative characteristics of crime that can be clearly measured, including its level, structure, dynamics and clearance rate [1].

The level of crime (state of crime) expresses the number of recorded criminal offences committed in each area over a defined period and is expressed in absolute numbers. Because it does not consider the demographic size of the area, this indicator has limited explanatory value. A more informative quantitative measure is the crime

rate (crime level), which adjusts for population size [1]. It is usually expressed as a crime index (I_k), indicating the number of offences per 100,000 inhabitants, calculated according to the formula presented in Equation (1):

$$I_k = \frac{Number\ of\ recorded\ crime\ (delinquency)}{Number\ of\ juveniles\ (minors)\ in\ the\ region} \cdot 100\,000 \quad (1)$$

The dynamics of crime describes changes in the absolute or relative rate of crime over a specified time period. This indicator makes it possible to identify the direction of crime trends, which may be increasing, decreasing or stable over time [1]. To understand which acts of crimes are conducted the indicator of crime structure is also considered. In the Slovak Republic crime structure consists of property crime, violent crime, moral crime, other crime, economic crime and remaining crime [1, 3].

Drawing on the above considerations, it can be concluded that official crime statistics provided by the Ministry of the Interior of the Slovak Republic and demographic data available via the DataCube portal of the Statistical Office of the Slovak Republic [12] provide a suitable basis for examining the dynamics and structure of crime. It is important to note that the accuracy of such statistical analyses depends on the reliability of reporting and recording within public administration. For the purposes of this paper, an overview is prepared of the delinquency index for minors (children under 6-13 years of age) and the crime index for juveniles (14–17 years of age). The development of these indices for the Slovak Republic over the period of 2010–2024 is presented in Figure 1.

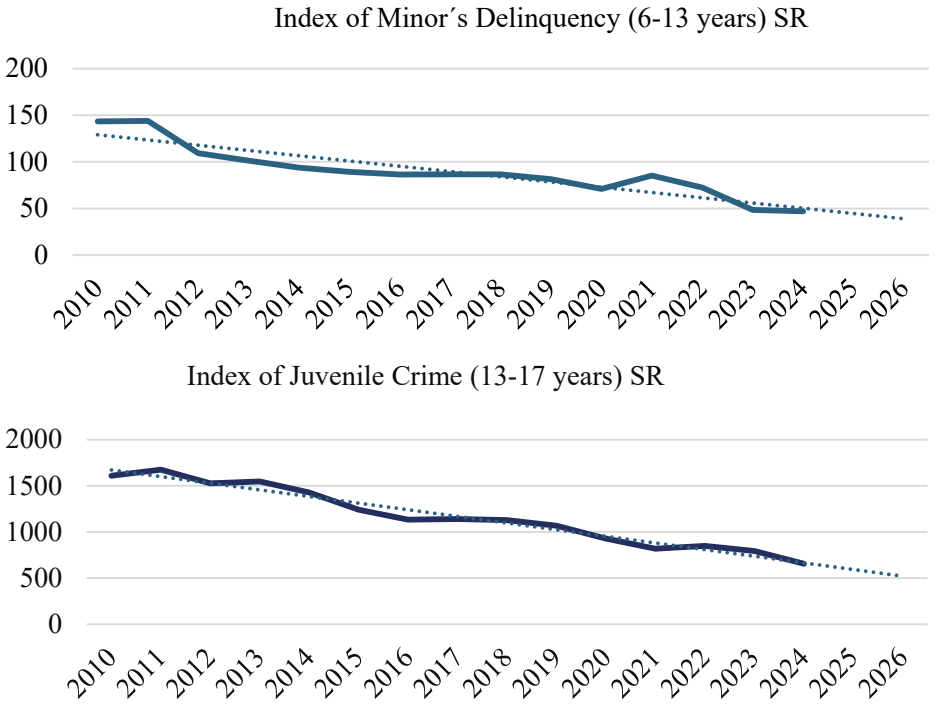


Figure 1. Grafické znázornenie vývoja indexu delikvencie a kriminality
Source: According to [6, 12]

In general, the analysis shows that the level of juvenile crime is approximately one order of magnitude higher than the level of delinquency among minors. At the same time, the results indicate a predominantly downward trend in both indicators, suggesting a gradual decline in minors' delinquency and juvenile crime. It must nevertheless

be emphasised that the future development of these phenomena cannot be predicted with certainty, as crime trends are influenced by a wide range of factors, including unemployment, divorce rates, overall living standards and changes in the legal framework [9, 2, 7].

3 Crime and Delinquency Dynamics in Regions of the Slovak Republic

According to the official statistical data [6, 12] it is possible to analyse average prevalence (for years 2016–2024) of youth crime and delinquency in the regions of the Slovak Republic according to the NUTS 3 division. The analysed data are presented in Figure 2.

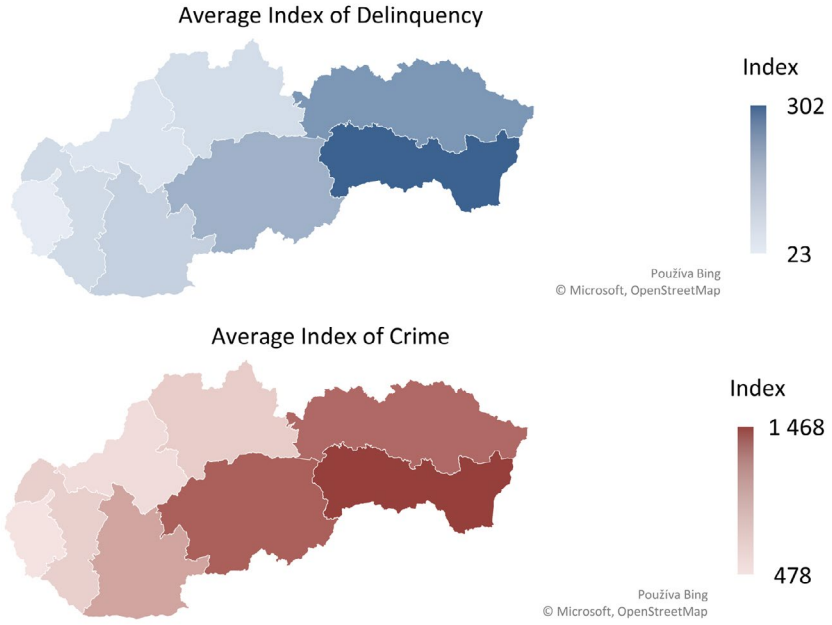


Figure 2. Index of Delinquency and Crime in the regions of the Slovak Republic
Source: According to [6, 12]

Figure 2 illustrates clear regional differentiation in the index of minors' delinquency and juvenile crime across the self-governing regions (NUTS 3) of the Slovak Republic, calculated as recorded offences per 100,000 inhabitants (juveniles and minors) using the same indicator as defined earlier in the paper. The Bratislava region exhibits the lowest levels of both minors' delinquency and juvenile crime, indicating a comparatively more favourable security situation for children and adolescents in the capital region. By contrast, the highest index values are concentrated in the eastern part of the country, particularly in regions such as Prešov and Košice, where both forms of youth offending substantially exceed the national average. This east–west gradient in youth crime broadly mirrors long standing socio economic disparities in Slovakia, where the economically strongest and most developed Bratislava region contrasts with structurally weaker eastern regions characterised by higher unemployment, lower average incomes and more limited labour market opportunities [13, 14].

Figure 3 captures the current dynamics of the delinquency and crime indices for minors and juveniles in individual regions over the years 2019–2024.

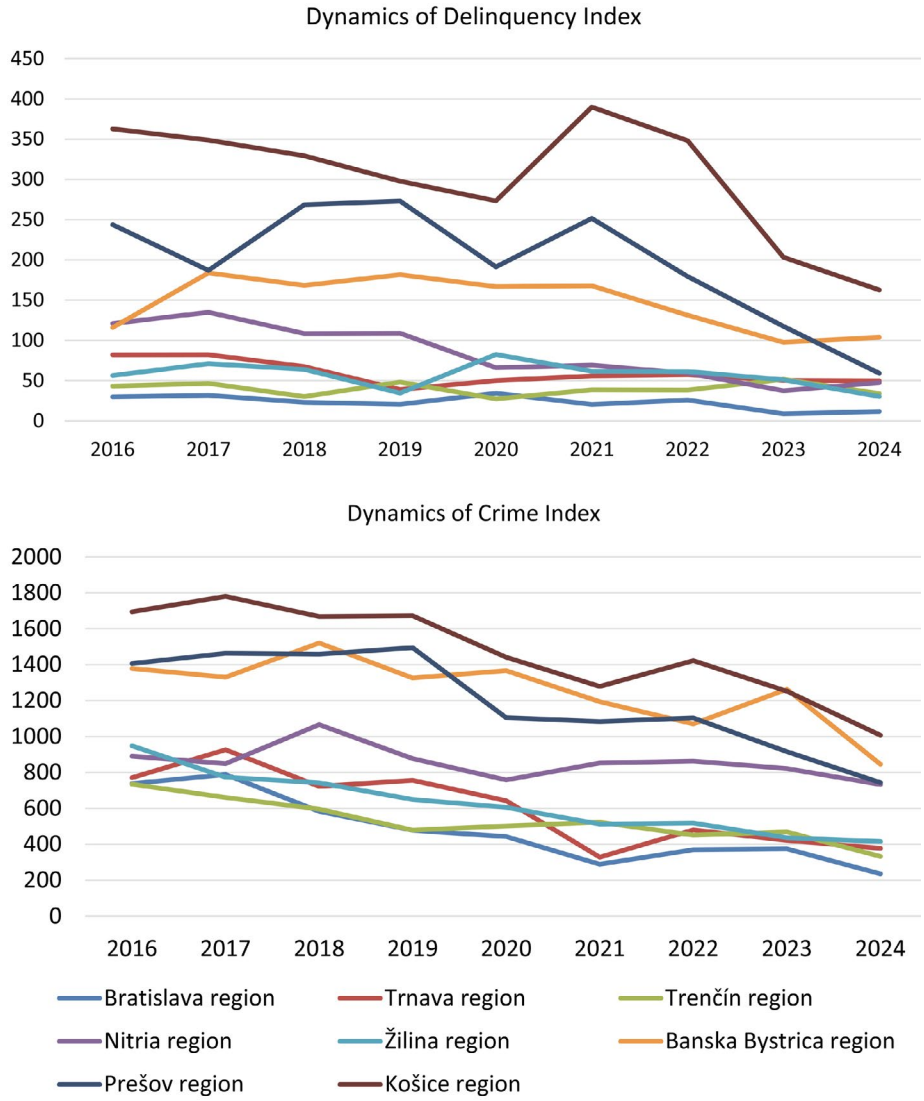


Figure 3. Dynamics of Delinquency and Crime Index in the regions of the Slovak Republic
Source: According to [6, 12]

In line with the national trend, most regions show a gradual decline in both indicators, suggesting a generally decreasing involvement of young people in criminal and delinquent behaviour over time. Despite this overall downward trajectory, the relative positions of the regions according to the frequency of crime and delinquency occurrence remains largely stable: the Bratislava region consistently ranks among the regions with the lowest levels, while the eastern regions maintain the highest indices throughout the observation period, indicating possible relationship with persistent regional inequalities.

3.1 Specifics of Delinquency in Regions of the Slovak Republic

Figure 4 presents the average structure and prevalence of specific types of delinquent behaviour committed by minors across the regions of the Slovak Republic (for years 2019–2024). In general, it can be stated, that the property crime and delinquency is the most frequent overall [1].

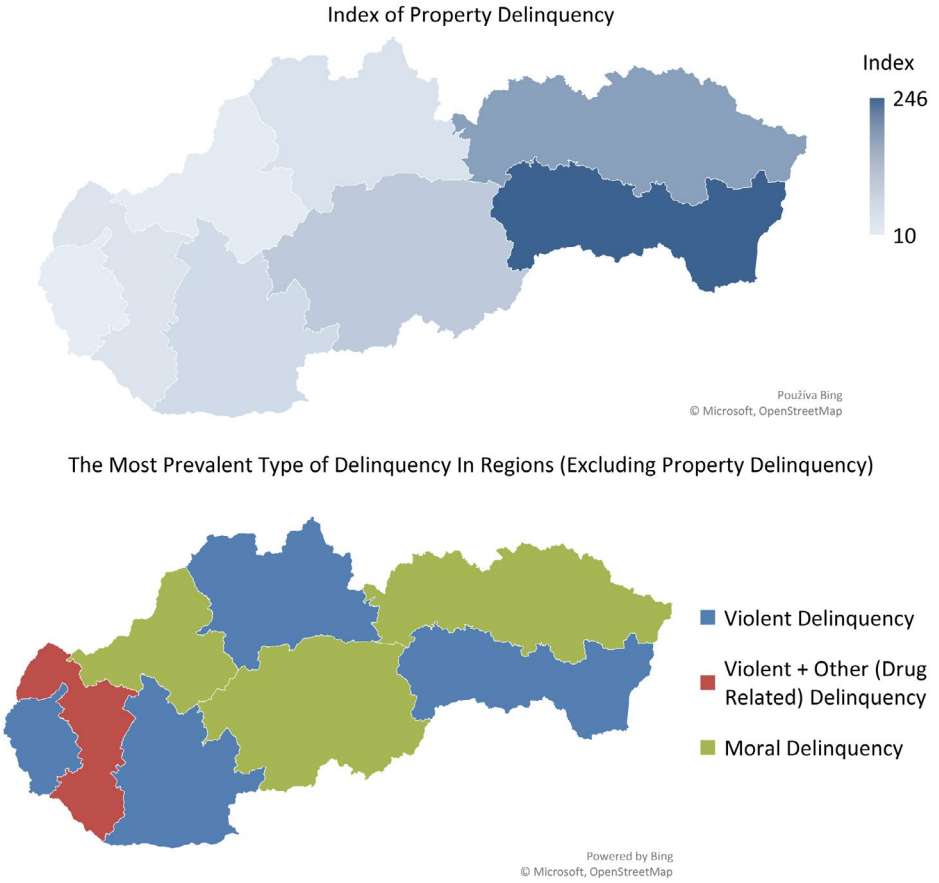


Figure 4. Prevalence of Specific Types of Delinquency in Regions of the Slovak Republic for 2014–2024
Source: According to [6, 12]

The figure shows that regional differences are not limited to the overall volume of delinquency but can also be observed in several main categories of offences, with eastern regions tending to reach higher relative values across multiple types of problematic behaviour. This suggests that minors in socio economically disadvantaged regions may face a more complex combination of risk factors – including poverty, weaker family resources and limited access to quality leisure time and educational activities – which can increase their vulnerability to various forms of delinquency.

3.2 Specifics of Juvenile Crime in Regions of the Slovak Republic

Figure 5 focuses on the average prevalence of specific categories of criminal offences committed by juveniles in the individual regions for years 2014–2024.

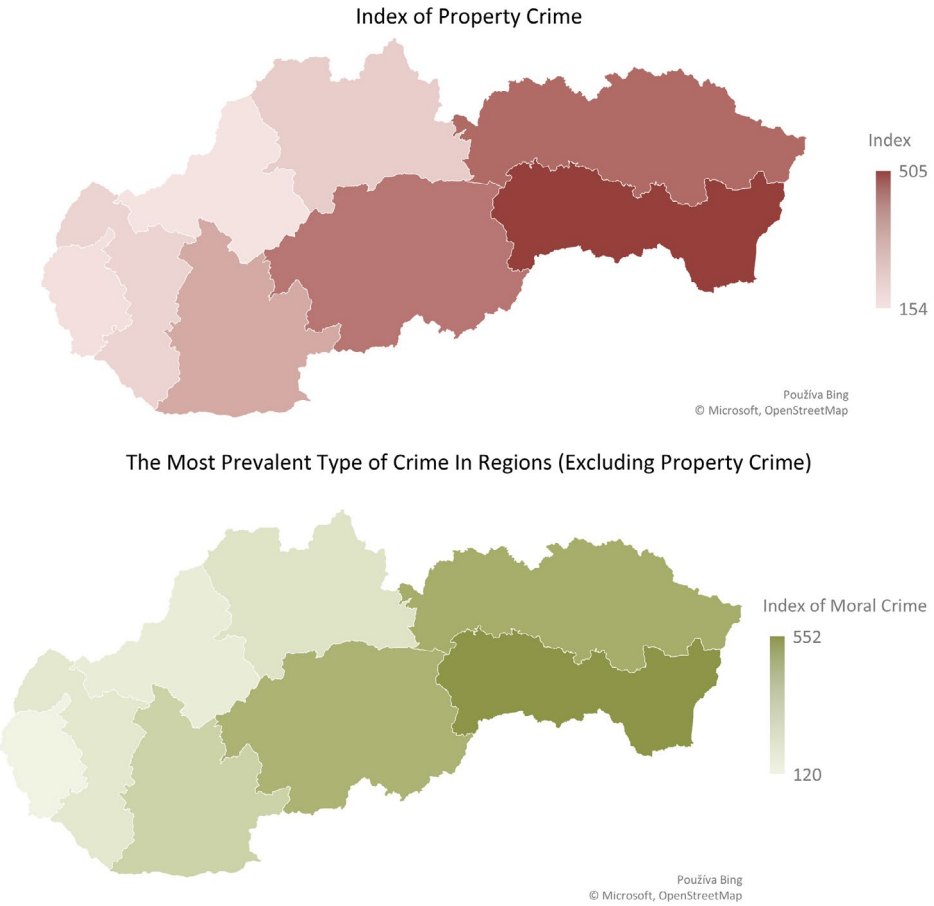


Figure 5. Prevalence of Specific Types of Crime in regions of the Slovak Republic
Source: According to [6, 12]

Like minors' delinquency, the pattern again highlights the Bratislava region as having comparatively lower levels across most offence types, while eastern regions reach the highest indices for several categories of juvenile crime. The concentration of more serious juvenile offending in regions with weaker socio economic development is consistent with broader evidence that unfavourable labour market conditions, higher unemployment and long term poverty are associated with an elevated risk of youth crime and social exclusion.

Interestingly, while property crime is generally considered as the most prevalent type of crime in Slovakia, this pattern is not true for juvenile crime. Across the Slovak regions, the most prevalent juvenile crime is moral crime followed by property crime, which points of to the need for specific crime prevention programs among youth.

4 Conclusion

Across regions, higher levels of minors' delinquency are associated with higher juvenile crime indices, indicating that areas with more frequent early problematic behaviour also tend to record more serious offending among older youth. The relationship is depicted in Figure 6. The values represent average 10-year index of juvenile crime and minor's delinquency.

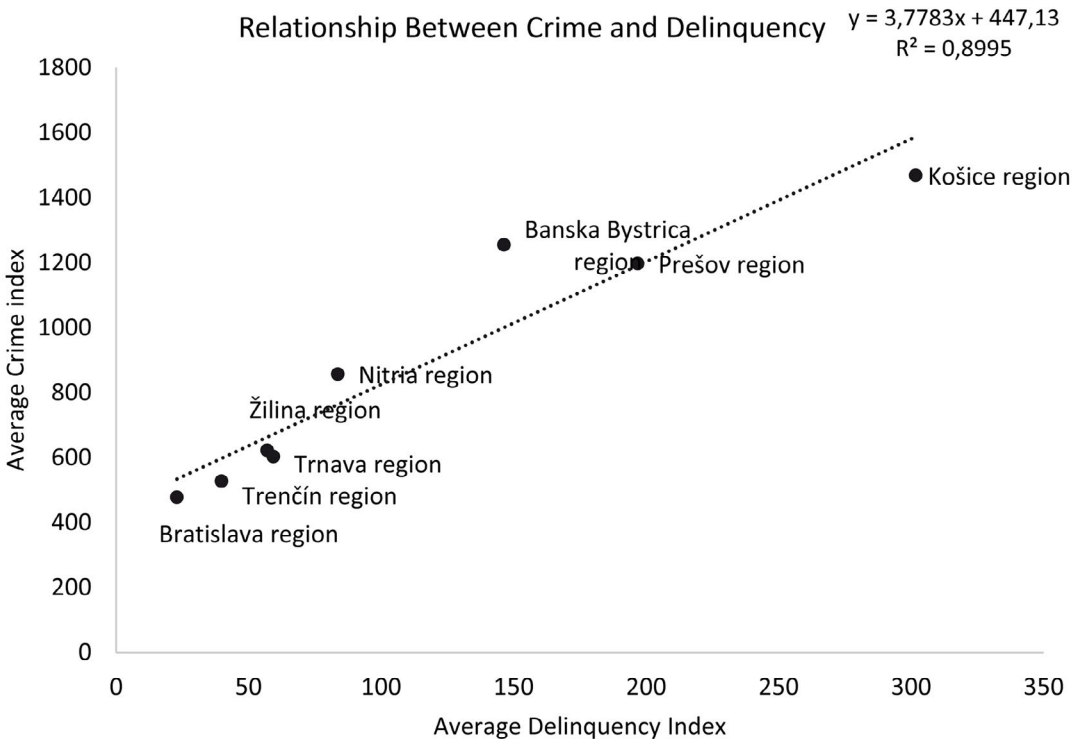


Figure 6. Relationship between Delinquency and Crime

This relationship supports the assumption that common regional risk factors – such as socio economic deprivation, long term unemployment and limited access to services – shape a broader risk environment that affects children and adolescents across developmental stages, with the most pronounced impact observed in the eastern regions of Slovakia.

To answer the RQ1: *"In which regions is the highest proportion of juvenile crime and minors' delinquency recorded?"*, the previously analysed and interpreted data can be used. The regions which are impacted by youth crime and delinquency are Košice, Banská Bystrica and Prešov. These NUTS 3 regions have the highest prevalence of juvenile crime and minor´s delinquency. This finding is an important indicator for the need of specific crime prevention programmes tailored for this specific socio-economic background of central in eastern Slovakia.

To answer the RQ2: *"What is the dynamics of delinquency and crime in the individual regions of the Slovak Republic over the last ten years?"*, it is also possible to use previously analysed data. The overall dynamics tends to have a downward trend, especially in the regions with highest crime prevalence. Even though the trend tends to be declining, the differences among western and eastern Slovakia are significant. These differences open the question of uneven socio-economic development of Slovak regions, directly having impact on youth safety and security. The most prevalent time of delinquency is property delinquency, followed by violent and other (drug) delinquency. Juveniles have different structure of crime, with most prevalent being moral crime, followed by property crime. These findings can help to specify the needs of regions for specific crime prevention needs.

Acknowledgement

This research and contribution were carried out within the framework of project KEGA 058ŽU-4/2025 Gamifikácia a inovácia učebných pomôcok v oblasti kriminológie a verejnej správy; and project UNIZA IGP no. 21103 Development of a Software Tool for Vulnerability Analysis of Primary and Secondary Schools.

Reference

[1] ŠOLTÉS, V. 2022. Kriminológia – Prevencia kriminality a inej protispoločenskej činnosti v regiónoch Slovenska. Žilina: Edis, 2022. ISBN 978-80-554-1889-6

[2] AXFORD, Nick and HUMAYUN, Sajid, 2026. Preventing Youth Crime and Violence: Intervention and evaluation issues. Behavioral Sciences. Online. 9 February 2026. Vol. 16, no. 2, p. 247. DOI 10.3390/bs16020247

[3] GAŠPIERIK, L. 2010. Prevencia kriminality a inej protispoločenskej činnosti. Žilina: Multiprint s. r. o. 2010. ISBN 978-80-970410-0-7

[4] Act No. 583/2008 Coll. on the Prevention of Crime and Other Antisocial Activities, as amended

[5] Act No. 300/2005 Coll. Criminal Code

[6] Crime Statistics in the Slovak Republic, Ministry of the Interior of the Slovak Republic. https://www.minv.sk/?statistika-kriminality-v-slovenskej-republike-xml

[7] RAMANA, B. Venkata, HRUTHIK, Pottolla, ANIL, Nadumpally, KUMAR, Kokku Vinith, SRINIVAS, Sunikari. and SRINIVAS, 2026. Crime rate prediction and analysis using socioeconomic indicators and geospatial data. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT. Online. 19 February 2026. Vol. 10, no. 02, p. 1–9. DOI 10.55041/ijsrem56680

[8] VAIRETTI, Carla, MALDONADO, Sebastián and WEBER, Richard, 2026. Deep learning for crime analytics: A prioritization system for user reports from safety apps. Expert Systems with Applications. Online. 14 February 2026. Vol. 314, p. 131694. DOI 10.1016/j.eswa.2026.131694

[9] ROSSER, Gabriel, DAVIES, Toby, BOWERS, Kate J., JOHNSON, Shane D. and CHENG, Tao, 2016. Predictive crime mapping: arbitrary grids or street networks? Journal of Quantitative Criminology. Online. 9 September 2016. Vol. 33, no. 3, p. 569–594. DOI 10.1007/s10940-016-9321-x

[10] ICENOGLE, G., Steinberg, L., Duell, N., Chein, J., Chang, L., Chaudhary, N., Di Giunta, L., Dodge, K. A., Fanti, K. A., Lansford, J. E., Oburu, P., Pastorelli, C., Skinner, A. T., Sorbring, E., Tapanya, S., Uribe Tirado, L. M., Alampay, L. P., Al-Hassan, S. M., Takash, H. M. S., & Bacchini, D. (2019). Adolescents' cognitive capacity reaches adult levels prior to their psychosocial maturity: Evidence for a "maturity gap" in a multinational, cross-sectional sample. Law and Human Behavior, 43(1), 69–85. https://doi.org/10.1037/lhb0000315

[11] STEINBERG, L., Cauffman, E., Woolard, J., Graham, S., & Banich, M. (2009). Are adolescents less mature than adults? Minors' access to abortion, the juvenile death penalty, and the alleged APA „flip-flop." American Psychologist, 64(7), 583–594. https://doi.org/10.1037/a0014763

[12] Statistical Office of the Slovak Republic (2025). Demographic statistics. Retrieved from? https://datacube.statistics.sk/#!/folder/sk/1001471

[13] MICHÁLEK, A. (2023). Income inequalities and poverty in Slovakia: Development and changes. European Spatial Research and Policy, 30(2), 207-233. https://doi.org/10.18778/1231-1952.30.2.12

[14] KLAMÁR, R. (2011): Development of Regional Disparities in Slovakia with Special Regard to the Region of Eastern Slovakia. In: Acta Facultatis Studiorum Humanitatis et Naturae UniversitatisPrešoviensis, Folia Geographica 18, ISSN 1336-6157, roč. LIII, PU Prešov, 89-170

SWOT analýza vybraných kultúrnych pamiatok

Michal Huliak[1], Iveta Marková[2]

[1] Žilinská univerzita, Fakulta bezpečnostného inžinierstva,
1. mája, 010 26 Žilina, michal.huliak@uniza.sk

[2] Žilinská univerzita, Fakulta bezpečnostného inžinierstva,
1. mája, 010 26 Žilina, iveta.markova@uniza.sk

Abstrakt:

Tento článok sa zaoberá požiarnou bezpečnosťou historických budov divadiel, ktoré vzhľadom na svoj vek, konštrukciu a pamiatkovú hodnotu čelia špecifickým výzvam pri plnení súčasných bezpečnostných noriem. Hlavným cieľom štúdie je systematická identifikácia vnútorných a vonkajších faktorov ovplyvňujúcich ich požiarnu odolnosť prostredníctvom SWOT analýzy. Použitá metodika sa sústredila na divadlá v mestskom prostredí. Pomocou podrobného kontrolného zoznamu bol preverený stav protipožiarnych prvkov, technického vybavenia, používanie ochranných náterov, manipulácia s otvoreným ohňom a činnosť požiarnych hliadok. Výsledná SWOT analýza definovala kľúčové silné stránky, ako sú upravené kulisy a vyhovujúce únikové cesty, no poukázala aj na slabé stránky v podobe chýbajúcich technológií či absencie reálnych evakuačných cvičení s divákmi. Príležitosti vidí výskum v lepšom zaškolení personálu a prechode na elektrické náhrady ohňa, zatiaľ čo hlavné hrozby predstavujú riziká počas predstavení a technické prekážky brániace funkcii požiarnych uzáverov. Zistenia poskytujú strategický základ pre rozvoj cielených metód prevencie a ochrany týchto kultúrnych pamiatok.

Kľúčové slova: kultúrne pamiatky, divadlá, požiarna ochrana, požiarna prevencia, SWOT analýza.

1 Úvod

Historické budovy predstavujú jedno z najcennejších historických bohatstiev každej civilizácie alebo krajiny. [1] Historické budovy sú neoceniteľnou súčasťou kultúrneho dedičstva, ich zraniteľnosť voči požiarom si vyžaduje špecifický prístup. Zachovanie pamiatkových objektov je dôležité nielen pre ich kultúrny a historický význam, ale aj pre ich jedinečné charakteristiky, vrátane architektúry, výzdoby a cenných predmetov, ktoré sa v nich nachádzajú. Pamiatkové budovy nemožno prestavať tak, aby spĺňali dnešné normy, a preto nemožno považovať za úplne bezpečné. Vzhľadom na ich pamiatkový význam nesmie dôjsť k žiadnym zmenám architektúry ani konštrukčných prvkov týchto budov, preto musíme k protipožiarnej ochrane týchto budov pristupovať odlišne.

Skutočnosť, že ide o budovy so spoločenskou hodnotou, znamená, že ich zachovanie a ochrana pred požiarom sú na prvom mieste. Identifikácia a opatrenia proti požiaru sa preto musia prijať čo najskôr po jeho vzniku. (Torero, 2019) [2] Požiarne riziká predstavujú významnú výzvu pre ochranu kultúrnych pamiatok. Riziko požiaru je v týchto budovách výrazne vyššie kvôli ich konštrukčným metódam a vlastnostiam materiálov. (Neto, 2020) [3]

Kaplan vo svojom článku rozoberá potrebu hodnotenia požiarnych rizík a výberu vhodných protipožiarnych zlepšení pre historické budovy. Zdôrazňuje dôležitosť zohľadnenia fyzického vplyvu týchto zlepšení na historický charakter a význam budov. Zdôrazňuje minimálny fyzický zásah, pričom ako primárne stratégie obhajuje riadenie a prevenciu pred požiarmi. Článok sa zaoberá aj dôležitosťou priebežnej údržby a naznačuje, že budúci technologický pokrok poskytne menej invazívne riešenia požiarnej bezpečnosti. [4]

Vásconez a kolektív (2021) v ich článku rozoberajú príčiny a dôsledky požiarov kultúrnych pamiatok po celom svete, za obdobie 1990 až 2019. Identifikovali päť hlavných príčin vzniku požiaru a to vandalizmus, činnosti počas rekonštrukcii, skraty elektrických rozvodov, nehody a z nezistených príčin. Výskum poukazuje na prirodzenú zraniteľnosť týchto historických stavieb vzhľadom na ich vek a absenciu protipožiarnych a ochranných opatrení počas ich pôvodnej výstavby. Štúdia zdôrazňuje kritickú potrebu prispôsobených protipožiarnych opatrení na ochranu týchto kultúrne a historicky významných stavieb pred katastrofami súvisiacimi s požiarom. [5]

Bernardini a kolektív (2016) sa vo svojej štúdii venovali evakuácii osôb z historického divadla. Poukázali na dôležitosť správania osôb v objektoch počas evakuácie, architektonické prvky priestorov, ako aj neznalosť prostredia a stiesnenosť priestorov v ktorých sa pohybujú, vzhľadom k počtu osôb v objekte. Navrhli najlepšie možné únikové cesty, s využitím núdzového osvetlenia, ako aj hlasovej signalizácii požiaru, ktoré naviedlo osoby v objekte na najkratšie možné únikové východy a použitie sekundárnych únikových ciest. Čas evakuácie sa znížil o 26 %, zvýšilo as využitie sekundárnych únikových ciest o 88 % čím sa zároveň znížilo nebezpečenstvo preplnenia únikovej cesty a zníženiu rýchlosti osôb. [6]

V mestských prostrediach sú najčastejšími príčinami vzniku a šírenia požiarov úzke uličky medzi budovami, spoločné steny medzi viacerými budovami, obyvatelia alebo správcovia budov, ktorí nie sú ochotní investovať do opráv, skladovanie horľavých materiálov, nedostatok otvorených priestorov a nekvalitné rozvodné siete elektriny a plynu. [7, 8]

2 Metodológia

V tomto článku sme sa rozhodli zahrnúť medzi objekty výskumu kultúrne pamiatky, ktoré slúžia ako divadlá, alebo divadlá v kultúrnych pamiatkach. Bolo to z viacerých dôvodov:

- Ide o objekty, v ktorých sa ľudia pravidelne zdržiavajú po dlhú dobu, niekoľkokrát týždenne počas divadelnej sezóny.
- Sú to miesta stretávania s pevnými sedadlami v hlavných sálach.
- Sú to budovy v mestskom prostredí.
- Budovy obsahujú veľké množstvo horľavých materiálov používaných na divadelné účely, ako sú kulisy, rekvizity a kostýmy.
- Divadlá v pamiatkových budovách sa od seba líšia vekom a architektonickým štýlom, takže sú to budovy s rovnakým účelom, ale odlišnou konštrukciou a funkčným dizajnom.

Vybrali sme tieto objekty:

- Národný dom, Slovenské komorné divadlo Martin;
- Historická budova Národného divadla Košice;
- Malá scéna Národného divadla Košice;
- Divadlo Jána Palárika;
- Historická budova Divadla Jonáša Záborského;
- Stavovské divadlo v Prahe;
- Národní divadlo v Prahe;
- Státní opera v Prahe.

Obrázok 1. Vybrané kultúrne pamiatky

Na účely preskúmania súčasného stavu protipožiarnej ochrany sme vypracovali kontrolný zoznam. Pre väčšiu prehľadnosť a presné vymedzenie oblastí, na ktoré sa zameriavame, sme ho rozdelili do niekoľkých kategórií:

- typ konštrukcie budovy, kapacita zhromažďovacích priestorov, ich umiestnenie, typ sedenia,
- používanie otvoreného ohňa počas predstavení, horľavé materiály v budove, kulisy a opony, skladovanie kulís a rekvizít,
- požiarne vybavenie v budove, protipožiarne bariéry, protipožiarne koberce, protipožiarne nátery,
- prítomnosť protipožiarnych hliadok počas predstavení, ich počet, umiestnenie, identifikácia, povinnosti, vybavenie na zásah a či sú usporiadatelia členmi protipožiarnej hliadky,
- vykonávanie protipožiarnych cvičení.

Na zistenia aplikujeme SWOT analýzu, aby sme identifikovali súčasné silné a slabé stránky, ako aj budúce hrozby a príležitosti. Podstatou SWOT analýzy je identifikovať silné a slabé stránky vnútorného prostredia nehnuteľnosti a príležitosti a hrozby vonkajšieho prostredia. Posúdením dôležitosti faktorov, ktoré ovplyvňujú stav budov, a faktorov, ktoré ovplyvňujú ich okolie, je možné zvoliť vhodný typ stratégie na ich ochranu. [9]

Silné stránky sa týkajú vnútorných faktorov, ktoré zvyšujú odolnosť budovy voči vzniku a následkom požiarov. Slabé stránky sú vnútorné faktory, ktoré oslabujú budovy voči požiarom a znižujú ich schopnosť dosiahnuť požadovanú protipožiarnu ochranu. Príležitosti predstavujú vonkajšie faktory, ktoré môže organizácia využiť na dosiahnutie svojich cieľov – zvýšenie požiarnej odolnosti budovy. Hrozby predstavujú vonkajšie faktory, ktoré môžu ohroziť bezpečnosť budovy a sú rovnaké pre všetky budovy tohto typu. Rozdiely medzi budovami spočívajú v ich schopnosti prispôsobiť sa vplyvu hrozieb a nebezpečenstiev. [9]

3 Výsledky

Tabuľka 1. Kvalitatívna SWOT analýza pre vybrané kultúrne pamiatky

	Pozitíva	**Negatíva**
Súčasnosť	***Silné stránky***	***Slabé stránky***
	1. Kulisy ošetrené protipožiarnym náterom 2. Prítomnosť požiarnotechnických zariadení 3. Vybavenie a počet členov asistenčnej protipožiarnej hliadky na predstaveniach 4. Hlavný sklad kulís umiestnený mimo priestoru objektu 5. Dobrý stav únikových ciest a ich počet	1. Absencia niektorých druhov požiarnotechnických zariadení v objektoch 2. Používanie otvoreného ohňa počas predstavení 3. Nevykonávanie cvičnej evakuácie s osobami v priestore hľadiska a cvičenia zásahu do objektu jednotkami HaZZ 4. Absencia osvetlenia komunikácii v priestore hľadiska počas predstavenia 5. Chýbajúce požiarne uzávery
Budúcnosť	***Príležitosti***	***Hrozby***
	1. Preškolenie uvádzačov na členov asistenčnej protipožiarnej hliadky 2. Požiarny koberec do priestoru javiska 3. Vykonanie cvičnej evakuácie s osobami v objekte spolu s cvičným zásahom HaZZ 4. Obmedzenie používania otvoreného ohňa výmenou za elektrické alternatívy, projekcie, laserové efekty 5. Vytvorenie čiastočne chránených únikových ciest v priestoroch mimo hľadiska	1. Vznik požiaru počas predstavenia 2. Oneskorenie začiatku evakuácie, obmedzenia pri evakuácii 3. Obmedzenia požiarnej opony v prípade vzniku požiaru 4. Nemožnosť rýchleho zásahu členmi APH k vznikajúcemu požiaru kvôli kulisám 5. Založenie úmyselného požiaru

Silné stránky

To, že kulisy sú ošetrené protipožiarnym náterom predstavuje výrazne pozitívny faktor, pri znižovaní rizika šírenia požiaru v objekte. Kulisy sú odolnejšie na plameň a šírenie tepla. Vďaka tomu je znížené riziko rozvoja požiaru a prenosu z kulís na iné materiály a neprispievajú k rozvoju požiaru v počiatočnej fáze. Kulisy boli ošetrené protipožiarnym náterom ošetrené v siedmych sledovaných objektoch.

Vo väčšine skúmaných objektov bolo prítomné aspoň jedno požiarnotechnické zariadenie. V siedmych objektoch je inštalovaná EPS, v šiestich ZOTaSH a v štyroch SHZ. Tieto zariadenia výrazným spôsobom zvyšujú požiarnu bezpečnosť v objektoch, ako aj ochranu osôb, ktoré sa v nich zdržujú.

Prítomnosť asistenčnej protipožiarnej hliadky hodnotíme ako pozitívny faktor. V siedmych divadlách bol počet členov hliadky dvoch a viac. Vybavenie členov bolo vyhovujúce v každom sledovanom objekte.

Umiestnenie hlavného skladu kulís mimo objektov, hodnotíme kladne. Znižuje sa tým množstvo horľavého materiálu ktoré sa nachádza v objektoch.

Aj keď únikové cesty vo väčšine priestoroch pre divákov sú nechránené únikové cesty, ich počet a riešenie v objekte považujeme za silnú stránku. Iba jeden priestor má z hlavného sálu jednu únikovú cestu, zvyšné priestory majú dve a viac únikových ciest.

Slabé stránky

Vo väčšine objektov je inštalovaný aspoň jeden druh požiarnotechnického zariadenia. Absenciu ostatných však považujeme za slabú stránku. Zariadenie na odvod tepla a splodín horenia chráni priestor hľadiska a javiska, čo absentuje v niektorých objektoch, ako aj stabilné hasiace zariadenie, ktoré by mohlo chrániť priestor javiska a skladu. Bez týchto zariadení nebude v objektoch dosiahnutý najvyšší level požiarnej ochrany.

Otvorený oheň počas predstavení popredstavuje negatívny faktor v ochrane pred požiarmi. Môže spúšťať požiarne hlásiče v priestore, ale aj viesť k vzniku požiaru či ohrozeniu života a zdravia hercov. Taktiež môže dôjsť k poruche pri zakladaní otvoreného ohňa či skladovaní horľavých materiálov a iniciačných zdrojov čo taktiež zvyšuje riziko vzniku a šírenia požiaru.

Nevykonávanie cvičnej evakuácie s osobami v priestore hľadiska považujeme za slabú stránku pri ochrane osôb, ktoré sa môžu nachádzať v priestoroch divadla. Ide o osoby neznalé objektu, kedy môže medzi nimi vzniknúť panika či dezorientácia. Neznalosť zasahujúcich jednotiek do objektu s vnútorným zhromažďovacím priestorom považujeme za negatívnu stránku, nakoľko to môže predstavovať predĺženie reakčného času na mieste zásahu.

Neosvetlenie komunikácii v priestore počas predstavení považujeme za slabú stránku. V prípade výpadku elektrickej energie, alebo inej technickej chybe nebude možné mať zapnuté osvetlenie v priestore. To by mohlo spôsobiť spomalenie evakuácie, či pády a nehody pri evakuácii divákov z priestoru.

Chýbajúce požiarne uzávery, zo skladov, zo zhromažďovacích priestorov, na únikových cestách, či medzi požiarnymi úsekmi považujeme za slabú stránku, nakoľko sa zvyšuje riziko prenosu požiaru, medzi týmito požiarnymi úsekmi. To vytvára zvýšené riziko pre celý objekt, ako aj pre osoby ktoré sa v ňom nachádzajú.

Príležitosti

Preškolenie uvádzačov na členov evakuačnej hliadky príležitosť na výrazné zvýšenie bezpečnosti v divadle. Ich znalosti a prítomnosť môžu výrazne skrátiť reakčný čas a zefektívniť únik ľudí v prípade požiaru.

Inštalácia protipožiarneho koberca na javisko je príležitosť, ako výrazne zvýšiť bezpečnosť divadla. Pôsobí ako účinná bariéra, ktorá odoláva vysokým teplotám a bráni šíreniu ohňa po povrchu javiska. Jeho prítomnosť pomáha zamedziť poškodeniu javiskovej podlahy a zároveň zabezpečuje, že aj v prípade požiaru je priestor pre prácu hasičov a evakuáciu osôb oveľa bezpečnejší

Vykonávaním týchto cvičení by sa odstránili chyby či nedostatky riešenia evakuácie v objekte a dodalo by to zamestnancom zručnosti pri riadení evakuácie. Jednotky HaZZ by si precvičovali zásah do celého objektu, vedeli by kde sa nachádzajú rizikové miesta, ako aj kde by sa mohli nachádzať osoby ktoré boli prítomné na predstavení ktoré nestihli uniknúť na voľné priestranstvo.

Nahradenie otvoreného ohňa za alternatívne zariadenia, ako elektronické cigarety, sviečky a podobne, ako aj znázorňovanie ohňa pomocou projekcii či laserových efektov by znížilo riziko vzniku a šírenia požiaru počas predstavení, ako aj spúšťania falošných poplachov EPS. Taktiež by to malo pozitívny vplyv na divákov, nakoľko by nedochádzalo k šíreniu dymu do priestoru hľadiska čo môže u niektorých divákov so zdravotnými problémami vyrušovať či pôsobiť im kašeľ alebo dusenie.

Vytvorenie čiastočne chránených únikových ciest v priestoroch mimo hľadiska je dôležitou príležitosťou na zvýšenie bezpečnosti v divadle. Táto zmena by chránila evakuačné trasy pred dymom a teplom a zabezpečila by, že sa ľudia budú môcť pohybovať bezpečne a plynule.

Hrozby

Používanie otvoreného ohňa počas predstavení predstavuje hrozbu vzniku a šírenia požiaru počas predstavení. Mohlo by dôjsť k neodpornej manipulácii, či k nehode, kedy by došlo k rozšíreniu požiaru na rekvizity a mohlo by to ohroziť hercov a divákov, ale mohlo by dôjsť ak k rozšíreniu požiaru tak, že by došlo k poškodeniu samotného objektu.

V nami sledovaných objektoch sme zistili viacero príčin, prečo by mohlo dôjsť k oneskoreniu evakuácie, či by boli isté obmedzenia pri evakuácii. Chýbajúca elektrická požiarna signalizácia môže spomaliť čas evakuácie, najmä jej začiatok. Chýbajúce požiarne uzávery na únikových cestách taktiež berieme ako slabú stránku, ako aj menej ako 2 únikové cesty zo zhromažďovacích.

Nemožnosť zatiahnutia opony kvôli kulisám presahujúcim do oblasti opony predstavuje výraznú hrozbu, nakoľko sa neguje vlastnosť požiarnej opony. Protipožiarna opona, ktorá nezastaví šírenie požiaru ako aj splodín horenia, neplní svoju základnú funkciu izolovať javisko od sály. To znižuje celkovú bezpečnosť divákov.

Nemožnosť rýchleho zásahu členmi APH kvôli kulisám predstavuje vážnu hrozbu, nakoľko v priestore bývajú vysoké kulisy, alebo komplikovaný prístup pre ich usporiadanie a komplexnosť. V prípade vzniku požiaru je rýchla reakcia kritická. Ak sa členovia APH nedokážu kvôli kulisám na javisku, alebo v zákulisí rýchlo dostať k ohnisku požiaru, môže sa oheň nekontrolovateľne rozšíriť skôr, než bude možné ho uhasiť. To sťažuje počiatočné potlačenie požiaru a zvyšuje riziko pre všetkých prítomných v divadle.

Pri kultúrnych pamiatka, ktoré sú známe svojím kultúrnym významom a využívajú sa zhromažďovanie osôb či reprezentatívne účely, hrozí založenie úmyselného požiaru. Môže ísť ako pri iných typoch objektu o záležitosť zamestnanca, ale najmä niekoho z divákov, či teroristických útokov alebo diverzii iných krajín.

4 Záver

Tento výskum využil SWOT analýzu na systematické hodnotenie požiarnej bezpečnosti kultúrnych pamiatok, ktoré slúžia ako divadlá a ktoré čelia jedinečným výzvam vzhľadom na svoj historický význam a neschopnosť spĺňať súčasné bezpečnostné normy. Štúdia sa zamerala na divadlá v mestskom prostredí a zdôraznila riziká vyplývajúce z pevných sedadiel a značného množstva horľavých divadelných materiálov, ako sú kulisy a kostýmy. Analýza identifikovala kľúčové silné stránky, ako sú kulisy ošetrené protipožiarnym náterom a dostatočný počet a dobrý stav únikových ciest. Zistili sa však aj kritické slabé stránky, medzi ktoré patrí absencia niektorých protipožiarnych zariadení, používanie otvoreného ohňa počas predstavení a nevykonávanie evakuačných cvičení s ľuďmi v hľadisku. Existujú možnosti zvýšenia bezpečnosti, ako napríklad preškolenie usporiadateľov na členov protipožiarnej hliadky a obmedzenie používania otvoreného ohňa v prospech elektrických alternatív alebo projekcií. Medzi hlavné hrozby patrí vznik požiaru počas predstavenia, obmedzenia protipožiarnych závesov v dôsledku vyčnievajúcich kulís a oneskorená alebo obmedzená evakuácia. Požiarna opona poskytuje strategický základ pre vývoj cielených stratégií riadenia a prevencie požiarov s cieľom riešiť jedinečné zraniteľné miesta týchto kultúrnych pamiatok. Ochrana týchto neoceniteľných pamiatkových budov si vyžaduje uprednostnenie neintervenčných opatrení na zvýšenie ich odolnosti voči požiarom.

Referencie

[1] Salleh, N.H.; Mohtar, M.A.W. Active Fire Safety Measures In The Heritage Timber Buildings In Malaysia. PLANNING MALAYSIA 2020, Vol. 18. DOI: 10.21837/pm.v18i12.741.citace 2

[2] Torero, J.L. Fire Safety of Historical Buildings: Principles and Methodological Approach. International Journal of Architectural Heritage 2019, Vol. 13(7), pp. 926–940. https://doi.org/10.1080/15583058.2019.1612484

[3] Neto, J.T.; Ferreira, T.M. Assessing and mitigating vulnerability and fire risk in historic centres: A cost-benefit analysis. Journal of Cultural Heritage 2020, Vol. 45, pp. 279–290. https://doi.org/10.1016/j.culher.2020.04.003

[4] Kaplan, Marilyn. (2003). Considering Fire-Safety Improvements to Historic Buildings. APT Bulletin. 34. 10. 10.2307/1504865

[5] Venegas Vásconez, Diego & Ayabaca Sarria, César & Erazo, Oswaldo & Medina, Ana & Farias, Oscar. (2021). Fires in World Heritage Buildings. Artificial Intelligence. 1. 1-15. 10.1007/978-3-030-68080-0_32

[6] Bernardini, G., Azzolini, M., D'orazio, M., Quagliarini, E. (2016). Intelligent evacuation guidance systems for improving fire safety of Italian-style historical theatres without altering their architectural characteristics. Journal of Cultural Heritage. in press,. 10.1016/j.culher.2016.06.008

[7] Himoto, K., Tanaka, T. (2008) Development and validation of a physics-based urban fire spread model, Fire Saf. J. 43 (October (7)) (2008) 477–494, http://dx.doi.org/10.1016/j.firesaf.2007.12.008

[8] Ferreira, T.M., (2019) Notre Dame cathedral: another case in a growing list of heritage landmarks destroyed by fire, Fire 2 (April (2)) (2019) 20, http://dx.doi.org/10.3390/fire2020020

[9] Hudáková, M., Buganová, K. 2020. Metódy a techniky manažmentu rizík v podniku. 1. vydanie. Žilina: EDIS-vydavateľstvo UNIZA. 2020. 155 s. ISBN 978-80-554-1674-8

Interaktívny AI agent pre prácu s geografickými informačnými systémami

Daniel Chovanec[1], Jozef Ristvej[2], Jozef Kubás[3], Ivan Buday[4]

[1] Žilinská univerzita, Fakulta bezpečnostného inžinierstva, 1. mája, 010 26 Žilina, daniel.chovanec@uniza.sk

[2] Žilinská univerzita, Fakulta bezpečnostného inžinierstva, 1. mája, 010 26 Žilina, jozef.ristvej@uniza.sk

[3] Žilinská univerzita, Fakulta bezpečnostného inžinierstva, 1. mája, 010 26 Žilina, jozef.kubas@uniza.sk

[4] Žilinská univerzita, Fakulta bezpečnostného inžinierstva, 1. mája, 010 26 Žilina, ivan.buday@uniza.sk

Abstrakt:

Článok predstavuje praktické riešenie GIS AI agenta pre podporu rozhodovania v krízovom manažmente, ktoré spája mapovú vizualizáciu, operatívne priestorové operácie a dôkazovo orientované generovanie odpovedí. Riešenie je navrhnuté pre lokálnu prevádzku v prostredí Streamlit a využíva lokálne nasadený jazykový model cez Ollama, čím eliminuje potrebu cloudovej infraštruktúry. Jadrom prístupu je integrácia ortofotomapy ako rastrového referenčného podkladu (WMS) a tematických mapových vrstiev, ktoré sa aktivujú podľa zámeru používateľského dopytu. Nad týmto podkladom systém vykresľuje vektorové prvky a výsledky priestorových operácií, pričom buffer zóny sú pre operatívne účely realizované ako kruhový overlay s polomerom definovaným v metroch v mapovom klientovi. Aby sa minimalizovali halucinácie a zvýšila auditovateľnosť, odpovede sú podporené mechanizmom retrieval augmented generation (RAG) nad lokálnou knižnicou dokumentov a vektorovým indexom v Chroma.

Klíčová slova: geografický informačný systém, umelá inteligencia, krízový manažment, priestorové informácie, dátový manažment.

1 Úvod

Geografické informačné systémy (GIS) predstavujú dôležitú oblasť v krízovom manažmente, nakoľko sú učinným nástrojom podpory rozhodovania a vyhodnocovania vstupných dát ako aj ich vizualizácie. V praxi GIS umožňuje integrovať priestorové dáta z rôznych zdrojov (mapové podklady, infraštruktúra, zraniteľnosť, aktuálne pozorovania) do jednotného obrazu situácie, čím skracuje čas potrebný na orientáciu v udalosti a zvyšuje kvalitu rozhodnutí počas prípravy aj zásahu [1].

Pri plánovaní a odozve je dôležité, že GIS dokáže integrovať heterogénne zdroje dát (napr. mapové podklady, infraštruktúru, administratívne hranice, rizikové vrstvy, pozorovania z terénu) do jednotného „operačného obrazu“, ktorý je použiteľný pre koordináciu medzi aktérmi aj pre komunikáciu s verejnosťou. Konkrétne prístupy, ako sú hodnotenia zraniteľnosti, priestorové indexy a syntetické mapy rizika, ukazujú, že priestorová dimenzia je zároveň základom pre porovnateľné hodnotenie dopadov naprieč územiami a sociálnymi skupinami. Zároveň sa v praxi ukazuje, že v krízach nestačí mať k dispozícii veľa dát, ale rozhodujúce je vedieť ich rýchlo pretaviť do zdieľaného a zrozumiteľného obrazu situácie, ktorý znižuje koordinačné a informačné trenie medzi zložkami. Koncept „common operational picture“ sa v literatúre uvádza práve ako mechanizmus na prekonanie problémov

zdieľania informácií a koordinácie počas odozvy, pričom jeho prínos je najvyšší vtedy, keď je postavený na integračnej platforme (GIS) a je použiteľný naprieč rolami [2, 3]. Z tohto dôvodu je dôležité prinášať riešenia, ktoré integrujú viaceré čiastkové nástroje (mapové podklady, tematické vrstvy, jednoduché priestorové operácie, reporting) do jedného workflow, pričom používateľsky musia zostať jednoduché, rýchle a operatívne aby sa v čase tlaku minimalizoval počet manuálnych krokov, preklikov a transformácií medzi aplikáciami. Tento dôraz na použiteľnosť a rýchlosť je v súlade aj so smerovaním výskumu v oblasti priestorových rozhodovacích podporných systémov (SDSS), kde sa integrácia dát a postupov považuje za kľúčovú podmienku pre reálne nasadenie v rozhodovacích procesoch [4].

Umelá inteligencia môže GIS v krízovom manažmente významne posilniť tým, že automatizuje spracovanie veľkých objemov priestorových dát a urýchľuje extrakciu relevantných informácií (napr. z diaľkového prieskumu Zeme alebo zo senzorických prúdov). Pre rozhodovanie je pritom kľúčové, aby boli AI výstupy transparentné a interpretovateľné, keďže krízové rozhodnutia musia byť auditovateľné a obhájiteľné [5]. Z tohto dôvodu sa v praxi čoraz viac uplatňuje kombinácia GIS, AI a dôkazovo orientovaných pracovných postupov, kde AI slúži ako akcelerátor analýz a syntézy informácií, zatiaľ čo GIS poskytuje priestorový rámec pre ich interpretáciu, kontrolu konzistencie a vizuálnu validáciu v kontexte územia. Zároveň platí, že účinné prepojenie týchto prístupov si vyžaduje jasné pravidlá práce so zdrojmi a „dôkazový režim“ odpovedí, aby sa minimalizovala tendencia modelov dopĺňať chýbajúce informácie neoverenými tvrdeniami [5, 6].

V súčasnosti sa AI v GIS využíva najmä na spracovanie priestorových dát, automatizáciu analýz a tvorbu máp. Moderné nástroje už dokážu pracovať nielen s klasickými geodátami, ale aj s textom, obrazom a databázami súčasne. Vďaka tomu je možné zadávať úlohy prirodzeným jazykom a AI následne pripraví dotazy, spracuje dáta alebo navrhne vhodný analytický postup. Veľký prínos má AI pri získavaní a kontrole dát. Pomáha napríklad pri vyhľadávaní údajov z geodatabáz, opravách chýb v OpenStreetMap, extrakcii informácií zo sociálnych sietí či vyhodnocovaní údajov zo snímok a fotografií. Zároveň sa čoraz viac využíva aj pri kartografii, kde vie generovať skripty, automatizovať priestorové operácie a pripravovať mapové výstupy v GIS softvéroch, napríklad v QGIS. Dôležitou oblasťou je aj interpretácia máp. Multimodálne modely dokážu rozpoznávať legendy, mierku, symboly a tematický obsah máp, čo otvára priestor pre inteligentnejšiu analýzu priestorových javov. Napriek veľkým možnostiam má AI v GIS aj svoje limity. Problémom môže byť napríklad nepresnosť výstupov alebo nedostatok kvalitných tréningových dát, ktoré môžu spôsobovať halucinácie [7, 8].

V nadväznosti na tieto požiadavky článok predstavuje praktické riešenie GIS AI agenta, ktoré spája mapovú vizualizáciu (ortofoto ako referenčný podklad a tematické vrstvy), operatívne priestorové operácie (napr. buffer zóny) a RAG mechanizmus pre dôkazové odpovede, pričom celé riešenie je navrhnuté na lokálnu prevádzku s dôrazom na rýchlosť, jednoduchosť používania a auditovateľnosť výstupov, ktoré má za snahu poukázať na možnosť práce s geopriestorovými údajmi aj bez odbornej expertízy v GIS.

2 Návrh prístupu a praktické spracovanie

V rámci praktického riešenia bol vytvorený GIS AI agent, ktorý je vzhľadom na vysoké výpočtové nároky súčasných jazykových modelov a hardvérové obmedzenia prevádzkovaný lokálne (offline) pomocou runtime prostredia Ollama. Použitý bol kompaktný model triedy 3.2B (kvantizovaný variant podľa dostupnej pamäte), nasadený v používateľskom rozhraní vybudovanom v Streamlit. Riešenie je navrhnuté ako evidence-first systém na princípe RAG (retrieval augmented generation), t. j. generovanie odpovede je primárne podporené vyhľadanými úryvkami z lokálne spravovaných zdrojov viazaných na konkrétneho špecializovaného agenta. Ak relevantné úryvky nie sú dostupné alebo sú irelevantné, systém prechádza na odpoveď z všeobecných znalostí modelu bez

falošného citovania dokumentov. Tým sa zachová použiteľnosť nástroja aj v situáciách s neúplnou knižnicou dokumentov, pričom sa minimalizuje riziko vymyslených odkazov.

V rámci systému používateľ pracuje v lokálnom UI, kde vyberá aktívneho GIS agenta. GIS agent je súčasťou viacerých agentov, ktoré boli vytvorené, a má vlastný profil (doména, pravidlá správania, požadovaný štýl odpovede) a vlastnú bázu znalostí. Profil sa ukladá v registri agentov a obsahuje odkazy na dve agent-špecifické úložiská:

- priečinok knižnice dokumentov,
- kolekciu vektorového indexu.

Zdroje (vrátane metadátových súborov k datasetom) sa ukladajú do adresárovej štruktúry. GIS agent pri odpovediach uprednostňuje zdroje určené pre svoju doménu (napr. metodiky, technické špecifikácie vrstiev, legendy, mapové štandardy, popisy atribútov, postupy pre QGIS), pričom systém môže podľa konfigurácie dopĺňať kontext aj z „core“ knižnice spoločnej pre viacerých agentov (napr. základné SOP dokumenty alebo všeobecné smernice). Knižnica „core“ predstavuje spoločnú bázu znalosti pre všetkých agentov.

Po nahratí dokumentu systém vykoná:

- extrakciu textu z dokumentu (parser podľa formátu),
- segmentáciu textu na chunky,
- tvorbu embeddingov pre každý chunk lokálnym embedding modelom,
- uloženie embeddingov a metadát do vektorovej databázy (Chroma), pričom každému agentovi prislúcha samostatná kolekcia.

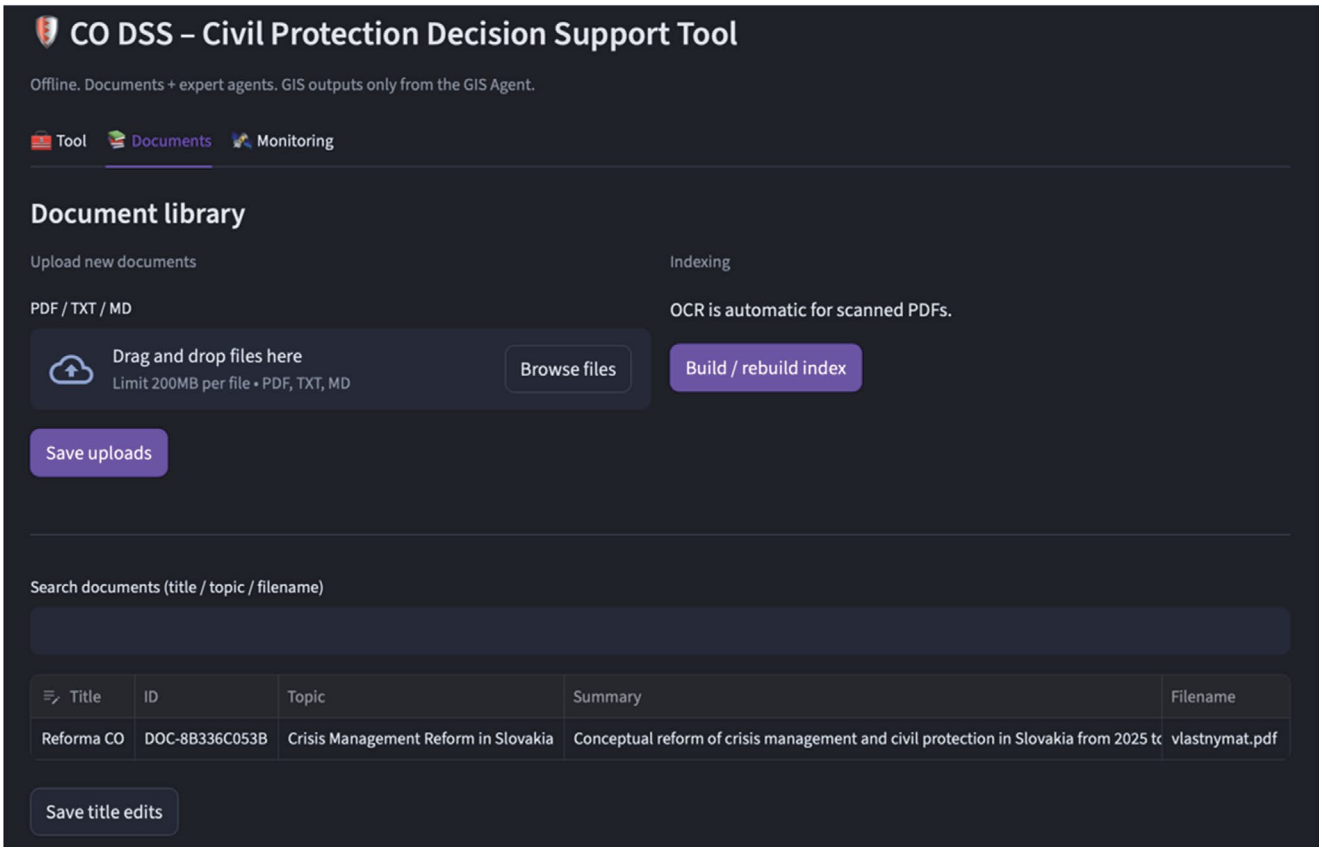
Ak dokument nie je spoľahlivo strojovo čitateľný (napr. sken), pipeline môže použiť OCR režim ingestu, aby sa minimalizovala strata informácie.

Pri prompte systém vytvorí embedding dotazu a vykoná vyhľadanie top-k najbližších chunkov v relevantných kolekciách, minimálne v kolekcii aktívneho agenta, prípadne aj v spoločnej „core“ kolekcii podľa zvoleného rozsahu znalostnej bázy. Výstupom je množina „evidence excerpts“, t. j. úryvkov s metadátami, ktoré sú priložené k promptu. Súčasťou metadát sú minimálne názov dokumentu (Title) a interný identifikátor (ID), aby bolo možné generovať prirodzené citovanie. Vizualizácia RAG inputov sa nachádza na Obrázku 1.

Zostavený prompt obsahuje:

- explicitnú sekciu evidence excerpts (vyhľadané úryvky),
- pravidlo, že faktické tvrdenia musia vychádzať len z týchto úryvkov v prípade, že úryvky sú prítomné a relevantné,
- požadovanú štruktúru výstupu.

Týmto krokom sa minimalizuje tendencia modelu halucinovať v prípade detailov, ktoré nie sú v zdrojoch. Zároveň je dôležité, že systém explicitne zabraňuje citovaniu dokumentov, ak sa nevyhľadal relevantný úryvok, tým sa redukuje riziko nesprávnej atribúcie.



Obrázek 1. Input do znalostních báz RAG

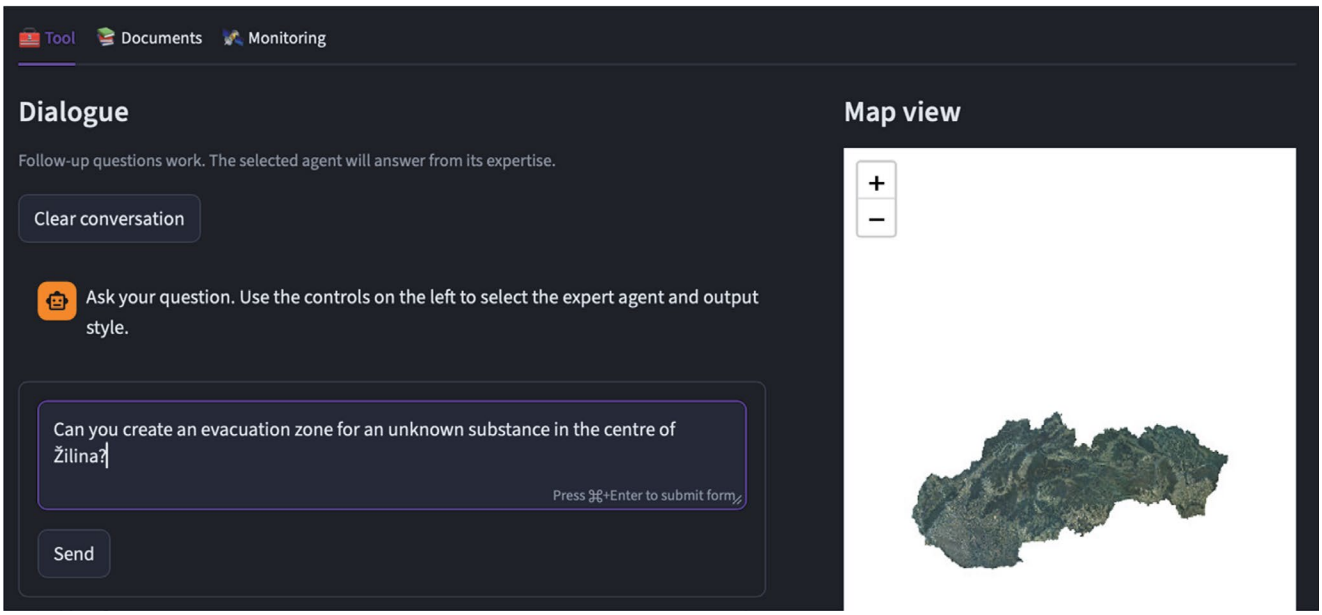
V konečnej fáze je používateľovi zobrazená len finálna odpoveď. Interné medzikroky (draft, kontrola tvrdení, syntéza) sú skryté a sú vyvolané internými promptami pre každý prompt, aby používateľ nebol zahltený viacerými variantmi odpovedí. Z hľadiska metodiky to zodpovedá viacstupňovej kontrole kvality, kde sa oddelene vykonáva verifikácia tvrdení voči evidence excerpts a následná syntéza do jednotného výstupu. Pre GIS agenta sa v tomto režime navyše uplatňuje špecializovaná kontrola konzistencie. Agent musí generovať výstup kompatibilný s mapovou vizualizáciou v UI (napr. aktivácia ortofota a tematických WMS vrstiev podľa zámeru a vykreslenie buffer zóny ako kruh v metroch), pričom mapový klient (Folium/Leaflet) vykonáva samotné vykreslenie.

Integrácia ortofotomapy v implementovanom systéme je navrhnutá ako súčasť mapovej vizualizačnej vrstvy priamo prepojenej s používateľským rozhraním v Streamlit. Ortofotomapa sa v tomto riešení používa ako rastrový referenčný podklad, ktorý poskytuje stabilný vizuálny kontext pre interpretáciu priestorových výstupov. Zmyslom ortofota nie je, aby ho systém analyzoval (nejde o multimodálne spracovanie obrazu), ale aby používateľ videl výsledky priestorových operácií v realistickom kontexte územia a vedel ich okamžite vizuálne overiť. Prakticky to znamená, že ortofoto je načítané ako externá mapová služba, typicky WMS, a mapový klient integrovaný do Streamlit aplikácie ho vykresľuje ako najnižšiu vrstvu mapovej scény. Keďže ide o rastrovú službu, systém ortofoto lokálne negeneruje a nekopíruje, iba ho načítava ako dlaždice (tiles) v čase vykresľovania, čo znižuje nároky na úložisko a zároveň zvyšuje reprodukovateľnosť vizualizácie.

Nad ortofotom sa následne vykresľujú ďalšie vrstvy. Tematické vrstvy, ako sú administratívne hranice, rieky alebo povodňové zóny, sú v implementácii realizované ako samostatné WMS overlay vrstvy. Podstatné je, že tieto vrstvy sa neaktivujú náhodne, ale na základe interpretácie zámeru používateľského promptu. GIS agent alebo mapová logika systému z promptu identifikuje, či používateľ chce vidieť hranice, vodstvo, rizikové zóny

alebo potrebuje vykonať zónovanie okolo incidentu, a podľa toho zostaví mapovú scénu. Používateľ tak nemusí manuálne prepínať vrstvy. Vektorové výstupy, ako je lokalizačný bod incidentu alebo buffer zóna, sa vykresľujú ako najvyššia vrstva, aby boli vždy čitateľné a neprekrývali ich rastrové podklady. Vrstvenie má preto pevný význam: ortofoto poskytuje vizualizáciu, tematické WMS vrstvy dopĺňajú analytický kontext a vektorové prvky reprezentujú konkrétnu úlohu, ktorú systém rieši.

Dôležitou vlastnosťou celej integrácie je priestorová konzistencia. Mapový klient (Leaflet cez Folium) pracuje v geografickom priestore a dokáže vykresliť ortofoto aj tematické WMS vrstvy v jednotnom mapovom rámci. Pri výpočtoch vzdialeností však vzniká typický problém, pretože geografické súradnice sú v stupňoch a nie v metroch. V tvojom riešení je táto praktická požiadavka vyriešená tak, že buffer pre účely operatívnej vizualizácie nevzniká ako klasická geodetická operácia v projektovanom CRS, ale ako kruhový overlay priamo v mapovom klientovi. Leaflet poskytuje objekt kruhu (Circle), ktorému sa zadáva polomer v metroch; systém teda odovzdá mapovému klientovi referenčný bod a hodnotu polomeru a mapový klient vykreslí zónu ohrozenia tak, aby bola metricky interpretovaná. Tento prístup je účelový pre kontext krízového manažmentu, kde je často dôležitejšie mať rýchlo a zrozumiteľne zobrazenú zónu, než realizovať komplexnú geodetickú transformáciu, ktorá je vhodnejšia pre presné kartografické analýzy. Zároveň platí, že ak je potrebná prenositeľnosť do externých GIS nástrojov (napr. QGIS), systém môže zónu exportovať aj ako GeoJSON, buď ako polygonálnu aproximáciu kruhu, alebo ako vektorovú geometriu, ak je implementované jej generovanie. Na Obrázku 2 je možné vidieť UI rozhranie pre GIS agenta pre zadaním promptu.

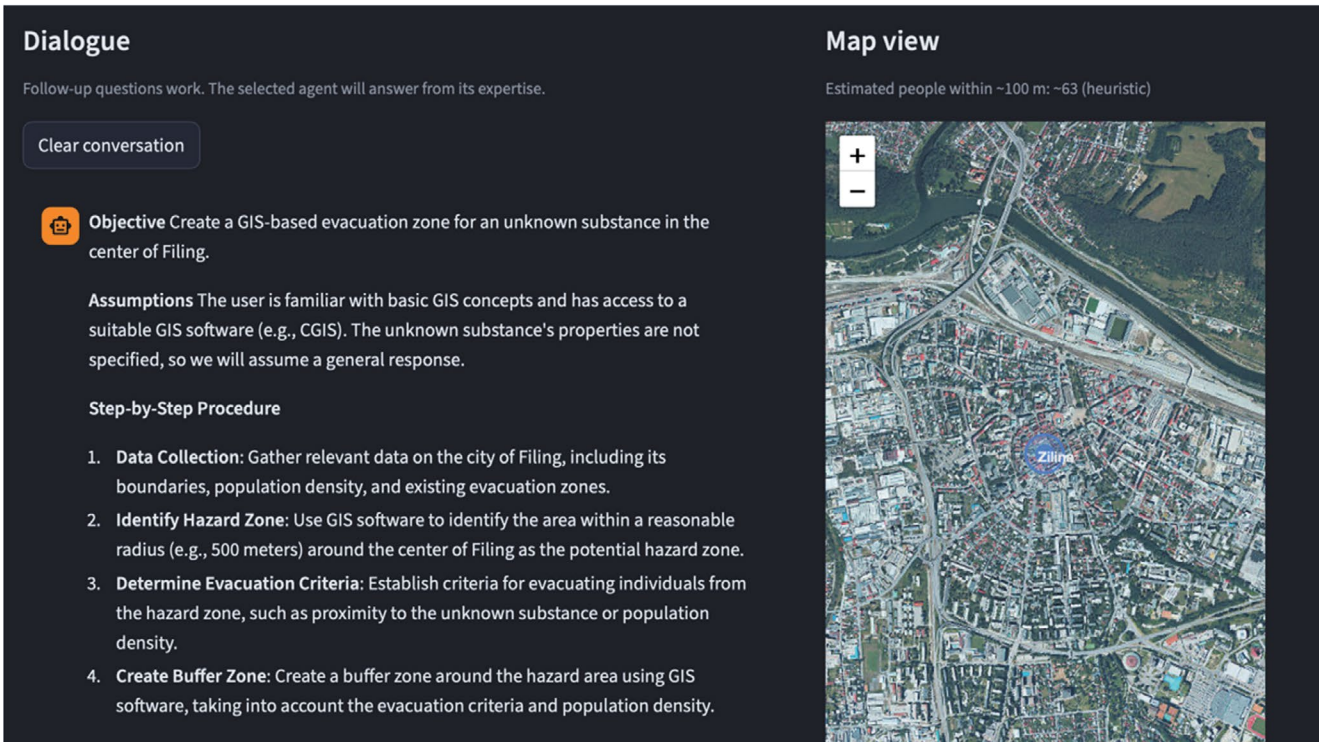


Obrázek 2. UI GIS agenta v prostredí Streamlitu s vykreslenou ortofoto mapou Slovenskej republiky

Samotné vytvorenie bufferu v systéme nadväzuje na to, ako sa určí lokalita incidentu. Používateľ v promptoch môže zadávať súradnice, názov mesta, prípadne adresu alebo ulicu. Systém sa najskôr pokúsi z tejto informácie určiť referenčný bod. Ak sú k dispozícii súradnice, ide o priamy a jednoznačný vstup. Ak používateľ zadá adresu alebo ulicu, vstup sa mapuje na bod pomocou geokódovania. Ak geokódovanie nie je dostupné alebo je vstup príliš všeobecný, systém môže použiť približný bod (napríklad centrum obce). Keď je bod určený, systém z promptu alebo z metodiky stanoví polomer zóny. Ak je polomer uvedený explicitne, použije sa priamo. Ak nie, agent sa snaží odvodiť ho z lokálnej dokumentácie v RAG knižnici. Typicky ide o interné metodiky, normy alebo postupy, ktoré definujú, aká zóna má byť použitá pre konkrétny typ udalosti. Ak taká definícia nie je dostupná,

systém môže použiť pracovný default, ktorý musí byť jasne označený ako predpoklad a nie ako fakt. Následne sa zóna vykreslí ako polopriesvitný kruhový overlay nad ortofotom a tematickými vrstvami, aby bolo možné posúdiť jej zásah v teréne. Vizuálna validácia je v tomto workflow kľúčová, pretože používateľ vie okamžite identifikovať typické symptómy chyby, napríklad nerealisticky veľkú zónu alebo posun voči očakávanej lokalite.

V tejto architektúre je GIS AI agent koncipovaný ako riadiaca a vysvetľujúca vrstva, nie ako samostatný GIS engine. Agent z promptu vytvára metodicky konzistentný postup, odporúča relevantné vrstvy, vysvetľuje význam parametrov a navrhuje kontrolné kroky. Zároveň má agent fungovať v dôkazovom režime, čo znamená, že pri tvrdeniach, ktoré vyplývajú z dokumentov, používa RAG ako zdroj a v odpovedi jasne uvádza, že ide o informáciu z konkrétneho dokumentu (Title, ID). To je významné najmä v krízovom manažmente, kde sa vyžaduje transparentnosť a auditovateľnosť, keďže parametre ako rozsah zóny ohrozenia, typ rizika alebo odporúčané kroky musia byť spätne obhájiteľné. RAG vrstva preto nie je len doplnok pre presnosť odpovede, ale mechanizmus, ktorý umožňuje odlíšiť tvrdenia podložené evidenciou od pracovných predpokladov. Výsledkom je reprodukcibilný workflow, v ktorom sa spojí mapová vizualizácia (ortofoto a tematické vrstvy), operatívna priestorová operácia (buffer) a znalostná opora (RAG), pričom používateľ dostáva súčasne textový výklad aj mapový výstup v jednotnom rozhraní. Konečnú vizualizáciu po zadaní promptu ako aj vykreslenie je znázornené na Obrázku 3.



Obrázek 3. Odpoveď na prompt a vykonanie vizualizácie

3 Diskusia, záver a obmedzenia

Navrhnuté riešenie GIS AI agenta demonštruje nástroj podpory rozhodovania pre krízový manažment, ktorý spája mapovú vizualizáciu, jednoduché priestorové operácie a dôkazovo orientované generovanie odpovedí. Praktický prínos spočíva najmä v tom, že používateľ získava konzistentný vizuálny kontext v podobe ortofotomapy a tematických vrstiev a zároveň vytvára možnosť dostávania textových odporúčaní viazaných na konkrétnu úlohu. V súčasnom stave riešenie podporuje najmä rýchle situačné hodnotenie a vizuálnu validáciu zón, ktoré

sú kľúčové v čase tlaku, keď je potrebné zrozumiteľne definovať rozsah zásahu a komunikovať ho v rámci koordinácie a plánovania.

Z technického hľadiska je hlavným obmedzením veľkosť a kvalita použitého jazykového modelu, ktorá je priamo podmienená dostupným hardvérom. Nasadenie kompaktného kvantizovaného modelu umožňuje lokálnu prevádzku, no zároveň znižuje robustnosť pri komplexnejších úlohách, pri práci s dlhými dokumentmi alebo pri jemných doménových nuansách. V porovnaní s väčšími modelmi je nutné počítať s vyššou citlivosťou na formuláciu promptu, s občasnými nepresnosťami a s potrebou posilňovať odpovede dôkazovou vrstvou (RAG), ktorá kompenzuje slabšie generatívne schopnosti menšieho modelu.

Zároveň je potrebné zdôrazniť, že rozhranie aj samotný agent sú stále vo fáze priebežnej úpravy. Nejde o finálne používateľské rozhranie ani o uzavretý produkt, ale o kontinuálne rozvíjané riešenie, na ktorom sa priebežne pracuje, testuje sa a iteratívne zlepšuje. Už samotná integrácia mapovej vizualizácie do Streamlit prostredia a dopĺňanie ďalších vrstiev ukazuje, že systém je vhodný pre postupné rozširovanie o ďalšie scenáre a funkcie bez nutnosti zásadnej zmeny architektúry.

Veľký priestor na zlepšenie sa aktuálne sústreďuje na presnejšiu prácu s adresnými bodmi. Cieľom je, aby systém vedel v rámci definovanej zóny vypísať aj zasiahnuté ulice alebo časti ulíc a tým podporil praktické rozhodovanie pri evakuácii a operatívnom plánovaní. V súčasnosti je hlavné využitie riešenia najmä vizualizačné, t. j. zobrazenie potreby a rozsahu evakuačnej zóny nad ortofotom a relevantnými vrstvami. Na základe vloženého promptu (Obrázek 2) systém následne podľa metodického usmernenia pre evakuáciu pri pôsobení neznámej látky zvolil rádius 100 m, čím demonštruje schopnosť prepojiť zadanie používateľa s pravidlom z metodiky a premietnuť ho do mapového výstupu.

Do riešenia bol zapracovaný aj odhad počtu obyvateľov v danej zóne, avšak v aktuálnom stave ide len o vizuálny efekt a orientačný indikátor, pretože údaje o počte osôb v konkrétnych budovách nie sú verejne dostupné a teda nie sú integrované do lokálnej databázy systému. Ak by bola spolu s adresnými bodmi dostupná aj informácia o počte osôb (napríklad z interných evidencií, štatistických zdrojov alebo z údajov správcov objektov), bolo by možné realizovať výrazne presnejší odhad počtu osôb v zóne a prepojiť ho s prioritizáciou evakuačných opatrení a postupov.

Celkovo možno konštatovať, že prezentovaný GIS AI agent predstavuje funkčný základ pre offline rozhodovaciu podporu v krízovom manažmente. Jeho aktuálny prínos spočíva v rýchlej vizualizácii zón a v prepojení mapového výstupu s metodickými pravidlami. Súčasne však ostáva otvorený priestor pre ďalší vývoj, predovšetkým v oblasti presnej lokalizácie na úrovni ulíc a adresných bodov, v rozšírení dátových vrstiev a v zvyšovaní spoľahlivosti odpovedí prostredníctvom kvalitnejších modelov alebo optimalizovaného RAG, ak to hardvérové možnosti umožnia.

Poďakovanie

Táto práca bola podporená Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-24-0153.

Reference

[1] JEFFERSON, Theresa L. a JOHANNES, Tay W. Using geographic information systems to support decision making in disaster response. Intelligent Decision Technologies. 2016, 10(2), 193–207. DOI: 10.3233/IDT-160255. Dostupné z: https://doi.org/10.3233/IDT-160255

[2] WOLBERS, Jeroen a BOERSMA, Kees. The Common Operational Picture as Collective Sensemaking. Journal of Contingencies and Crisis Management. 2013. Dostupné z: https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-5973.12027

[3] COVA, Thomas J. GIS in emergency management. In: Geographical Information Systems: Principles, Techniques, Management and Applications (abridged). [online]. Dostupné z: https://www.geos.ed.ac.uk/~gisteac/gis_book_abridged/files/ch60.pdf

[4] KEENAN, Peter B. Spatial Decision Support Systems: Three decades on. Decision Support Systems. 2019. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0167923618301672

[5] GHAFFARIAN, Saman; TAGHIKHAH, Firouzeh Rosa; MAIER, Holger R. Explainable artificial intelligence in disaster risk management: Achievements and prospective futures. International Journal of Disaster Risk Reduction. 2023, 98, 104123. DOI: 10.1016/j.ijdrr.2023.104123

[6] LINARDOS, Vasileios; DRAKAKI, Maria; TZIONAS, Panagiotis; KARNAVAS, Yannis L. Machine Learning in Disaster Management: Recent Developments in Methods and Applications. Machine Learning and Knowledge Extraction. 2022, 4(2), 446–473. Dostupné z: https://doi.org/10.3390/make4020020

[7] GÓRNY, Piotr. Selection of artificial intelligence tools to support GIS systems. GIS Odyssey Journal. 2024, 4(1), 25–37. DOI: 10.57599/gisoj.2024.4.1.25. Dostupné z: https://doi.org/10.57599/gisoj.2024.4.1.25

[8] SUN, Chenzhen; LAN, Tian; WU, Zhiwei; SHI, Xing; CHENG, Donglin; JIANG, Songlin. Generative Artificial Intelligence and Its Applications in Cartography and GIS: an Exploratory Review. Journal of Geodesy and Geoinformation Science. 2025, 8(2), 74–89. Dostupné z: https://www.sciopen.com/article/10.11947/j.JGGS.2025.0205

Hodnocení připravenosti jednotlivce na zvládání násilných incidentů

Lukáš Kotek[1], Martin Hromada[2]

[1] Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky,
Nad Stráněmi 4511, 760 05 Zlín, kotek@utb.cz

[2] Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky,
Nad Stráněmi 4511, 760 05 Zlín, hromada@utb.cz

Abstrakt:
Článek pojednává o tématu ochrany měkkých cílů před násilnými útoky. Prezentuje dosavadní výzkum v rámci doktorského studia a představuje nové pojetí měkkých cílů, kde za tyto považuje přímo osoby dotčené útokem, tedy konkrétní a přímé cíle útoku. K tomuto záměru představuje novou definici pojmu měkký cíl, který zohledňuje lidský aspekt problematiky ochrany měkkých cílů, lépe odpovídá řešeným charakteristikám a jejich pojetí v rámci autorského výzkumu. Po rámcovém ukotvení terminologického aparátu nutného k vyjasnění chápání této problematiky autory práce představuje záměr vytvoření metodiky hodnocení připravenosti jednotlivce pro zvládání situací právě takových útoků. K tomu jsou analyzovány a definovány klíčové oblasti, které hrají roli při řešení násilného útoku jednotlivcem a stanoveny konkrétní znalosti, dovednosti, schopnosti a materiální vybavení, které mohou mít pozitivní vliv na efektivní zvládání takové situace. Následně je představen hodnotící mechanismus, který umožňuje jednotlivé parametry objektivně kvantifikovat a komparovat. Na základě toho je představena struktura hodnotící metodiky, popsán současný stav tohoto výzkumu a nastíněny další kroky, které je nutné realizovat k finálnímu výstupu disertační práce. Výzkum následně může sloužit jako základ pro další výzkum cíleného zodolňování společnosti pomocí zvyšování připravenosti jednotlivců jako aktivního prvku bezpečnosti společnosti, který má možnost reagovat v místě a čase útoku jako první díky tomu, že jsou přímými aktéry násilného útoku.

Klíčová slova: měkké cíle, osobní bezpečnost, hodnocení, připravenost, násilný útok.

1 Úvod

Ochrana měkkých cílů je aktuálním a společensky velmi významným tématem. Touto problematikou se zabývá řada českých i zahraničních odborníků a dá se považovat za specifickou disciplínu bezpečnostních věd. Jejími východisky jsou zejména zkušenosti, z již proběhlých útoků a odbornost bezpečnostních expertů, kteří se snaží najít taková opatření, která by v budoucnu podobným parametrům incidentů zamezila, případně snížila jejich pravděpodobnost či dopad. Jedná se tak o prakticky orientovanou disciplínu, která těží primárně z rozboru a analýzy násilných útoků a snaze nalézt generalizovatelné ponaučení aplikovatelné jako prevence. Přesto, že i v této oblasti probíhá vědecko-výzkumná činnost, není příliš ucelena a dostatečně rozpracována a spíše doplňuje praxi o popisný rámec a málokdy přináší nové trendy, které by posouvali reálné možnosti zabezpečení měkkých cílů dále.

Zásadní problém spatřuje autor v optice, kterou se na ochranu měkkých cílů díváme. Z vlastní praktické i akademické zkušenosti si lze všimnout trendu, kdy jsou měkké cíle často chápány v kontextu objektové bezpečnosti. Lidé, kteří jsou potenciálními oběťmi násilného útoku, který je na ně přímo zaměřen, jsou mnohdy chápány jako pasivní subjekty ochrany, ne aktivní aktéři bezpečnosti. Přitom právě lidé, kteří jsou přítomni

násilnému útoku (a jsou právě jeho cílem) mají několik aspektů, které poskytují potenciál k preventivnímu působení, pohotové a efektivní reakce a pozitivnímu působení na zmírnění dopadu.

Mnoho příkladů ze světa poukazuje na fakt, že pohotový a odhodlaný člověk může efektivně reagovat na násilného útočníka a pozitivně přispět k tomu, jak incident dopadne. Tento článek prezentuje koncept metodiky, která je součástí disertační práce a která má za cíl definovat klíčové oblasti, které v takovém případě hrají zásadní roli a nastavit systém metodického hodnocení připravenosti jednotlivce v definovaných klíčových aspektech.

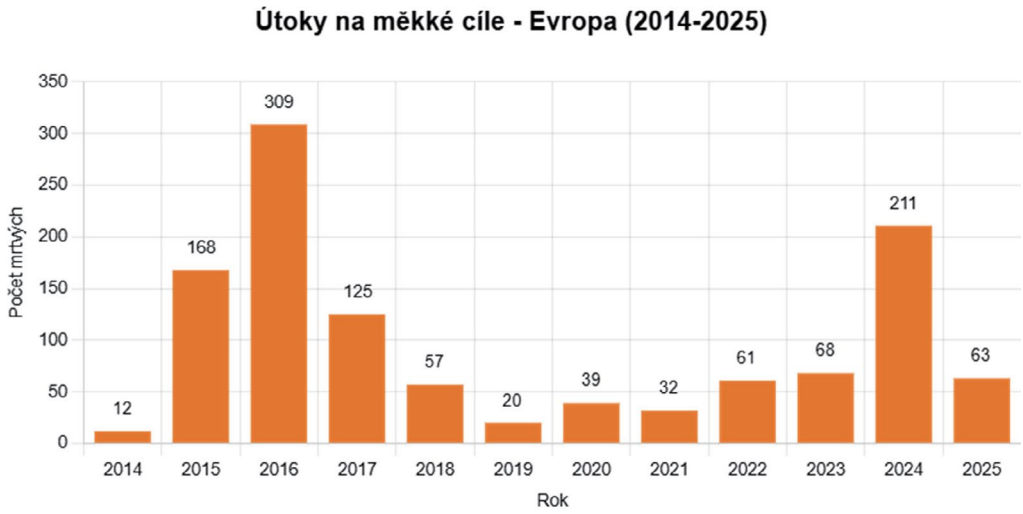
2 Současný stav řešené problematiky

Téma ochrany měkkých cílů je aktuální problematikou, kterou se zabývá řada českých i zahraničních odborníků z oblasti bezpečnosti. Přesto, že je mnohdy vnímána zejména v kontextu teroristických útoků, modus operandi a motivace útočníků je různá. Statistické údaje poukazují na fakt, že incidenty v rámci Evropy, které lze klasifikovat jako útoky na měkké cíle v posledních letech narůstají, přestože vlna teroristických útoků v Evropě již není tak intenzivní, jako v období aktivního působení Islámského státu v Evropě. Obrázek 1 ilustruje vývoj útoků na měkké cíle v prostředí České republiky od roku 2014. Mezi významné útoky sem patří střelba a barikádová situace v Uherském Brodě [1], střelba ve Fakultní nemocnici v Ostravě [2] nebo střelba na Filosofické fakultě Univerzity Karlovy [3]. Zdaleka se však nejedná o ojedinělé případy násilného napadení větší skupiny osob s cílem je usmrtit.

Obrázek 1. Počet útoků na měkké cíle v České republice (2014–2025) [4]

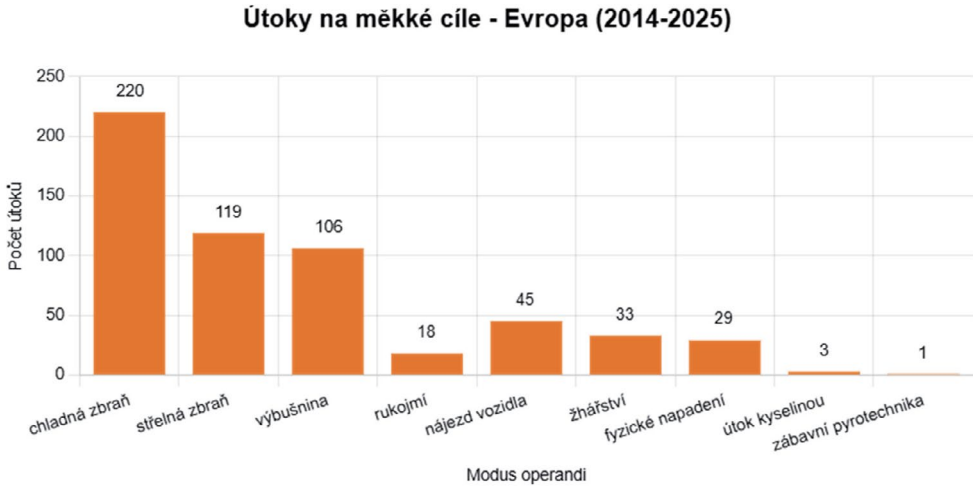
V celoevropském kontextu je nárůst v posledních letech obdobný jako v tuzemském prostředí. Dílčí výkyvy jsou způsobené zejména teroristickými útoky, jejichž cílem Česká republika nebyla a nárůstem násilné kriminality v souvislosti se specifickými kulturními, migračními a společenskými problémy v některých státech.

Přestože jsou mediálně nejzajímavější, a tudíž veřejnosti nejznámější, případy útoků s palnou zbraní, relevantní jsou také útoky s použitím jiných prostředků, které v České republice i v Evropě dosahují obdobného zastoupení, zejména použití chladných zbraní a výbušnin. Obrázek 3 zobrazuje prostředky využité pro realizaci násilného útoku na měkký cíl v České republice. Nutné je podotknout, že v některých případech může u jednoho incidentu dojít také k jejich kombinaci. [4]



Obrázek 2. Počet útoků na měkké cíle v Evropě (2014–2025) [4]

Obrázek 3. Použité prostředky pro útoky na měkké cíle v České republice (2014–2025) [4]



Obrázek 4. Použité prostředky pro útoky na měkké cíle v Evropa (2014–2025) [4]

V celoevropském měřítku jsou nejčastěji použité prostředky a jejich vzájemný poměr obdobné. Rozdíl je opět způsoben zejména teroristicky motivovanými útoky, které v české statistice nenalezneme díky absenci takových útoků. [4]

V České republice je několik segmentů, které se zabývají ochranou měkkých cílů a teoretickým, institucionálním a praktickým rozvojem v této oblasti.

Prvním z nich je stát, zejména Ministerstvo vnitra České republiky (dále jen „MVČR“), jako gestor ochrany měkkých cílů. V rámci jejich činnosti bylo vydáno několik metodik, které pomáhají provozovatelům měkkých cílů zorientovat se v této problematice a vhodně své prostředí zabezpečit. [5–10]

Druhou oblastí je česká komunita bezpečnostních odborníků, kteří aktivně sdílí své zkušenosti a názory a tímto propojením akcelerují diskuzi o možných bezpečnostních řešeních. Hlavním nosným tématem je analýza proběhlých útoků a snaha najít v těchto případech ponaučení přenositelné do další praxe. Hledaná řešení jsou zejména z oblasti technické ochrany, fyzické ostrahy a režimových opatření, a jejich kvality, efektivity a vzájemného propojení. Častým tématem je také otázka zda, jakou formou a s jakým obsahem realizovat školení personálu objektu klasifikovaného jako měkký cíl.

Třetí segment zastupují komerční společnosti, které poskytují bezpečnostní poradenství, auditní a analytické služby a tematická školení a tréninky.

Čtvrtou oblastí je akademický sektor, kde dochází k vědecko-výzkumné činnosti v oblasti ochrany měkkých cílů. Oproti předchozím zdrojům je zde patrná snaha o implementaci vědeckých metod a jasnou metodologii.

Všechny čtyři pilíře, které definují, udržují a posouvají znalostní bázi v ochraně měkkých cílů mají však společný rys, kterým je dominantní vnímání jednotlivce, na kterého může být cílen násilný útok, jako pasivního prvku, který je potřeba chránit, nikoli aktivního participanta útoku, který má potenciál a reakceschopnost na situaci pozitivně působit – ať už jí předejít, včas detekovat, efektivně a pohotově reagovat nebo pomáhat se zmírněním dopadů proběhlého útoku. Přestože některé české i zahraniční dokumenty popisují nutnost zapojit občany do širšího konceptu veřejné bezpečnosti a popisují občana jako osobu s možností první reakce (*first responder*) [11], popřípadě jej vnímají jako součást obranného systému státu [12], není tato myšlenka příliš rozpracována a směřuje spíš k situacím ohrožení státu a zapojení občanů k jeho obraně, nikoli k ochraně sebe a svého okolí proti násilným útokům nestátního charakteru. [12]

Jedním z možných problémů je nevhodná formulace pojmu měkký cíl a jeho následná desinterpretace. Současně platná česká definice měkkých cílů je popisuje jako *„…objekty, prostory nebo akce, které jsou charakterizované častou přítomností vyššího počtu osob a současně absencí či nízkou úrovní zabezpečení proti násilným útokům.“* [13]

Tato formulace může vést k vnímání ochrany měkkých cílů z pohledu objektové bezpečnosti, kdy chráněnými aktivy jsou právě objekty, prostory nebo akce a vše co obsahují je jejich specifickým parametrem a interní součástí. Přesto je v definici obsažena informace, že se jedná o situace násilných útoku, tedy aktivitě, kdy dochází k záměrnému použití fyzické síly proti osobě nebo osobám s úmyslem tyto osoby usmrtit. [14]

Při chybnému pochopení toho, co je měkký cíl, může docházet k zabezpečování objektů v domnění, že chráníme měkký cíl bez reflektování skutečnosti, že chráněnými aktivy v případě ochrany měkkých cílů jsou právě lidé.

3 Vymezení pojmu měkké cíle

Vzhledem k vnímanému problému s pochopením významu a podstaty měkkých cílů a jejich ochrany je vhodné, aby došlo k vytvoření nové definice, která reflektuje podstatné atributy měkkých cílů, a to:

- Měkkými cíli jsou přímo lidé.
- Prostor a čas, ve kterém se nachází, je jen jejich místní a časovou charakteristikou.
- Charakter měkkého cíle je vlastností, která setrvává na lidském faktoru, je nepřenositelná na objekt, místo nebo prostor.
- Připravenost lidí jakožto potencionálního cíle snižuje atraktivitu pro útočníka a snižuje dopad násilného útoku.

Současná česká definice měkkých cílů ve znění vycházejícím ze zahraničních formulací je na stránkách MVČR prezentována se záměrem nahrazení za pojem „veřejný místa“, kterým je údajně celosvětově nahrazován [13]. Tento pojem však stále nedostatečně reflektuje osoby, jako primárně chráněná aktiva. Proto v rámci svého výzkumu navrhuji novou podobu definice měkkých cílů, která do svého středu staví lidský charakter cíle a zbylé okolnosti vyjadřuje jako prostorové a časové atributy.

Současná podoba zamýšlené definice je ve znění:

„Měkké cíle jsou koncentrované skupiny osoby ve stejném prostoru a čase, které mohou být cílem násilného útoku s úmyslem velkého počtu nezúčastněných obětí splňující symboličnost pro útočníka a s absencí schopnosti profesionálně reagovat na násilný útok, což zvyšuje atraktivnost při výběru cíle.“

4 Hodnocení připravenosti jednotlivce

Budeme-li vycházet z premisy, že měkkým cílem jsou přímo lidé dotčení násilným útokem, ochranou měkkých cílů je tedy problematika zajištění toho, aby k takovému útoku nedošlo (prevence, odrazení), včasné detekce symptomatické fáze a začátku realizace útoku, pohotové a efektivní reakce na útočníka a včasné a účinné zahájení kroků zmírňujících dopad realizovaného útoku.

Tím, že v kontextu předchozího textu jsou lidé konkrétním a záměrným cílem, nachází se v místě útoku kauzálně vždy první. Toto jim dává potenciál na situaci bezpečnostního incidentu reagovat jako první, dříve, než se na místo incidentu dostaví profesionální pomoc. V mnoha příkladech útoků v minulosti se ukázalo, že včasná a odhodlaná reakce dokázala násilný útok zastavit v poměrně rané fázi, přestože potenciál obětí byl mnohem větší a zároveň přestože aktivní obránci nebyli bezpečnostními profesionály očekávajícími nutnost takové reakci. [15–23]

Prezentovaný výzkum se zabývá související otázkou – jaké dovednosti, znalosti, schopnosti a prostředky hrají klíčovou roli v takových situacích a umožňují jednotlivcům situaci zvládnout lépe? A Následně hledá způsob jako objektivně, kvantifikovatelně a komparovatelně tyto klíčové parametry hodnotit a porovnávat.

Na základě výzkumného předpokladu, že lidé – cíle útoku jsou v místě incidentu jako první a mohou jako první na něj reagovat a také případů, kdy takové jednání vedlo k efektivního působení na násilný incident, byly analyzována struktura vhodných znalostí, dovedností, schopností a materiálního vybavení, které hrají roli. Tyto aspekty byly v rámci výzkumu označeny jako „parametry cíle“ nebo jen „parametry“.

Přestože je mnoho zdrojů, které problematiku vhodných parametrů řeší, jedná se zpravidla o zdroje zaměřené úzce na dílčí problematiku, která vychází z vlastních zkušeností bez konceptuálního zasazení do širšího kontextu a kvantifikovatelného hodnocení, které popisuje význam a důležitost jednotlivých parametrů. Právě absence možnosti objektivního, vyčíslitelného a komparovatelného hodnocení je předmětem tohoto výzkumu a vstupní ambicí takový systém vytvořit.

Zvolená metoda pro transformaci dostupných, odborných ale přesto subjektivních názorů do objektivního hodnocení zahrnuje využití dostupných znalostí odborníků a jejich následného zpracování.

Na základě rešerše informací o proběhlých incidentech, jejich průběhu a následcích byly identifikovány čtyři oblasti, které hrají klíčovou roli pro zvládání násilných incidentů libovolným jednotlivcem. Těmito identifikovanými oblastmi jsou:

- **Laická první pomoc** (základní opatření realizovaná v případě náhlého ohrožení života, která cíleně omezují rozsah následků a prováděná bez specializovaného vybavení a léků mimo zdravotnické zařízení). [24]
- **Krizová komunikace** (specifický způsob komunikace v případě nebezpečné události vedoucí k deeskalaci konfliktu a efektivní dorozumívání). [25]
- **Sebeobrana** (soubor proaktivních činností z oblasti osobní bezpečnosti vedoucí k řešení násilného útoku nebo prevenci před ním. Zahrnuje jak soubor dovedností fyzické obrany, tak preventivní chování, psychickou připravenost a znalost taktiky k zamezení nebo vyřešení násilného útoku). [26]
- **Taktika** (způsob promyšleného jednání s cílem dosažení stanovených cílů a zajištění výhody při řešení konfliktní situace). [27]

Následně byla navázána aktivní komunikace s řadou odborníků na jednotlivé dílčí oblasti, se kterými byly konzultovány dílčí parametry, které pro případ násilného útoku hrají roli, a to ve třech fázích násilného incidentu – Před útokem, kde hraje roli zejména odstrašující funkce vedoucí k snížení atraktivity při výběru cíle útočníkem:

- **Před útokem**, kde hraje roli zejména odstrašující funkce vedoucí k snížení atraktivity při výběru cíle útočníkem a preventivní příprava jednotlivce, která se projeví v dalších dvou fázích v případě realizovaného útoku.
- **Během útoku**, kde je nutné probíhající útok co nejrychleji detekovat, vyhodnotit a pohotově a efektivně na něj reagovat.
- **Po útoku**, kde je zdroj hrozby (útočník) eliminován nebo již nepředstavuje bezprostřední nebezpečí (je dostatečně vzdálen nebo zaměstnán) a je nutné zahájit kroky vedoucí k zastavení návazného působení útoku ve formě dopadů (první pomoc, koordinace odborné pomoci, informační činnost aj.). [28]

Na základě odborných konzultací byly definovány sestavy dílčích parametrů pro jednotlivé oblasti, jejichž ukázka je znázorněna na obrázku níže.

	Laická první pomoc
Teorie	Znalost lidské anatomie a fyziologie
	Znalost algoritmů první pomoci (C-ABCDE nebo MARCHE)
Zdravotnický materiál	Nošení zdravotnického materiálu a nástrojů nebo jeho přítomnost v místě - tlakový obvaz
	Nošení zdravotnického materiálu a nástrojů nebo jeho přítomnost v místě - škrtidlo
	Nošení zdravotnického materiálu a nástrojů nebo jeho přítomnost v místě - jehla pro hrudní punkci
	Nošení zdravotnického materiálu a nástrojů nebo jeho přítomnost v místě - nosní vzduchovod vč. Lubrikantu
	Nošení zdravotnického materiálu a nástrojů nebo jeho přítomnost v místě - hrudní chlopeň
	Nošení zdravotnického materiálu a nástrojů nebo jeho přítomnost v místě - záchranářské nůžky
	Nošení zdravotnického materiálu a nástrojů nebo jeho přítomnost v místě - hemostatická gáza
	Nošení zdravotnického materiálu a nástrojů nebo jeho přítomnost v místě - elastické obinadlo
	Nošení zdravotnického materiálu a nástrojů nebo jeho přítomnost v místě - termofolie
Zkušenosti se zdravotnickým materiálem	Zkušenost s aplikací tlakového obvazu
	Zkušenost s aplikací škrtidla
	Zkušenost s aplikací jehly pro hrudní punkci
	Zkušenost s aplikací nosního vzduchovodu
	Zkušenost s aplikací hrudní chlopně
	Zkušenost s obvazováním zranění
	Zkušenost s ošetřením osoby v bezvědomí
Znalosti	Znalost aplikace protišokové polohy
	Znalost aplikace stabilizované polohy
	Znalost aplikace Fowlerovy polohy
	Znalost aplikace autotransfúzní polohy
	Znalost aplikace Trendelenburgovy polohy
	Znalost ošetření zástavy masivního krvácení
	Znalost provedení tracheotomie
	Znalost aplikace nepřímé srdeční masáže
	Znalost ošetření popálenin
	Znalost ošetření pneumothoraxu
	Znalost postupu ošetření osoby v bezvědomí
	Znalost principů třídění raněných
	Znalost ošetření úrazu hlavy

Obrázek 5. Ukázka parametrů z oblasti „laické první pomoci“ [vlastní]

Každý jednotlivý parametr je v procesu hodnocení připravenosti jednotlivce ohodnocen na bodové stupnici 0 až 4, vyjadřující stupeň dosažení nebo dostupnosti parametru. Ke každému parametru a jejich jednotlivým hodnotám je současně připravována pomocná hodnotící tabulka, která respondentovi v procesu hodnocení jednotlivce pomůže správně přiřadit hodnotu na základě jejího významu (viz Obrázek 6.)

	Oblast parametrů cíle	**Hodnota**
Kategorie parametrů cíle	Parametr 1	
	Parametr 2	**2**
	Parametr 3	
	Parametr 4	
	Parametr 5	
	Parametr 6	
	Parametr 7	
	Parametr 8	
	Parametr 9	
	Parametr 10	

Hodnota	**Slovní hodnocení**
0	Lorem ipsum dolor sit amet
1	Lorem ipsum dolor sit amet
2	Lorem ipsum dolor sit amet
3	Lorem ipsum dolor sit amet
4	Lorem ipsum dolor sit amet

Obrázek 6. Vizualizace mechanismu hodnocení parametrů [vlastní]

V rámci plánovaného dotazníkového šetření, které bude obsahovat relevantní množství odborníků na dílčí oblasti, budou získávány informace o subjektivním vnímání významu jednotlivých parametrů dotazovanými odborníky pro jednotlivé fáze útoku (před, během, po).

Na základě získaných dat budou pro tyto tři fáze stanovena váha pro každou ze tří fází.

	Oblast parametrů cíle	**Hodnota**	**Váha**		
			před útokem	*během útoku*	*po útoku*
Kategorie parametrů cíle	Parametr 1				
	Parametr 2	**2**	**0,11**	**0,65**	**0,24**
	Parametr 3				
	Parametr 4				
	Parametr 5				
	Parametr 6				
	Parametr 7				
	Parametr 8				
	Parametr 9				
	Parametr 10				

Obrázek 7. Vizualizace mechanismu přepočtu váhy parametrů [vlastní]

Na základě vytvořeného systému stanovování konkrétních hodnot bude vytvořena výsledná metodika, která pomocí multikriteriální analýzy umožní porovnávat úroveň jednotlivých parametrů a následně celých oblastí a vyhodnocovat míru připravenosti jednotlivce, a to jak celkovou, tak v jednotlivých oblastech a dílčích parametrech.

5 Závěr

Článek představuje téma autorova výzkumu, jako součásti disertační práce mající za cíl vytvořit metodiku hodnocení připravenosti jednotlivce na zvládání násilných incidentů. Svým zaměřením je to práce ojedinělá, která se na problematiku ochrany měkkých cílů dívá novou optikou a zaměřuje se na roli běžného člověka jako cíle útoku, který není jen pasivním subjektem objektové ochrany ale aktivním aktérem majícím potenciál pohotově a efektivně reagovat na násilný incident.

Tento text prezentuje novou definic pojmu měkký cíl, která je dle autora nezbytná k správnému pochopení úhlu pohledu a předmětu ochrany měkkých cílů. Následně popisuje proces tvorby hodnotící metodiky, která vyžaduje transformaci dostupných informací odborníků z úzce zaměřeného a subjektivně vnímaného know-how na objektivní, kvantifikovatelné a komparovatelné hodnoty, se kterými lze následně dále pracovat.

Ambicí výzkumu a je implementovat vědecké metody a vědecké poznání do oblasti ochrany měkkých cílů, tedy oblasti praktické, která se vyvíjí zejména na základě praktických zkušeností bez dostatečného metodologického a vědeckého rámce. Zaměření se na analýzu a hodnocení konkrétních osob je novým úhlem pohledu, který může poskytnout základ pro další výzkumné aktivity, posunout tuto praktickou bezpečnostní disciplínu a zároveň vědeckou oblast zájmu a rozšířit znalostní bázi o nové poznatky. Autor v rámci dalšího navazujícího výzkumu plánuje věnovat se oblasti bezpečnostního vzdělávání a podpory bezpečnostní kultury tak, aby identifikoval vhodné způsoby a metody zvyšování individuální připravenosti jednotlivce v klíčových parametrech. Díky vzniklému metodickému postupu hodnocení takových parametrů lze následně stanovit vhodné způsoby

zvyšování připravenosti, simulovat je, testovat, evaluovat a optimalizovat. Bez systému vhodného hodnocení jsou takové snahy pouze odborným odhadem vzdělávacích potřeb na základě svých nebo cizích zkušeností bez možnosti opřít se o vědecké poznatky a objektivní metody.

Reference

[1] STRÁNSKÝ, Pavel B. Tragédie v Uherském Brodě. Online. Policie České republiky – KŘP Zlínského kraje, 2015. Dostupné z: https://policie.gov.cz/clanek/tragedie-v-uherskem-brode.aspx. [cit. 2026-01-31]

[2] JIROUŠKOVÁ, Pavla. Odložení případu. Online. Policie České republiky – KŘP Moravskoslezského kraje, 2020. Dostupné z: https://policie.gov.cz/clanek/krajske-reditelstvi-severomoravskeho-kraje-zpravodajstvi-odlozeni-pripadu.aspx. [cit. 2026-01-31]

[3] Policie ČR: Tisková konference: k vyhodnocení zásahu na FF UK v Praze. Online. Policie ČR (Policie České republiky), 2024. Dostupné z: https://www.youtube.com/watch?v=ymOExOvxdRU&t=741s. [cit. 2026-01-31]

[4] Database of Violent Attacks. Online. Dostupné z: https://dova.fai.utb.cz/cs/grafy. [cit. 2026-01-31]

[5] KALVACH, Zdeněk. ZÁKLADY OCHRANY MĚKKÝCH CÍLŮ: METODIKA. Online. Ministerstvo vnitra České republiky, 2016. Dostupné z: https://mv.gov.cz/chh/soubor/terorismus-web-dokumenty-metodika-zaklady-ochrany-mekkych-cilu-pdf.aspx. [cit. 2026-01-31]

[6] Koncepce ochrany měkkých cílů pro roky 2017-2020. Online. Ministerstvo vnitra České republiky, 2017. Dostupné z: https://mv.gov.cz/chh/soubor/koncepce-ochrany-mekkych-cilu-pro-roky-2017-2020-pdf.aspx. [cit. 2026-01-31]

[7] BEZPEČNOSTNÍ STANDARDY PRO POŘADATELE LETNÍCH SPORTOVNÍCH, KULTURNÍCH A SPOLEČENSKÝCH AKCÍ. Online. Centrum proti terorismu a hybridním hrozbám, Ministerstvo vnitra České republiky, 2019. Dostupné z: https://mv.gov.cz/chh/soubor/brozura-bezpecnostni-standardy-pro-poradatele-sportovnich-kulturnich-a-spolecenskych-akci.aspx. [cit. 2026-01-31]

[8] Bezpečnostní plán měkkého cíle: aneb co by nemělo být opomenuto při jeho zpracování. Online. Odbor bezpečnostní politiky, Ministerstvo vnitra České republiky, 2025. Dostupné z: https://mv.gov.cz/chh/soubor/bezpecnostni-plan-mekkeho-cile-aneb-co-by-nemelo-byt-opomenuto-pri-jeho-zpracovani-2-upravene-vydani.aspx. [cit. 2026-01-31]

[9] BEN DAVID, Gabriela. Jak se připravit na závažnou situaci?: Koordinační plány pro měkké cíle. Online. Odbor bezpečnostní politiky, Ministerstvo vnitra České republiky, 2025. Dostupné z: https://mv.gov.cz/chh/soubor/jak-se-pripravit-na-zavaznou-situaci-koordinacni-plany-pro-mekke-cile-1-vydani.aspx. [cit. 2026-01-31]

[10] BEN DAVID, Gabriela. Metodika koordinace měkkého cíle pro fáze po závažném incidentu: aneb jak se vyrovnat s nastalou závažnou situací. Online. Odbor bezpečnostní politiky, Ministerstvo vnitra České republiky, 2025. Dostupné z: https://mv.gov.cz/chh/soubor/metodika-koordinace-mekkeho-cile-pro-faze-po-zavaznem-incidentu-aneb-jak-se-vyrovnat-s-nastalou-zavaznou-situaci-2-upravene-vydani.aspx. [cit. 2026-01-31]

[11] U.S. DEPARTMENT OF HOMELAND SECURITY. Soft Targets and Crowded Places Security Plan Overview. Online. 2018. Dostupné z: https://www.hsdl.org/c/view?docid=812763. [cit. 2026-01-31]

[12] MINISTERSTVO OBRANY ČESKÉ REPUBLIKY. Koncepce přípravy občanů k obraně státu 2025-2030. Online. 2025. Dostupné z: https://mocr.mo.gov.cz/assets/informacni-servis/zpravodajstvi/koncepce-pripravy-obcanu-k-obrane-statu-2025-2030.pdf. [cit. 2026-02-28]

[13] WORLD HEALTH ORGANIZATION. Violence. Online. Dostupné z: https://www.emro.who.int/violence-injuries-disabilities/violence/. [cit. 2026-02-02]

[14] MUSIL, Adam a SVITÁK, Matěj. Útočníka z Londýna přemohli kolemjdoucí pomocí rohu narvala nebo hasicího přístroje. Online. 2019. Dostupné z: https://ct24.ceskatelevize.cz/clanek/svet/utocnika-z-londyna-premohli-kolemjdouci-pomoci-rohu-narvala-nebo-hasiciho-pristroje-56545. [cit. 2026-01-31]

[15] Útočnici s nožem v Hamburku zastavila dvojice cizinců, Syřan s Čečencem. Online. 2025. Dostupné z: https://zpravy.aktualne.cz/zahranici/utocnici-s-nozem-v-hamburku-zastavila-dvojice-cizincu-syran/r~f1cda84239ed11f0b589ac1f6b220ee8/?lp=1. [cit. 2026-01-31]

[16] ŠTĚPÁNEK, Jan. Útočník v Burnley pobodal v obchodě dva lidi, ostatní zákazníci pohotově zasáhli. Online. 2020. Dostupné z: https://www.novinky.cz/clanek/zahranicni-evropa-utocnik-v-burnley-pobodal-v-obchode-dva-lidi-ostatni-zakaznici-pohotove-zasahli-40344138. [cit. 2026-01-31]

[17] ŠEVČÍKOVÁ, Olga. Útok ve vlaku: Hrdinský čin pracovníka zabránil masakru, útočník mluvil o ďáblu. Online. 2025. Dostupné z: https://www.denik.cz/staty-mimo-eu/anglie-utok-ve-vlaku-hrdina-pobodani-kdo-je-utocnik.html. [cit. 2026-01-31]

[18] Při střelbě v americkém gay klubu zemřelo pět lidí. Útočníka zastavili návštěvníci, říká policie. Online. 2022. Dostupné z: https://www.irozhlas.cz/zpravy-svet/gay-klub-colorado-springs-strelba-usa_2211201152_ako. [cit. 2026-01-31]

[19] Muži, kteří zastavili hamburského útočníka, za svůj čin dostali cenu. Online. 2017. Dostupné z: https://www.idnes.cz/zpravy/zahranicni/hamburk-ocenil-muze-kteri-zastavili-utocnika-ze-supermarketu-nemecko-ahmad-a.A170802_175932_zahranicni_kha. [cit. 2026-01-31]

[20] Mladíci zabránili masakru ve vlaku. Online. 2015. Dostupné z: https://www.denik.cz/ze_sveta/utocnik-ktery-zranil-dva-lidi-v-rychlovlaku-je-navratilec-ze-syrie-20150822.html. [cit. 2026-01-31]

[21] KOPECKÁ, Radka. Útočník v texaském kostele zabil dva lidi, pak ho zastřelil bývalý agent FBI. Online. 2019. Dostupné z: https://www.idnes.cz/zpravy/zahranicni/fort-worth-texas-kostel-strelba-utocnik.A191230_070740_zahranicni_rko. [cit. 2026-01-31]

[22] HAVLICKÁ, Kateřina. Útočník v Norsku pobodal několik lidí, zranil i svou manželku. Online. 2022. Dostupné z: https://www.idnes.cz/zpravy/zahranicni/norsko-utok-pobodani.A220520_094530_zahranicni_bro. [cit. 2026-01-31]

[23] HASIČSKÝ ZÁCHRANNÝ SBOR ČESKÉ REPUBLIKY. ZÁKLADNÍ ZNALOSTI ZÁSAD PRVNÍ POMOCI. Online. Dostupné z: https://hzscr.gov.cz/soubor/zakladni-znalosti-zasad-prvni-pomoci-pdf.aspx. [cit. 2026-02-02]

[24] LUKÁŠ, Luděk. Konvergovaná bezpečnost. Zlín: Radim Bačuvčík – VeRBuM, 2019. ISBN 978-808-7500-996

[25] PAVELKA, Radim a STICH, Jaroslav. Sebeobrana: nebuďte snadnou obětí!. Praha: Ikar, 2015. ISBN 978-80-249-2800-5

[26] HAŠKA, Milan. Taktika řešení konfliktních situací. Online. Dostupné z: https://www.cudk.cz/taktika/. [cit. 2026-02-02]

[27] LAPKOVÁ, Dora, KOTEK, Lukáš. Soft Targets and Possibilities of Their Protection. 2017 International Conference on Logistics, Informatics and Service Sciences (LISS). New Jersey, Piscataway: IEEE, 2017, s. 548–552. ISBN 978-1-5386-1047-3

Návrh hodnocení bezpečnostních opatření měkkých cílů

Pavel Král[1], Dora Kotková[2], Martin Hromada[3]

[1] Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky,
Nad Stráněmi 4511, 760 05 Zlín, p_kral@utb.cz

[2] Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky,
Nad Stráněmi 4511, 760 05 Zlín, kotkova@utb.cz

[3] Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky,
Nad Stráněmi 4511, 760 05 Zlín, hromada@utb.cz

Abstrakt:

Článek se zabývá problematikou systematického hodnocení bezpečnostních opatření v prostředí měkkých cílů. Reaguje na rostoucí požadavky na efektivní zabezpečení těchto objektů a na potřebu cíleného výběru opatření odpovídajících konkrétním požadavkům a specifikům daného prostředí. Hlavním cílem článku je představit koncepční návrh strukturovaného hodnotícího rámce bezpečnostních opatření, který umožní jejich přehledné porovnání, filtraci a následný výběr na základě předem definovaných kritérií. V úvodní části je vymezen pojem měkký cíl a zdůrazněna nutnost vyhodnocení ohroženosti a provedení bezpečnostního posouzení jako základních vstupů pro cílený návrh zabezpečení. Následně je představeno základní rozdělení bezpečnostních opatření, přičemž je zdůrazněna jejich vzájemná provázanost a potřeba komplexního přístupu. Součástí je také návrh systematizovaného referenčního seznamu opatření, který zohledňuje různé varianty jejich provedení. Stěžejní část článku představuje návrh hodnotícího systému. Jeho cílem je kombinace přístupu hodnocení účinnosti ve fázích odstrašení, odhalení, reakce a absorpce s přístupem multikriteriálního hodnocení, v jehož rámci jsou představena uvažovaná kritéria zahrnující například míru snížení atraktivity, snadnost implementace či společenskou přijatelnost. U těchto kritérií je popsán jejich účel, rozsah zohlednění a dosavadní způsob kvalitativního hodnocení. Kombinace těchto přístupů umožní komplexní posouzení vhodnosti jednotlivých variant opatření a přizpůsobení jejich výběru konkrétním podmínkám organizace. Výstupem článku je koncepční návrh hodnotícího systému, který vytváří předpoklad pro objektivizovanější a cílenější rozhodování při výběru bezpečnostních opatření. Současně jsou identifikovány směry dalšího výzkumu představeného návrhu a myšlenek, včetně kvantifikace kritérií a stanovení váhových koeficientů pro praktickou aplikaci.

Klíčová slova: měkký cíl, bezpečnostní opatření, fyzická bezpečnost, klasifikace opatření.

1 Úvod

Ochrana měkkých cílů představuje vysoce aktuální, dynamické a společensky významné téma, jehož důležitost je opakovaně potvrzována. Zejména v souvislosti s vývojem bezpečnostního prostředí narůstá společenský tlak na zajištění adekvátní ochrany měkkých cílů. Provozovatelé těchto objektů však často disponují velmi omezenými finančními i personálními zdroji, a proto je nezbytné, aby byly dostupné prostředky využívány efektivně a cíleně. To vyvolává potřebu systematického přístupu k výběru bezpečnostních opatření, který bude respektovat specifika konkrétního měkkého cíle. Článek se proto zabývá návrhem systému hodnocení, jenž umožní strukturované porovnání a identifikaci vhodných bezpečnostních opatření.

Příspěvek nejprve vymezí pojem měkký cíl a představí základní východiska pro výběr bezpečnostních opatření. Následně popíše jejich základní členění, které slouží k zachování přehlednosti a k vytvoření referenčního seznamu opatření, včetně vymezení různých klasifikačních hledisek pro konkretizaci jednotlivých variant. Hlavní část článku bude věnována návrhu hodnotícího systému, který kombinuje využití matice OORA pro posouzení účinnosti opatření v jednotlivých fázích útoku s multikriteriálním hodnocením. Zde budou představena některá z kritérií, jejich dosavadní podoba, způsob hodnocení a možnosti dalšího rozvoje v rámci dalšího výzkumu.

2 Měkký cíl

Pojem měkký cíl není v odborné literatuře terminologicky sjednocen a u různých autorů je možné se setkat s odlišnými definicemi. V prostředí České republiky lze za ustálenou považovat definici vycházející z metodického dokumentu „Koncepce ochrany měkkých cílů pro roky 2017–2020“ [1] kde je měkký cíl definován takto: *„Termínem měkké cíle označujeme objekty, prostory nebo akce charakterizované častou přítomností většího počtu osob a současně absencí či nízkou úrovní zabezpečení proti násilným útokům.“* [1] Uvedená metodika zároveň zdůrazňuje hlavní specifikum ochrany měkkých cílů, kterým je priorita ochrany života a zdraví lidí nacházejících se v daném prostoru, nikoli primárně ochrana majetku či samotného objektu. Některé definice také uvádějí symbolický, kulturní či náboženský význam daného místa. Mezi typické příklady měkkých cílů patří školy a knihovny, náboženské objekty, kina a divadla, kulturní či politická shromáždění, restaurační zařízení, sportovní haly a další veřejně přístupné prostory. [1–3]

2.1 Atraktivita měkkého cíle

Atraktivitu měkkého cíle lze vnímat jako určitou míru, jak lákavý je daný objekt, prostor či událost jakožto vhodný cíl pro různé typy útočníků, zejména pro útočníky motivované extrémistickou ideologií nebo teroristické skupiny. Dokument „Metodika – Základy ochrany měkkých cílů“ [1] identifikuje několik významných faktorů, které atraktivitu měkkého cíle zvyšují (otevřenost pro veřejnost, množství a koncentrace osob, přítomnost médií a symboličnost cíle), nebo snižují (přítomnost bezpečnostního personálu a přítomnost policie). Tyto faktory mohou pomoci při identifikaci možných typů útoků, které danému měkkému cíli hrozí. [1, 3, 4, 5]

2.2 Vyhodnocení ohroženosti

Pro adekvátní aplikaci vhodných bezpečnostních opatření u každého objektu je nutné nejdříve zjistit jeho rizika, specifika, slabiny a další faktory. Z tohoto důvodu je potřeba vyhodnocení aktuální ohroženosti a bezpečnostní posouzení aktuálního stavu zabezpečení. [1]

Vyhodnocení ohroženosti slouží především k pochopení toho, kde, kdy, co a od koho danému cíli hrozí. Toto pochopení přispívá k efektivnímu využití vhodných a cílených bezpečnostních opatření. Konkrétnímu postupu vyhodnocení se věnuje například metodický dokument „Vyhodnocení ohroženosti měkkého cíle aneb co, kdy, kde a od koho vám hrozí“. [5]

Využít lze také bezpečnostní posouzení pro určení aktuální úrovně zabezpečení, jeho nedostatků a analýzu z tohoto plynoucí rizika. Samotné požadavky na bezpečnostní posouzení v kontextu návrhu zabezpečení jsou například uváděny v konkrétních technických normách. U poplachových zabezpečovacích a tísňových systémů (dále jen PZTS) se jedná o ČSN 50131-7, u kamerových systémů ČSN 62674-4 a u systémů elektronické kontroly vstupu (dále jen ESKV) o ČSN 60839-11-2. [6]

3 Bezpečnostní opatření

V úvodu je nutné určit, co se rozumí pojmem „bezpečnost“ v kontextu fyzické bezpečnosti. Bezpečností se rozumí stav, v němž jsou rizika vyplývající z identifikovaných hrozeb snížena na přijatelnou míru. K zajišťování bezpečnosti jsou tak využívána bezpečnostní opatření, která jsou aplikována na identifikované hrozby s cílem zvýšení bezpečnosti. [7]

3.1 Základní rozdělení bezpečnostních opatření

Za bezpečnostní opatření lze považovat každé opatření, které zvyšuje bezpečnost objektu. V rámci oblasti fyzické bezpečnosti, které se tento článek výhradně věnuje, lze tato opatření zařadit do tří základních oblastí zabezpečení: režimová opatření, fyzická ostraha a technické prostředky. [7–9]

Režimová opatření – cílem tohoto souboru opatření je stanovit jasná pravidla, zásady chování a oprávnění osob ve vymezeném prostoru. Určují také způsob zacházení s technickými bezpečnostními prvky a stanovují podmínky a způsob provádění bezpečnostních kontrol. Určují též postup kontroly dodržování a vynucování nastavených pravidel. [7, 9, 10]

Fyzická ostraha – plní celou řadu funkcí a je zabezpečována především zaměstnanci soukromé bezpečnostní služby, vlastními bezpečnostními pracovníky, policií, případně některé prvky této ochrany může plnit také ostatní zaměstnanci. Jedná se o neopomenutelnou složku ochrany díky možnosti dynamické reakce a řešení vzniklých narušení. [3, 7]

Technické prostředky – cílem těchto bezpečnostních prvků je detekovat, zamezit, ztížit nebo evidovat narušení bezpečnosti objektu nebo vymezeného prostoru. Mezi tyto prvky patří celá řada systémů, jako jsou zařízení ESKV, prvky PZTS, kamerové systémy a jiné. [3, 6, 7, 9]

Především v rámci ochrany měkkých cílů je kladen důraz na účelnost, vzájemnou kompatibilitu a provázanost s ostatními prvky bezpečnostního systému. [3]

3.2 Referenční vzorek bezpečnostních opatření

V rámci této podkapitoly je představen proces vytváření referenčního vzorku bezpečnostních opatření a jejich variant relevantních pro zabezpečení měkkých cílů. Pro zachování přehlednosti je využito základní členění na technické prostředky, režimová opatření a fyzickou ostrahu.

Technických prostředků je na trhu dostupné značné množství, proto je pro jejich systematické vyhodnocení nezbytné stanovit vhodná klasifikační kritéria při tvorbě seznamu bezpečnostních opatření. Technická opatření lze dělit například podle fáze bezpečnostního procesu, ve které působí, tedy zda je jejich cílem předejít útoku, detekovat jej, zpomalit či zastavit jeho průběh nebo spustit následnou reakci. Dalším možným hlediskem je jejich umístění, tedy zda chrání perimetr objektu, jeho plášť, vnitřní prostory, specificky vymezená místa nebo konkrétní předměty. [3, 7, 8]

Rozlišovat je lze rovněž na viditelné a skryté technické prvky, nebo podle technické povahy (mechanické, elektronické, konstrukční či kombinované) či dle režimu fungování na pasivní, automatizované nebo vyžadující obsluhu. Významným faktorem je také cenová náročnost, kvalitativní úroveň zpracování a způsob instalace, tedy zda se jedná o prvky pevně instalované nebo přenosné. Krátký výsek vybraných možností a jejich kombinací z takto strukturovaného seznamu technických bezpečnostních opatření je uveden níže (viz Tabulka 1). [3, 7]

Tabulka 1. Ukázka strukturovaného seznamu technických opatření [vlastní]

Kvalita zpracování	**Pevné / Přenosné**	**Místo aplikace**	**Opatření**
High end	Pevné	Na perimetru	Kamera s živým přenosem
			Kamera se záznamem
			Kamera s živým přenosem a záznamem
			Kamera s autonomními funkcemi
			Bariéra proti vozidlům
			Manuální brána
			Automatická brána
			Oplocení
			Detektor narušení
			Detektor střelby
			Detektor paniky
			Automatické osvětlení
			Statické osvětlení
		Na vstupních bodech	Kamera s živým přenosem
			Kamera se záznamem
			Kamera s živým přenosem a záznamem
			Kamera s autonomními funkcemi
			Bariéra proti vozidlům
			Manuální brána
			Automatická brána
			Detektor narušení
			Detektor střelby
			Detektor paniky
			Plnorozměrný turniket
			Tříbodový turniket
			Automatické osvětlení
			Statické osvětlení
		Na vjezdech	Kamera s živým přenosem
			Kamera se záznamem
			Kamera s živým přenosem a záznamem
			Kamera s autonomními funkcemi
			Bariéra proti vozidlům
			Manuální brána
			Automatická brána
			Detektor narušení
			Automatické osvětlení
			Statické osvětlení

Kvalita zpracování	Pevné / Přenosné	Místo aplikace	Opatření
High end	Pevné	Ve veřejné části objektu	Kamera s živým přenosem
			Kamera se záznamem
			Kamera s živým přenosem a záznamem
			Kamera s autonomními funkcemi
			Detektor narušení
			Detektor střelby
			Detektor paniky
			Rozhlasové zařízení

Režimová opatření představují specifickou kategorii bezpečnostních opatření, jejichž konkrétní podoba se může mezi jednotlivými objekty značně lišit. Přesto je i v tomto případě nezbytné stanovit vhodná klasifikační hlediska při tvorbě seznamu potenciálních bezpečnostních opatření. Jedním z možných přístupů je hodnocení kvality jejich zpracování. Dalším hlediskem je účel jejich použití, tedy zda slouží k prevenci, detekci narušení, stanovení postupů reakce nebo zajištění obnovy. Dále je lze členit podle časové působnosti na trvalá, dočasná či jednorázová, a podle způsobu aktivace, tedy zda působí kontinuálně, jsou aktivována rozhodnutím odpovědné osoby, nebo se spouštějí na základě předem definovaného externího podnětu. [6]

Rozlišovat je možné rovněž podle cílové skupiny, pro kterou jsou určena (zaměstnanci, návštěvníci, externí dodavatelé), podle míry závaznosti, tedy zda vyplývají z právních norem, interních předpisů nebo mají doporučující charakter. Nutné je také rozlišovat způsob kontroly jejich dodržování, který může být zajištěn fyzickou ostrahou, jinými zaměstnanci nebo technickými prostředky. Mezi některá významná režimová opatření patří:

- systém vydávání klíčů,
- provozní řád objektu,
- kontrola vstupu osob,
- kontrola vnášených zavazadel,
- vymezený prostor pro zadržení a kontrolu osob,
- koordinační plán,
- směrnice pro výkon fyzické ostrahy,
- stanovené postupy pro běžné události,
- stanovené postupy pro mimořádné události. [6]

Uvedená opatření jsou následně detailněji členěna podle vybraných parametrů za účelem vytvoření konkrétního referenčního seznamu režimových opatření, obdobně jako v případě technických prostředků (viz Tabulka 1).

Fyzická ostraha má řadu variant provedení, které je nutné zohlednit při vytváření seznamu bezpečnostních opatření. Významným parametrem je odborná úroveň pracovníků a jejich kvalifikace. Dále je třeba rozlišovat, zda se jedná o externí pracovníky bezpečnostní služby, interní bezpečnostní pracovníky nebo běžné zaměstnance organizace vykonávající doplňkové bezpečnostní úkoly. [3, 7]

Odlišnosti spočívají rovněž ve způsobu výkonu, tedy zda je ostraha uniformovaná nebo skrytá v civilním oděvu. Relevantním hlediskem je výstroj a případná výzbroj pracovníků. Rozlišovat lze dále délku a charakter využití (dlouhodobé, pravidelné, dočasné nebo nárazové) a pracovní režim, tedy zda je zajištěna nepřetržitě nebo pouze v provozní době objektu. Dalším klasifikačním kritériem je mobilita ostrahy, konkrétně zda se jedná o pracovníky vykonávající činnost staticky, obchůzkově nebo jde o mobilní hlídku. Podstatné je rovněž jejich prostorové

rozmístění, tedy zda působí na perimetru objektu, u vstupů, ve vnitřních prostorách nebo v neveřejném zázemí. Mezi některé typy opatření fyzické ostrahy lze zařadit například:

- pracovníka fyzické ostrahy na vstupu,
- pracovníka fyzické ostrahy ve veřejných prostorách objektu,
- hlídkovou službu,
- zásahovou skupinu,
- operátora kamerového systému,
- jiný personál vykonávající bezpečnostní funkci na vstupu. [3, 7]

Jednotlivá opatření jsou dále konkretizována podle výše uvedených parametrů za účelem vytvoření detailního seznamu využitelných variant fyzické ostrahy, obdobně jako v případě technických prostředků (viz Tabulka 1).

Je rovněž nezbytné zohlednit vzájemnou provázanost některých opatření, kdy účinnost jednoho prvku podmiňuje využití jiného. Typickým příkladem může být využití kamery s živým přenosem, jejíž efektivní využití vyžaduje přítomnost kvalifikovaného operátora. Tato vazba musí být při tvorbě referenčního seznamu bezpečnostních opatření dále reflektována.

3.3 Navrhovaný systém hodnocení bezpečnostních opatření

Při hodnocení bezpečnostních opatření je vhodné vycházet z multikriteriálního přístupu, který umožňuje lépe identifikovat vhodnost aplikace konkrétního bezpečnostního opatření s ohledem na aktuální požadavky vyplývající z vyhodnocení ohroženosti, bezpečnostního posouzení a specifických možností organizace.

Jedno z hodnotících rámců, podle něhož lze posuzovat efekt aplikace bezpečnostního opatření, je metodika DDRM, v české verzi OORA. Tento přístup rozděluje bezpečnostní opatření do čtyř základních kategorií podle jejich funkce v rámci fáze potenciálního útoku: odstrašení (deter), odhalení (detect), reakce (react) a absorpce (zmírnění dopadů – mitigate). Umožňuje tak posoudit, zda soubor využitých opatření tvoří funkční a vzájemně provázaný celek pokrývající všechny relevantní fáze možného útoku. [4]

Pro vhodnější rozlišení účinnosti jednotlivých opatření v rámci uvedených fází je navrženo zavedení číselného hodnocení jednotlivých parametrů. Hodnotící škála vychází ze zamýšleného primárního účelu daného opatření. Nejnižší hodnota stanovuje, že opatření v dané fázi nepůsobí nebo pouze zanedbatelně, zatímco nejvyšší hodnota vyjadřuje, že daná fáze představuje jeho primární funkci a lze předpokládat vysokou míru účinnosti v tomto aspektu.

Tabulka 2. Klasifikace kritéria OORA [vlastní]

Klasifikace opatření dle OORA	**Hodnocení**
Žádná nebo zanedbatelná funkce opatření	0
Okrajová funkce opatření	1
Dostatečná účinnost funkce opatření	2
Primární funkce opatření s vysokou mírou účinnosti	3

Tato hodnotící tabulka je následně aplikována v rámci matice OORA, čímž vzniká přehledný výstup znázorňující účinnost jednotlivých bezpečnostních opatření v jednotlivých fázích. V prostředí měkkého cíle je přitom žádoucí zajistit pokrytí všech těchto fází. Takto strukturovaný přehled umožňuje identifikovat případné nedostatky

v ochraně a zohlednit účinnost opatření v jednotlivých fázích při tvorbě nebo zodolňování bezpečnostního systému. Současně umožňuje filtrovat opatření podle požadované kategorie ochrany. Aplikace tohoto hodnocení je demonstrována na části seznamu technických prostředků.

Tabulka 3. Ukázka vyhodnocení opatření dle kritéria OORA [vlastní]

Kvalita zpracování	Pevné / Přenosné	Místo aplikace	Opatření	O	O	R	A
High end	Pevné	Na perimetru	Kamera s živým přenosem	3	3	0	0
			Kamera se záznamem	3	3	0	0
			Kamera s živým přenosem a záznamem	3	3	0	0
			Kamera s autonomními funkcemi	3	3	1	0
			Bariéra proti vozidlům	2	0	3	0
			Manuální brána	3	0	1	0
			Automatická brána	3	0	1	0
			Oplocení	3	0	1	0
			Detektor narušení	1	3	0	0
			Detektor střelby	0	3	0	0
			Detektor paniky	0	3	0	0
			Automatické osvětlení	3	0	0	0
			Statické osvětlení	3	0	0	0
		Na vstupních bodech	Kamera s živým přenosem	3	3	0	0
			Kamera se záznamem	3	3	0	0
			Kamera s živým přenosem a záznamem	3	3	0	0
			Kamera s autonomními funkcemi	3	3	1	0
			Bariéra proti vozidlům	2	0	3	0
			Manuální brána	3	0	1	0
			Automatická brána	3	0	1	0
			Detektor narušení	1	3	0	0
			Detektor střelby	0	3	0	0
			Detektor paniky	0	3	0	0
			Plnorozměrný turniket	3	0	2	0
			Tříbodový turniket	2	0	0	0
			Automatické osvětlení	3	0	0	0
			Statické osvětlení	3	0	0	0

Uvedený způsob ale umožňuje posuzovat bezpečnostní opatření pouze z jednoho úhlu pohledu. Z tohoto důvodu je vhodné zavedení dvoustupňového systému, který doplní hodnocení o další kritéria umožňující detailnější a komplexnější posouzení jednotlivých opatření. Výsledky hodnocení podle jednotlivých kritérií je vhodné porovnávat s ohledem na aktuální požadavky organizace a tím dospět k výběru nejvhodnější kombinace bezpečnostních opatření. Za tímto účelem je vytvářena druhá hodnotící tabulka zahrnující další významná kritéria výběru. Hodnoty z obou tabulek lze následně kombinovat, porovnávat nebo filtrovat podle specifických požadavků konkrétního objektu.

V rámci navrhovaného systému je proto uplatněn komplexní multikriteriální přístup. Aktuálně jsou uvažována tato kritéria: snížení atraktivity, snadnost implementace, časová náročnost, ekonomická náročnost, společenská přijatelnost a spolehlivost. Pro každé z těchto kritérií je navržena hodnotící škála v intervalu 1–5. Hodnocení je v současné fázi koncipováno kvalitativně, do budoucna je však žádoucí jeho podrobnější kvantifikace za účelem zvýšení objektivity. Tento aspekt představuje jeden ze směrů dalšího výzkumu.

Snížení atraktivity – toto kritérium vychází z významnosti míry atraktivity měkkého cíle a hodnotí míru, v jaké navrhované bezpečnostní opatření přispívá ke snížení atraktivity měkkého cíle pro potenciálního útočníka. Posuzuje zejména schopnost opatření působit preventivně a odrazujícím způsobem, tedy zda zvyšuje náročnost provedení útoku, pravděpodobnost odhalení nebo celkové riziko neúspěchu. Čím výrazněji opatření přispívá ke změně vnímání cíle jako snadno napadnutelného, tím vyšší je jeho hodnocení v rámci tohoto kritéria. Nejnižší hodnocení odpovídá opatřením, která atraktivitu nesnižují nebo pouze zanedbatelně, zatímco nejvyšší hodnota označuje opatření zásadně snižující vnímanou atraktivitu cíle.

Tabulka 4. Klasifikace snížení atraktivity [vlastní]

Klasifikace snížení atraktivity	**Hodnocení**
Zanedbatelné nebo žádné snížení atraktivity	1
Částečné snížení atraktivity	2
Zaznamenatelné snížení atraktivity	3
Výrazné snížení atraktivity	4
Zásadní snížení atraktivity	5

Snadnost implementace – další kritérium hodnotí míru organizační, technické a procesní náročnosti zavedení bezpečnostního opatření do provozu. Posuzuje rozsah a intenzitu stavebních úprav, omezení provozu, administrativní nároky i potřebu úprav interních předpisů či školení zaměstnanců. Význam spočívá v reálné proveditelnosti opatření, zejména u objektů s omezenými možnostmi zásahů (například u kulturních památek). Čím menší zásah do stávající struktury a procesů opatření vyžaduje, tím vyšší je jeho hodnocení. Nejnižší hodnota odpovídá opatřením vyžadujícím rozsáhlé zásahy a úpravy, zatímco nejvyšší hodnota označuje opatření, které lze zavést bez významných úprav.

Tabulka 5. Klasifikace snadnosti implementace [vlastní]

Klasifikace snadnosti implementace	**Hodnocení**
Rozsáhlé stavební úpravy, zásadní změny provozu	1
Náročné stavební úpravy, dílčí zásahy do provozu	2
Omezené stavební úpravy, běžný zásah do provozu	3
Zanedbatelné nebo žádné stavební úpravy, minimální dopad na provoz	4
Bez nutnosti významných úprav struktury a organizace objektu	5

Časová náročnost – tento parametr hodnotí dobu potřebnou k plnému zavedení bezpečnostního opatření do funkčního stavu. Zohledňuje délku přípravy, instalace a integrace do bezpečnostního systému objektu. Je významné zejména v situacích zvýšeného bezpečnostního rizika, kde je žádoucí rychlá implementace dodatečných opatření. Nejnižší hodnota odpovídá opatřením s dlouhou dobou přípravy a realizace, nejvyšší pak opatřením realizovatelným okamžitě nebo ve velmi krátkém časovém horizontu.

Tabulka 6. Klasifikace časové náročnosti [vlastní]

Klasifikace časové náročnosti	Hodnocení
Dlouhodobá příprava a zavádění do provozu	1
Časově náročná příprava a zavádění do provozu	2
Střední doba realizace a zavedení do provozu	3
Krátkodobé zavedení do provozu	4
Rychlé či okamžité zavedení do provozu	5

Ekonomická náročnost – jedná se o kritérium posuzující finanční zatížení spojené s implementací a provozem bezpečnostního opatření ve vztahu k rozpočtovým možnostem provozovatele měkkého cíle. Zohledňuje nejen pořizovací náklady, ale také náklady provozní, servisní, personální a náklady na školení. Význam kritéria spočívá v tom, že finanční limitace často zásadně určují výběr daných opatření či jejich kombinaci. Hodnocení umožní porovnat přínos opatření s jeho ekonomickou zátěží. Nejnižší hodnota odpovídá opatřením s vysokými počátečními a provozními náklady, zatímco nejvyšší hodnota opatřením ekonomicky nenáročným. Konkrétní finanční částky nejsou v této fázi zohledněny a budou předmětem dalšího výzkumu.

Tabulka 7. Klasifikace ekonomické náročnosti [vlastní]

Klasifikace ekonomické náročnosti	Hodnocení
Velmi vysoké náklady, obtížně financovatelné	1
Vysoké náklady, rozpočtově náročné	2
Střední nákladovost, rozpočtově udržitelné	3
Nízké náklady a rozpočtová zátěž	4
Minimální nebo žádná finanční náročnost	5

Společenská přijatelnost – je kritérium, které hodnotí míru akceptace opatření ze strany uživatelů prostoru, zaměstnanců a veřejnosti. Posuzuje, zda opatření nepůsobí nepřiměřeně restriktivně, nezasahuje nadměrně do soukromí nebo zásadně nenarušuje funkci objektu. Nízká míra akceptace může vést k obcházení pravidel, odporu ze strany uživatelů či ke snížení efektivity jejich aplikace. Nejnižší hodnota odpovídá opatřením vnímaným jako nepřiměřené, zatěžující nebo omezující, nejvyšší pak těm, která jsou uživatelsky přijatelná nebo jsou vnímána pozitivně.

Tabulka 8. Klasifikace společenské přijatelnosti [vlastní]

Klasifikace společenské přijatelnosti	Hodnocení
Nepřiměřené vůči charakteru objektu	1
Neoblíbené opatření, způsobující jeho obcházení	2
Obecně přijímáno s výhradami	3
Vnímáno neutrálně bez výhrad	4
Vnímáno pozitivně	5

Spolehlivost – toto kritérium hodnotí pravděpodobnost dlouhodobého plnění funkce opatření bez selhání. Posuzuje nároky na údržbu, aktualizaci, revizi dokumentace i kvalitu a četnost školení personálu. Význam kritéria spočívá v dlouhodobé udržitelnosti opatření v podmínkách konkrétní organizace. Nejnižší hodnota odpovídá opatřením vysoce náročným na údržbu, u nichž hrozí rychlá degradace účinnosti, zatímco nejvyšší hodnota označuje opatření stabilní a dlouhodobě funkční.

Tabulka 9. Klasifikace spolehlivosti [vlastní]

Klasifikace spolehlivosti	**Hodnocení**
Náročná a častá údržba či aktualizace, vysoká degradace účinnosti při zanedbání	1
Nutná častá a pravidelná údržba či aktualizace, snížení účinnosti při zanedbání	2
Nutná pravidelná údržba či aktualizace, minimální snížení účinnosti při zanedbání	3
Vhodná pravidelná údržba či aktualizace, udržení míry účinnosti v čase	4
Dlouhodobě stabilní bez nadstandardních zásahů	5

Uvedená kritéria budou následně zahrnuta do multikriteriální analýzy, která umožní variabilní nastavení vah jednotlivých parametrů. Tím bude umožněno metodiku přizpůsobit specifikům a požadavkům konkrétního měkkého cíle. Dalším krokem je vytvoření výpočtového modelu pro stanovení celkového hodnocení jednotlivých variant bezpečnostních opatření. Stanovení způsobu výpočtu váhových koeficientů a zohlednění specifických charakteristik objektu je předmětem dalšího výzkumu.

4 Závěr

Článek se zabýval problematikou systematického hodnocení bezpečnostních opatření v prostředí měkkých cílů a reaguje na potřebu efektivního využívání zdrojů jejich provozovatelů. Hlavním cílem bylo představit rozpracovaný návrh strukturovaného přístupu umožňujícího přehledné porovnání a výběr vhodných bezpečnostních opatření s ohledem na specifika objektu. V první části byl nejdříve vymezen pojem měkký cíl a zdůrazněna nutnost vyhodnocení bezpečnostních rizik. Současně bylo poukázáno na faktor atraktivity, který ovlivňuje specifika daného objektu. Dále bylo představeno základní dělení bezpečnostních opatření, a především komplexnost jejich specifik, podle nichž je lze klasifikovat a rozdělit na konkrétní varianty.

Hlavní část tvoří koncepční základ návrhu dvoustupňového hodnotícího systému. První částí je využití matice OORA k posouzení účinnosti opatření ve fázích odstrašení, odhalení, reakce a absorpce, čímž se umožňuje identifikovat žádoucí pokrytí jednotlivých fází. Druhá část představuje rozpracovanou myšlenku multikriteriálního hodnocení, které zahrnuje kritéria snížení atraktivity, snadnosti implementace, časové náročnosti, ekonomické náročnosti, společenské přijatelnosti a spolehlivosti. Cílem je kombinace těchto dvou přístupů, která umožní komplexní posouzení vhodnosti jednotlivých opatření a jejich následnou filtraci podle konkrétních požadavků organizace. Další výzkum bude směřovat k podrobnější kvantifikaci hodnotících kritérií, stanovení váhových koeficientů a vytvoření výpočtového modelu umožňujícího objektivizované stanovení celkového hodnocení variant bezpečnostních opatření.

Reference

[1] KAVLACH, Zdeněk. Koncepce ochrany měkkých cílů pro roky 2017–2020. Online. Ministerstvo vnitra České republiky. 2017. Dostupné z: https://mv.gov.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx. [cit. 2026-02-27]

[2] Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu. Online. Ministerstvo vnitra České republiky. 2016. Dostupné z: https://mv.gov.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx. [cit. 2026-02-27]

[3] KALVACH, Zdeněk. Základy ochrany měkkých cílů – metodika. Online. In: Ministerstvo vnitra České republiky. 2016. Dostupné z: https://mv.gov.cz/soubor/metodika-zaklady-ochrany-mekkych-cilu-pdf.aspx. [cit. 2026-02-27]

[4] NEVRKLA, Jakub. Měkké cíle: identifikace, ohroženost a jejich ochrana. Online. Praha: Soft Targets Protection Institute, 2019. ISBN 978-80-270-7066-4. Dostupné z: https://mekkecile.fai.utb.cz/wp-content/uploads/2022/01/Mekke-cile-kniha-final.pdf. [cit. 2026-02-27]

[5] KAVLACH, Zdeněk. Vyhodnocení ohroženosti měkkého cíle aneb co, kdy, kde a od koho vám hrozí. Online. In: Ministerstvo vnitra České republiky. 2025. Dostupné z: https://mv.gov.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx. [cit. 2026-02-27]

[6] VALOUCH, Jan. Projektování bezpečnostních systémů. Online. Digitální knihovna UTB. 2012. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/18663/Skripta%20PBS%20Valouch.pdf. [cit. 2026-02-27]

[7] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. Online. Zlín: VeRBuM, 2011. ISBN 978-80-87500-05-7. [cit. 2026-02-27]

[8] LUKÁŠ, Luděk. Teorie bezpečnosti I. Online. Zlín: VeRBuM, 2017. ISBN 978-80-87500-89-7. [cit. 2026-02-27]

[9] VALOUCH, Jan. Projektování bezpečnostních systémů. Online. In: Digitální knihovna UTB. 2019. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/45863/Projektov%c3%a1n%c3%ad_bezpe%c4%8dnostn%c3%adch_syst%c3%a9m%c5%af_2019.pdf. [cit. 2026-02-27]

[10] Vyhláška č. 528/2005 Sb. Vyhláška o fyzické bezpečnosti a certifikaci technických prostředků. Online. In: Zákony pro lidi. 2005. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528. [cit. 2026-02-27]

Využitie umelej inteligencie v kriminalistickom objasňovaní – tvorba kriminalistických verzií

Lukáš Lencsés[1], Veronika Adamová[2]

[1] Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva,
1. mája 32, 010 01 Žilina, lencses@uniza.sk

[2] Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva,
1. mája 32, 010 01 Žilina, veronika.adamova@uniza.sk

Abstrakt:

Predložený článok sa zaoberá možnosťami využitia umelej inteligencie pri tvorbe kriminalistických verzií v procese objasňovania trestných činov. Kriminalistická verzia predstavuje metodický nástroj založený na formulovaní a preverovaní logicky odôvodnených alternatívnych vysvetlení skúmanej udalosti. Jej kvalita zásadne ovplyvňuje smerovanie dokazovania a konečný výsledok vyšetrovania. Proces tvorby verzií je však podmienený limitmi ľudského poznávania, najmä kognitívnymi skresleniami, selektívnym hodnotením informácií a predčasnou fixáciou na jednu hypotézu. Súčasne sa kriminalistická prax vyznačuje rastúcim objemom digitálnych a dátovo náročných informácií, ktoré presahujú tradičné analytické kapacity jednotlivca. Cieľom článku je analyzovať teoretické východiská kriminalistických verzií, identifikovať riziká spojené s ich tvorbou výlučne človekom a preskúmať súčasné možnosti využitia umelej inteligencie v kriminalistickom objasňovaní. Na tomto základe je navrhnutý hybridný model, ktorý kombinuje analytické schopnosti AI s rozhodovacou a právnou zodpovednosťou človeka. Navrhovaný model zdôrazňuje pluralitu verzií, transparentnosť postupu a iteratívne vyhodnocovanie nových dôkazov. Článok poukazuje na potenciál umelej inteligencie zvýšiť objektivitu, systematickosť a metodickú stabilitu tvorby kriminalistických verzií.

Kľúčové slová: umelá inteligencia, kriminalistická verzia, objasňovanie trestných činov, analýza dát.

1 Úvod

Kriminalistické objasňovanie trestných činov je komplexný poznávací proces, ktorého cieľom je zistenie skutkového stavu bez dôvodných pochybností. Kľúčovým metodickým nástrojom tohto procesu je tvorba kriminalistických verzií, teda logicky odôvodnených a preveriteľných vysvetlení skúmanej udalosti. Prostredníctvom verzií sa zjednocujú zistené fakty, identifikujú možné príčinné súvislosti a určujú smery ďalšieho dokazovania. Kvalita a úplnosť vytvorených verzií pritom zásadne ovplyvňujú priebeh aj výsledok vyšetrovania.

Súčasná kriminalistická prax však čelí novým výzvam. Vyšetrovanie sa čoraz častejšie opiera o rozsiahle digitálne dáta, komplexné sieťové vzťahy a dynamické informačné prostredie, ktoré presahujú tradičné analytické kapacity jednotlivca. Zároveň je proces tvorby verzií nevyhnutne ovplyvnený limitmi ľudského rozhodovania, vrátane kognitívnych skreslení a rozdielov v skúsenostiach či metodickej disciplíne. Tieto faktory môžu viesť k predčasnej fixácii na jednu hypotézu, k neúplnosti alternatív alebo k nerovnomernému preverovaniu jednotlivých scenárov.

Rozvoj umelej inteligencie (ďalej „AI“, z angl. Artificial Intelligence) otvára otázku, do akej miery možno tieto technológie využiť ako podporu pri tvorbe kriminalistických verzií. Hoci sa AI v súčasnosti využíva najmä na analýzu dát, rozpoznávanie vzorcov či podporu rozhodovania, jej potenciál ako nástroja na systematické

generovanie a porovnávanie alternatívnych vysvetlení zatiaľ nie je plne rozpracovaný v rámci kriminalistickej taktiky ani implementovaný do kriminalistickej metodiky.

Cieľom tohto článku je analyzovať teoretické východiská kriminalistických verzií, poukázať na limity ich tvorby v podmienkach výlučne ľudského rozhodovania a následne navrhnúť hybridný model, v ktorom sa kombinuje analytická kapacita umelej inteligencie s rozhodovacou a právnou zodpovednosťou človeka. U takto koncipovanom prístupe sa predpokladá, že môže prispieť k vyššej objektivite, systematickosti a transparentnosti procesu kriminalistického objasňovania.

2 Teoretické východiská

2.1 Kriminalistické verzie

Objasňovanie trestného činu je základnou úlohou kriminalistickej praxe. Jeho cieľom je zistiť skutkový stav veci tak, aby o ňom nevznikali dôvodné pochybnosti, teda čo najpresnejšie rekonštruovať, čo sa v minulosti skutočne stalo. Nejde iba o zhromažďovanie jednotlivých informácií, ale o ich systematické vyhodnocovanie a prepájanie. V procese objasňovania sa posudzuje význam zistených skutočností, ich vzájomné súvislosti, ako aj ich právna relevancia a vzťah ku konkrétnym osobám. Kriminalistické verzie vstupujú do tohto procesu objasňovania ako metodický nástroj usporiadania poznania [1,2].

Kriminalistická verzia predstavuje odôvodnený, logicky konštruovaný predpoklad o existencii, priebehu a okolnostiach kriminalisticky relevantnej udalosti, najmä o spôsobe spáchania skutku, jeho príčinách, následkoch a možných páchateľoch. Ide o špecifickú formu hypotézy vychádzajúcej z predbežne zistených faktov, ako sú poznatky z miesta činu, kriminalistické stopy, výpovede osôb či iné dôkazne významné informácie. Jej podstatou je vytváranie a následné systematické preverovanie všetkých racionálne odôvodnených alternatívnych vysvetlení skúmanej udalosti s cieľom dosiahnuť objektívne zistenie skutkového stavu veci bez dôvodných pochybností [1].

Je možné tvrdiť, že kriminalistická verzia je metodicky formulovaný predpoklad, ktorý je založený na logických postupoch, najmä indukcii, dedukcii a analógii, smerujúci k vytvoreniu dočasného záveru, podliehajúceho ďalšiemu overovaniu. Kriminalistické verzie tak predstavujú základný metodický nástroj poznávacieho procesu v kriminalistike, umožňujúci usporiadať zistené fakty, identifikovať vzťahy medzi nimi a cielene smerovať ďalšie úkony objasňovania [3].

2.2 Tvorba kriminalistických verzií

Tvorba kriminalistických verzií je teda **štruktúrovaný logický proces**, v ktorom sa z počiatočného súboru rozptýlených informácií prostredníctvom analýzy, syntézy a deduktívno-induktívneho uvažovania vytvárajú systematické vysvetlenia skúmanej udalosti, ktoré sú následne podrobované overovaniu [2].

Proces tvorby kriminalistických verzií možno rozdeliť na tri na seba nadväzujúce etapy:

- zhromažďovanie a logická analýza faktického materiálu,
- vyvodenie a formulácia domnienok ako základu verzií,
- určenie dôsledkov jednotlivých verzií a ich preverovanie [2].

Prvá etapa spočíva v zabezpečení dostatočného množstva kriminalisticky relevantných informácií. Ide o zhromažďovanie všetkých dostupných faktov a stôp bez ohľadu na to, či svedčia v prospech alebo neprospech určitej osoby. Zdroje informácií môžu byť rôznorodé – od obhliadky miesta činu, výpovedí osôb, evidencií, operatívnych poznatkov až po analógiu s inými prípadmi. Samotné zhromaždenie faktov však nepostačuje. Nasleduje ich logická analýza, triedenie a hodnotenie, pri ktorom sa skúmajú vzájomné súvislosti, časové a príčinné väzby a význam jednotlivých zistení pre objasňovanú udalosť. Výsledkom tejto fázy je vytvorenie usporiadaného faktického základu, ktorý umožňuje prechod k formulácii domnienok [2].

Druhá etapa predstavuje vlastnú tvorbu kriminalistických verzií. Na základe vyhodnotených faktov sa vyvodzujú logické domnienky, ktoré vysvetľujú ich vzájomný vzťah a smerujú k záveru o priebehu, príčine alebo mechanizme udalosti. Domnienka je logický úsudok založený na súbore faktov, medzi ktorými možno identifikovať určitý vzťah (miestny, časový, príčinný alebo iný). Kriminalistická verzia je následne presne formulovaná a systematicky usporiadaná podoba takejto domnienky. Každá verzia musí byť objektívne podložená existujúcimi faktami, musí z nich logicky vyplývať a nesmie byť vnútorne rozporná. Zároveň je potrebné vytvoriť všetky reálne možné verzie, ktoré prichádzajú do úvahy, pričom ich počet závisí od zložitosti prípadu. Tým sa zabezpečuje všestrannosť a objektívnosť vyšetrovania [2].

Tretia etapa spočíva vo vyvodzovaní dôsledkov z jednotlivých verzií. Ak je určitá verzia pravdivá, musia z nej vyplývať konkrétne následky, ktoré by mali alebo mohli existovať v objektívnej realite. Rozlišujú sa nevyhnutné dôsledky (tie, ktoré musia existovať, ak je verzia správna) a reálne možné dôsledky (tie, ktoré mohli vzniknúť, ale nie sú nevyhnutné). Tieto predpokladané dôsledky slúžia ako základ pre ďalšie dokazovanie a preverovanie. Myšlienkový postup sa tu spravidla pohybuje od následku späť k príčine, pričom cieľom je potvrdiť alebo vyvrátiť jednotlivé verzie. Celý proces má pravdepodobnostný charakter a jeho výsledkom je postupné zužovanie okruhu možných vysvetlení až k verzii, ktorá zodpovedá zisteným faktom [2].

2.3 Problémy súčasného stavu

Kriminalistické verzie predstavujú základný metodický nástroj objasňovania trestných činov. Ich praktické využívanie v aplikačnej praxi však naráža na viaceré systémové aj individuálne limity. Hlavné problematické oblasti je možné systematicky zhrnúť do nasledujúcich oblastí:

Podceňovanie teoretického základu a prevaha neformálne osvojenej praxe:

- učenie sa „podľa kolegov“ bez systematického pochopenia logickej štruktúry procesu,
- reprodukcia zaužívaných postupov bez reflexie špecifík konkrétneho prípadu,
- formalizmus pri tvorbe verzií (verzie len „do spisu“) [3].

Intuitívne a nevedomé používanie kriminalistických verzií:

- absencia explicitného formulovania alternatív,
- nevymedzenie všetkých reálne možných verzií,
- nedostatočné systematické vyvodzovanie dôsledkov z jednotlivých verzií [3].

Nedostatky v aplikácii logických metód:

- používanie indukcie, dedukcie a analógie bez metodickej kontroly,
- unáhlené závery a predčasná fixácia na jednu verziu,
- nedostatočné preverovanie príčinných a časových súvislostí,
- zúženie vyšetrovacieho rámca ignorovaním alternatív [3].

Nedostatok skúseností alebo ich jednostrannosť:

- automatizácia myslenia a stereotypné postupy,
- slabé rozvíjanie analytických schopností,
- obmedzená schopnosť generovať netradičné, no reálne možné verzie [3].

Zvýšenú pozornosť v procese kriminalistického objasňovania je nutné venovať problematike **kognitívneho skreslenia**. Kognitívne skreslenie predstavuje systematickú odchýlku v procese vnímania, hodnotenia a interpretácie informácií, ktorá vzniká v dôsledku fungovania prirodzených mentálnych mechanizmov človeka. Nejde o náhodnú chybu ani o nedostatok inteligencie, ale o predvídateľný efekt spôsobu, akým ľudský mozog spracováva informácie v podmienkach obmedzeného času, kapacity pozornosti, neistoty a ďalších negatívnych aspektov [4].

Kognitívne skreslenia pri tvorbe kriminalistických verzií:

- **Konfirmačné skreslenie** – tendencia vyhľadávať, uprednostňovať a interpretovať informácie tak, aby potvrdzovali už vytvorenú predstavu/verziu.
- **Ukotvenie** – prvé informácie (prvotný podnet, prvá výpoveď, prvá operatívna verzia) sa stanú „kotvou“, od ktorej sa ďalšie úvahy odvíjajú.
- **Tunelové videnie** – kombinácia viacerých skreslení.
- **Heuristika dostupnosti** – to, čo si vyšetrovateľ ľahko vybaví, sa javí ako pravdepodobnejšie, než v skutočnosti je [4].

Význam kognitívnych skreslení pri tvorbe kriminalistických verzií poukazuje na potrebu nástrojov, ktoré pomáhajú zmierňovať ich vplyv. Umelá inteligencia môže v tomto smere slúžiť ako podporný analytický prostriedok, ktorý systematicky generuje viacero alternatívnych vysvetlení a umožňuje ich konzistentné porovnávanie. Na rozdiel od intuitívneho ľudského uvažovania nie je viazaná na prvotnú hypotézu ani osobnú skúsenosť, čím znižuje riziko predčasnej fixácie na jednu verziu. V hybridnom modeli, kde rozhodovanie zostáva na človeku, môže AI prispieť k vyššej objektivite a metodickej presnosti procesu objasňovania [5].

2.4 Umelá inteligencia

Umelá inteligencia (artificial intelligence, AI) je oblasť informatiky zameraná na vývoj systémov, ktoré dokážu vykonávať úlohy vyžadujúce určitú formu ľudského myslenia. Ide najmä o schopnosť analyzovať údaje, rozpoznávať vzorce, učiť sa zo skúseností a vyvodzovať závery na základe dostupných informácií. Súčasný rozvoj AI je úzko spojený so strojovým učením, teda s metódami, ktoré umožňujú algoritmom identifikovať vzťahy v dátach bez toho, aby boli vopred presne naprogramované pre každú konkrétnu situáciu. Osobitne významné je hlboké učenie, ktoré sa využíva pri spracovaní obrazu, textu či rozsiahlych digitálnych databáz [6].

V oblasti bezpečnosti sa AI využíva predovšetkým ako podporný nástroj, ktorý spracúva a analyzuje informácie, zatiaľ čo konečné rozhodnutie a zodpovednosť zostávajú na človeku. Umelá inteligencia teda nenahrádza ľudský úsudok, ale rozširuje jeho analytické možnosti [7].

Pre kriminalistiku je dôležité, že AI dokáže pracovať s veľkým množstvom rôznorodých údajov, systematicky ich vyhodnocovať a upozorňovať na menej zjavné súvislosti. Táto schopnosť vytvára teoretický predpoklad pre jej využitie nielen pri analýze dôkazov, ale aj pri podpore tvorby a porovnávania kriminalistických verzií [7].

Zároveň je potrebné zdôrazniť, že účinnosť umelej inteligencie závisí od kvality vstupných dát, spôsobu jej nastavenia a kontroly jej výstupov. Bez metodického rámca a kritického hodnotenia zo strany človeka môže AI reprodukovať existujúce chyby alebo skreslenia. Preto musí byť jej využívanie v kriminalistike vždy sprevádzané odborným dohľadom a jasne stanovenými pravidlami aplikácie [7].

3 Súčasné využitie AI v procese kriminalistického objasňovania

Rozvoj umelej inteligencie v posledných rokoch výrazne ovplyvnil aj oblasť kriminalistiky. V procesoch kriminalistického objasňovania sa AI uplatňuje predovšetkým ako analytický nástroj na spracovanie veľkého objemu dát, identifikáciu vzorcov správania a podporu rozhodovania. Nejde o autonómne rozhodovanie, ale o technologickú podporu jednotlivých fáz poznávacieho procesu.

Analýza veľkých dát a informačných súvislostí – moderné vyšetrovanie generuje rozsiahle množstvo údajov. Manuálne spracovanie takéhoto objemu informácií je časovo náročné a zvyšuje riziko prehliadnutia významných väzieb. AI môže identifikovať vzťahy medzi osobami, miestami a udalosťami, detegovať opakujúce sa vzorce správania alebo upozorniť na anomálie, ktoré by inak mohli zostať nepovšimnuté. Využíva sa pritom najmä sieťová analýza, klastrovanie, klasifikácia a detekcia odchýlok od bežných modelov správania [8].

Ako príklad technologického riešenia možno uviesť projekt VALCRI (Visual Analytics for Sense-making in Criminal Intelligence Analysis), ktorý kombinuje vizuálne analytické skúmanie , spracovanie prirodzeného jazyka a big-data technológie s cieľom podporiť rozhodovanie vyšetrovateľov [9].

Prediktívna analýza a prediktívne mapovanie kriminality – prediktívna analýza predstavuje využitie algoritmov strojového učenia na identifikáciu priestorových a časových vzorcov kriminality na základe historických dát. Systémy analyzujú údaje o predchádzajúcich trestných činoch, ich lokalizácií, čase výskytu a ďalších kontextových faktoroch (napr. demografické či environmentálne premenné) a vytvárajú modely pravdepodobnosti budúceho výskytu podobných udalostí. Výsledkom bývajú tzv. „rizikové mapy“, ktoré označujú oblasti alebo časové úseky so zvýšenou pravdepodobnosťou určitého druhu kriminality [10].

Rozpoznávanie obrazu a biometria – v rámci kriminalistického objasňovania sa umelá inteligencia čoraz častejšie využíva pri analýze obrazu a videozáznamov. AI-založené technológie rozpoznávania tváre a ďalších biometrických znakov umožňujú identifikovať osoby na kamerových záznamoch či porovnávať ich s databázami evidovaných jedincov, čo môže urýchliť pátranie a podporiť orientáciu vyšetrovania [11].

AI pri generovaní hypotéz v súčasnej kriminalistickej praxi – napriek tomu, že sa v súčasnosti umelá inteligencia v kriminalistickej praxi nevyužíva priamo na systematické generovanie kriminalistických verzií, teoretické aj empirické výskumy naznačujú, že takýto potenciál existuje. Práce z oblasti strojového učenia, ako napr. štúdia *Machine Learning as a Tool for Hypothesis Generation* (Ludwig & Mullainathan, 2023), poukazujú na schopnosť algoritmov identifikovať nové a netriviálne hypotézy v komplexných dátových prostrediach. Ak je strojové učenie schopné generovať zmysluplné vysvetľujúce hypotézy v ekonomických či spoločenských vedách, analogicky možno uvažovať o jeho využití aj pri tvorbe alternatívnych kriminalistických verzií, najmä v prípadoch s rozsiahlym a štruktúrne zložitým dôkazným materiálom [5].

4 Návrh hybridného modelu tvorby kriminalistických verzií (človek + AI)

S prihliadnutím na identifikované limity čisto ľudského rozhodovania a na možnosti analytických nástrojov umelej inteligencie možno navrhnúť hybridný model tvorby kriminalistických verzií. Podstatou modelu nie je nahradenie vyšetrovateľa algoritmom, ale funkčné rozdelenie úloh medzi človeka a AI tak, aby sa minimalizovali kognitívne skreslenia a zároveň zvýšila rýchlosť a efektivita procesov kriminalistického objasňovania.

Hybridný model je založený na funkčnom rozdelení úloh medzi ľudský subjekt objasňovania (vyšetrovateľa) a analytický systém umelej inteligencie.

Úlohy subjektu objasňovania:

- **Zber, selekcia a procesné sprístupnenie dôkazov AI** – Systém pracuje len s tým, čo je zákonným spôsobom poskytnuté.
- **Právne a hodnotové posúdenie** – Posúdenie zákonnosti, prípustnosti a relevancie jednotlivých verzií a navrhovaných úkonov,
- **Zodpovednosť za výsledok** – Plná odborná a právna zodpovednosť za smerovanie a výsledok objasňovania ostáva na človeku.
- **Finálny verdikt** – Konečné hodnotenie kriminalistických verzií, výber ďalšieho postupu a procesné rozhodnutia vykonáva vždy oprávnený subjekt.

Úlohy umelej inteligencie:

- **Analytická podpora spracovania dát** – Štrukturalizácia veľkého objemu informácií, identifikácia vzorcov a vzťahov medzi dátami.
- **Generovanie alternatívnych verzií** – Systematické vytváranie viacerých realistických scenárov vyplývajúcich zo vstupných údajov.
- **Zabezpečenie plurality verzi**í – Prevencia predčasnej fixácie na jednu hypotézu prostredníctvom algoritmického generovania alternatív.
- **Modelovanie dôsledkov** – Identifikácia pravdepodobných následkov jednotlivých verzií a upozornenie na logické rozpory.
- **Dynamické overovanie/vyhodnocovanie/úprava verzií** – AI zabezpečuje priebežné prehodnocovanie pravdepodobnosti jednotlivých verzií a ich aktualizáciu na základe nových vstupných údajov, čím sa predchádza dlhodobej fixácii na pôvodnú hypotézu.

4.1 Fázy hybridného modelu

Navrhovaný hybridný model je rozdelený do jednotlivých fáz z dôvodu metodickej prehľadnosti a analytickej presnosti. Tvorba kriminalistických verzií totiž neprebieha ako jednorazový úkon, ale ako postupný proces pozostávajúci zo zberu dát, ich analýzy, formulovania hypotéz a ich následného preverovania.

Fáza 1 – Štrukturalizácia vstupných dát

Prvá fáza predstavuje vytvorenie spoľahlivého faktického základu pre ďalší analytický proces. Človek zabezpečuje zákonný zber dôkazov prostredníctvom procesných úkonov a rozhoduje o tom, ktoré informácie sú relevantné pre objasňovanie udalosti. Následne sa tieto údaje štrukturalizujú a pripravujú na analytické spracovanie. Umelá inteligencia v tejto fáze napomáha organizovať rozsiahle množstvo dát, identifikovať vzťahy medzi osobami,

miestami a udalosťami a vytvárať prehľadné analytické mapy súvislostí. Cieľom je premeniť rozptýlené informácie na konzistentný a systematicky usporiadaný základ pre tvorbu verzií.

Fáza 2 – Generovanie alternatívnych verzií

V druhej fáze dochádza k samotnej tvorbe kriminalistických verzií. Na základe analyzovaných dát umelá inteligencia generuje viacero realistických alternatívnych scenárov priebehu udalosti a vyhodnocuje ich pravdepodobnosť. Tento postup zabezpečuje pluralitu verzií a znižuje riziko predčasnej fixácie na jedinú hypotézu. Človek následne posudzuje navrhnuté verzie z hľadiska ich právnej relevancie, logickej konzistentnosti a praktickej realizovateľnosti v podmienkach konkrétneho prípadu.

Fáza 3 – Vyvodzovanie dôsledkov a testovanie

Tretia fáza je zameraná na preverovanie jednotlivých verzií prostredníctvom vyvodzovania ich logických dôsledkov. Ak je určitá verzia pravdivá, musia z nej vyplývať konkrétne overiteľné následky v podobe dôkazov alebo iných zistení. Umelá inteligencia môže modelovať možné dôsledky jednotlivých scenárov, identifikovať rozpory či chýbajúce informácie a upozorniť na slabé miesta hypotéz. Človek rozhoduje o vykonaní konkrétnych procesných úkonov a hodnotí výsledky dokazovania v súlade so zásadou voľného hodnotenia dôkazov.

Fáza 4 – Priebežná aktualizácia verzií

Posledná fáza predstavuje dynamickú aktualizáciu kriminalistických verzií na základe nových zistení. Každý nový dôkaz alebo informácia môže meniť hodnotenie pravdepodobnosti jednotlivých scenárov. Umelá inteligencia umožňuje priebežné prehodnocovanie verzií a identifikáciu zmien v ich logickej štruktúre, čím sa predchádza dlhodobej fixácii na pôvodnú hypotézu. Človek zároveň vykonáva kontrolu primeranosti a zákonnosti ďalšieho postupu. Tento iteratívny charakter modelu zabezpečuje, že proces objasňovania zostáva otvorený, adaptívny a metodicky konzistentný.

4.2 Očakávané prínosy modelu

Navrhovaný hybridný model predstavuje metodické prepojenie analytickej kapacity umelej inteligencie s rozhodovacou a hodnotiacou kompetenciou človeka. Jeho cieľom nie je automatizácia vyšetrovania, ale zvýšenie kvality, objektivity a systematickosti procesu tvorby a preverovania kriminalistických verzií. Očakávané prínosy modelu možno identifikovať v nasledujúcich rovinách.

Zvýšenie objektivity a redukcia kognitívnych skreslení

Jedným z hlavných prínosov modelu je zmiernenie vplyvu kognitívnych skreslení, najmä potvrdzovacieho skreslenia, predčasného ukotvenia a tendencie zužovať okruh alternatív. Algoritmické generovanie viacerých verzií na základe rovnakých vstupných dát podporuje pluralitu hypotéz a systematické porovnávanie alternatív. Tým sa znižuje riziko jednostranného zamerania vyšetrovania a posilňuje zásada objektívnosti.

Rozšírenie analytickej kapacity

Umelá inteligencia umožňuje spracovanie rozsiahleho množstva štruktúrovaných aj neštruktúrovaných dát, identifikáciu vzorcov a súvislostí, ktoré by pri manuálnej analýze mohli zostať nepovšimnuté. Hybridný model tak zvyšuje schopnosť pracovať s komplexnými dátovými štruktúrami, najmä v prípadoch s veľkým objemom digitálnych dôkazov alebo rozsiahlymi sieťami vzťahov medzi osobami.

Zvýšenie efektívnosti vyšetrovania

Vďaka systematizácii analytických krokov a automatizácii časti hodnotiacich procesov možno očakávať skrátenie času potrebného na vytvorenie a preverenie alternatívnych verzií. Uvoľnená kapacita vyšetrovateľa môže byť následne využitá na kvalitatívne hodnotenie dôkazov, plánovanie úkonov a právne posúdenie prípadu.

Obrázok 1. Očakávané prínosy hybridného modelu

5 Záver

Tvorba kriminalistických verzií predstavuje kľúčový metodický nástroj objasňovania trestných činov, ktorého kvalita priamo ovplyvňuje smerovanie a výsledok vyšetrovania. Ako bolo ukázané, ide o komplexný poznávací proces, v ktorom sa z neúplných a často rozporných informácií vytvárajú logicky odôvodnené a preveriteľné vysvetlenia skúmanej udalosti. Súčasne však tento proces podlieha prirodzeným limitom ľudského rozhodovania, najmä v podobe kognitívnych skreslení a individuálnych rozdielov v analytickej praxi.

Navrhnutý hybridný model tvorby kriminalistických verzií predstavuje koncepčný rámec, ktorý spája rozhodovaciu a právnu zodpovednosť človeka s analytickými možnosťami umelej inteligencie. Jeho cieľom nie je nahradiť človeka, ale metodicky ho podporiť, rozšíriť spektrum alternatív a zvýšiť konzistentnosť preverovania verzií. Pri rešpektovaní zásady zákonnosti, transparentnosti a procesnej kontroly môže takýto model prispieť k vyššej objektivite, efektívnosti a systematickosti objasňovania trestných činov.

Budúci výskum by sa mal zamerať na technické overenie funkčnosti navrhovaného modelu, jeho normatívne ukotvenie a identifikáciu podmienok, za ktorých môže byť bezpečne a účinne implementovaný do kriminalistickej praxi.

Referencie

[1] STARGAZDOVÁ, Simona. 2017. Význam kriminalistickej teórie – tvorba kriminalistických verzií pre kriminalistickú prax a proces plánovania vyšetrovania. Košice: Vysoká škola bezpečnostného manažmentu v Košiciach. Diplomová práca. 72 s. Dostupné na: https://opac.crzp.sk/?fn=detailBiblioForm&sid=9921973E4D44D17B1B3B19EA286A

[2] TESAŘOVÁ, Cyntia, 2024. Kriminalistické verzie a kriminalistické pátranie ako metódy kriminalistickej taktiky. Bratislava: Paneurópska vysoká škola v Bratislave, Fakulta práva. Rigorózna práca. 94 s. Dostupné na: https://opac.crzp.sk/?fn=detailBiblioForm&sid=8DA5F85D14F67EBBAAD8E6D69B73

[3] JAKUBÍK, Ľuboš, 2020. Kriminalistické verzie v procese vyšetrovania kriminalisticky relevantnej udalosti [online]. Bratislava: Akadémia Policajného zboru v Bratislave, Fakulta kriminálnej polície a forenzných vied. Diplomová práca. 69 s. Dostupné na: https://opac.crzp.sk/?fn=detailBiblioForm&sid=669792990D135F3F5CBFA80DC5E0

[4] Meterko, V. Cooper, G. 2021. Cognitive biases in criminal case evaluation: A review of the research. Journal of Police and Criminal Psychology. Dostupné na: https://link.springer.com/article/10.1007/s11896-020-09425-8

[5] LUDWIG, Jens – MULLAINATHAN, Sendhil. 2023. Machine Learning as a Tool for Hypothesis Generation. Chicago: Becker Friedman Institute for Economics at the University of Chicago. Dostupné na: https://www.nber.org/system/files/working_papers/w31017/w31017.pdf

[6] RUSSELL, Stuart – NORVIG, Peter. 2021. Artificial Intelligence: A Modern Approach. 4th ed. Harlow: Pearson. ISBN 978-0134610993. Dostupné na: http://lib.ysu.am/disciplines_bk/efdd4d1d4c2087fe1cbe03d9ced67f34.pdf

[7] SURDEN, Harry. 2019. Artificial Intelligence and Law: An Overview. Georgia State University Law Review. 2019, roč. 35, č. 4, s. 1305–1335. ISSN 1042-3915. Dostupné na: https://scholar.law.colorado.edu/cgi/viewcontent.cgi?article=2340&context=faculty-articles

[8] DUNSIN, Dipo, GHANEM, Mohamed C., OUAZZANE, Karim a VASSILEV, Vassil, 2024. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. Forensic Science International: Digital Investigation, 48, 301675. ISSN 2666-2817. Dostupné na: https://www.sciencedirect.com/science/article/pii/S2666281723001944?via%3Dihub

[9] MIHULKA, Stanislav, 2017. Systém VALCRI: Při vyšetřování zločinů budou pomáhat umělé inteligence [online]. 20. 5. 2017. Dostupné na: https://www.stoplusjednicka.cz/valcri-pri-vysetrovani-zlocinu-budou-pomahat-umele-inteligence [cit. 2026-03-03]

[10] BRANTINGHAM, P. Jeffrey, VALASIK, Matthew a MOHLER, George O., 2018. Does Predictive Policing Lead to Biased Arrests? Results From a Randomized Controlled Trial. Statistics and Public Policy, 5(1), 1–6. Dostupné na: https://www.tandfonline.com/doi/full/10.1080/2330443X.2018.1438940

[11] SAGANA, Anna, ZHANG, Mengying a SAUERLAND, Melanie, 2026. Public attitudes towards police use of AI-driven face recognition technology. Computers in Human Behavior. Dostupné na: https://www.sciencedirect.com/science/article/pii/S0747563225002687

Skenovanie zraniteľností ako nástroj kybernetickej odolnosti pri ochrane kritickej infraštruktúry v podmienkach SR

Timotej Mačuha[1], Katarína Kampová[2]

[1] Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva,
1. mája 32, 010 01 Žilina, macuha@uniza.sk

[2] Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva,
1. mája 32, 010 01 Žilina, kampova@uniza.sk

Abstrakt:

Kybernetické útoky v posledných rokoch výrazne narastajú a čoraz častejšie zasahujú prevádzkovateľov prvkov kritickej infraštruktúry. Jednou z najčastejších príčin kybernetických incidentov zostávajú známe, no neodstránené zraniteľnosti. Smernica NIS2 zavádza povinnosť systematického riadenia rizík a zraniteľností pre kľúčové a dôležité subjekty, medzi ktoré môžu patriť aj prevádzkovatelia prvkov kritickej infraštruktúry. Na Slovensku je táto povinnosť implementovaná najmä prostredníctvom národnej legislatívy v oblasti kybernetickej bezpečnosti. V tomto kontexte sa pravidelné skenovanie zraniteľností stáva nielen technickým opatrením, ale aj významným nástrojom budovania kybernetickej odolnosti a zabezpečenia kontinuity prevádzky organizácií. V príspevku analyzujeme legislatívne požiadavky na skenovanie zraniteľností v prostredí informačných technológií (IT) aj prevádzkových technológií (OT) a predstavujeme praktický postup ich implementácie v podmienkach obmedzených personálnych a finančných zdrojov. Ako referenčnú platformu používame OPENVAS v komunitnej edícii a popisujeme odporúčané nastavenia, procesy, metriky prioritizácie a spôsob dokumentovania výsledkov. Zohľadňujeme aj požiadavku auditovateľnosti celého cyklu riadenia zraniteľností. Diskutujeme špecifiká skenovania v segmentovaných sieťach a v prostredí OT, kde je potrebné minimalizovať riziko narušenia prevádzky. Navrhujeme model reportingu pre technickú aj manažérsku úroveň. Výstupom je návrh kontrolného zoznamu krokov, ktorý pomáha splniť požiadavky na plánovanie, evidenciu a nápravu zraniteľností v súlade s požiadavkami regulácie a zároveň umožňuje merať zvyšovanie odolnosti pomocou ukazovateľov.

Kľúčové slová: kybernetická bezpečnosť, odolnosť, kritická infraštruktúra, riadenie zraniteľností, skenovanie zraniteľností, OPENVAS.

1 Úvod

Kybernetická bezpečnosť patrí medzi najdôležitejšie výzvy súčasnosti. Rastúca frekvencia a sofistikovanosť útokov spôsobuje, že aj krátkodobý výpadok informačných systémov môže mať významné dopady na dostupnosť služieb, ochranu majetku či dôveru verejnosti. Z praktického hľadiska sa veľká časť incidentov opiera o zneužitie známych zraniteľností, ktoré organizácia neidentifikovala alebo neodstránila včas. Kybernetická bezpečnosť je zároveň kľúčovým pilierom ochrany kritickej infraštruktúry. V odvetviach ako energetika, doprava, zdravotníctvo a ďalšie regulované sektory môže aj relatívne krátky výpadok IT či OT spôsobiť rozsiahle obmedzenia poskytovania základných služieb, ohrozenie bezpečnosti obyvateľov či vážne ekonomické škody. Dopady sú ešte výraznejšie v dôsledku prepojenia IT a OT prostredí, ktoré zvyšuje celkovú zraniteľnosť systémov. Súčasne rastie aj požiadavka na nepretržitú prevádzku, čo kladie na organizácie vyšší tlak zabezpečiť odolnosť a rýchlu obnovu kritických služieb.

Na tieto rastúce riziká reaguje aj regulačný rámec Európskej únie.

Európska smernica o bezpečnosti sietí a informácií (známa ako NIS2) [7] rozširuje rozsah regulovaných sektorov a zároveň presúva dôraz z formálneho plnenia požiadaviek na systematické riadenie kybernetických rizík a zvyšovanie odolnosti organizácií a ich kritických služieb. Cieľom je, aby organizácie aktívne identifikovali a riadili riziká vyplývajúce z prevádzky IT a OT a tak dokázali účinne predchádzať kybernetickým incidentom alebo minimalizovali ich dopady.

V podmienkach Slovenskej republiky sa uvedené požiadavky premietajú do legislatívneho rámca v oblasti kybernetickej bezpečnosti. Osobitnú pozornosť táto právna úprava venuje aj riadeniu technických zraniteľností ako významného prvku riadenia rizík. Požiadavky na identifikáciu, analýzu a ich riadenie sú zakotvené najmä v zákonnej úprave o kybernetickej bezpečnosti [8] a v súvisiacej vykonávacej vyhláške [9], ktorá bližšie špecifikuje bezpečnostné opatrenia pre IT aj OT.

Pravidelné skenovanie zraniteľností je v tomto kontexte základným technicko-organizačným mechanizmom, ktorý podporuje včasnú detekciu slabých miest, prioritizáciu nápravy a spätné meranie účinnosti prijatých opatrení. Ako uvádza Railkar, nástroje na skenovanie zraniteľností umožňujú organizáciám identifikovať bezpečnostné zraniteľností v systémoch ešte pred tým, než budú zneužité útočníkom, čím podporujú prevenciu útokov a zvyšujú bezpečnosť siete [1]. Výskum v oblasti vulnerability managementu a penetračného testovania naznačuje, že systematická identifikácia a prioritizácia zraniteľností významne prispieva k znižovaniu pravdepodobnosti bezpečnostných incidentov a k posilňovaniu kybernetickej odolnosti organizácií [2].

Význam vulnerability assessmentu a nástrojov na skenovanie zraniteľností zdôrazňujú aj štúdie [3] zamerané na využitie nástrojov ako OpenVAS, ktoré ukazujú, že systematické skenovanie umožňuje identifikovať bezpečnostné zraniteľnosti v IT infraštruktúre a poskytuje podklady pre návrh účinných bezpečnostných opatrení.

Cieľom príspevku je zhrnúť legislatívne požiadavky na skenovanie zraniteľností vo vzťahu k odolnosti a ochrane kritickej infraštruktúry, navrhnúť nákladovo efektívny postup implementácie pomocou open-source riešenia OPENVAS Community Edition a odporučiť procesné kroky, ktoré zabezpečia dlhodobú udržateľnosť riadenia zraniteľností.

2 Odolnosť a riadenie zraniteľností v kontexte kritickej infraštruktúry

Odolnosť v kybernetickej bezpečnosti možno chápať ako schopnosť organizácie predchádzať incidentom, odolať útokom, adaptovať sa na zmeny hrozieb a rýchlo obnoviť kľúčové funkcie. Podľa National Institute of Standards and Technology (NIST) je kybernetická odolnosť definovaná ako schopnosť „predvídať, odolať, zotaviť sa a prispôsobiť sa nepriaznivým podmienkam, stresu alebo útokom na kybernetické zdroje“, čo zdôrazňuje prepojenie medzi prevenciou, reakciou a obnovou systémov [4]. Podľa normy ISO/IEC 27032 [5] sa pojem kybernetická odolnosť (cyber resilience) chápe v kontexte schopnosti organizácie udržať bezpečné fungovanie svojich informačných systémov aj pri výskyte incidentov alebo útokov. Norma vychádza z princípov riadenia rizík a ochrany informačných aktív a zdôrazňuje potrebu kombinácie preventívnych, detekčných, reakčných a obnovovacích opatrení.

Pre prevádzkovateľov kritickej infraštruktúry je odolnosť úzko prepojená s dostupnosťou, integritou a dôvernosťou informácií, ako aj s bezpečnou a spoľahlivou prevádzkou technologických procesov. Riadenie zraniteľností predstavuje jeden zo základných pilierov tejto odolnosti, pretože umožňuje systematicky identifikovať technické zraniteľnosti, posudzovať riziká spojené s ich zneužitím a plánovať primerané nápravné opatrenia.

V prostredí OT, napríklad v systémoch SCADA alebo v priemyselných riadiacich systémoch, sa riadenie zraniteľností často dostáva do konfliktu s požiadavkou na nepretržitú prevádzku technologických procesov, keďže bezpečnostné opatrenia musia byť implementované tak, aby neohrozili ich dostupnosť a spoľahlivosť [6]. Z tohto dôvodu je riadenie zraniteľností v týchto systémoch založené na kombinácii technických a organizačných opatrení. Medzi kľúčové technické opatrenia patrí najmä segmentácia siete, ktorá umožňuje oddeliť kritické systémy od menej dôležitých častí infraštruktúry a obmedziť laterálny pohyb útočníka. Ďalším dôležitým prvkom je napríklad aplikácia politiky povolených položiek (application whitelisting), pri ktorej sú povolené len vopred definované, dôveryhodné a kontrolované aplikácia či procesy, čím sa minimalizuje riziko spustenia škodlivého kódu.

V praxi však technické opatrenia často nestačia. Niektoré komponenty nie je možné jednoducho odstaviť alebo aktualizovať, najmä v OT prostredí, kde by aj krátkodobá nedostupnosť mohla ohroziť kontinuitu prevádzky. Z tohto dôvodu je nevyhnutné doplniť technické oparenia o procesné mechanizmy riadenia. Patria sem najmä procesy riadenia zmien či plánovania časových slotov na údržbu.

Dôležitým prvkom efektívneho riadenia zraniteľností je aj inteligentná prioritizácia nápravných opatrení. Pri určovaní priorít je možné využívať skórovacie metriky , ako napríklad Common Vulnerability Scoring System (CVSS), ktorý hodnotí závažnosť zraniteľnosti na základe technických parametrov, ako je vektor útoku, požadovaná úroveň oprávnení, dopad na dôvernosť, integritu a dostupnosť či komplexnosť útoku. Na tento technický pohľad nadväzuje Exploit Prediction Scoring System (EPSS), ktorý rozširuje hodnotenie CVSS o dimenziu pravdepodobnosti reálneho zneužitia v blízkej budúcnosti na základe dát z exploit kitov, trendov v aktivite útočníkov a historických vzorcov. Kombinácia týchto metrík umožňuje organizáciám sústrediť obmedzené kapacity na zraniteľnosti, ktoré predstavujú najvyššie reálne riziko pre kontinuitu prevádzky. Z tohto dôvodu musí byť riadenie zraniteľností v týchto systémoch založené na kombinácii technických a organizačných opatrení, ktoré zohľadňujú špecifické požiadavky na bezpečnosť a kontinuitu prevádzky.

3 Legislatívny rámec: požiadavky na skenovanie zraniteľností na Slovensku

Smernica EÚ o bezpečnosti sietí a informácií (NIS2) [7] zavádza povinnosť riadiť riziká kybernetickej bezpečnosti a požaduje opatrenia na predchádzanie incidentom a minimalizáciu ich dopadov. V podmienkach Slovenskej republiky je rámec povinností upravený národnou právnou úpravou v oblasti kybernetickej bezpečnosti [8], ktorá po poslednej novelizácii rozširuje okruh regulovaných subjektov a kladie dôraz na riadenie rizík, vrátane identifikácie a odstraňovania zraniteľností. Vykonávacia vyhláška Národného bezpečnostného úradu [9] následne špecifikuje štruktúru bezpečnostných opatrení a rozlišuje opatrenia všeobecné, minimálne, rizikové a sektorové; rizikové opatrenia sú priamo naviazané na výsledky analýzy rizík a na priebežné zistenia z monitorovania a skenovania.

Prakticky to znamená, že organizácia musí:

- pravidelne vykonávať skenovanie zraniteľností,
- vyhodnocovať výsledky a stanovovať priority,
- prijímať nápravné opatrenia v primeranom čase a
- celý proces dokumentovať (harmonogram, rozsah, výsledky, zodpovednosti a stav nápravy).

Tieto požiadavky sa týkajú informačných technológií, ale pri mnohých subjektoch aj prevádzkových technológií. Z pohľadu odolnosti je kľúčové, aby bol proces prepojený s riadením rizík a plánovaním kontinuity. Zraniteľnosti, ktoré môžu spôsobiť výpadok kritickej služby, musia mať prednostné riešenie alebo kompenzačné opatrenia.

4 Voľba nástroja: OPENVAS (GVM) ako open-source platforma pre riadenie zraniteľností

Pri výbere nástroja na skenovanie zraniteľností zohrávajú úlohu technické možnosti, licenčné náklady, dostupné kapacity a požiadavka na kontrolu nad dátami. V praxi sú rozšírené komerčné nástroje (napr. Nessus), avšak pre menšie organizácie alebo organizácie s obmedzeným rozpočtom môžu byť licenčné náklady bariérou. OPENVAS Community Edition (predtým Greenbone Community Edition) predstavuje bezplatnú, auditovateľnú a rozšíriteľnú alternatívu, ktorá umožňuje on-premise nasadenie bez závislosti na externých cloudových službách.

OPENVAS je agentless riešenie, čo zjednodušuje nasadenie v heterogénnych prostrediach a v sieťach so segmentáciou, kde je inštalácia agentov komplikovaná. Súčasťou ekosystému je tzv. feed (sada testov zraniteľností – NVT), ktorý sa pravidelne aktualizuje. Platforma podporuje hodnotenie závažnosti pomocou CVSS (vrátane verzie 4.0) a v novších verziách aj integráciu EPSS, čo umožňuje lepšie priorizovať nápravu na základe pravdepodobnosti zneužitia v reálnom svete.

Porovnanie vybraných nástrojov

Tabuľka 1 uvádza orientačné porovnanie vybraných nástrojov pre skenovanie zraniteľností z pohľadu dostupnosti bezplatnej verzie, licencie a orientačných nákladov.

Tabuľka 1. Porovnanie vybraných nástrojov pre skenovanie zraniteľností

Nástroj	Bezplatná verzia	Open-source	Agentless	Orientačná cena licencie*
OPENVAS	Áno	Áno	Áno	2450 € / rok
Nessus	Áno (Obmedzená na maximálne 16 IP)	Nie	Áno	4580 € / rok
Nexpose	Nie (30 dní)	Nie	Áno	6570 € / rok (InsightVM)**

* Pri každom nástroji je uvedená najnižšia dostupná cena licencie k 5. septembru 2025, konkrétne OPENVAS BASIC a Nessus Professional.

** Cena nástroja Nexpose nie je verejne dostupná. Uvedená hodnota vychádza z približnej ceny cloudového riešenia InsightVM pre 250 aktív a naznačuje, že cena Nexpose bude rovnaká alebo vyššia.

5 Implementácia v praxi: postup nasadenia v prostredí s obmedzenými zdrojmi

Nasadenie nástroja naskenovanie zraniteľností má význam len vtedy, ak je súčasťou opakovateľného procesu. V organizáciách s obmedzenými zdrojmi je preto dôležité zvoliť jednoduchý model prevádzky, jasne určiť rozsah skenovania (kritické podsiete, servery, OT segmenty), nastaviť periodicitu a definovať zodpovednosti. Na základe skúseností z implementácie možno odporučiť nasledujúce kroky:

- Príprava prostredia: vyčleniť virtuálny alebo fyzický server (min. 2 vCPU, 4 GB RAM, 20 GB disk) a umiestniť ho do izolovaného segmentu s kontrolovaným prístupom.
- Nasadenie: využiť oficiálny predpripravený obraz (VM) komunitnej edície, ktorý znižuje riziko chýb pri kompilácii a zrýchľuje uvedenie do prevádzky.
- Inicializácia a aktualizácie: zabezpečiť pravidelné aktualizácie feedu (NVT, CVE, CPE) a synchronizáciu času (NTP) pre korektnú koreláciu logov a forenznú analýzu.
- Hardening: zmeniť predvolené heslá, obmedziť prístup k webovému rozhraniu na dôveryhodné IP adresy, vypnúť nepoužívané služby a zaviesť auditný záznam prístupov.

- Konfigurácia skenovania: definovať ciele (IP rozsahy, VLAN), zvoliť vhodné profily skenovania pre IT/OT (v OT preferovať šetrnejšie profily s nižšou invazívnosťou) a naplánovať skenovanie mimo prevádzkových špičiek.
- Spracovanie výsledkov: exportovať reporty (PDF/CSV), zaradiť nálezy do evidencie, priradiť zodpovednosti a termíny nápravy; pri opakovaných falošných pozitívach využiť mechanizmus „override".
- Prioritizácia nápravy: kombinovať CVSS (dopad) a EPSS (pravdepodobnosť zneužitia) a zohľadniť kritickosť aktíva (napr. systém podporujúci kritickú službu) a kompenzačné opatrenia.
- Prepojenie na procesy: začleniť výsledky do riadenia rizík, zmenového riadenia a plánov kontinuity (BCP/DR); nápravy plánovať do časových slotov na údržbu.

Organizačné a procesné aspekty

Technické nasadenie nástroja je iba prvým krokom. Z dlhodobého hľadiska rozhoduje, či organizácia nastaví zrozumiteľné procesy: pravidelnosť skenovania (mesačne/štvrťročne, podľa rizika), workflow pre triedenie a prioritizáciu zraniteľností (kto vyhodnocuje výsledky), spôsob eskalácie kritických zraniteľností a kontrolu uzatvárania nápravných opatrení. Odporúča sa zaviesť minimálne dve úrovne reportingu: detailný technický report pre správcov a manažérsky prehľad (trend, počet kritických zraniteľností, priemerný čas odstránenia). Tým sa zvyšuje odolnosť organizácie, pretože vedenie dostáva merateľné indikátory a môže alokovať zdroje tam, kde sú dopady najvyššie.

6 Diskusia: limity, riziká a odporúčania pre kritickú infraštruktúru

Komunitná edícia OPENVAS poskytuje funkcie postačujúce pre základné riadenie zraniteľností, avšak v rozsiahlych sieťach môže naraziť na výkonnostné limity a vyžaduje viac manuálnej práce (automatizácia reportovania, integrácie so SIEM/ticketing). Pre prevádzkovateľov kritickej infraštruktúry je zásadné bezpečné nastavenie skenovania v OT: agresívne testy môžu spôsobiť nestabilitu starších zariadení, preto treba voliť šetrné profily, testovať v pilotnej fáze a úzko spolupracovať s prevádzkou.

Z pohľadu odolnosti je užitočné doplniť skenovanie o kontext:

- inventarizáciu aktív a klasifikáciu kritickosti,
- mapovanie závislostí (aký systém podporuje akú službu),
- definovanie cieľových časov nápravy podľa rizika (SLA pre zraniteľnosti) a
- overenie účinnosti kompenzačných opatrení.

Skúsenosti ukazujú, že bez jasného vlastníctva procesu (vlastník služby, správca, bezpečnostný manažér) môže skenovanie postupne upadnúť do formálnosti. Preto je potrebné zakotviť proces v interných predpisoch a priradiť zodpovednosti.

7 Záver

Pravidelné skenovanie zraniteľností je kľúčovým prvkom ochrany informácií a budovania kybernetickej odolnosti. V podmienkach slovenskej legislatívy, ktorá implementuje požiadavky smernice EÚ o bezpečnosti sietí a informácií (NIS2) [7], ide zároveň o povinnosť regulovaných subjektov, vrátane tých, ktoré prevádzkujú prvky kritickej infraštruktúry, prípadne kombinujú IT a OT prostredia. Ukázali sme si, že aj v prostredí obmedzených zdrojov je možné zaviesť účinné riadenie zraniteľností pomocou open-source riešenia ako napríklad OPENVAS

Community Edition, ak je technické nasadenie podporené procesmi pre plánovanie skenovania, vyhodnocovanie výsledkov, prioritizáciu nápravy a dokumentovanie.

Za prínos považujeme najmä praktický rámec, ako prepojiť výsledky skenovania s riadením rizík a kontinuitou prevádzky. Pre budúci výskum je vhodné zamerať sa na špecifiká OT skenovania, na kombinovanie metriky CVSS s dynamickými pravdepodobnostnými metrikami (EPSS a prípadne LEV) a na automatizáciu workflowu nápravy v prostredí verejnej správy a kritickej infraštruktúry.

Poďakovanie

Financované Európskou úniou NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu č. 17R05-04-V01-00005.

Referencie

[1] Railkar, Dipali, "A Study on Vulnerability Scanning Tools for Network Security," International Journal of Scientific Research in Computer Science Engineering and Information Technology, 2022, DOI: 10.32628/CSEITCN228641

[2] Egbedion, G. E., "Impact of vulnerability management and penetration testing on security-informed IT project planning and implementation" Journal of Multidisciplinary Engineering Science and Technology (JMEST), vol. 11, no. 4, 2024, [Online]. Dostupné: https://www.jmest.org/wp-content/uploads/JMESTN42354380.pdf

[3] Saktiansyah, A., Muharrom, M., "Analysis of Vulnerability Assessment Technique Implementation on Network Using OpenVAS," International Journal of Engineering and Computer Science Applications, vol. 2, no. 2, pp. 51–58, 2023, [Online]. Dostupné: https://www.researchgate.net/publication/374300263_Analysis_of_Vulnerability_Assessment_Technique_Implementation_on_Network_Using_OpenVas

[4] National Institute of Standards and Technology, "NIST SP 800-160 Vol. 2: Developing Cyber-Resilient Systems," NIST, 2018, [Online]. Dostupné: https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final

[5] International Organization for Standardization, "ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity," ISO, 2012

[6] Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., Hahn, A., "Guide to Industrial Control Systems (ICS) Security (NIST Special Publication 800-82 Rev. 2)," National Institute of Standards and Technology, 2015, [Online]. Dostupné: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

[7] European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)," Official Journal of the European Union, L 333, 27 December 2022, pp. 80–152, [Online]. Dostupné: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

[8] Slovenská republika, „Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov," Zbierka zákonov Slovenskej republiky, 2018, [Online]. Dostupné: https://static.slov-lex.sk/static/SK/ZZ/2018/69/20250101.html

[9] Národný bezpečnostný úrad, „Vyhláška Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach," Zbierka zákonov Slovenskej republiky, 2025, [Online]. Dostupné: https://static.slov-lex.sk/static/SK/ZZ/2025/227/vyhlasene_znenie.html

Plošné bezpečnostní vzdělávání prostřednictvím technologie Text to speech

Tereza Mičulková[1], Martin Hromada[2], Dora Kotková[3], Lukáš Kotek[4]

[1] Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky,
Nad Stráněmi 4511, 760 05 Zlín, miculkova@utb.cz

[2] Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky,
Nad Stráněmi 4511, 760 05 Zlín, hromada@utb.cz

[3] Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky,
Nad Stráněmi 4511, 760 05 Zlín, kotkova@utb.cz

[4] Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky,
Nad Stráněmi 4511, 760 05 Zlín, kotek@utb.cz

Abstrakt:

Tento příspěvek se zaměřuje na problematiku plošného vzdělávání osob v oblasti fyzické bezpečnosti představující téma, jímž by měla být pravidelně školena ideálně každá osoba v dané organizaci. Vzdělávání v této oblasti je zásadní nejen z hlediska posilování celkové odolnosti organizace prostřednictvím zvyšování bezpečnostního povědomí jejích členů, ale především proto, že přispívá k ochraně samotných jednotlivců. Článek tak reaguje na potřebu nalézt efektivní způsob, jak proškolit co největší počet osob. Současně nabízí možné řešení problémů spojených s realizací běžného vzdělávání většího rozsahu, a to prostřednictvím využití technologie *Text to speech*. Součástí je také rešerše poskytovatelů této technologie, která rozebírá dostupné možnosti s ohledem na stanovení kritérií relevantní pro jejich výběr. Následně jsou vybrány tři konkrétní služby poskytující tuto technologii, které jsou mezi sebou porovnány a na základě vybraných preferencí důležitých pro tvorbu vzdělávacích materiálů je poté vybrána nejvhodnější varianta. Pozornost je věnována také navazující fázi, tedy samotnému procesu tvorby vzdělávacích materiálů, s důrazem na faktory, jež mohou hrát klíčovou roli z hlediska dosažení požadované kvality výsledného výstupu. Ačkoli se pořízení služby využívající tuto technologii nemusí na první pohled jevit jako finančně nejlevnější řešení, v konečném důsledku však může díky celé řadě výhod přinést významnou úsporu času i finančních prostředků a zároveň tak zvýšit dostupnost a efektivitu vzdělávání.

Klíčová slova: bezpečnost, vzdělávání, vzdělávací materiály, umělá inteligence, text to speech.

1 Úvod

Téma bezpečnosti je velice důležité a nemělo by být podceňováno, neboť ani ty nejmodernější bezpečnostní technologie nedokážou samy o sobě potenciální rizika plně eliminovat. A právě lidský faktor může sehrát klíčovou roli co se týče adekvátní reakce na vzniklou situaci. K tomu je však nezbytné poskytnout vzdělávání předávající potřebné znalosti, dovednosti a schopnosti, a to ideálně v co největším počtu proškolených osob napříč organizací. Takovýmto vzděláváním by měl projít každý člen organizace.

Ačkoli je pro dosažení maximální efektivity vzdělávání potřeba vytvořit komplexně promyšlenou strukturu nejrůznějších prvků, tento článek se bude zaměřovat pouze na určitou část dané problematiky. Autorka se přitom v rámci svého výzkumu zaměřuje především na vzdělávání v prostředí univerzit. Článek tak nejprve představí jednotlivé způsoby umožňující realizaci plošného vzdělávání, včetně jejich výhod a limitů, a nabídne možná řešení reagující na zmíněná negativa i kladené požadavky. Následně se zaměří na proces související s výběrem

dostupných možností zahrnující stanovení kritérií a vzájemné porovnání vybraných možností. Pozornost bude věnována také procesu samotné tvorby vzdělávacích materiálů s využitím daného nástroje, včetně upozornění na faktory, které mohou významně ovlivnit kvalitu výsledného výstupu, a je proto nezbytné jim při tvorbě věnovat náležitou pozornost.

2 Způsoby plošného vzdělávání

Mezi základní způsoby realizace plošného vzdělávání patří tradiční prezenční školení vedené lektorem nebo jeho online alternativa ve formě webináře. Proškolit tímto způsobem všechny osoby však může být značně komplikované, obzvlášť pokud se jedná o prostředí s větším počtem osob rozmístěných na více pracovištích. Typickým příkladem mohou být univerzity disponující několika objekty jako jsou jednotlivé fakulty, výzkumná centra a podobně. Navíc cílovou skupinou vzdělávání v oblasti bezpečnosti nejsou pouze zaměstnanci, ale také i jednotliví studenti, čímž se celkový počet požadovaných proškolených osob výrazně zvyšuje. Klasické prezenční školení tak může být problémové jak z časového hlediska školitele i účastníků, tak i z kapacitního omezení prostor, ve kterých by dané školení probíhalo. Online webinář se může jevit jako flexibilnější alternativa, jelikož umožňuje připojení odkudkoli a eliminuje problém s fyzickou kapacitou místnosti, avšak i to má svá úskalí nejen v podobě časového hlediska či technických komplikací jako například problémy s internetovým připojením, ale zároveň dochází k oslabení přímé interakce mezi lektorem a publikem. Vhodným řešením se může zdát také vytvoření nahrávky takového to školení, ale to s sebou přináší nároky na postprodukci, zejména v případě jakýchkoli úprav, ať už chyb či aktualit. Na výklad jakéhokoli člověka totiž neustále působí nejrůznější fyziologické a psychologické faktory (např. únava, slovní vata, zdravotní stav), které mohou velmi negativně ovlivnit konečnou kvalitu výstupu. Alternativou může být také samostudium prostřednictvím zveřejněných PDF dokumentů, lze však předpokládat, že bez další motivační či kontrolní složky si tyto materiály skutečně prostuduje pouze minimální počet osob. Každá z uvedených variant má tak své výhody i limity, a proto neexistuje pouze jedno řešení, které by se dalo považovat za ideální. [1, 2]

Z těchto důvodů se jeví jako ideální kombinace každé varianty. Avšak i to s sebou přináší spoustu úskalí. Existuje však řešení, které, i když také není zcela dokonalé, splňuje většinu potřebných kritérií. Jedná se o využití technologií umělé inteligence (AI), a to konkrétně technologie *Text to speech* (TTS). Tato technologie využívající strojové učení a neuronové sítě umožňuje z předem zadaného textu generovat audio nahrávky syntetické řeči. [3] Výsledná řeč však působí přirozeně, plynule a při vhodném výběru služby může být dokonce až k nerozeznání od lidského projevu – ovšem je potřeba dbát na několik důležitých faktorů, jež jsou dále popsány v kapitole 4. Díky této technologii odpadá mnoho problémů spojených jak tradičním prezenčním vzděláváním, tak s online variantou. Lze tak připravit vzdělávací materiály, které mohou být využitelné v rámci nejrůznějších variant. Toho je možno docílit pomocí dvou verzí různých vzdělávacích prezentací – plné verze a zkrácené verze. [1, 2]

V tabulce 1 lze vidět přehledné srovnání jednotlivých možností, z něhož jakožto nejlepší varianta vyplývá video prezentace vytvořená pomocí AI společně s PDF dokumentem. Přičemž obě tyto varianty vycházejí ze zmíněných dvou verzí vzdělávacích prezentací – video prezentace vycházející ze zkrácené verze prezentace a PDF dokument vycházející z plné verze prezentace.

Tabulka 1. Srovnání jednotlivých možnosti vzdělávání [1, 2, 4]

	Prezenční školení	**Online webinář**	**Videonahrávka vytvořená skutečným člověkem**	**PDF dokument**	**Video prezentace vytvořená AI**
Kapacitní omezení prostor	✓	✗	✗	✗	✗
Časová náročnost vzhledem k účastníkům nebo lektora	✓	✓	✓, ✗	✗	✗
Náročná postprodukce v případě úprav	–	–	✓	✗	✗
Technické problémy	✓	✓	✓	✗	✗
Celková cenová náročnost	✓	✗	✓	✗	✗
Jedna varianta využití	✓	✓	✓	✓	✗

Plná verze obsahuje úplný soubor informací formulovaných v celých srozumitelných větách, bez nutnosti dalšího dodatečného výkladu lektora, a je tak vhodná ke samostudiu. Zkrácená verze představuje stejně hodnotný vzdělávací obsah, ovšem ve stručnější podobě obsahující pouze klíčové informace, protože zbytek informací je dále rozveden prostřednictvím mluveného projevu. Přičemž se v této zkrácené verzi nabízejí dvě varianty. První varianta představuje podobu klasického prezenčního školení, kdy je prezentace doprovázena výkladem samotného lektora. Druhá varianta však představuje řešení bez nutnosti zapojení skutečného lektora (či profesionálního dabéra), a to pomocí propojení této prezentace s audio nahrávkou syntetického hlasu, čímž vzniká vzdělávací video prezentace. Takto připravené videoškolení pak mohou osoby určené ke vzdělání absolvovat v jakýkoliv čas a na jakémkoliv místě, pokud jsou umístěny na vhodném online úložišti. Největší předností této technologie je, že oproti člověka zajišťuje konzistentní kvalitu řeči. Každý výstup zachovává stejné parametry hlasu jako je zabarvení, intonace či hlasitost (pokud tedy nejsou parametry záměrně upravovány), a tak záleží pouze na samotném obsahu, nikoli na vstupující negativní faktory člověka. Díky tomu je také snadné s materiály pracovat v případě budoucích úprav, a to kdykoli a odkudkoli. To vše vede k výraznému snížení celkových nákladů i časové náročnosti ve srovnání s využitím skutečného lidského lektora. [1, 2, 4]

Pro dosažení maximálně efektivního výsledku je však potřeba zahrnout i další prvky, jako jsou různé kurzy, praktické nácviky apod, a všechny je propojit do vhodně vytvořené struktury obohacené o marketingové prvky. Celá struktura by pak měla být zasazená do vhodně stanoveného harmonogramu, který umožní vést vzdělávací proces účinně i v dlouhodobějším měřítku. [1] Tento článek se však dále zaměřuje pouze na problematiku spojenou s využíváním technologie *Text to speech*.

3 Rešerše dostupných možností

Pro realizaci varianty plošného vzdělávání zaměstnanců jako bylo popsáno v předchozí kapitole 2, je potřeba zvolit vhodný nástroj. Na trhu existuje velké množství služeb poskytující tuto technologii využívající umělé inteligence, proto je potřeba nejprve stanovit kritéria, podle kterých bude následně možné vybrat nejvhodnější variantu. Ovšem je nutné podotknout, že parametrově nejlépe hodnocená varianta nemusí být vždy ta nejvhodnější, záleží totiž i na konkrétním účelu použití. To znamená, že například při generování hlasu pro účely vyprávění, je potřeba mít výrazné ale příjemné zabarvení hlasu s emocionální dynamikou. Naopak pro účely vzdělávání

je lepší se příliš výraznému zabarvení vyhnout a zvolit radši hlas s jasnou artikulací, neutrálním emocionálním projevem a středním tempem, aby byl posluchač schopný se naplno soustředit co nejdéle.

3.1 Stanovení kritérií

Důležitým kritériem při výběru vhodného hlasu není pouze počet druhů hlasu, ale také jeho rozmanitost. To zahrnuje nejen rozlišení mezi mužským a ženským hlasem, ale i zastoupení různých věkových kategorií, od dětských hlasů po hlasy starších osob, dále různé akcenty a podobně. S tím úzce souvisí i tón a zabarvení hlasu, tedy jakýsi charakter daného hlasu, který je vhodný pro konkrétní účel. Jiné zabarvení se hodí pro vyprávění příběhů, jiné pro komentování hraní her a jiné pro vzdělávání. Kromě toho je však důležitá i dynamika a intonace, tedy vhodné stoupání a klesání hlasu, důraz na určitá slova a také celkový styl projevu, který vyjadřuje způsob, jakým se daný hlas projevuje – jak je schopen vyjádřit emoce, jaký má rytmus, tempo a jak pracuje s pauzami. Všechny tyto prvky dodávají generovanému hlasu určitou přirozenost a plynulost. Stejně důležitá je však i srozumitelnost a konzistentnost hlasu během celého výstupu. Celková kvalita výsledného hlasu tak závisí na souhře několika různých faktorů.

Možnost dodatečné úpravy hlasu, tedy možnost si daný hlas dále přizpůsobit podle svých preferencí, jako je rychlost mluveného slova, výška hlasu, styly přizpůsobující daný hlas konkrétním účelům či zvýšení větší emoční intenzity, může být dalším relevantním kritériem.

V případě práce s více jazyky je vhodné věnovat pozornost také na nabízenému počtu podporovaných jazyků. Ovšem to, že daná služba podporuje určitý jazyk, ještě automaticky nezaručuje, že generovaný výstup bude na kvalitní úrovni.

Důležitou roli při stanovování kritérií pro výběr služeb hraje bezpochyby také cena. Ačkoli mohou existovat služby zcela zdarma, může tím být následně velice ovlivněna konečná kvalita a dostupnost dalších funkcí či nástrojů pro úpravy. Pro běžného uživatele s menším účelem využití této technologie však může být bezplatná zkušební verze dostatečná, obvykle však bývá značně omezená. U větších projektů se bezplatná varianta ukazuje jako nedostačující a vzniká potřeba zakoupit některý z placených tarifů. Ty mohou být nastaveny na bázi měsíčního nebo ročního poplatku, případně individuálně přizpůsobeny po dohodě s poskytovatelem služby. Cena tarifu bývá obvykle stanovená za počet kreditů spotřebovaných na převod textu na řeč anebo za určitý počet minut vytvořené audio nahrávky. Při výběru lze rovněž zohlednit bonusy v podobě dalších kreditů navíc – některé služby totiž tyto bonusy přidávají jednorázově k platbě anebo se denně přičítají k celkovému počtu kreditů. Aby byl zvolený tarif optimální, je vhodné předběžně odhadnout, kolik kreditů či minut bude pro daný projekt potřeba. Zároveň je nutné počítat s tím, že výsledky nemusí být napoprvé perfektní a mohou vyžadovat úpravy, proto je vhodné mít určitou rezervu navíc.

Pro práci s generovanými audio výstupy je nezbytné, aby daná služba umožňovala jejich stažení. Nejedná se totiž o funkci, kterou by automaticky poskytoval každý poskytovatel služby, některé umožňují generování hlasu pouze v podobě přečtení bez možnosti exportu pro další použití mimo danou službu.

Možným kritériem může být také druh platforem, prostřednictvím kterých je služba poskytována, a to ať už se jedná o webové rozhraní, mobilní či desktopovou aplikaci, rozšíření pro internetový prohlížeč či API rozhraní. S tím může souviset i jednoduchost ovládání, možnosti automatizace, kompatibilita s dalšími nástroji a podobně.

Důležitý je rovněž celkový výkon a stabilita služby, zahrnující například rychlost generování audio výstupů či limity počtu znaků při zadávání dlouhých textových vstupů.

Kromě technických parametrů však nejzásadnějším kritériem zůstává kvalita generovaného hlasu. Ta se ověřuje prostřednictvím vhodně navržené testovací věty, která umožní zkontrolovat správnost výslovnosti, schopnost projevu emocí, ideální rytmus a další parametry. Takovouto větu pak lze vyzkoušet u všech vybraných služeb a následně výsledky mezi sebou porovnat, což umožní odhalit rozdíly ve výstupech a vybrat nejvhodnější řešení.

3.2 Srovnání vybraných služeb

Ačkoli existuje nespočet nástrojů pro převod textu na řeč, například *Fish Audio*, *Speechify, Speaktor*, *ElevenLabs*, *Dazbog.ai*, *NaturalReader*, *Balabolka* a další, ne všechny umožňují generovat hlas v českém jazyce. A i pokud češtinu podporují, mnohé služby mají problém vytvořit výstup, který by zněl opravdu přirozeně a ne „roboticky“. Proto je vhodné po stanovení kritérii vybrat několik slibných služeb a na základě jejich vzájemného srovnání a určených preferencí vybrat nejvhodnější řešení. Pro účely tohoto srovnání byly vybrány následující tři služby: *Speechify* z důvodu, že se jedná o jednu z nejznámějších služeb poskytující převod textu na řeč, *Dazbog.ai* jelikož se jedná o službu vzniklou v České republice a *Google Translate TTS*, protože se jedná o jeden z nejpoužívanějších nástrojů pro překládání textů na světě, který však mimo jiné umožňuje právě i převod textu na řeč. [5, 6, 7]

Speechify patří mezi nejpopulárnější služby pro generování hlasu díky široké nabídky různých hlasů, včetně klonů hlasů celebrit a rozsáhlé jazykové podpoře. U některých jazyků však může být kvalita syntetické řeči nižší a konečný výstup tak nemusí znít zcela přirozeně. Výhodou je příznivá cena ve srovnání s konkurencí, což z něj činí oblíbenou volbu mezi běžnými uživateli. [5]

Dazbog.ai, jakožto služba pocházející z České republiky, klade zvláštní důraz na kvalitu českého jazyka, takže je konečný výstup v kvalitní podobě a syntetický hlas zní velmi přirozeně. Mimo jiné tato služba nenabízí pouze převod textu na řeč, ale i mnoho dalších nástrojů využívající technologií umělé inteligence pro nejrůznější práci s obrazem, videem či textem. Poskytuje tak spoustu nejrůznějších funkcí se všemi formáty v rámci jednoho tarifu, což ji činí vhodnou i pro větší projekty. [6]

Google Translate TTS umožňuje kromě překladu textu z jednoho jazyka do druhého, také i převod textu do mluveného projevu. Jedná se však o základní úroveň technologie *Text to speech* nepodporující žádná pokročilá nastavení, takže kvalita výstupu může být na nižší úrovni. Kromě toho tato funkce není podporována pro všechny dostupné jazyky a v podporovaných jazycích je k dispozici pouze jeden typ hlasu. Nabízí však úpravu rychlosti řeči a je zcela zdarma. [7]

V Tabulce 2 lze vidět porovnání jednotlivých parametrů těchto tří vybraných služeb.

Tabulka 2. Srovnání vybraných služeb [5–7]

	Speechify	**Dazbog.ai**	**Google Translate TTS**
Kvalita hlasů	Vysoká, ale občas robotická čeština	Vysoká, přirozená	Nízká, robotická
Počet hlasů	1000+	17	1
Počet jazyků hlasového výstupu	60+	2 (CZ/EN)	~70+
Emoce a styly	✓	✓	✗
Platformy	Webové rozhraní, mobilní a desktopová aplikace, rozšíření ve webovém prohlížeči	Webové rozhraní, mobilní aplikace	Webové rozhraní, mobilní aplikace
Přizpůsobení rychlosti	✓	✗	✓
Možnost stažení	✓	✓	✗
Cena	Dle typu tarifu a dle měsíční/roční platby, mírně levnější	Dle typu tarifu a dle měsíční/ roční platby, mírně dražší	Zdarma
Bonus k danému tarifu	✗	✓ (denní bonus)	✗
Extra funkce	Hlasový asistent, AI podcasty, klonování hlasu, skenování textu	Multimodální využití AI (práce s obrázky, videí, texty a audií)	Překlad do jiného jazyka

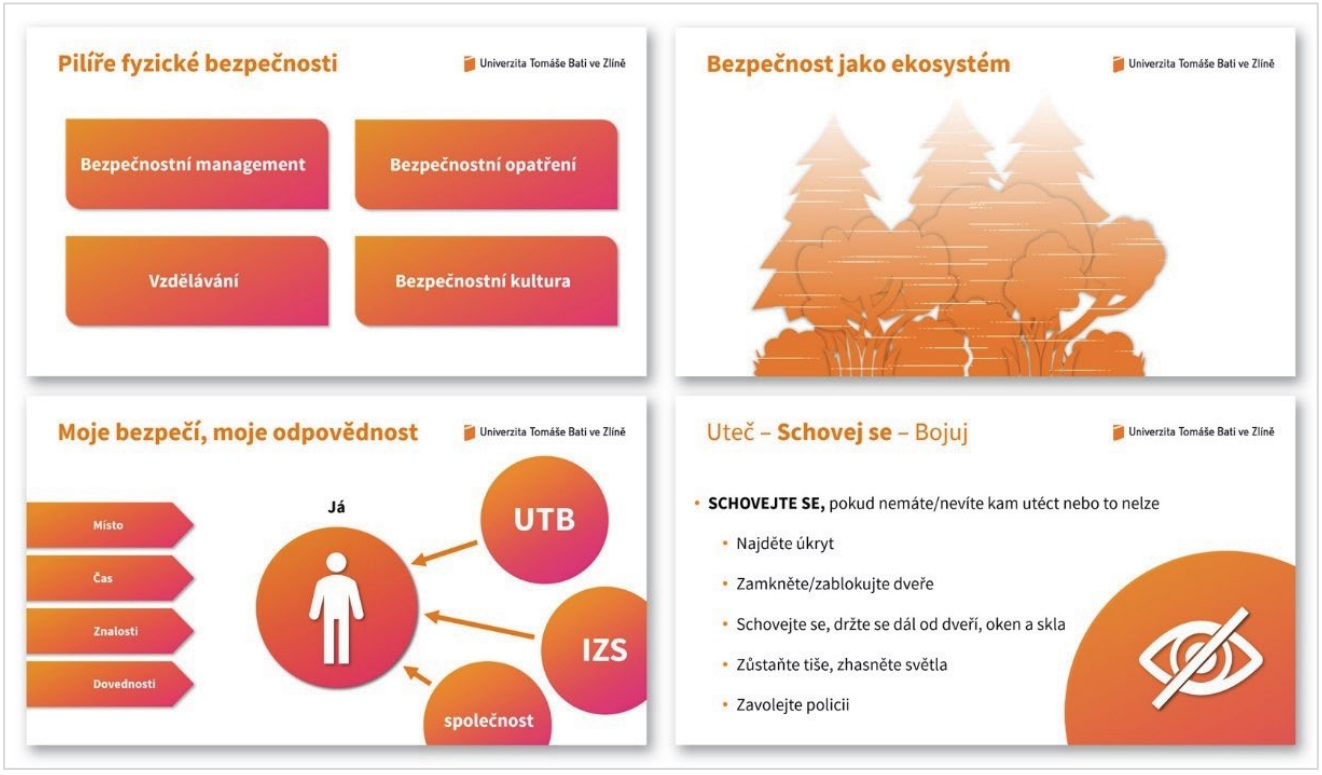
Ze všech porovnávaných kritérií považuji za důležité především kvalitu hlasu, možnost výběru z různých hlasů, schopnost vyjadřování emocí a možnost stažení. Proto pro účely vhodné k vytváření vzdělávacích materiálů v českém jazyce a případnému překladu do anglické verze pokládám službu *Dazbog.ai* za zcela dostačující řešení, které zároveň nabízí příznivý poměr ceny a výkonu. Lze tak tuto službu pro zmíněné účely považovat za ideální variantu.

4 Proces tvorby vzdělávacích materiálů s využitím umělé inteligence

Podle [1, 2] je potřeba v rámci procesu tvorby vzdělávacích materiálů a dosažení kvalitních výsledků při použití technologie *Text to speech* dbát na několik důležitých faktorů, které jsou popsány v následujících odstavcích.

Jak již bylo popsáno v kapitole 2, video prezentace představuje zkrácenou verzi vzdělávací prezentace doprovázenou syntetickým hlasem. Pro její vytvoření je nejprve zapotřebí připravit scénář, podle kterého bude následně vygenerována audio nahrávka. Zde je však potřeba myslet na to, že umělá inteligence převádí text na řeč přesně takovým způsobem, jakým je ve scénáři uveden, což znamená, že je nutné tento text psát foneticky. Tedy aby bylo dosaženo žádaného zvukového výsledku, bude v určitých případech potřeba psát text záměrně s pravopisnými chybami a špatnou gramatikou, diakritikou či interpunkcí. Takovým příkladem může být zkratka názvu *Univerzita Tomáš Bati*. Ačkoli by se tato zkratka správně zapisovala jako *„UTB“*, s ohledem na fonetiku a požadovaný výsledek je nutno ve scénáři toto slovo uvést jako *„útébé“*. S tím úzce souvisí také zachování přirozeného rytmu a intonace mluveného projevu, což lze často ovlivnit vhodným vkládáním pauz. Tohoto efektu je však v některých situacích možno dosáhnout pouze pomocí záměrně špatného umístění interpunkčních znamének.

Obrázek 1. Příklad plné verze vzdělávací prezentace [1]



Obrázek 2. Příklad zkrácené verze vzdělávací prezentace [1]

Po sestavení scénáře následuje výběr vhodného hlasu, zahrnující různé typy zabarvení, tempo apod. Hlas je třeba volit tak, aby školenou osobu dokázal zaujmout a udržel její pozornost ideálně během celé doby výkladu. Proto je v případě vzdělávacích materiálů lepší se tišším, pomalejším a příliš monotónním hlasům zcela vyhnout.

Také je vhodné, aby se zvolený hlas hodil k danému tématu a působil přirozeně v daném kontextu. Tedy například pro školení první pomoci může být vhodnější klidnější ženský hlas, který bývá často spojován s podporou a péči, zatímco pro téma sebeobrany může být lepší důrazný mužský hlas. Udržení pozornosti však souvisí nejen se zvukovou, ale i s vizuální stránkou prezentace. Na názorném příkladu z obrázků 1 a 2 lze vidět rozdíl mezi plnou verzí prezentace obsahující kompletní informace a zkrácenou verzí určenou pro videoškolení s využitím doprovodného synteticky namluveného projevu. Lze si všimnout, že vizuál v tomto případě hraje důležitou roli. To může zahrnovat použití nejrůznějších grafických prvků jako jsou obrázky, ilustrace, efekty a animace, či přechody mezi jednotlivými snímky, které mimo jiné mohou celému vzdělávacímu materiálu dodat navíc i jakousi dynamiku. Kromě toho je však nutné dbát i na celkovou délku této video prezentace. Ta by měla být optimálně v rozsahu okolo 15 až 30 minut, protože delší doba člověku způsobuje výrazný úpadek plné pozornosti a soustředění. Příliš rozsáhlé materiály mohou navíc účastníky od vzdělávání dokonce odrazovat.

Aby opravdu mohlo dojít ke vzdělání ideálně každé osoby v dané organizaci, je potřeba brát ohled i na osoby pocházející ze zahraničí. To vytváří potřebu připravit verzi materiálu také v anglickém jazyce.

V případě nutných oprav či aktualizace informací může být díky aplikování této technologie následná úprava také mnohem flexibilnější, časově rychlejší a celkově jednodušší. Není totiž potřeba nahrávku vytvářet znovu ani v rámci postprodukce složitě upravovat nově změněnou část tak, aby plynule zapadala do zbytku původního obsahu, jak by tomu bylo při nahrávání mluveného projevu skutečného člověka.

5 Závěr

Cílem článku je představit širší veřejnosti možné řešení plošného vzdělávání v oblasti fyzické bezpečnosti s využitím technologie *Text to speech*. Pozornost je přitom zaměřena na rešerši služeb poskytujících tuto technologii, včetně procesu jejich výběru, při němž je na základě komparace vybraných řešení určen vhodný kandidát splňující stanovená kritéria. Článek zároveň upozorňuje na nutnost zohlednění určitých faktorů při tvorbě vzdělávacích materiálů tak, aby bylo dosaženo kvalitního a efektivního výstupu. Implementace této technologie totiž může výrazně zjednodušit a zefektivnit samotný proces vzdělávání.

Reference

[1] MIČULKOVÁ, Tereza. Informační a vzdělávací strategie fyzické bezpečnosti UTB. Diplomová práce. Zlín: Univerzita Tomáše Bati ve Zlíně, 2025

[2] MIČULKOVÁ, Tereza. Systém bezpečnostního vzdělávání s využitím moderních trendů. Online. Krízový manažment. 2025, roč. 24, č. 2. Dostupné z: https://doi.org/https://doi.org/10.26552/krm.C.2025.2.174-180. [cit. 2026-02-21]

[3] What is text to speech? Online. IBM. Dostupné z: https://www.ibm.com/think/topics/text-to-speech. [cit. 2026-02-25]

[4] AI vs voice-overs. Online. Speechify. C2026. Dostupné z: https://speechify.com/blog/ai-vs-voice-overs/. [cit. 2026-02-25]

[5] Speechify: Free Text to Speech Reader | 1M+ 5-Star Reviews. Online. Dostupné z: https://speechify.com/. [cit. 2026-02-22]

[6] Dazbog.ai | Přinášíme umělou inteligenci do Čech. Online. C2026. Dostupné z: https://www.dazbog.ai/. [cit. 2026-02-22]

[7] Překladač Google. Online. Dostupné z: https://translate.google.cz/. [cit. 2026-02-22]

Riziká vyplývajúce z používania pokrokových monitorovacích technológií

Michal Miške[1]

[1] Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva,
Univerzitná 1, 010 26 Žilina, michal.miske@uniza.sk

Abstrakt:

Monitorovanie mostov prešlo v posledných rokoch významnou transformáciou v dôsledku integrácie pokrokových technológií, medzi ktoré patria systémy monitorovania stavu konštrukcií (SHM), senzory internetu vecí (IoT), bezpilotné lietadlá (UAV), umelá inteligencia (AI) a cloud computing. Uvedené technológie umožňujú nepretržité získavanie, prenos a spracovanie údajov v reálnom čase, čím prispievajú k presnejšej diagnostike technického stavu mostných objektov, včasnej detekcii porúch a efektívnejšiemu plánovaniu údržby. Ich využitie zároveň zvyšuje schopnosť správcov infraštruktúry prijímať rozhodnutia na základe aktuálnych a rozsiahlych dátových súborov. Napriek týmto prínosom však implementácia pokrokových monitorovacích systémov prináša aj viaceré nové riziká, ktoré môžu negatívne ovplyvniť bezpečnosť, spoľahlivosť a celkovú efektívnosť monitorovania. Článok sa zameriava na identifikáciu a klasifikáciu hlavných rizík spojených s nasadením moderných systémov monitorovania mostov, pričom osobitná pozornosť je venovaná zraniteľnostiam v oblasti kybernetickej bezpečnosti, spoľahlivosti a odolnosti technických systémov, kvalite a interpretácii získaných údajov, právnym a etickým aspektom ich používania, ako aj otázkam dlhodobej ekonomickej udržateľnosti. Cieľom príspevku je poukázať na potrebu komplexného prístupu k zavádzaniu týchto technológií, ktorý zohľadňuje nielen ich prínosy, ale aj potenciálne riziká a možnosti ich zmierňovania.

Kľúčové slová: monitorovanie mostov, pokrokové technológie, riziko, hodnotenie rizík, infraštruktúra.

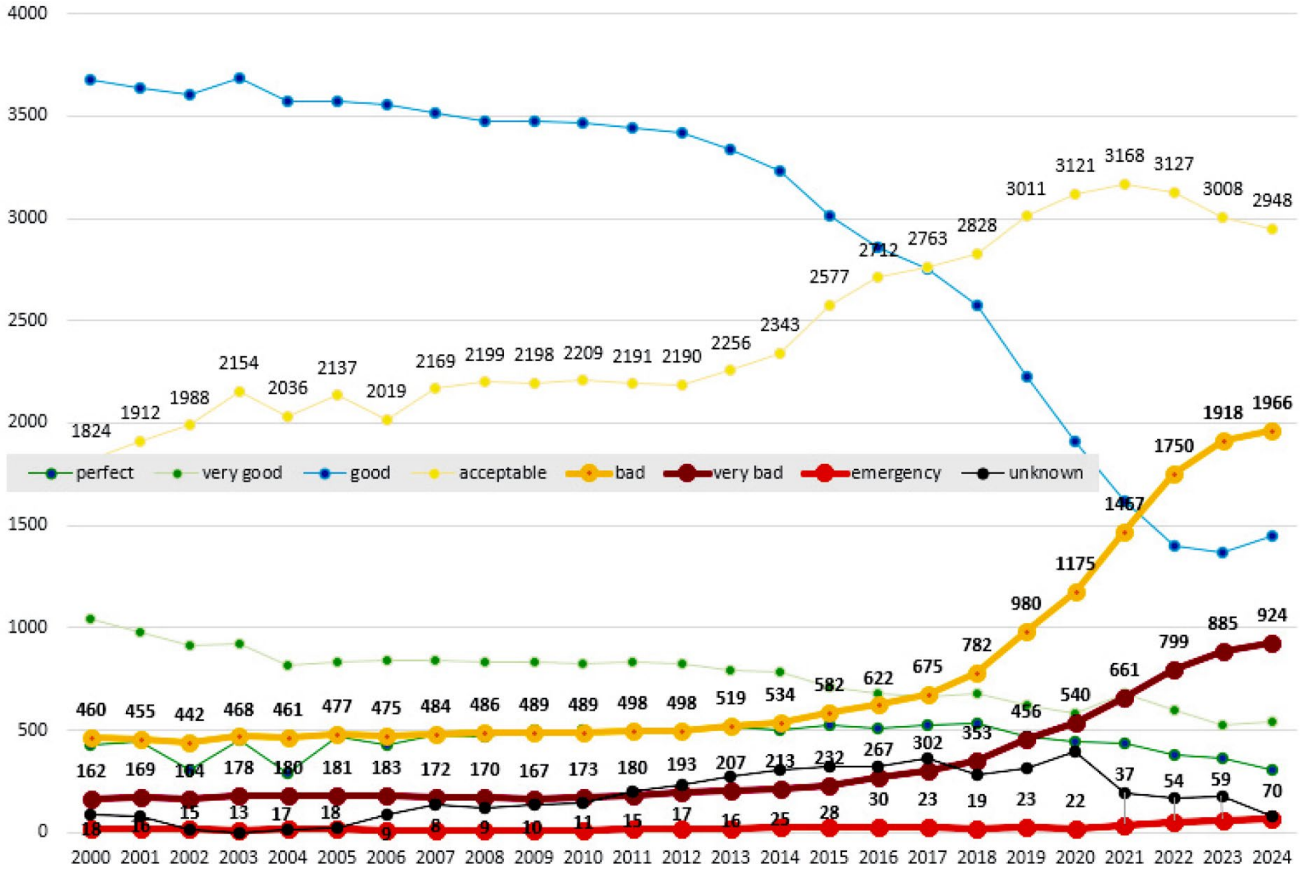
1 Úvod

Starnutie mostov, meniace sa klimatické podmienky a zvyšujúce sa dopravné zaťaženie v súčasnosti vyžadujú zavedenie účinných, spoľahlivých a komplexných systémov na monitorovanie ich konštrukčného a technického stavu. Mnohé mosty boli navrhnuté a postavené v minulom storočí, často podľa dnes už zastaraných noriem, a ich materiálová kapacita, konštrukčný návrh a prevádzkové zaťaženie už nespĺňajú súčasné požiadavky. V dôsledku toho sa ich stav postupne zhoršuje v dôsledku prirodzeného starnutia, vplyvov klímy a intenzívneho používania. V prípade Slovenska túto degradáciu potvrdzujú štatistiky Správy slovenských ciest a národnej databázy ciest, ktoré poukazujú na rastúci počet mostov klasifikovaných ako mosty v zlom, veľmi zlom alebo havarijnom stave, ako je znázornené na Obrázku 1.

Hodnotenie stavu sa tradične vo veľkej miere spolieha na pravidelné vizuálne kontroly a odborné posúdenie, ktoré sa vykonáva raz za 4 roky. To často vedie k subjektivite, nezrovnalostiam medzi inšpektormi a obmedzenej porovnateľnosti v čase. Okrem toho absencia nepretržitého monitorovania mnohých infraštruktúrnych objektov znižuje schopnosť zistiť poškodenia alebo poruchy v ranom štádiu (napr. mikrotrhliny, skrytá korózia, poškodenie únavou) teda skôr, ako sa stanú kritickými. V dôsledku toho sa rozhodnutia o údržbe prijímajú prevažne reaktívne, až keď sa poruchy prejavia, a nie proaktívne, resp. preventívne, na základe objektívnych ukazovateľov stavu. Ďalším zhoršujúcim faktorom je oneskorené prideľovanie finančných prostriedkov na obnovu a renováciu, čo môže viesť k odkladaniu zásahov, hromadeniu nevykonaných údržbových prác a postupnému prechodu mostov

do horšieho stavebnotechnického stavu. Nedostatočné pokrytie monitorovania, subjektívne rozhodovanie a oneskorené alebo nedostatočné financovanie spoločne prispievajú k urýchlenému zhoršovaniu stavu a zvýšeným bezpečnostným a prevádzkovým rizikám v rámci slovenskej mostnej infraštruktúry [1].

Tradičné diagnostické metódy, najmä vizuálna kontrola vykonávaná pracovníkmi v teréne, zostávajú dôležité, ale čoraz častejšie narážajú na svoje obmedzenia. Medzi obmedzenia patria časové a personálne nároky, subjektívnosť pri hodnotení a najmä obmedzená schopnosť včas odhaliť skryté defekty, ako sú mikrotrhliny, vnútorná korózia alebo poškodenie únavou [2–4].



Obrázok 1. Stavebnotechnický stav Slovenských mostov

V tejto súvislosti sa moderné technológie stávajú kľúčovými, efektívne dopĺňajúcimi alebo automatizujúcimi nástrojmi pre konkrétne fázy monitorovania mostov. Patria sem napríklad senzorové systémy na monitorovanie stavu konštrukcie (Structural Health Monitoring – SHM), ktoré zabezpečujú nepretržité meranie kľúčových fyzikálnych parametrov konštrukcie (napr. napätie, vibrácie, teplota, vlhkosť), drony (Unmanned Aerial Vehicles – UAV) s vysokým rozlíšením používané na vizuálnu kontrolu ťažko dostupných častí konštrukcie alebo umelá inteligencia (Artificial Intelligence – AI), ktorá dokáže spracovať veľké objemy údajov a automaticky identifikovať chyby [5, 6]. Tieto technológie poskytujú správcom infraštruktúry okamžité a objektívne informácie o aktuálnom technickom stave mosta. Vďaka tomu je možné rýchlejšie a cielenejšie rozhodovať o potrebných zásahoch, plánovaní údržby a preventívnych bezpečnostných opatreniach. Mosty sú neoddeliteľnou súčasťou dopravnej infraštruktúry a slúžia ako kľúčové spojenia pre ľudí dochádzajúcich do práce, školy alebo iných dôležitých destinácií [7]. Keď takáto infraštruktúra zlyhá, ľudia sú nútení používať zdĺhavé obchádzky, čo má za následok meškania, zvýšené náklady na dopravu, narušenie ich denného režimu a väčší vplyv na životné prostredie.

Okrem toho, predĺžený čas potrebný na obnovu alebo výmenu týchto mostov môže zaťažiť zdroje a zvýšiť celkovú ekonomickú záťaž, čo ovplyvní jednotlivcov aj širšiu spoločnosť. Následné účinky týchto zrútení zdôrazňujú potrebu robustnejšieho a proaktívnejšieho prístupu k údržbe, hodnoteniu a bezpečnosti infraštruktúry v Európe [8, 9].

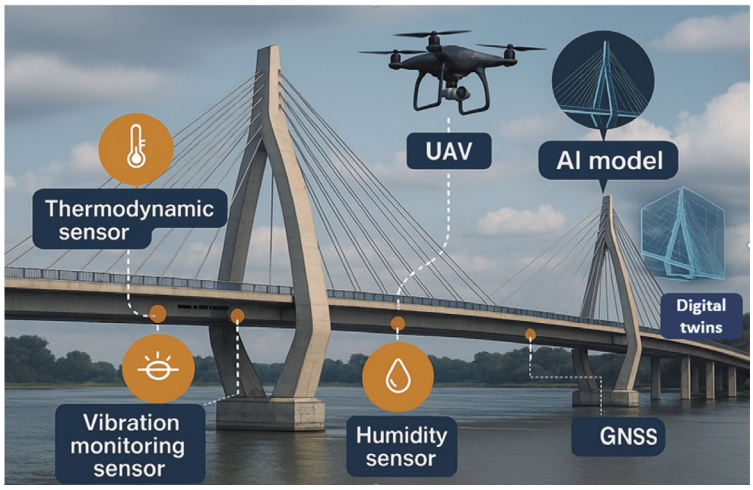
2 Identifikácia rizík využívania pokrokových technológií

Pokročilé technológie monitorovania mostov (napr. systémy SHM, platformy s podporou IoT, bezdrôtové senzorové siete a geodetické metódy) ponúkajú podstatné výhody, ale zároveň prinášajú nové kategórie rizík, ktoré presahujú samotnú konštrukciu a zahŕňajú kvalitu merania, dátovú infraštruktúru a interpretáciu výsledkov [10]. V prostrediach založených na IoT patria medzi kritické zraniteľnosti obmedzenia napájania, oneskorenie komunikácie, spoľahlivosť prenosu a metrologická integrita, ktoré všetky priamo ovplyvňujú spoľahlivosť údajov a následne aj rozhodnutia zodpovedných osôb [11]. Skúsenosti získané z dlhodobého nasadenia SHM ďalej naznačujú, že hlavnou výzvou nie je len zber údajov, ale zabezpečenie časovej synchronizácie, zabezpečenie kvality, robustné riadenie údajov a, čo je najdôležitejšie, spoľahlivý odvodzovanie signálov od stavu konštrukcie, čo je tiež kľúčové pre vývoj kyberneticko-fyzikálnych systémov pre infraštruktúru. Vytvorenie inteligentných platforiem SHM pre mosty s veľkým rozpätím si preto vyžaduje koherentnú komplexnú stratégiu spracovania údajov (získavanie – spracovanie – riadenie – analýza – vizualizácia) a jasné prepojenie s rozhodovacím procesom; inak sa monitorovanie rizík stane nákladným zdrojom nevyužitých alebo ťažko porovnateľných dátových súborov [12]. Jednotlivé technológie majú tiež obmedzenia špecifické pre danú oblasť – napríklad vysokorýchlostný GNSS môže poskytovať priame odhady posunu, ale jeho presnosť a stabilita silne závisia od spracovateľských postupov a podmienok merania, čo môže spôsobiť značnú neistotu pri hodnotení deformácií. Nakoniec, rozsiahle historické nasadenie bezdrôtového snímania v teréne na skutočných mostoch (napr. testovacie zariadenie ISHMP/Jindo Bridge) demonštruje realizovateľnosť takýchto systémov a zároveň zdôrazňuje potrebu spoľahlivej dlhodobej prevádzky, správy údajov a interpretácie pracovných postupov [13, 14].

Proces monitorovania a následného hodnotenia odolnosti má 4 hlavné kroky: získavanie údajov, vizuálna kontrola, inteligentná diagnostika a preventívne merania. V prípade nových rizík je potrebné dodržať proces hodnotenia rizík (identifikácia rizík, analýza rizík a vývoj rizík). V tomto dokumente sa zameriame na technológie, ktoré sú v súčasnosti najviac používané a ktoré sú uvedené v poradí, v akom vstupujú do procesu monitorovania aktuálneho stavu a následného hodnotenia, medzi ktoré patria:

- Systémy SHM na získavanie údajov;
- Senzorové siete založené na internete vecí (IoT) na získavanie údajov;
- Bezpilotné lietadlá (UAV – drony) na vizuálnu kontrolu;
- Umelá inteligencia (AI) na inteligentnú diagnostiku;
- Digitálne dvojčatá (DT) na inteligentnú diagnostiku a preventívne merania.

Na Obrázku 2 sú znázornené pokročilé technológie dostupné pre pokročilé monitorovanie. Oranžové bubliny slúžia ako senzory pre SHM založené na IoT, ktoré monitorujú vibrácie vo vertikálnom aj horizontálnom smere. Druhý senzor meria teplotu mosta a cesty. Podobne drony skenujú celý most a generujú mračno bodov, ktoré sa používa na vytvorenie digitálneho dvojčaťa. Nakoniec, aplikovaný model umelej inteligencie dokáže detekovať praskliny, koróziu a iné defekty, čím poskytuje informácie o aktuálnom stave konštrukcie mosta.



Obrázok 2. Pokrokové technológie monitorovania mostov

Tabuľka 1. Riziká vyplývajúce z používania pokrokových monitorovacích technológií

Kategória	Krok v procese monitorovania	Riziko	P (1–5)	D (1–5)	R	Priorita
Technické	Získavanie údajov	Porucha senzora alebo zariadenia	4	4	**16**	**Vysoká**
Technické	Inteligentná diagnostika	Nízka presnosť modelov umelej inteligencie v reálnych podmienkach	3	4	**12**	Stredná
Technické	Získavanie údajov	Nesprávny výklad údajov	3	3	**9**	Stredná
Technické	Získavanie údajov / Vizuálna inšpekcia	Technologická zastaranosť/ nekompatibilita	4	3	**12**	Stredná
Kybernetické	Inteligentná diagnostika	Hekerstvo a neoprávnený prístup (Manipulácia s údajmi)	3	5	**15**	**Vysoká**
Kybernetické	Získavanie údajov / Inteligentná diagnostika	Nedostatočné šifrovanie počas prenosu	3	4	**12**	Stredná
Kybernetické	Získavanie údajov	Závislosť od internetu/cloudu (Strata pripojenia)	3	4	**12**	Stredná
Legálne/Etické	Vizuálna inšpekcia	Porušenie GDPR (bezpilotné lietadlá v blízkosti obytných oblastí)	3	4	**12**	Stredná
Legálne/Etické	Inteligentná diagnostika / Preventívne opatrenia	Nejasná zodpovednosť v prípade zlyhania systému	3	4	**12**	Stredná
Legálne/Etické	Preventívne opatrenia	Nedostatok noriem a usmernení v stavebníctve	3	3	**9**	Stredná
Organizačno-operačné	Získavanie údajov / Preventívne opatrenia	Nedostatok kvalifikovaného personálu	4	4	**16**	**Vysoká**
Organizačno-operačné	Preventívne opatrenia	Slabá integrácia s procesmi údržby	4	3	**12**	Stredná
Organizačno-operačné	Získavanie údajov / Preventívne opatrenia	Závislosť od dodávateľa (konkrétny poskytovateľ/softvér)	3	3	**9**	Stredná

Pre manažérov v oblasti bezpečnosti a krízového riadenia predstavujú pokročilé technológie kľúčové nástroje na rýchle a sofistikované rozhodovanie, pričom zároveň prinášajú dodatočné riziká, ktoré je potrebné riadiť. Možno však konštatovať, že moderné technológie predstavujú pre spoločnosť väčšiu príležitosť ako hrozbu. V Tabuľke 1 sú uvedené riziká spojené s využívaním pokročilých technológií na monitorovanie mostov, ktoré sú rozdelené do štyroch kategórií: technické, kyberbezpečnostné, právne a etické a organizačné a prevádzkové. Tabuľka uvádza hodnotu každého rizika vypočítanú ako Riziko (R) = Pravdepodobnosť udalosti (P) * Dopad udalosti (I).

Hodnoty rizika boli odvodené na základe odborných posudkov. Každé riziko bolo hodnotené z hľadiska pravdepodobnosti a dopadu na stupnici od 1 do 5 piatimi odborníkmi s praxou v oblasti inšpekcie mostov, SHM a správy majetku. Hodnotenia boli agregované pomocou mediánu, aby sa znížila citlivosť na extrémne hodnoty. Boli posúdené nezhody, potom sa uskutočnilo druhé kolo diskusie a hodnotenia sa zopakovali. Konečné skóre rizika bolo vypočítané ako pravdepodobnosť × dopad. Implementácia moderných technológií do monitorovania mostov zvyšuje presnosť a efektívnosť, ale vyžaduje aj systematické riadenie rizík. Najlepší prístup spočíva v kombinácii:

- tradičné metódy s podporou digitálnych metód,
- zálohovanie systémov,
- školenie personálu,
- riadne zavedená legislatíva a bezpečnostná politika v oblasti kybernetickej bezpečnosti.

Technické riziká pokrokových monitorovacích technológií

Hardvérové alebo softvérové poruchy senzorov, výpadky napájania, nesprávne kalibrácie alebo nedostatočná správa údajov môžu viesť k falošným poplachom alebo k nezisteniu kritických stavov. Aktan a kol. poukazujú na výzvy súvisiace so synchronizáciou a archiváciou veľkých objemov údajov [13]. Kľúčové metriky a pojmy spoľahlivosti úzko súvisia s pravdepodobnosťou zistenia poruchy. To znamená, či je možné zistiť poruchu pomocou použitých senzorov, ale samozrejme, či je možné zistiť, že senzor stráca svoju spoľahlivosť. Ide o kľúčový ukazovateľ používaný na posúdenie pravdepodobnosti, že systém zistí skryté štrukturálne poškodenie. Pravdepodobnosť zistenia je obzvlášť relevantná pre techniky ako ultrazvuk a vedené vlny. Štúdie spoľahlivosti tiež zohľadňujú schopnosť systému lokalizovať poruchu a presne odhadnúť jej veľkosť [15].

Metriky kvality informácií sú nové metriky, ktoré hodnotia vplyv kvality údajov na spoľahlivosť štrukturálnych modelov. Zahŕňajú faktory, ako je presnosť senzorov, rozlíšenie signálu a vplyv environmentálneho šumu na interpretáciu údajov. Bayesovské prístupy sa často používajú na aktualizáciu hodnotení spoľahlivosti v reálnom čase, keď sa zhromažďujú nové údaje [16]. V súčasnosti nie je typické, aby sa zrútenie mostov odohrávalo v dôsledku porúch senzorov, nespoľahlivých meraní alebo falošných údajov, pretože hlavnou príčinou zrútenia mostov sú konštrukčné podmienky. V Singapure sa zistilo, že senzory na detekciu napätia inštalované na opornom múre výkopu boli zakopané 2 dni pred zrútením a neboli vykonané žiadne merania. Napriek zaznamenaným pohybom, dozorcovia na základe týchto údajov nepodnikli žiadne kroky. Trhliny boli ošetrené povrchovo a neboli prijaté žiadne nápravné opatrenia [17]. Na druhej strane existuje mnoho prípadov, keď senzory nefungovali kvôli cestným prácam, čo malo okamžité následky, ako napríklad v prípade mosta Morandi v Taliansku a mosta Zijin v Číne. Týmto mimoriadnym udalostiam by sa dalo predísť pomocou iných externých systémov (pravidelné spracovanie obrazu, monitorovanie pomocou bezpilotných lietadiel atď.), pretože nainštalované senzory musia byť neaktívne [18, 19].

Kybernetické riziká pokrokových monitorovacích technológií

Všetky pripojené systémy sú zraniteľné voči hrozbám kybernetickej bezpečnosti. Hrozby kybernetickej bezpečnosti pre systémy IoT sa bežne klasifikujú podľa trojice CIA: dôvernosť, integrita a dostupnosť [18]:

- Dôvernosť: Zabezpečuje, aby citlivé údaje SHM (napr. stav konštrukcie, prevádzkové parametre) boli prístupné len oprávneným používateľom a systémom. Porušenie môže viesť k porušeniu súkromia, úniku konkurenčných informácií alebo cieleným útokom na kritickú infraštruktúru.
- Integrity: Zaručuje presnosť, autentickosť a spoľahlivosť údajov SHM počas celého ich životného cyklu. Ohrozenie integrity môže viesť k falošným poplachom, zmeškaným detekciám alebo nevhodným údržbárskym zásahom, čo môže potenciálne ohroziť verejnú bezpečnosť.
- Dostupnosť: Zabezpečuje, aby boli služby a údaje SHM dostupné v prípade potreby. Útoky na dostupnosť (napr. odmietnutie služby) môžu narušiť monitorovanie, oneskoriť núdzové reakcie a podkopať dôveru v systém.

Legislatívne a etické riziká

Používanie bezpilotných lietadiel, internetu vecí a cloud computingu vyvoláva otázky týkajúce sa GDPR, ochrany osobných údajov a zodpovednosti v prípade poruchy senzora alebo modelu umelej inteligencie. Normy na národnej úrovni sú vyvinuté len čiastočne. V budúcnosti je potrebné zlepšiť túto oblasť prostredníctvom strategického riadenia, ako je napríklad európska smernica, ktorá by mala byť záväzná v celej Európskej únii, keďže medzi krajinami existujú rozdiely. Rastúci záujem o bezpilotné lietadlá na komerčné a rekreačné účely si vyžaduje jasné pravidlá ich bezpečného používania. Európska únia poverila touto úlohou Európsku agentúru pre bezpečnosť letectva (EASA) [17], ktorej úlohou bolo navrhnúť a harmonizovať predpisy týkajúce sa dronov v celej EÚ. V dôsledku toho boli prijaté nariadenia EÚ 2019/945 [20] a 2019/947 [21, 22], ktoré definujú podmienky registrácie používateľov dronov, kategorizujú UAS (bezpilotné letecké systémy) a stanovujú pravidlá bezpečnej prevádzky. Tieto nariadenia sú v platnosti od 31. decembra 2020, ale ich uplatňovanie sa v jednotlivých členských štátoch EÚ líši. Európska únia zaviedla pravidlá pre používanie dronov, ktoré klasifikujú bezpilotné systémy do troch kategórií: otvorené, špecifické a certifikované. Za správu tejto klasifikácie je zodpovedný Úrad civilného letectva.

Etické riziká spojené s využívaním pokrokových technológií pri monitorovaní infraštruktúry sa týkajú predovšetkým súkromia, transparentnosti, zodpovednosti a širšieho sociálneho vplyvu týchto systémov. Jednou z najnaliehavejších obáv je neoprávnené zhromažďovanie citlivých osobných údajov alebo údajov týkajúcich sa polohy, najmä prostredníctvom bezpilotných lietadiel a inteligentných senzorov. To vyvoláva otázky týkajúce sa sledovania, súhlasu a hraníc osobného súkromia.

Organizačné a operačné riziká pokrokových monitorovacích technológií

Nejasné riadenie a rozhodovanie počas anomálií patria medzi najvýznamnejšie riziká. Jeden prípad sa stal v Miami v roku 2018. Národný úrad pre bezpečnosť dopravy (NTSB) identifikoval chyby v konštrukcii a nedostatočné odborné posúdenie ako pravdepodobnú príčinu zrútenia mosta. Tiež poznamenal, že napriek výrazným prasklinám nebola cesta uzavretá a práce pokračovali, čo predstavovalo zlyhanie rozhodovacích postupov a riadenia rizík. Most s dĺžkou 174 stôp (53 m) sa zrútil z výšky približne 18,5 stôp (5,6 m) na SW 8th Street, ktorá pozostáva zo štyroch jazdných pruhov a jedného pruhu na odbočenie vľavo v smere na východ a troch jazdných pruhov v smere na západ. Dva z jazdných pruhov smerujúcich na západ pod severným koncom mosta boli v čase zrútenia uzavreté, jeden jazdný pruh smerujúci na západ a všetkých päť jazdných pruhov smerujúcich na východ však zostali otvorené. V deň zrútenia stavebná partia pracovala na opätovnom napínaní predpínacích tyčí v prvku 11, ktorý spájal mostný nadstrešok s mostnou konštrukciou na severnom konci. Osem

vozidiel nachádzajúcich sa pod mostom bolo úplne alebo čiastočne rozdrvených. Zomrel jeden pracovník mosta a päť osôb vo vozidlách. Päť pracovníkov mosta a päť ďalších osôb bolo zranených [23].

3 Záver

Výsledky príspevku poukazujú na zásadné napätie, ktoré je dnes prítomné pri zavádzaní pokrokových technológií do monitorovania mostov. Na jednej strane moderné systémy monitorovania stavu konštrukcií, senzory internetu vecí, bezpilotné prostriedky, umelá inteligencia či digitálne dvojčatá jednoznačne zvyšujú úroveň situačného povedomia, umožňujú priebežné sledovanie technického stavu objektov a skracujú čas potrebný na identifikáciu porúch a prijatie zásahu. Na druhej strane však tieto technológie vytvárajú nové, vzájomne previazané kyberneticko-fyzické závislosti, ktoré môžu v prípade nedostatočne koordinovaného riadenia znižovať celkovú odolnosť systému. Ukazuje sa preto, že samotné technologické zlepšenie ešte automaticky neznamená zvýšenie bezpečnosti a resilience monitorovaného objektu.

Kľúčovým zistením je, že posudzovanie technickej spoľahlivosti a kybernetickej bezpečnosti ako dvoch oddelených oblastí vedie k prehliadaniu spoločných mechanizmov zlyhania. V praxi môže dôjsť napríklad k situácii, keď je odchýlka merania spôsobená odchýlkou senzora prekrytá predspracovaním dát, alebo keď sa narušenie polohových údajov prostredníctvom GNSS spoofingu premietne do stavu digitálneho dvojčaťa a následne ovplyvní rozhodnutia o údržbe. Práve z tohto dôvodu je nevyhnutné uplatňovať jednotný pohľad na riziká, založený na spoločných metrikách, zdieľaných rozhodovacích kritériách a integrovanom hodnotení technických aj kybernetických hrozieb. Významnou prekážkou ostáva aj neúplný regulačný rámec, najmä v oblasti nasadzovania UAV, IoT a AI v monitorovaní mostov, ako aj chýbajúce ekonomické analýzy, ktoré by umožnili objektívne posúdiť prínosy a náklady týchto technológií v jednotlivých fázach životného cyklu mosta pre využitie digitálneho dvojčaťa.

Na základe uvedených zistení možno konštatovať, že ďalší výskum by sa mal orientovať na tvorbu komplexnej metodiky hodnotenia rizík a resilience, ktorá bude prepájať technické, organizačné, právne, ekonomické a kybernetické aspekty do jedného funkčného nástroja. Súčasne je potrebné rozvíjať realistické testovacie scenáre zamerané na výpadky napájania senzorových sietí, narušenie integrity dát alebo chybné interpretácie výstupov umelej inteligencie. Dôležitou oblasťou ostáva vytvorenie právno-etického rámca, ktorý bude riešiť ochranu súkromia, zodpovednosť pri zlyhaní systému a transparentnosť rozhodovania AI v kontexte bezpečnosti infraštruktúry. Perspektívnym smerom je aj integrácia technológií, najmä prepojenie BIM, digitálnych dvojčiat a algoritmov umelej inteligencie do jednotného prostredia podporujúceho vizualizáciu, diagnostiku a plánovanie údržby.

V závere možno zdôrazniť, že budúcnosť monitorovania mostov nebude závisieť len od technickej vyspelosti použitých nástrojov, ale predovšetkým od schopnosti zavádzať ich systematicky, bezpečne a v súlade s princípmi holistického riadenia rizík. Len tak bude možné naplno využiť ich potenciál pri súčasnom zachovaní požadovanej úrovne bezpečnosti, spoľahlivosti a dôveryhodnosti v správe infraštruktúry.

Poďakovanie

Tento článok bol podporený projektom REMAKE 3D – Strengthening the REsilience MAnagement of Key infrastructue Elements using advances in 3D modeling pod číslom projektu APVV-22-0562.

Referencie

[1] Slovenská správa ciest a cestná databanka. [cit. 25.02.2026] Available at: https://www.cdb.sk/sk/Vystupy-CDB/Statisticke-prehlady/Cestne-objekty-pocty-a-stav.alej

[2] Daponte, P.; Olivito, R.S. Crack detection measurements in concrete. Proc. of the ISMM Int. Conf. on Microcomputer Applications, Los Angeles (U.S.A.), 14-16/Dec./1989, pp. 123–127

[3] Daponte, P.; Olivito, R.S. Frequency analysis for crack detection in concrete. Proc. of 9th Int. Conference on Experimental Mechanics, Copenhagen, 20-24/Aug./1990, vol.4, pp. 1355–1364

[4] Neyestani, A.; Ahmed, I.; Daponte, P.; De Vito, L. Concrete crack detection and segmentation in civil infrastructures using UAVs and deep learning, Prof. of 7th International Conference on Internet of Things and Applications, IoT 2023, Isfahan, Iran, October 25–26, 2023, [cit. 25.02.2026] https://dx.doi.org/10.1109/IoT60973.2023.10365340

[5] Neyestani, A.; Picariello, F.; Tudosa, I.; Daponte, P.; De Vito, L. Triplet loss-based concrete crack verification for structural health monitoring and digital twin applications, 2024 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE), October 21-23, 2024, St Albans – London, UK. [cit. 25.02.2026]. Dostupné z: https://dx.doi.org/10.1109/MetroXRAINE62247.2024.10797100

[6] Prakash, V.; Debono, C.J.; Musarat, M.A.; Borg, R.P.; Seychell, D.; Ding, W.; Shu, J. Structural Health Monitoring of Concrete Bridges Through Artificial Intelligence: A Narrative Review. Appl. Sci. 2025, 15, 4855. https://doi.org/10.3390/app15094855

[7] Ciampa, E.; De Vito, L.; Pecce, M. Practical issues on the use of drones for construction inspections. In: J. Phys.: Conf. Ser. 2019, 1249 012016

[8] D'Angelo, M.; Civera, M.; Giordano, P.F.; Borlenghi, P.; Ballio, F.; Limongelli, M.P.; Chiaia, B. Bridge collapses in Italy in the 21st century: survey and statistical analysis. Civil Engineering and Infrastructure Engineering, 2025, p. 1–23. https://doi.org/10.1080/15732479.2025.2483500

[9] Figuli, L.; Gattulli, V; Hoterová, K.; Ottaviano E. Recent Developments on Inspection Procedures for Infrastructure Using UAVs. In book: Modern Technologies Enabling Safe and Secure UAV Operation in Urban Airspace. IOS Press. DOI: 10.3233/NICSP210003

[10] Balestrieri, E.; De Vito, L.; Lamonaca, F.; Picariello, F.; Rapuano, S.; Tudosa, I. Research challenges in measurements for Internet of Things systems, ACTA IMEKO, 2018 vol. 7, N. 4, p. 82 - 94, [cit. 25.02.2026] https://acta.imeko.org/index.php/acta-imeko/article/view/IMEKO-ACTA-07%20%282018%29-04-14/pdf

[11] Spencer, B.F.; et al. ISHMP – Jindo Bridge Project. [cit. 20.02.2026] Available at: https://web.archive.org/web/20110827045524/http://shm.cs.uiuc.edu/about.html

[12] Aktan, E.; Bartoli, I.; Glišić, B.; Rainieri, C. Lessons from Bridge Structural Health Monitoring (SHM) and Their Implications for the Development of Cyber-Physical Systems. Infrastructures 2024, 9, 30. https://doi.org/10.3390/infrastructures9020030

[13] Xie, Y.; Meng, X.; Nguyen, D.T.; Xiang, Z.; Ye, G.; Hu, L. A Discussion of Building a Smart SHM Platform for Long-Span Bridge Monitoring. Sensors 2024, 24, 3163. https://doi.org/10.3390/s24103163

[14] Qu, X.; Shu, B.; Ding, X.; Lu, Y.; Li, G.; Wang, L. Experimental Study of Accuracy of High-Rate GNSS in Context of Structural Health Monitoring. Remote Sens. 2022, 14, 4989. [cit. 20.02.2026] https://doi.org/10.3390/rs14194989

[15] Zorzi, S.; Broccardo, M.; Tonelli, D.; Zonta, D. Reliability-based metrics for structural health monitoring information quality assessment. Structural Health Monitoring. 24, 2024, 5, :3028-3045. [cit. 25.02.2026] doi:10.1177/14759217241265956

[16] Mardanshahi, A.; Sreekumar, A.; Yang, X.; Barman, S.K.; Chronopoulos, D. Sensing Techniques for Structural Health Monitoring: A State-of-the-Art Review on Performance Criteria and New-Generation Technologies. Sensors 2025, 25, 1424. https://doi.org/10.3390/s25051424

[17] ENISA. Good practices for security and IoT, November 2019, [cit. 25.02.2026] https://www.enisa.europa.eu/sites/default/files/publications/WP2019%20-%20O.1.1.1%20Good%20practices%20for%20security%20of%20IoT.pdf

[18] Coston, I.; Plotnizky, E.; Nojoumian, M. Comprehensive Study of IoT Vulnerabilities and Countermeasures. Appl. Sci. 2025, 15, 3036. https://doi.org/10.3390/app15063036

[19] Tan, J.-S.; Elbaz, K.; Wang, Z.-F.; Shen, J.S.; Chen, J. Lessons Learnt from Bridge Collapse: A View of Sustainable Management. Sustainability 2020, 12, 1205. [cit. 25.02.2026] https://doi.org/10.3390/su12031205

[20] European Union Regulation 2019/945

[21] European Union Regulation 2019/947

[22] European Union AI Act – harmonised rules on artificial intelligence and amending

[23] Wu, W.; Cantero-Chinchilla, S.; Prescott, D.; Remenyte-Prescott, R.; Chiachío, M. A general approach to assessing SHM reliability considering sensor failures based on information theory. Reliability Engineering & System Safety, 250, 2024, 110267, ISSN 0951-8320, doi: 10.1016/j.ress.2024.110267

Komunikační vzorce organizovaných teroristických skupin a osamělých aktérů v online prostředí

Jana Neuwirthová[1], Martin Haváček[2]

[1] VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství, Lumírova 13, 700 30 Ostrava - Výškovice

[2] VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství, Lumírova 13, 700 30 Ostrava - Výškovice, martin.havacek@vsb.cz

Abstrakt:

Tento článek se věnuje současnému fenoménu zneužívání digitálního prostoru k šíření teroristických ideologií a propagaci násilí. Zaměřuje se na komunikační strategie, které využívají teroristické skupiny i jednotlivci na sociálních sítích. Výzkumná část vychází z analýzy autentických manifestů a tematicky zaměřených datových souborů. Tyto texty jsou hodnoceny podle osmi definovaných kritérií, mezi něž patří například démonizace, dehumanizace či fúze identity. Cílem článku je zachytit charakteristické rysy teroristického diskurzu napříč ideologickým spektrem. Výsledky výzkumu ukazují, že nejčastějším a nejvýraznějším jevem je démonizace vnější skupiny, která byla identifikována ve 100 % případů. S vysokým podílem se dále vyskytují výzvy k násilí (95 %) a jazyk spojený s fúzí identity (90 %). Závěr potvrzuje, že i přes značnou ideologickou různorodost existují v projevech teroristů společné jazykové rysy. Identifikace a odhalení těchto narativů může zásadně napomoci k včasné detekci nebezpečných obsahů a přispět k efektivnější prevenci radikalizace v digitálním prostředí.

Klíčová slova: terorismus, sociální sítě, kyberterorismus, komunikační strategie, radikalizace, propaganda.

1 Úvod

Terorismus představuje jeden z nejvýraznějších globálních fenoménů současnosti, který zásadně ovlivňuje politickou, ekonomickou i společenskou stabilitu mnoha zemí. Jeho podstata spočívá v záměrném a cíleném užívání násilí či jeho hrozby za účelem dosažení politických, ideologických nebo náboženských zájmů. Ačkoliv se mezinárodní společenství dosud neshodlo na jedné univerzální definici, Evropská unie tyto činy chápe jako útoky s cílem vážně zastrašit obyvatelstvo nebo destabilizovat základní struktury státu [1]. S neustálým technologickým vývojem a rostoucí orientací společnosti na digitální prostředí se však pole působnosti extremistů významně rozšiřuje a transformuje.

Tento posun dal vzniknout takzvanému kyberterorismu, což je specifická forma teroristické činnosti, která přenáší tyto aktivity do virtuálního kyberprostoru. Podle vymezení Severoatlantické aliance jde o útoky, které využívají počítačové a komunikační sítě k vyvolání destrukce a zastrašení společnosti za účelem dosažení ideologických cílů [2]. Kyberteroristé se zaměřují na narušení kritické infrastruktury – například energetiky, logistiky či zdravotnictví – s cílem způsobit masový chaos. Výraznou výhodou pro tyto aktéry je přitom vysoká míra anonymity, kterou online prostředí nabízí, a relativně nízké finanční náklady na samotné provedení útoku.

Klíčovým aspektem tohoto nového digitálního bojiště jsou sociální sítě, jež se staly pro teroristy vysoce účinným nástrojem pro šíření radikalizačního obsahu [3]. Od tradičních médií se liší především vyšší mírou interaktivity, okamžitou dostupností, globálním dosahem a možností obousměrné komunikace. Každý uživatel těchto platforem tak může aktivně vstupovat do komunikačního procesu nejen jako pasivní příjemce, ale přímo jako tvůrce a šiřitel obsahu.

Teroristické organizace využívají sociální platformy velmi systematicky z několika strategických důvodů. Tyto služby jsou bezplatné, uživatelsky přívětivé a umožňují přímý kontakt s širokým publikem bez nutnosti dalšího zprostředkování. Mimořádně efektivní je pro ně strategie tzv. narrowcastingu – na základě veřejně dostupných uživatelských dat mohou teroristé analyzovat postoje či zájmy jednotlivců a následně na ně velmi přesně a na míru cílit svou propagandu [3]. Online platformy tak neslouží jen k prostému šíření ideologie, ale k aktivnímu náboru nových členů a operativní koordinaci.

Tento fenomén digitální radikalizace a způsob šíření teroristických narativů představuje vysoce aktuální bezpečnostní výzvu. Cílem tohoto článku je proto komplexně analyzovat komunikační strategie teroristických aktérů v prostředí moderních digitálních platforem. Text si klade za úkol zhodnotit a komparovat, jaké konkrétní jazykové prostředky, narativní struktury a psychologické taktiky jsou při těchto radikalizačních a náborových aktivitách v online prostoru nejčastěji využívány.

2 State of the art

Současný stav poznání potvrzuje, že digitální platformy zásadně proměnily komunikační modus operandi teroristických aktérů: umožňují okamžitý přenos sdělení, přesné cílení, škálování, přesun do šifrovaných či polouzavřených prostředí a provázání propagandy s rekrutací a koordinací. V bezpečnostním rámce na úrovni Aliance se tato změna promítá do kyberobrany a protiteroristických politik NATO (uznání kyberprostoru jako domény, posílení schopností a rámců reakce). [2, 4]

V lingvistickém a narativním výzkumu posledních let se napříč ideologiemi opakovaně potvrzují čtyři klíčové vzorce: (a) polarizující rámec „my vs. oni“ a krizové narativy; (b) démonizace a dehumanizace out-group; (c) fúze identity a pozitivní sebeprezentace in-group; (d) výzvy k násilí a rekrutaci. Tyto struktury byly doloženy jak v prostředí salafistických stránek a kázání, tak v krajně pravicových kanálech a fórech. [5, 6]

Korpusová a lexikometrická analýza ukazuje, že s rostoucí mírou radikalizace se zhušťuje výskyt exkluzivních zájmen, stigmatizujících etiket a hodnotících adjektiv, které stabilně rozlišují otevřené skupiny na sociálních sítích od komunikace v uzavřených/trestně stíhaných kruzích. [7]

Longitudinální modelování chování uživatelů na bílém supremacistickém fóru a na fringe platformách zachycuje trajektorie od „mírnějších předsudků“ k explicitní podpoře násilí; to je důležité zejména pro včasnou identifikaci rizikových signálů u „osamělých aktérů“. [8, 6]

Současné systematické přehledy zároveň upozorňují, že detekce online extremismu vyžaduje více než klíčová slova: je nutné zachytit kontext, ironii a funkci sdělení (rekrutace vs. bonding) a řešit vícejazyčnost i datovou chudobu mimo dominantní jazyky. [9]

V oblasti automatické detekce se vedle transparentních modelů (SVM, Naïve Bayes, logistická regrese) prosadily transformery (BERT, mDistilBERT) a vícejazyčné přístupy; nově se zkouší i zero-shot klasifikace s LLM, která slibuje zachytit komplexnější jazykové markery (ideologie vs. násilná dimenze). [10, 11]

Pro arabské a vícejazyčné datasety se ukazuje, že kombinace standardních rysů s doménově specifickými reprezentacemi (náboženství / extremistická ideologie / hate) zvyšuje citlivost vůči ambigvitě a polysemii. [12, 13]

Vedle skupinových materiálů zůstávají klíčovým zdrojem i manifesty „osamělých aktérů“, které umožňují přímo hodnotit fúzi identity, narativy existenční hrozby a normalizaci násilí. Metodicky to potvrzuje i rámec srovnávací analýzy manifestů, který pracuje s lingvistickými proxy pro fúzi identity a dehumanizaci. [14]

3 Metodologie

Zatímco současný výzkum se posouvá k automatizované detekci, tento článek se zaměřuje na detailní kvalitativní analýzu primárních textů, která umožňuje hlubší pochopení skrytých narativů. Výzkumný vzorek tvoří devět primárních zdrojů, které zahrnují jak rozsáhlé akademické datasety (např. MIWS 2021, databáze Stormfront, archiv Harmony), tak i pět specifických manifestů osamělých útočníků z let 2011–2022 (mj. A. B. Breivik, B. Tarrant, P. Gendron). Z těchto dat bylo vyčleněno deset analyzovaných kategorií aktérů, zahrnujících organizované skupiny (ISIS, Al-Káida, Taliban) i individuální extremisty.

Pro vyhodnocení přítomnosti osmi vybraných kritérií (viz Tabulka 1) byla zvolena manuální kvalitativní obsahová analýza. Tento přístup byl nezbytný pro zachycení kontextu a nuancí, které mohou automatizovaným modelům unikat. Na základě systematického a opakujícího se výskytu (minimálně 10 výskytů či 10–15 % obsahu) byl každý text kódován tak, aby indikoval, zda je daný narativ plně přítomen (A), částečně přítomen (A/N), nebo zcela chybí (N).

Analytický vzorek tvoří následující datové soubory a manifesty, jež reprezentují autentické výstupy ideologicky motivovaných aktérů:

- MIWS dataset (2021): Akademický soubor obsahující 40 000 příspěvků z platformy Twitter (nyní X), rovnoměrně rozdělených mezi džihádisticko-islamistickou a bělošsky-supremacistickou tématiku [15].
- Harmony Documents Archive: Archiv deklasifikovaných materiálů spravovaný Centrem pro boj proti terorismu při West Pointu. Obsahuje interní směrnice, korespondenci a hlášení skupin jako Al-Káida či Taliban [16].
- Hate Speech Dataset from Stormfront (2018): Korpus více než 10 000 manuálně anotovaných vět extrahovaných z krajně pravicového internetového fóra Stormfront [17].
- Extremist Manifesto Database (2021) a vybrané manifesty: Z dostupné databáze textů tzv. osamělých útočníků [18] bylo pro detailní analýzu vybráno pět klíčových manifestů, které pokrývají různé motivační profily:
  - *A. B. Breivik (2011):* Rozsáhlý text kombinující prvky nacionalismu a islamofobie [19].
  - *E. Rodger (2014):* Autobiografický dokument pramenící z osobní frustrace, izolace a misogynie [20].
  - *B. Tarrant (2019)* a na něj navazující *P. Gendron (2022):* Manifesty stavící na konspirační teorii „velké výměny“, islamofobii a bělošském supremacismu [21, 22].
  - *J. Earnest (2019):* Otevřený dopis propojující rasovou nenávist s náboženským extremismem [23].

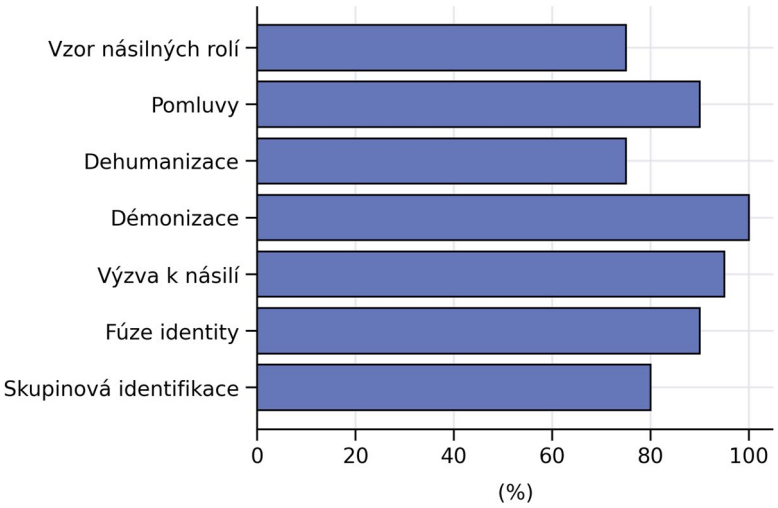
Přehled osmi analytických kritérií a jejich stručná charakteristika je uveden v Tabulce 1.

Tabulka 1. Zkrácený přehled narativních klasifikací a hodnoticích kritérií

Kategorie	Kritérium	Stručná definice pro účely analýzy
V rámci skupiny	Skupinová identifikace	Ztotožnění se se sociální skupinou prostřednictvím jazyka (používání zájmen „my“, „naši“) a sdílených hodnot.
	Fúze identity	Prolínání osobní a skupinové identity, často vyjadřované rodinnými či příbuzenskými metaforami (např. „bratr“, „naše krev“).
Vně skupiny	Výzva k násilí	Explicitní podněty k vykonání násilných činů (např. „zabij“, „zmasakruj“) nebo deklarace plánovaného útoku.
	Démonizace	Přisuzování destruktivních a nepřátelských vlastností cílové skupině, která je činěna zodpovědnou za neúspěchy (např. „ďáblové“, „zlo“).
	Dehumanizace	Vnímání druhých jako méněcenných bytostí, typicky prostřednictvím přirovnávání ke zvířatům (např. „opice“, „paraziti“) či odosobnění.
	Pomluvy	Využívání hanlivých a urážlivých výrazů cílících na etnicitu, rasu, pohlaví či náboženství (např. „kufr“, rasové urážky).
Další	Vzor násilných rolí	Odkazování na známé pachatele ideologicky motivovaného násilí, kteří slouží jako inspirace či objekt obdivu.
	Sentiment	Celkové jazykové a postojové ladění textu, určující, zda vyjadřuje převážně pozitivní, negativní, nebo neutrální postoj.

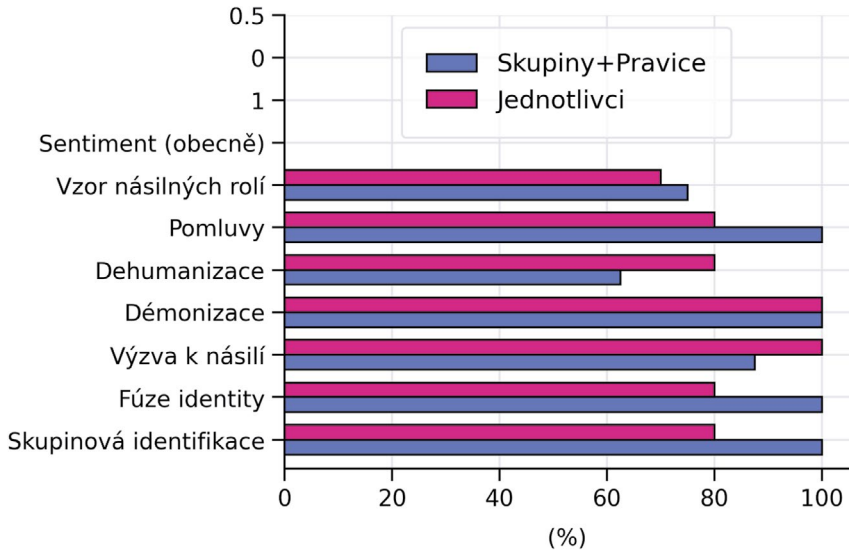
4 Výsledky

Analýza jazykových a obsahových vzorců napříč deseti sledovanými kategoriemi aktérů odhalila výraznou přítomnost opakujících se motivů. Nejčastěji se objevuje démonizace vnější skupiny, identifikovaná ve 100 % případů (tj. u všech zkoumaných skupin i jednotlivců). Ta se projevuje specifickou slovní zásobou, jako jsou výrazy *„křižáci“*, *„ďáblové“* či *„kulturní marxisti“*. S velmi vysokým podílem se vyskytují také výzvy k násilí (95 %), využívající imperativy typu *„zmasakrovat“* nebo *„zničit nepřítele“*. Jazyk spojený s fúzí identity (90 %) prokazuje silnou tendenci autorů propojovat osobní identitu s kolektivem prostřednictvím rodinných a náboženských metafor (např. *„naši bratři“*, *„synové islámu“*, *„bílé bratrstvo“*). Časté využívání rétoriky *„my versus oni“* potvrzují také pomluvy (90 %) a skupinová identifikace (80 %). Nejnižší zastoupení zaznamenaly kategorie dehumanizace (časté přirovnávání k *„krysám“* či *„parazitům“*) a vzor násilných rolí (shodně 75 %).



Obrázek 1. Frekvence výskytu komunikačních prvků

Při bližším srovnání organizovaných teroristických skupin (včetně krajní pravice) a individuálních aktérů (tzv. osamělých vlků) jsou patrné zřetelné rozdíly. Data ukazují, že skupiny a pravicoví aktéři vykazují téměř ve všech sledovaných kritériích vyšší výskyt analyzovaných prvků než jednotlivci. Zatímco u obou typů aktérů se démonizace a výzvy k násilí objevují ve 100 % případů, u jiných kritérií se hodnoty rozcházejí. Například dehumanizace dosahuje u skupin 80 %, ale u jednotlivců pouze 62,5 %. Podobně je tomu u fúze identity (100 % u skupin oproti 80 % u jednotlivců). Výrazný kontrast se ukázal také u skupinové identifikace: u organizovaných skupin je přítomna vždy, zatímco u jednotlivců má spíše nepřímý charakter. Neváže se na formální členství v organizaci, ale spíše na ideologickou či symbolickou sounáležitost, například s kulturou bílé nadřazenosti či misogynií.



Obrázek 2. Komparace skupin a jednotlivců

Z hlediska sentimentu v analyzovaných textech většinou převažuje negativně laděný obsah zaměřený vůči vnějším skupinám, které jsou vykreslovány jako nepřátelé či cíle násilí. Pozitivní prvky se objevují primárně směrem dovnitř vlastní skupiny, typicky ve formě glorifikace mučednictví nebo oslav rasové či náboženské příslušnosti, což má posílit vnitřní soudržnost. Značnou výjimku v tomto ohledu představovaly materiály Al-Káidy, u nichž převažoval neutrální sentiment a texty připomínaly spíše vnitřní zpovědní diskurz bez otevřeně agresivního tónu.

Tento kontrast lze interpretovat rozdílnými cíli obou typů aktérů. Zatímco organizované skupiny využívají systematickou dehumanizaci (80 %) k vojenské mobilizaci a ospravedlnění hromadného násilí, u osamělých aktérů (62,5 %) má násilí často kořeny v osobní frustraci a egocentrismu (typicky u manifestu E. Rodgera). Skupinová identifikace u jednotlivců proto není vázána na formální členství, ale spíše na abstraktní ideologickou sounáležitost (např. kultura bílé nadřazenosti).

5 Závěr

I přes značnou různorodost jednotlivých teroristických proudů a jejich ideologií analýza ukázala, že mezi jejich projevy existují společné jazykové rysy a opakující se komunikační strategie. Jak organizované skupiny, tak osamělí aktéři systematicky využívají polarizující rétoriku postavenou na principu *„my versus oni“*. Tento přístup slouží nejen k posílení vnitroskupinové soudržnosti, ale především k cílené démonizaci vnější společnosti, což má v online prostoru silný radikalizační potenciál.

Právě pochopení a včasné odhalení těchto specifických narativů je zcela stěžejní pro úspěšnou detekci nebezpečného obsahu na sociálních sítích. Schopnost spolehlivě identifikovat tyto varovné jazykové signály představuje klíčový krok k efektivnější prevenci radikalizace a násilného terorismu v digitálním prostředí. Ať už extremističtí aktéři volí jakékoliv platformy či komunikační metody, jejich ultimátním cílem zůstává šíření strachu a společenská destabilizace, čemuž lze právě včasnou analýzou digitální stopy proaktivně čelit.

Určitou limitací tohoto výzkumu je skutečnost, že z důvodu omezené dostupnosti digitalizovaných a veřejně přístupných dat nebyly do analýzy zahrnuty texty spojené s levicovým extremismem. Budoucí výzkum by se tak mohl zaměřit na komparaci zjištěných pravicových a džihádistických vzorců s levicovými narativy, a to i s využitím pokročilých nástrojů pro zpracování přirozeného jazyka (NLP) k analýze ještě objemnějších datasetů.

Poděkování

Tato práce byla podpořena z prostředků Ministerstva školství, mládeže a tělovýchovy ČR v rámci řešení projektu Studentské grantové soutěže VŠB-TUO č. SP2026/002.

Reference

[1] EUROPEAN UNION. Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA [online]. Official Journal of the European Union, L 88, 2017 [cit. 2025-04-09]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32017L0541

[2] NORTH ATLANTIC TREATY ORGANIZATION (NATO). Cyber defence | NATO Topic. [online]. Updated 30 July 2024 [cit. 2026-03-05]. Dostupné z: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

[3] WEIMANN, Gabriel. New Terrorism and New Media [online]. Wilson Center, 2014 [cit. 2025-04-11]. Dostupné z: https://www.wilsoncenter.org/sites/default/files/media/documents/publication/STIP_140501_new_terrorism_F.pdf

[4] NATO. NATO's Policy Guidelines on Counter-Terrorism: Aware, Capable and Engaged for a Safer Future. [online]. 10 July 2024 [cit. 2026-03-05]. Dostupné z: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/natos-policy-guidelines-on-counter-terrorism

[5] BOUKO, C. et al. Discourse patterns used by extremist Salafists on Facebook: identifying potential triggers to cognitive biases in radicalized content. Critical Discourse Studies, 2021. https://doi.org/10.1080/17405904.2021.1879185

[6] SCRIVENS, R.; DAVIES, G.; FRANK, R. Measuring the Evolution of Radical Right-Wing Posting Behaviors Online. Deviant Behavior, 2020. https://doi.org/10.1080/01639625.2018.1556994

[7] MÜLLER, P.; HARRENDORF, S.; MISCHLER, A. Linguistic Radicalisation of Right-Wing and Salafi Jihadist Groups in Social Media: a Corpus-Driven Lexicometric Analysis. European Journal on Criminal Policy and Research, 2022. https://doi.org/10.1007/s10610-022-09509-7

[8] SCHULZE, H. et al. Far-right conspiracy groups on fringe platforms: a longitudinal analysis of radicalization dynamics on Telegram. Convergence, 2022. https://doi.org/10.1177/13548565221104977

[9] ALDERA, S. et al. Online Extremism Detection in Textual Content: A Systematic Literature Review. IEEE Access, 2021. https://doi.org/10.1109/ACCESS.2021.3064178

[10] ZERROUKI, K.; BENBLIDIA, N.; BOUSSAID, O. Preprocessing multilingual text for the detection of extremism and radicalization in social networks using deep learning. Studies in Engineering and Exact Sciences, 2024. https://doi.org/10.54021/seesv5n2-594

[11] DONG, B. et al. Assessing Large Language Models for Online Extremism Research: Identification, Explanation, and New Knowledge. arXiv, 2024. https://doi.org/10.48550/arXiv.2408.16749

[12] ALKHRAIJI, A.; AZMI, A. Stance Detection in Arabic Tweets: A Machine Learning Framework for Identifying Extremist Discourse. Mathematics, 2025. https://doi.org/10.3390/math13182965

[13] KURSUNCU, U. et al. Modeling Islamist Extremist Communications on Social Media using Contextual Dimensions. Proceedings of the ACM on Human-Computer Interaction, 2019. https://doi.org/10.1145/3359253

[14] EBNER, J.; KAVANAGH, C.; WHITEHOUSE, H. Is There a Language of Terrorists? A Comparative Manifesto Analysis. Studies in Conflict & Terrorism, 2022. https://doi.org/10.1080/1057610X.2022.2109244

[15] GAIKWAD, Mayur, AHIRRAO, Swati, PHANSALKAR, Shraddha a KOTECHA, Ketan. Multi-Ideology ISIS/Jihadist White Supremacist (MIWS) Dataset for Multi-Class Extremism Text Classification. Data [online]. 2021, 6(11). Dostupné z: https://doi.org/10.3390/data6110117

[16] COMBATING TERRORISM CENTER AT WEST POINT. Harmony Documents Archive [online]. 2023. Dostupné z: https://ctc.westpoint.edu/harmony-program/

[17] DE GIBERT, Ona, PEREZ, Naiara, GARCÍA-PABLOS, Aitor a CUADROS, Montse. Hate Speech Dataset from a White Supremacy Forum. Proceedings of the 2nd Workshop on Abusive Language Online [online]. 2018, s. 11-20. Dostupné z: https://doi.org/10.18653/v1/W18-5102

[18] GRIGORYAN, Lusine. Motivations for Violent Extremism: Evidence from Lone Offenders' Manifestos: Dataset [online]. 2021. Dostupné z: https://osf.io/mvxkd

[19] BREIVIK, Anders Behring. 2083: A European Declaration of Independence [online]. 2011. Dostupné z: https://www.rai.it/dl/docs/13115255886322083-A-European-Declaration-of-Independence.pdf

[20] RODGER, Elliot. My Twisted World [online]. 2014. Dostupné z: https://www.documentcloud.org/documents/1173808-elliot-rodger-manifesto.html

[21] TARRANT, Brenton. The Great Replacement [online]. 2019. Dostupné z: https://dl1.cuni.cz/mod/resource/view.php?id=522947

[22] GENDRON, Payton. The Buffalo Attack [online]. 2022. Dostupné z: https://www.hoplofobia.info/wp-content/uploads/2022/05/PG-Manifesto.pdf

[23] EARNEST, John T. An Open Letter [online]. 2019. Dostupné z: https://bcsh.bard.edu/files/2019/06/Earnest-Manifesto-042719.pdf

Vliv koncentrace vodných roztoků methanolu na teploty vzplanutí

Vojtěch Pelech[1], Hana Věžníková[2]

[1] VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství,
Lumírova 13, 700 30 Ostrava - Výškovice, vojtech.pelech@vsb.cz

[2] VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství,
Lumírova 13, 700 30 Ostrava - Výškovice, hana.veznikova@vsb.cz

Abstrakt:

Práce se zabývá stanovením bodu vzplanutí vodných roztoků methanolu a porovnáním výsledků získaných na přístrojích PMP 4 a NPM 440 metodou Pensky Martens podle ČSN EN ISO 2719. Úvod shrnuje nebezpečné vlastnosti methanolu se zaměřením na jeho hořlavost a hořlavost jeho vodných roztoků. Experimentální část popisuje postup měření a podmínky chlazení vzorků. Naměřené hodnoty byly statisticky vyhodnoceny. Korelační analýza potvrdila velmi silnou shodu teplot vzplanutí mezi oběma přístroji a Studentův test neprokázal významné rozdíly. Ačkoli mezi naměřenými teplotami vzplanutí nebyl prokázán statisticky významný rozdíl, použití odlišných přístrojů vedlo u některých koncentrací směsí methanolu s vodou k rozdílnému zatřídění podle ČSN 65 0201.

Klíčová slova: methanol, bod vzplanutí, ČSN EN ISO 2719, hořlavé kapaliny.

1 Úvod

Methanol představuje jednu z nejvýznamnějších průmyslových chemikálií a jeho směsi s vodou se široce uplatňují v chemickém a energetickém sektoru. Díky jeho hojnému průmyslovému využití, kde se často používá ve formě směsí s vodou, se jedná o jednu z nejvíce přepravovaných chemických látek [1]. Vzhledem k vysoké hořlavosti methanolu a skutečnosti, že hořlavost přetrvává i při výrazném naředění, je přesné stanovení bodu vzplanutí těchto směsí zásadní pro jejich bezpečné používání, skladování i přepravu.

Za normálních podmínek je methanol bezbarvá a vysoce hořlavá kapalina s celou řadou nebezpečných vlastností. Požadavky na bezpečnost používání hořlavých kapalin jsou přímo svázány s teplotou vzplanutí, která je definována jako *„nejnižší teplota přepočtená na standardní tlak, při které kapalina uvolňuje za podmínek definovaných ve zkušební metodě páry v takovém množství, že se z nich ve zkušební nádobce vytvoří hořlavá směs se vzduchem“* [2]. V odborné literatuře nebo také v bezpečnostních listech se mohou uvedené teploty vzplanutí hořlavých kapalin často lišit. Teplota vzplanutí není fyzikálně-chemickou konstantou a může být ovlivněna různými okolnostmi. Vliv na výsledné hodnoty mohou mít například podmínky okolního prostředí, postup zkušební metody, konstrukce a stav použité přístrojové techniky, pracovní postup apod. [3].

Cílem tohoto příspěvku je poukázat na možné rozdíly v naměřených hodnotách teplot vzplanutí směsí methanol-voda získaných prostřednictvím rozdílných přístrojů, vyhodnotit jejich význam pro klasifikaci směsí do tříd nebezpečnosti a zdůraznit potřebu správného stanovení bodu vzplanutí pro běžnou praxi.

2 Hořlavost methanolu

Methanol je vysoce hořlavá kapalina s teplotou vzplanutí v nejčastěji udávaném rozsahu 10 ± 2 °C a teplotou vznícení okolo 470 °C, meze výbušnosti se pohybují v rozmezí 6–36 % [4, 5]. Hoření methanolu je díky jeho molekulární struktuře velmi efektivní – při dostatečném přístupu vzduchu vzniká převážně oxid uhličitý a voda bez výrazné tvorby ostatních produktů, kouře či sazí [4]. Plamen je světle modré barvy – se zvyšujícím se naředěním s vodou se zhoršuje také jeho viditelnost na denním světle, jak je vidět na Obrázku 1.

Obrázek 1. Plamen směsi methanolu s vodou (vlevo) a plamen nezředěného methanolu [5]

Výpary methanolu se v uzavřeném prostoru drží při zemi díky skutečnosti, že jsou těžší než vzduch (poměrná molekulová hmotnost je 1,1). V otevřených prostorech se výpary rychle rozptylují, v uzavřených nebo špatně větraných místech mohou stékat do nižších prostor a při vznícení způsobit zpětný tok plamene ke zdroji úniku [4].

V souvislosti s výbušností a hořlavostí methanolu došlo v minulosti k různým haváriím. Jednou z nich byl výbuch zásobníku methanolu v čistírně odpadních vod Bethune Point na Floridě, který byl způsoben selháním protiexplozivní pojistky. Ta byla vyrobena z hliníku, vůči němuž je methanol korozivní [6]. Hořlavost methanolu se projevila například při závodě Indianapolis 500, kde při doplňování paliva do závodního vozu došlo k úniku a následnému vzniku požáru (Obrázek 2). Zde byl zásah navíc komplikován špatnou viditelností plamenů hořícího methanolu na denním světle [7].

Obrázek 2. Požár methanolu při závodě Indianapolis 500 [7]

Vodné roztoky methanolu vykazují hořlavost i při vysokém naředění. Závislost bodu vzplanutí na koncentraci vody v roztoku není lineární a lze jej určit až do 7 % obsahu methanolu ve směsi [4]. Hašení požárů methanolu vodou je proto neúčinné a může potenciálně vést k přenosu požáru do větších vzdáleností [4]. V oblasti vysokých koncentrací methanolu ve směsi s vodou se hodnoty bodu vzplanutí liší zhruba o 1–2 °C při změnách poměrů koncentrací o 5 % obj. Kolem koncentrace 20 % obj. se začínají projevovat změny v chování směsi a při dalším ředění dochází k výraznému nárůstu teplot vzplanutí. Rozdíly mohou dosahovat až 5–6 °C.

3 Použité metody a materiály pro ověření teplot vzplanutí vodných roztoků methanolu

Pro experimentální stanovení bodu vzplanutí metodou Pensky-Martens byl použit automatický přístroj NPM-440. Hodnoty jsou porovnávány s teplotami vzplanutí získanými prostřednictvím poloautomatického přístroje PMP-4, který byl použit v diplomové práci „Vliv koncentrace směsí methanol a voda na jejich bezpečné používání“ [8]. Použit byl methylalkohol p.a. (99,8 %) společnosti PENTA s.r.o. a demineralizovaná voda, která byla získávána pomocí přístroje AQUAL 29 [9].

Při stanovení teplot vzplanutí různých koncentrací směsí methanol-voda byl použit postup A podle ČSN EN ISO 2719. Podstata zkoušky spočívá v zahřívání určeného množství hořlavé kapaliny ve zkušebním kelímku za stálého míchání a aplikaci zkušebního zapalovacího zařízení ve stanovených intervalech [3].

Podle ČSN EN ISO 2719 musí být při stanovení teplot vzplanutí provedena první aplikace zapalovacího zařízení při teplotě vzorku v rozmezí 23 ± 5 °C pod očekávaným bodem vzplanutí a poté v 1 °C teplotních intervalech [3]. Výsledek není platný, pokud se bod vzplanutí nenachází v intervalu 18 °C až 28 °C nad teplotou první aplikace zapalovacího zařízení [3]. Protože se bod vzplanutí methanolu pohybuje v rozmezí 10 ± 2 °C, musí být u většiny zvolených koncentrací řešen způsob chlazení vzorků. Bez chlazení vzorků je možné stanovit teploty vzplanutí směsí pouze do 25 % obj. methanolu, ostatní zvyšující se koncentrace methanolu ve směsi musí být chlazeny.

V rámci práce byly uvažovány celkem tři způsoby chlazení vzorků. První dva postupy byly inspirovány postupem chlazení podle ČSN EN ISO 13736. Podle této metody je možné vzorky s nízkými teplotami vzplanutí i přístroj podle Abela chladit pomocí externí chladicí lázně. K tomuto účelu byl použit cirkulační chladič JULABO FP50-MA s rozsahem pracovních teplot -50 až 200 °C, který byl naplněn chladicí kapalinou určenou do -20 °C. Třetí postup byl převzat z již zmiňované diplomové práce [8].

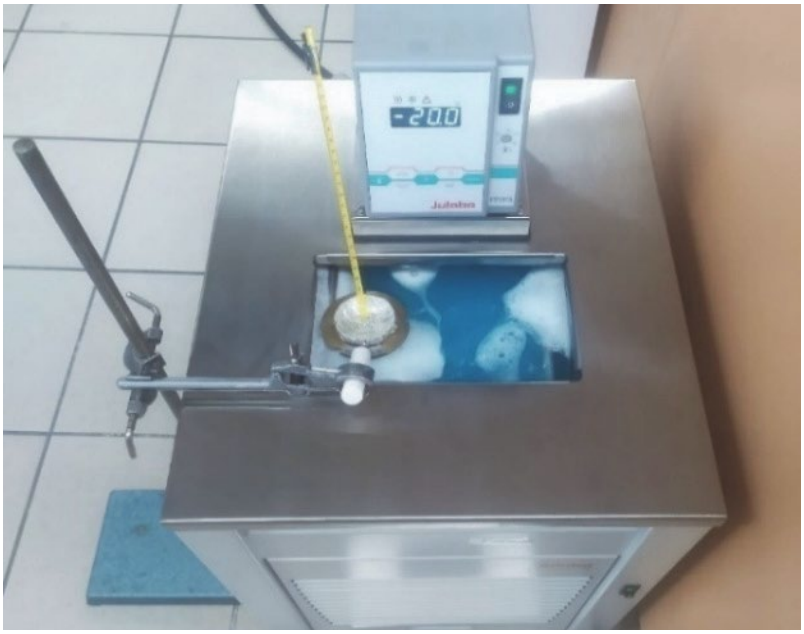
3.1 Využití chladicího okruhu přístroje NPM-440

Přístroj NPM-440 disponuje chladicím okruhem. Zamýšlené použití chladicího okruhu spočívalo v jeho napojení na cirkulační chladič s chladicí kapalinou. Při tomto postupu byl objeven zásadní problém – chladicí okruh přístroje je vybaven automaticky ovládaným ventilem, který se uzavře, pokud je teplota hnízda přístroje v rozmezí od 0–60 °C. Chlazení vzorků pod teplotu nižší než 0 °C tedy není tímto způsobem možné [9].

Popsaný problém lze obejít servisní funkcí přístroje, která umožňuje samostatně kontrolovat správnou funkci jednotlivých komponentů přístroje, včetně otevření daného ventilu. Po konzultaci s odborníkem bylo této možnosti upuštěno, protože dle jeho předchozí zkušenosti vedl tento postup k prasknutí topného hnízda díky velkému rozdílu teplot zahřátého hnízda přístroje a chladicí kapaliny [9].

3.2 Přímé využití cirkulačního chladiče

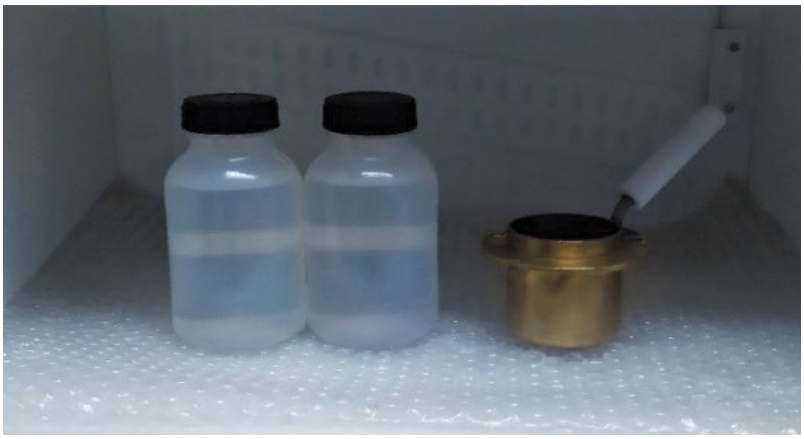
Umístěním vzorků ve zkušebním kelímku přímo v chladicí kapalině uvnitř cirkulačního chladiče bylo možné vzorky chladit velmi rychle až na teplotu -17 °C (Obrázek 3). Nevýhody tohoto způsobu chlazení vzorků však převyšovaly výhodu skrytou v rychlosti chlazení. Experimentálně bylo zjištěno, že tento způsob chlazení vzorků ovlivňuje teploty vzplanutí díky mísení výparů chladicí kapaliny s parami methanolu. Chladicí kapalina je také hořlavá – po ochlazení vzorků bylo nutné zkušební kelímek před vložením do přístroje důkladně otřít. Čištění kelímku bylo nepraktické a vzorek se mimo chladicí lázeň velmi rychle ohříval. Od tohoto postupu bylo upuštěno také z důvodu, že při neúplném očištění kelímku by mohl být potenciálně nebezpečný [9].



Obrázek 3. Chlazení vzorků pomocí cirkulačního chladiče [9]

3.3 Chlazení vzorků v mrazicím boxu

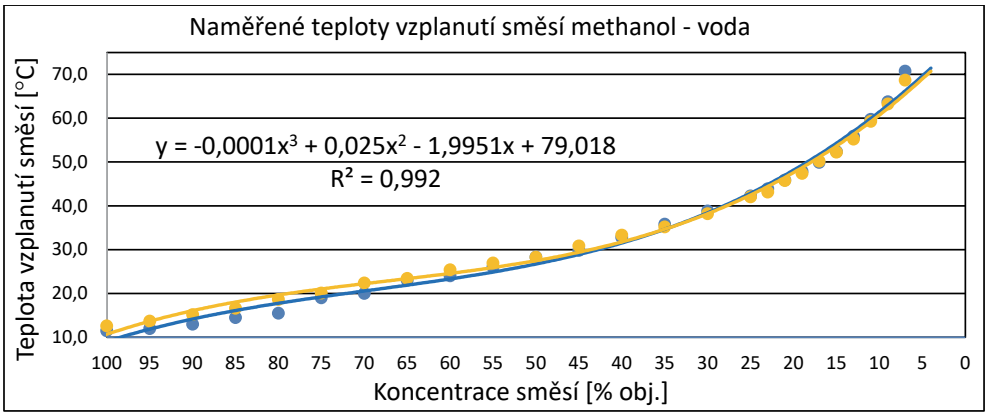
Nejpomalejší, avšak nejspolehlivější byl způsob chlazení vzorků uveden na Obrázku 4. Umístěním vzorků v PET lahvičkách v mrazícím boxu společně se zkušebním kelímkem trvalo ochlazení vzorků na teplotu -12 °C přibližně 1 hodinu. Po ochlazení byly vzorky přelity do zkušebního kelímku. [9]



Obrázek 4. Chlazení vzorků v mrazícím boxu [9]

4 Výsledky měření a jejich vyhodnocení

Celkem bylo proměřeno 26 koncentrací, pro každý vzorek byly provedeny 2 měření. Zjištěné teploty vzplanutí jsou uvedeny na Obrázku 5 společně s hodnotami naměřenými v práci „Vliv koncentrace směsí methanol a voda na jejich bezpečné používání“.

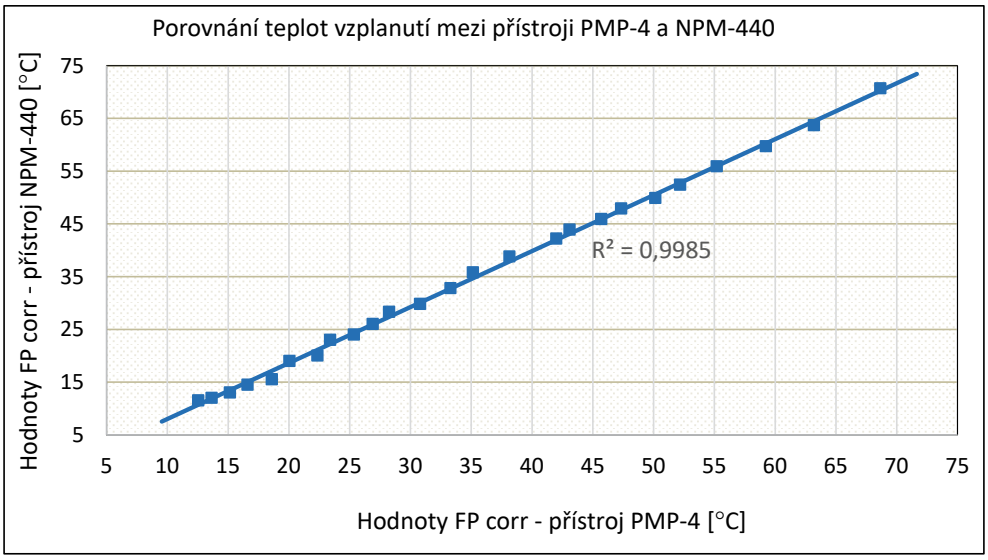


Obrázek 5. Naměřené teploty vzplanutí směsí methanol-voda [9]

Laboratorním měřením byl potvrzen předpoklad, že 7 % obj. koncentrace methanolu má stále definovanou teplotu vzplanutí. Mezi naměřenými výsledky je největší rozdíl 3,1 °C při 80 % obj. koncentrace methanolu [9].

4.1 Výsledky korelační analýzy

Lineární závislost mezi hodnotami teplot vzplanutí získanými prostřednictvím přístrojů NPM-440 a PMP-4 byla vyhodnocena pomocí Pearsonova korelačního koeficientu. Pro provedení korelační analýzy byla použita funkce „CORREL“ programu Excel. Výsledná hodnota r = 0,9992 značí velmi silnou pozitivní korelaci mezi výsledky měření. Vztah mezi hodnotami FP corr naměřenými přístroji NPM 440 a PMP 4 je znázorněn na Obrázku 6. Tento obrázek zobrazuje regresní přímku a koeficient determinace R^2, který doplňuje korelační koeficient r.



Obrázek 6. Porovnání FP corr hodnot mezi přístroji PMP 4 a NPM 440 [9]

Pro porovnání naměřených výsledků získaných přístrojích NPM-440 a PMP-4 jsou použity hodnoty bodu vzplanutí, které jsou přepočteny na standardní atmosférický tlak a nejsou zaokrouhleny na nejbližších 0,5 °C (FP corr). Tyto hodnoty je možné považovat za přesnější. Z pohledu platné legislativy nejsou nezaokrouhlené hodnoty platným výsledkem zkoušky a nejsou tedy použitelné pro klasifikaci nebezpečných látek.

Na základě výsledků analýzy je možné stanovit, že hodnoty teplot vzplanutí získané pomocí obou přístrojů vykazují téměř totožný trend závislosti na koncentraci [9].

4.2 Výsledky studentova testu

Pro porovnání naměřených hodnot byl použit dvouvýběrový párový Studentův t test, který ověřuje, zda se dvě závislá měření statisticky liší. Tento test se běžně využívá k posouzení shody výsledků získaných různými přístroji, pracovníky či laboratořemi [10]. Hladina významnosti byla zvolena $\alpha = 0{,}05$. Použité parametry pro vyhodnocení Studentova testu jsou uvedeny v Tabulce 1. Nulová a alternativní hypotéza byla sestavena následovně:

- H_0: oba přístroje poskytují stejné výsledky teplot vzplanutí;
- H_a: oba přístroje poskytují rozdílné výsledky teplot vzplanutí [9].

Tabulka 1. Parametry pro vyhodnocení Studentova testu [9]

Průměr rozdílu hodnot $\bar{d}$	**Směrodatná odchylka s_d**	**Počet pozorování**	**Stupně volnosti**	**t_{stat}**	**t_{krit}**
0,43	1,22	25	24	1,78	2,06

Při vyhodnocení bylo uvažováno 25 pozorování, protože u 5 % obj. koncentrace methanolu nedošlo ke vzplanutí. Z výsledků je patrné, že $t_{stat} < t_{krit}$, takže se nezamítá nulová hypotéza o shodě výsledků. Studentův test tedy potvrdil, že mezi průměrnými teplotami vzplanutí přepočtenými na standardní tlak není na hladině významnosti $\alpha = 0{,}05$ statisticky významný rozdíl [9].

5 Zařazení směsí methanol-voda do tříd nebezpečnosti

Na základě naměřených hodnot bylo možné zatřídit směsi methanol-voda do tříd nebezpečnosti podle ČSN 65 0201 (Tabulky 2 a 3). I když jsou rozdíly v bodech vzplanutí malé, u některých koncentrací ovlivnily výslednou kategorii – při použití přístroje NPM 440 došlo ke změně třídy u 70 % obj. a 13 % obj. směsi. Tyto rozdíly mohou mít v praxi dopad na požadovaná bezpečnostní opatření. Na rozdíl od klasifikace podle nařízení CLP nejsou koncentrace 7 % obj. a 9 % obj. považovány za hořlavé, protože CLP vychází z limitní teploty vzplanutí 60 °C [12], zatímco ČSN 65 0201 třídí kapaliny podle definovaného bodu vzplanutí. [9]

Tabulka 2. Třídy nebezpečnosti směsí methanol-voda za použití přístroje PMP-4 [8, 11]

Přístroj	**Třída nebezpečnosti**	**Bod vzplanutí [°C]**	**Koncentrace methanolu [%]**
PMP-4	I	≤ 21 °C	100–75
	II	> 21 °C ≤ 55 °C	70–13
	III	> 55 °C ≤ 100 °C	11–7
	IV	> 100 °C	

Tabulka 3. Třídy nebezpečnosti směsí methanol voda za použití přístroje NPM-440 [9, 11]

Přístroj	Třída nebezpečnosti	Bod vzplanutí [°C]	Koncentrace methanolu [%]
NPM-440	I	≤ 21 °C	100–70
	II	> 21 °C ≤ 55 °C	65–15
	III	> 55 °C ≤ 100 °C	13–7
	IV	> 100 °C	

Výsledky roztřízení směsí methanol-voda do tříd nebezpečnosti podle ČSN 65 0201 tak ukazují, že přesnost stanovení bodu vzplanutí a volba použité přístrojové techniky mohou mít praktický dopad klasifikaci a další třízení hořlavých kapalin a následně i na požadavky pro jejich bezpečné používání, skladování a přepravu.

6 Závěr

Výsledky provedených měření potvrdily, že vodné roztoky methanolu si zachovávají definovanou teplotu vzplanutí až do koncentrace 7 % obj. methanolu. Experiment rovněž ukázal, že volba vhodného způsobu chlazení vzorků je zásadní pro dodržení podmínek zkoušky podle ČSN EN ISO 2719. V laboratorních podmínkách se jako nejspolehlivější a současně nejbezpečnější metoda ukázalo chlazení vzorků v mrazicím boxu, zatímco použití chladicího okruhu přístroje či externího cirkulačního chladiče se ukázalo jako nevhodné nebo potenciálně rizikové.

Porovnání teplot vzplanutí získaných na přístrojích NPM 440 a PMP 4 prokázalo velmi vysokou shodu. Pearsonův korelační koeficient r = 0,9992 potvrzuje téměř totožnou odezvu obou přístrojů na změnu koncentrace směsi. Studentův párový t-test dále ukázal, že rozdíly mezi průměrnými hodnotami nejsou statisticky významné na hladině α = 0,05. Přestože jsou rozdíly malé, mohou v některých případech ovlivnit zatřídění směsí do tříd nebezpečnosti podle ČSN 65 0201, což má praktické dopady na požadavky pro jejich bezpečné používání, skladování a přepravu.

Z provedených zkoušek vyplývá, že stanovení bodu vzplanutí je citlivé na řadu faktorů a výsledky je nutné interpretovat s ohledem na podmínky měření i použité zařízení. Správné určení teploty vzplanutí je klíčové nejen pro klasifikaci hořlavých kapalin, ale také pro návrh adekvátních bezpečnostních opatření v praxi.

Reference

[1] Innovation outlook: Renewable methanol [online]. Abu Dhabi: IRENA AND METHANOL INSTITUTE, 2021 [cit. 2023-04-04]. ISBN 978-92-9260-320-5. 38 Dostupné z: https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2021/Jan/IRENA_Innovation_Renewable_Methanol_2021.pdf

[2] Nařízení Komise (ES) č. 440/2008 ze dne 30. května 2008, kterým se stanoví zkušební metody podle nařízení Evropského parlamentu a Rady (ES) č. 1907/2006 o registraci, hodnocení, povolování a omezování chemických látek

[3] ČSN EN ISO 2719. Stanovení bodu vzplanutí v uzavřeném kelímku podle PenskyhoMartense. 4. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017

[4] MEDINA, Enrique, George C. WELLON a Franz EVERGREN. METHANOL SAFE HANDLING MANUAL [online]. 4TH EDITION. Canada: Methanol Institute, 2017 [cit.2023-04-04]. Dostupné z: https://www.methanol.org/wp-content/uploads/2017/03/Safe-Handling-Manual.pdf

[5] EVERGREEN, Franz. ProFLASH: Methanol fire detection and extinguishment. SAFETY & TRANSPORT FIRE RESEARCH [online]. Švédsko: RISE Research Institutes of Sweden, 2017 [cit. 2023-04-04]. ISSN 0284-5172. Dostupné z: http://www.diva-portal.org/smash/get/diva2:1094660/FULLTEXT02.pdf

[6] MERRITT, Carolyn W., John S. BRESLAND, Gary VISSCHER, William WARK a William WRIGHT. Investigation report: Methanol tank explosion and fire [online]. No. 2006-03-I-FL. U.S. CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD: U.S. Chemical safety and hazard investigation board, 2007 [cit. 2023-04-04]. Dostupné z: https://www.csb.gov/assets/1/20/bethune_final_report.pdf?13742

[7] Chamlee, V. (2026, January 2). In 1981, a nearly invisible fire at the Indy 500 led to one of the most dangerous incidents in racing history. People. https://people.com/rick-mears-invisible-fire-indy-500-11870317

[8] KLUZ, Antonín. Vliv koncentrace směsí methanol a voda na jejich bezpečné používání [online]. Ostrava, 2016 [cit. 2022-12-05]. Dostupné z: https://dspace.vsb.cz/handle/10084/114183. Diplomová práce. Vedoucí práce Ing. Hana Věžníková, Ph.D. Vysoká škola báňská - Technická univerzita Ostrava

[9] Pelech, V. Ověření hodnoty bodu vzplanutí směsí metanol–voda [online]. Ostrava, 2023. [cit. 2022-12-05]. Dostupné z: https://dspace.vsb.cz/items/e7aad18e-3b2f-4ddc-9aeb-8a28ad36c194. Bakalářská práce. Vedoucí práce Ing. Hana Věžníková, Ph.D. Vysoká škola báňská - Technická univerzita Ostrava

[10] OTEYPKA, Michal, Pavel BANÁŠ a Eva OTEYPKOVÁ. Základy zpracování dat [online]. Liberec: Technická univerzita v Liberci, 2017, 16.2.2007, 35 [cit. 2023- 03-21]. Dostupné z: https://multiedu.tul.cz/~jiri.rozkovec/ST1/ST1_materialy /UPOL_ST1_2.pdf

[11] ČSN 65 0201. Hořlavé kapaliny – Prostory pro výrobu, skladování a manipulaci. Praha: Český normalizační institut, 2003

[12] Nařízení Evropského parlamentu a Rady (ES) č. 1272/2008 ze dne 16. prosince 2008 o klasifikaci, označování a balení látek a směsí a o změně a zrušení směrnic č. 67/548/EHS, č. 1999/45/ES a o změně nařízení ES č. 1907/2006

Komparatívna analýza súladu vnútroštátnej legislatívy v oblasti kybernetickej bezpečnosti s regulačnými rámcami Európskej únie (NIS2, CER, DORA a AI Act)

Martin Pipíška[1], Katarína Kampová[2]

[1] Žilinská univerzita v Žiline, Fakulta bezpečnostního inžinierstva,
1. mája 32, 010 26 Žilina, m.pipiska@amavex.sk

[2] Žilinská univerzita v Žiline, Fakulta bezpečnostního inžinierstva,
1. mája 32, 010 26 Žilina

Abstrakt:

Článok sa zameriava na komparatívnu analýzu regulačných rámcov Európskej únie v oblasti kybernetickej, prevádzkovej a digitálnej odolnosti smerníc Európskeho parlamentu a Rady (EÚ) 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS2), smernice Európskeho parlamentu a Rady (EÚ) 2022/2557 o odolnosti kritických subjektov (CER), nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora (DORA) a nariadenia (EÚ) 2024/1689 o harmonizovaných pravidlách pre umelú inteligenciu (AI Act) a na ich implementáciu v právnom poriadku Slovenskej republiky. Vychádza z normatívnej a komparatívnej právnej analýzy a posudzuje súlad vnútroštátnej legislatívy, najmä zákona o kybernetickej bezpečnosti č. 366/2024 Z. z. a zákona o kritickej infraštruktúre č. 367/2024 Z. z., s požiadavkami európskych právnych aktov. Cieľom je identifikovať regulačné presahy, rozdiely a aplikačné výzvy vyplývajúce zo súbežného uplatňovania viacerých režimov v základných a kritických sektoroch. Osobitná pozornosť sa venuje postaveniu nariadenia DORA ako lex specialis pre finančný sektor a novému regulačnému rozmeru zavedenému AI Act, ktorý rozširuje koncept odolnosti o algoritmické a rozhodovacie systémy. Výstupom je syntetický prehľad legislatívnych povinností a návrh integrovaného prístupu k riadeniu rizík, governance, kontinuite činností a oznamovaniu incidentov podporujúci koordinovanú implementáciu komplexnej odolnosti v podmienkach Slovenskej republiky.

Kľúčové slová: NIS2, CER, DORA, AI Act, kybernetická a prevádzková odolnosť, vnútroštátna legislatíva.

1 Úvod

Rozsiahla digitalizácia základných a kritických služieb v Európskej únii významne prehĺbila závislosť spoločnosti od prepojených informačných, prevádzkových a rozhodovacích systémov. Tento vývoj zvýšil potrebu posilniť nielen kybernetickú bezpečnosť, ale aj celkovú odolnosť spoločensky nevyhnutných služieb voči širokému spektru hrozieb, od kybernetických incidentov a technologických zlyhaní až po fyzické a organizačné narušenia. V reakcii na tieto riziká Európska únia vytvorila súbor prepojených regulačných rámcov zameraných na systematické zvyšovanie bezpečnosti, stability a krízovej pripravenosti kľúčových subjektov.

Základ predstavuje smernica (EÚ) 2022/2555 (NIS2), ktorá ustanovuje horizontálny rámec riadenia kybernetických rizík, bezpečnostných opatrení a oznamovania incidentov v oblasti sietí a informačných systémov. Tento rámec dopĺňa smernica (EÚ) 2022/2557 o odolnosti kritických subjektov (CER), rozširujúca regulačný pohľad o fyzickú, technickú a organizačnú odolnosť nevyhnutnú pre kontinuitu základných služieb. Obe smernice sledujú spoločný cieľ ochrany kritických funkcií, avšak líšia sa rozsahom a predmetom regulácie [6, 7, 4].

Vo finančnom sektore sa uplatňuje osobitný režim lex specialis podľa nariadenia (EÚ) 2022/2554 (DORA), ktoré zavádza jednotné požiadavky na riadenie ICT rizík, testovanie digitálnej odolnosti, dohľad nad tretími stranami a harmonizovaný reporting incidentov. V oblastiach detailnej úpravy má tento režim prednosť pred všeobecným rámcom NIS2 [8].

Regulačný ekosystém dopĺňa nariadenie o umelej inteligencii (AI Act), ktoré zavádza rizikovo orientovaný rámec pre vývoj a používanie AI systémov. Rozširuje koncept odolnosti o riadenie algoritmických a rozhodovacích rizík, najmä tam, kde AI ovplyvňuje bezpečnosť, základné práva alebo poskytovanie kritických služieb.

Slovenská republika transponovala smernice NIS2 a CER novelou zákona o kybernetickej bezpečnosti č. 366/2024 Z. z. a prijatím zákona o kritickej infraštruktúre č. 367/2024 Z. z., účinných od 1. januára 2025. Spolu s priamo uplatniteľným nariadením DORA a povinnosťami vyplývajúcimi z AI Act vytvárajú tieto akty komplexný regulačný rámec, ktorý zásadne ovplyvňuje fungovanie organizácií v regulovaných sektoroch v Slovenskej republike [8–10].

Cieľom článku je komparatívne analyzovať obsah, pôsobnosť a aplikačné dopady uvedených rámcov, identifikovať ich vzájomné presahy a potenciálne kolízie a formulovať odporúčania pre ich koordinované zosúladenie v podmienkach Slovenskej republiky, so zohľadnením kybernetickej, prevádzkovej a algoritmickej odolnosti [4].

2 Ciele a rozsah článku

Cieľom článku je analyzovať a porovnať európske regulačné rámce NIS2, CER a DORA so slovenskou implementáciou, konkrétne novelizovaným zákonom o kybernetickej bezpečnosti č. 366/2024 Z. z. a zákonom o kritickej infraštruktúre č. 367/2024 Z. z., a identifikovať praktické povinnosti vyplývajúce od roku 2025 pre organizácie pôsobiace v základných a kritických sektoroch Slovenskej republiky [6–10, 4].

Pozornosť sa nesústredí len na normatívny opis rámcov, ale predovšetkým na ich organizačné a prevádzkové implikácie, najmä v oblastiach riadenia rizík, governance, kontinuity činností, oznamovania incidentov a výkonu dohľadu. Osobitne sú analyzované situácie súbežnej pôsobnosti viacerých režimov (napr. NIS2 a CER, resp. NIS2 a DORA), ktoré v aplikačnej praxi zvyšujú nároky na koordináciu bezpečnostných a compliance procesov.

Súčasťou analýzy je aj nariadenie o umelej inteligencii (AI Act) ako nový regulačný prvok rozširujúci rámec odolnosti o algoritmické a rozhodovacie systémy. Skúma sa jeho prepojenie s požiadavkami NIS2, CER a DORA, najmä v oblastiach governance, riadenia rizík, dohľadu nad dodávateľským reťazcom a oznamovania závažných incidentov.

Analytický rámec vychádza zo štyroch kľúčových právnych aktov EÚ. Smernice NIS2 ako horizontálneho rámca kybernetickej bezpečnosti, smernice CER zameranej na komplexnú odolnosť kritických subjektov, nariadenia DORA ako sektorového režimu digitálnej odolnosti finančného sektora a AI Act ako rámca regulácie vysokorizikových AI systémov [6–10].

Hlavné výskumné ciele článku sú:

- rozlíšiť koncept kybernetickej bezpečnosti podľa NIS2/ZoKB a komplexnej odolnosti podľa CER/KI z hľadiska pôsobnosti a rozsahu povinností,
- identifikovať regulačné presahy medzi NIS2 a CER a ich dôsledky pre integrované riadenie rizík, kontinuitu a dohľad,

- analyzovať postavenie DORA ako lex specialis, najmä v oblastiach TPRM, TLPT a harmonizovaného reportingu,
- preskúmať AI Act ako nový rozmer algoritmickej odolnosti a jeho väzby na existujúce rámce,
- navrhnúť minimálny integrovaný compliance rámec mapujúci kľúčové povinnosti a dohľadové mechanizmy.

Metodologicky článok využíva komparatívnu právnu analýzu doplnenú o mapovanie regulačných povinností vo vybraných sektoroch (energetika, zdravotníctvo, telekomunikácie, verejná správa, finančný sektor). Komparačné tabuľky slúžia na identifikáciu rozdielov v požiadavkách na governance, riadenie rizík, kontinuitu, incident reporting, dodávateľský dohľad a testovanie odolnosti [4, 9, 10].

Prínos článku spočíva vo formulovaní integrovaného pohľadu na kybernetickú, prevádzkovú a algoritmickú odolnosť a v návrhu praktického rámca pre zosúladenie compliance povinností v prostredí narastajúcej regulačnej komplexity.

3 Teoretický rámec a základné pojmy

Kybernetická bezpečnosť predstavuje súbor technických, organizačných a procesných opatrení zameraných na ochranu sietí, informačných systémov a prevádzkovej technológie (OT) pred incidentmi, ktoré môžu ohroziť dôvernosť, integritu a dostupnosť údajov a služieb. Jej cieľom je zabezpečiť spoľahlivé fungovanie digitálnych infraštruktúr nevyhnutných pre chod štátu, hospodárstva a spoločnosti.

Základným regulačným rámcom EÚ v tejto oblasti je smernica (EÚ) 2022/2555 (NIS2), ktorá ustanovuje povinnosti pre základné a dôležité subjekty v oblasti riadenia kybernetických rizík, implementácie bezpečnostných opatrení a oznamovania incidentov. Vytvára horizontálny, rizikovo orientovaný rámec uplatniteľný naprieč sektormi [6].

Smernica (EÚ) 2022/2557 (CER) rozširuje perspektívu ochrany na komplexnú odolnosť kritických subjektov. Zahŕňa nielen digitálne, ale aj fyzické, organizačné a personálne aspekty poskytovania základných služieb, ktorých narušenie by malo závažný spoločenský alebo hospodársky dopad. Kybernetická bezpečnosť tu predstavuje jednu z dimenzií širšieho systému odolnosti zahŕňajúceho kontinuitu činností, krízové riadenie a ochranu dodávateľských reťazcov [7].

Tento prístup zodpovedá modelu tzv. comprehensive resilience, v ktorom sa technické, prevádzkové a organizačné opatrenia integrujú do jednotného rámca ochrany kritických služieb [4].

Osobitný sektorový režim predstavuje nariadenie (EÚ) 2022/2554 (DORA), ktoré ako lex specialis pre finančný sektor špecifikuje požiadavky riadenia ICT rizík. Zavádza povinné testovanie digitálnej odolnosti vrátane Threat-Led Penetration Testing (TLPT), rozšírený dohľad nad poskytovateľmi ICT služieb a harmonizovaný reporting incidentov s cieľom minimalizovať systémové dopady narušení na finančný trh EÚ [8].

Regulačný rámec dopĺňa nariadenie o umelej inteligencii (AI Act), ktoré zavádza rizikovo orientovaný režim pre vývoj a používanie AI systémov. Rozširuje koncept odolnosti o algoritmické a rozhodovacie systémy a ustanovuje povinnosti v oblastiach governance, dokumentácie, riadenia rizík, ľudského dohľadu a post-deployment monitoringu. Vysokorizikové AI systémy podliehajú osobitnému režimu s cieľom zabezpečiť ochranu bezpečnosti, základných práv a kontinuity služieb.

V aplikačnej praxi sa rámce NIS2, CER, DORA a AI Act významne prelínajú. Kritické sektory často podliehajú súbežne viacerým režimom, čo zvyšuje nároky na koordináciu bezpečnostných a compliance procesov. Výsledkom je potreba integrovaného prístupu prepájajúceho kybernetické, prevádzkové a algoritmické opatrenia do jednotného systému riadenia rizík [4].

Tabuľka 1. Pojmové vymedzenie bezpečnosti a odolnosti v rámcoch EÚ [autor]

Rámec	Primárny objekt ochrany	Typ rizika	Charakter regulácie
NIS2	Siete a informačné systémy	Kybernetické riziká	Horizontálny
CER	Základné a kritické služby	Prevádzkové a systémové riziká	Horizontálny
DORA	Finančné procesy a ICT	Digitálne a systémové riziká	Sektorový (lex specialis)
AI Act	AI a rozhodovacie systémy	Algoritmické a modelové riziká	Horizontálny (rizikový)

4 Normatívny rámec Európskej únie

Normatívny rámec Európskej únie v oblasti kybernetickej, prevádzkovej a digitálnej odolnosti je tvorený súborom prepojených právnych aktov zameraných na ochranu a kontinuitu poskytovania základných a kritických služieb v digitálne prepojenej spoločnosti. Jeho jadro tvoria smernice (EÚ) 2022/2555 (NIS2) a 2022/2557 (CER) a nariadenie (EÚ) 2022/2554 (DORA), doplnené nariadením o umelej inteligencii (AI Act) ako regulačnou vrstvou zameranou na algoritmické a rozhodovacie systémy [6–8].

Smernica NIS2 predstavuje horizontálny legislatívny rámec kybernetickej bezpečnosti pre základné a dôležité subjekty v kľúčových sektoroch hospodárstva a verejnej správy. Ustanovuje povinnosti v oblasti riadenia kybernetických rizík, implementácie technických a organizačných opatrení, zodpovednosti vrcholového manažmentu a harmonizovaného hlásenia incidentov. Súčasťou rámca je aj zosilnený dohľad a sankčný mechanizmus s cieľom dosiahnuť jednotnú úroveň ochrany v rámci EÚ [6].

Smernica CER rozširuje regulačný pohľad nad rámec kybernetickej bezpečnosti a zavádza komplexný prístup k odolnosti kritických subjektov v sektoroch, ako sú energetika, doprava, zdravotníctvo či digitálna infraštruktúra. Vyžaduje systematické hodnotenie rizík, zavedenie mechanizmov business continuity managementu, krízového riadenia a pravidelné testovanie pripravenosti. Kybernetická bezpečnosť je v tomto kontexte jednou z dimenzií širšieho systému prevádzkovej odolnosti [7].

Tretí pilier predstavuje nariadenie DORA, priamo uplatniteľné vo všetkých členských štátoch, ktoré zavádza sektorový režim digitálnej prevádzkovej odolnosti finančného sektora. Upravuje riadenie ICT rizík, povinné testovanie odolnosti vrátane Threat-Led Penetration Testing (TLPT), riadenie rizík tretích strán (TPRM) a harmonizovaný reporting incidentov. Súčasťou rámca je aj dohľad nad kritickými poskytovateľmi ICT služieb, reflektujúci koncentráciu technologických rizík [8].

Regulačný systém dopĺňa AI Act, ktorý zavádza jednotný rámec pre vývoj a používanie systémov umelej inteligencie na základe rizikovo orientovaného prístupu. Osobitne reguluje vysokorizikové AI systémy a ustanovuje povinnosti v oblasti governance, dokumentácie, ľudského dohľadu, monitorovania po nasadení a oznamovania závažných incidentov. Tým rozširuje existujúce rámce o reguláciu algoritmických a rozhodovacích rizík.

Uvedené právne akty vytvárajú viacvrstvový, funkčne previazaný regulačný systém. NIS2 ako horizontálny rámec kybernetickej bezpečnosti, CER ako rámec komplexnej prevádzkovej odolnosti, DORA ako sektorový režim pre finančný trh a AI Act ako reguláciu algoritmickej odolnosti. Ich spoločným menovateľom je dôraz na prevenciu, riadenie rizík, zodpovednosť manažmentu a koordinovanú reakciu na incidenty v prostredí digitálnej a kritickej infraštruktúry [4].

Tabuľka 2. Porovnanie základných právnych aktov EÚ v oblasti odolnosti [autor]

Právny akt	**Typ regulácie**	**Primárny cieľ**	**Oblasť pôsobnosti**
NIS2	Smernica (horizontálna)	Kybernetická bezpečnosť	Základné a dôležité subjekty
CER	Smernica (horizontálna)	Prevádzková a fyzická odolnosť	Kritické subjekty
DORA	Nariadenie (sektorové)	Digitálna prevádzková odolnosť	Finančný sektor
AI Act	Nariadenie (rizikové)	Algoritmická a rozhodovacia odolnosť	AI systémy v EÚ

5 Národná transpozícia legislatívy EÚ

Slovenská republika transponovala požiadavky smerníc NIS2 a CER do vnútroštátneho právneho poriadku prostredníctvom dvoch kľúčových právnych predpisov účinných od 1. januára 2025: novely zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti vykonanej zákonom č. 366/2024 Z. z. a zákona č. 367/2024 Z. z. o kritickej infraštruktúre. Gestorom kybernetickej bezpečnosti je Národný bezpečnostný úrad, zatiaľ čo dohľad nad kritickou infraštruktúrou vykonáva Ministerstvo vnútra SR [9, 10]. Spolu s priamo uplatniteľným nariadením DORA tvoria tieto predpisy základ národného rámca kybernetickej a prevádzkovej odolnosti.

Implementácia smernice NIS2 prostredníctvom novely zákona o kybernetickej bezpečnosti rozšírila vecnú pôsobnosť regulácie a zaviedla kategorizáciu subjektov na základné a dôležité, reflektujúc ich význam pre fungovanie štátu a hospodárstva. Posilnila sa zodpovednosť štatutárnych orgánov, čím sa riadenie kybernetických rizík presunulo na úroveň strategického riadenia. Novela zároveň zaviedla centrálny register regulovaných subjektov a spresnila mechanizmy a lehoty hlásenia incidentov, čo podporuje koordináciu dohľadu a výmenu informácií [9].

Zákon o kritickej infraštruktúre implementujúci smernicu CER zavádza komplexný prístup k identifikácii kritických subjektov a k riadeniu ich odolnosti. Dôraz sa kladie na systematické hodnotenie rizík, plánovanie kontinuity činností, krízové riadenie a pravidelné testovanie pripravenosti voči fyzickým, technickým aj organizačným narušeniam. Koordinačnú úlohu zabezpečuje Ministerstvo vnútra SR v spolupráci so sektorovými orgánmi [10].

Primárnu legislatívu dopĺňajú vykonávacie predpisy Národného bezpečnostného úradu účinné od 1. septembra 2025. Vyhláška č. 227/2025 Z. z. konkretizuje bezpečnostné opatrenia vrátane ochrany OT systémov a vyhláška č. 226/2025 Z. z. upravuje kategorizáciu incidentov, lehoty a formálne náležitosti oznamovania [15, 16]. Regulačnú kontinuitu zabezpečujú aj staršie predpisy upravujúce audit, odborné štandardy a činnosť CSIRT jednotiek [11–14].

Na rozdiel od smerníc NIS2 a CER je AI Act priamo uplatniteľným nariadením, nevyžadujúcim transpozíciu. Jeho praktická aplikácia si však vyžiada vytvorenie vnútroštátnych dohľadových mechanizmov a koordináciu s existujúcimi režimami, najmä v oblastiach governance, riadenia rizík, dodávateľského dohľadu a incident reporting.

Výsledný legislatívny rámec vytvára v Slovenskej republike komplexný systém pokrývajúci identifikáciu regulovaných subjektov, riadenie rizík, implementáciu bezpečnostných opatrení, oznamovanie incidentov a výkon dohľadu. Národná implementácia tak predstavuje nielen splnenie transpozičných povinností, ale aj kvalitatívny posun v riadení bezpečnosti a odolnosti [4].

Tabuľka 3. Mapovanie európskych právnych aktov na národnú implementáciu v SR [autor]

Právny akt EÚ	Forma v SR	Gestor / dohľad
NIS2	Zákon č. 366/2024 Z. z. (ZoKB)	Národný bezpečnostný úrad
CER	Zákon č. 367/2024 Z. z. (KI)	Ministerstvo vnútra SR
DORA	Priama uplatniteľnosť	NBS / sektorové orgány
AI Act	Priama uplatniteľnosť	Určovaný vnútroštátny orgán

6 Komparatívna analýza prístupov EÚ a SR

Komparatívna analýza rámcov NIS2/ZoKB, CER/KI a DORA poukazuje na vysokú mieru ich vzájomného presahu, najmä v sektoroch poskytujúcich základné a kritické služby, ako sú energetika, doprava, zdravotníctvo, vodné hospodárstvo či digitálna infraštruktúra. Subjekty pôsobiace v týchto oblastiach často podliehajú viacerým regulačným režimom súčasne, čo vedie ku kumulácii povinností v oblasti riadenia rizík, bezpečnostných opatrení a incident reportingu [6, 7].

Rámec NIS2, transponovaný zákonom o kybernetickej bezpečnosti, sa zameriava predovšetkým na ochranu sietí, informačných systémov a prevádzkovej technológie. Naopak rámec CER, implementovaný zákonom o kritickej infraštruktúre, rozširuje regulačný pohľad o fyzické, organizačné a prevádzkové aspekty odolnosti vrátane kontinuity činností, krízového riadenia a ochrany dodávateľských reťazcov. Ide o funkčne komplementárne prístupy, ktoré spolu vytvárajú širší model ochrany základných služieb [6, 7].

Z aplikačného hľadiska to vytvára potrebu integrovaného prístupu k bezpečnosti prepájajúceho kybernetické, prevádzkové a organizačné opatrenia do jednotného systému riadenia rizík. Tento posun smerom k modelu comprehensive resilience predpokladá zosúladenie riadiacich štruktúr, metodík hodnotenia rizík a bezpečnostnej dokumentácie využiteľnej pre audit a dohľad [4].

Vo finančnom sektore sa uplatňuje nariadenie DORA ako režim lex specialis vo vzťahu k NIS2. V oblastiach podrobnejšej úpravy majú jeho ustanovenia prednosť, pričom rozširujú základné princípy kybernetickej bezpečnosti o sektorovo špecifické požiadavky, najmä v oblastiach riadenia rizík tretích strán (TPRM), Threat-Led Penetration Testing (TLPT), evidencie zmluvných vzťahov a harmonizovaného reportingu incidentov [8].

Z normatívneho hľadiska tak rámce NIS2, CER a DORA vytvárajú viacvrstvový regulačný systém, horizontálny základ kybernetickej bezpečnosti, rozšírenie na prevádzkovú odolnosť a sektorovú špecializáciu pre finančný trh. Ich spoločným cieľom je posilniť prevenciu, riadenie rizík a reakciu na incidenty v prostredí kritickej infraštruktúry [4].

Do tohto ekosystému vstupuje AI Act, ktorý dopĺňa existujúce režimy o reguláciu algoritmických a rozhodovacích rizík. Nenahrádza NIS2, CER ani DORA, ale rozširuje ich o nový typ hrozby, modelové a algoritmické zlyhania s potenciálnym dopadom na bezpečnosť, kontinuitu služieb a základné práva. Zavádza povinnosti v oblasti governance, dokumentácie, ľudského dohľadu a monitorovania AI systémov, pričom sa v praxi prelína najmä s požiadavkami NIS2 a DORA.

Tabuľka 4. Komparácia regulačných rámcov NIS2, CER, DORA a AI Act [autor]

Kritérium	**NIS2/ZoKB**	**CER/KI**	**DORA**	**AI Act**
Typ regulácie	Horizontálna	Horizontálna	Sektorová (lex specialis)	Horizontálna (riziková)
Primárny cieľ	Kybernetická bezpečnosť	Prevádzková a fyzická odolnosť	Digitálna prevádzková odolnosť	Algoritmická a rozhodovacia odolnosť
Objekt ochrany	Siete a IS	Základné služby	Finančné procesy a ICT	AI systémy
Riadenie rizík	ICT riziká	Multidimenzionálne riziká	ICT a TPRM	Modelové a systémové riziká
Incident reporting	Povinný, presné lehoty	Bez zbytočného odkladu	Harmonizovaný	Závažné incidenty a poruchy

Tabuľka 5. Praktické implikácie pre organizácie v SR [autor]

Oblasť	**NIS2/ZoKB**	**CER/KI**	**DORA**	**AI Act**
Governance	Zodpovednosť vedenia	Zodpovednosť prevádzky	Zodpovednosť vedenia	Zodpovednosť za AI systémy
Kontinuita činností	ICT kontinuita	BCM a krízové plány	Digitálna kontinuita	Spoľahlivosť rozhodovania
Dodávateľský reťazec	ICT dodávatelia	Kritickí dodávatelia	Kritickí ICT poskytovatelia	AI modely a poskytovatelia
Testovanie	Technické testy	Cvičenia	TLPT	Validácia a monitoring
Dohľad	NBÚ	MV SR	NBS/EÚ orgány	Určený AI orgán

Komparatívna analýza potvrdzuje, že rámce NIS2, CER, DORA a AI Act smerujú k vytvoreniu integrovaného európskeho systému riadenia rizík a odolnosti, v ktorom sa horizontálne a sektorové nástroje navzájom dopĺňajú. Pre Slovenskú republiku z toho vyplýva potreba harmonizovanej implementácie, najmä zosúladenia terminológie, interných procesov a dohľadových mechanizmov s cieľom minimalizovať duplicity a zvýšiť efektívnosť bezpečnostného riadenia.

Kľúčovým aplikačným záverom je potreba prechodu od izolovaného plnenia jednotlivých regulačných povinností k integrovanému compliance modelu prepájajúcemu kybernetickú, prevádzkovú a algoritmickú odolnosť.

7 Stav riešenia problematiky v SR

Od roku 2025 sú organizácie pôsobiace v Slovenskej republike povinné zosúladiť svoje vnútorné procesy, riadiace mechanizmy a bezpečnostné opatrenia s požiadavkami vyplývajúcimi z novely zákona o kybernetickej bezpečnosti č. 366/2024 Z. z., zákona o kritickej infraštruktúre č. 367/2024 Z. z. a priamo uplatniteľného nariadenia DORA. Praktické dopady sa koncentrujú najmä do oblastí riadenia rizík, incident reportingu, auditu, kontinuity činností a dohľadu nad dodávateľským reťazcom v oblasti ICT [8–10].

Kľúčovým vykonávacím predpisom pre oznamovanie incidentov je vyhláška NBÚ č. 226/2025 Z. z., ktorá definuje kategórie incidentov, lehoty hlásenia a zavádza aj reporting tzv. near-miss udalostí, identifikujúcich významné zraniteľnosti bez priameho dopadu [15]. Organizácie sú povinné viesť systematické záznamy o hrozbách, incidentoch a prijatých opatreniach, čo zvyšuje nároky na interné evidenčné a analytické kapacity.

Oznamovacie povinnosti podľa ZoKB sa prelínajú s reportingom podľa DORA a perspektívne aj s požiadavkami AI Act, čím vzniká potreba koordinovaného incident managementu naprieč regulačnými režimami.

Technické a organizačné opatrenia konkretizuje vyhláška NBÚ č. 227/2025 Z. z., ktorá rozširuje bezpečnostné požiadavky aj na prevádzkovú technológiu (OT) a ustanovuje minimálny rozsah opatrení v oblastiach riadenia rizík, správy prístupov, segmentácie sietí, kontinuity prevádzky a testovania odolnosti [16]. Povinnou súčasťou bezpečnostnej dokumentácie sú najmä bezpečnostná politika, plán reakcie na incidenty, register aktív a hodnotenie rizík.

Audit kybernetickej bezpečnosti sa vykonáva podľa vyhlášky NBÚ č. 493/2022 Z. z., pričom odborné predpoklady audítorov upravuje vyhláška č. 492/2022 Z. z. Tieto predpisy zabezpečujú jednotnú metodiku auditu, no zároveň zvyšujú nároky na dostupnosť kvalifikovaných odborníkov, najmä pre menšie organizácie [13, 14].

Rámec kritickej infraštruktúry kladie dôraz na zavedenie Business Continuity Managementu a krízového riadenia. Kritické subjekty sú povinné identifikovať závislosti, vypracovať plány kontinuity a obnovy a pravidelne testovať ich funkčnosť prostredníctvom cvičení [10]. Oznamovanie narušení poskytovania základných služieb Ministerstvu vnútra SR predstavuje ďalší reportingový kanál, ktorý je potrebné zosúladiť s režimami ZoKB a DORA.

Vo finančnom sektore prináša DORA nové povinnosti v oblastiach evidencie ICT zmlúv, riadenia rizík tretích strán (TPRM) a testovania digitálnej odolnosti prostredníctvom TLPT. Harmonizovaný reporting podľa regulačných technických štandardov predstavuje formalizovanejší režim dohľadu v porovnaní so ZoKB [8].

AI Act, hoci nevyžaduje transpozíciu, bude vyžadovať vytvorenie vnútroštátnych dohľadových mechanizmov a zavedenie procesov klasifikácie AI rizík, dokumentácie, ľudského dohľadu a monitorovania systémov. Jeho požiadavky sa budú prelínať najmä s governance, dodávateľským dohľadom a incident reportingom.

Tabuľka 6. Prehľad aplikačných povinností v SR od roku 2025 [autor]

Oblasť	**ZoKB/NIS2**	**CER/KI**	**DORA**	**AI Act**
Incident reporting	Presné lehoty, near-miss	Bez zbytočného odkladu	Harmonizovaný	Závažné incidenty
Riadenie rizík	ICT riziká	Multidimenzionálne	ICT + TPRM	Modelové riziká
Kontinuita	ICT kontinuita	BCM, krízové plány	Digitálna kontinuita	Spoľahlivosť rozhodovania
Audit / dohľad	NBÚ	MV SR	NBS/EÚ orgány	AI dohľadový orgán
Dokumentácia	Bezpečnostná dokumentácia	Program odolnosti	Registre, RTS/ITS	Technická a governance dokumentácia

Z hodnotiaceho hľadiska Slovenská republika od roku 2025 disponuje robustným legislatívnym základom pre implementáciu európskych rámcov odolnosti. Súčasne však rastie komplexita compliance povinností, čo si vyžaduje prechod od izolovaného plnenia regulačných požiadaviek k integrovanému modelu riadenia bezpečnosti a odolnosti na úrovni organizácií [4].

8 Odporúčania pre aplikačnú prax

Komparatívna analýza rámcov NIS2, CER, DORA a AI Act poukazuje na potrebu integrovaného prístupu k riadeniu rizík a odolnosti na úrovni celej organizácie. Fragmentácia bezpečnostných zodpovedností medzi IT, OT, prevádzku, compliance a manažment vedie k duplicitám a neúplnému obrazu o rizikovom profile. Odporúča sa preto zaviesť jednotný rámec riadenia rizík prepájajúci kybernetické, prevádzkové, fyzické aj algoritmické aspekty odolnosti [3, 4].

Základným nástrojom je integrovaný register rizík zahŕňajúci technické, fyzické aj modelové hrozby súvisiace s AI. Register má byť previazaný s hodnotením dopadov, plánmi kontinuity činností (BCM) a procesmi reakcie na incidenty, čím umožňuje auditovateľné riadenie rizík naprieč regulačnými režimami [4].

Kľúčové je aj vytvorenie koordinovaného systému oznamovania incidentov reflektujúceho požiadavky NIS2, CER, DORA a AI Act. Organizácie by mali zaviesť jednotný interný incident management, z ktorého sa generujú hlásenia pre jednotlivé orgány dohľadu. Efektívnosť zvyšuje využívanie štandardizovaných formulárov, spoločných dátových štruktúr a automatizovaných rozhraní (API) [15, 16].

Osobitná pozornosť má byť venovaná dodávateľskému reťazcu, najmä v oblastiach ICT, cloudových služieb, OT a AI systémov. Zmluvy a SLA by mali reflektovať požiadavky na bezpečnosť, dostupnosť, oznamovanie incidentov a práva na audit. Hoci je takýto prístup povinný najmä podľa DORA, jeho uplatnenie je vhodné aj v ostatných regulovaných sektoroch [8].

Kritickým faktorom implementácie je aktívne zapojenie vrcholového manažmentu. NIS2, DORA aj AI Act explicitne zdôrazňujú zodpovednosť vedenia za dohľad nad odolnosťou organizácie, čo si vyžaduje systematické vzdelávanie a zvyšovanie regulačného povedomia [6, 4].

Tabuľka 7. Odporúčania pre aplikačnú prax v kontexte NIS2, CER, DORA a AI Act [autor]

Oblasť	**Odporúčanie**	**Relevantné rámce**
Riadenie rizík	Integrovaný register rizík (ICT, fyzické, AI)	NIS2, CER, DORA, AI Act
Kontinuita činností	Prepojenie BCM, IT/OT a AI procesov	CER, DORA
Incident management	Jednotný proces + koordinovaný reporting	NIS2, DORA, AI Act
Dodávateľský reťazec	SLA, auditovateľnosť, TPRM	DORA, NIS2, AI Act
Governance	Aktívny dohľad manažmentu	NIS2, DORA, AI Act
Kompetencie	Systematické vzdelávanie vedenia	NIS2, CER

Uvedené opatrenia smerujú k vytvoreniu integrovaného compliance a resilience modelu umožňujúceho zosúladenie požiadaviek analyzovaných rámcov. Kľúčovým posolstvom je prechod od formálneho plnenia povinností k strategickému riadeniu odolnosti ako kontinuálneho procesu zahŕňajúceho technické, organizačné aj rozhodovacie dimenzie bezpečnosti [4].

9 Záver

Od 1. januára 2025 má Slovenská republika transponované smernice NIS2 a CER prostredníctvom novely zákona o kybernetickej bezpečnosti č. 366/2024 Z. z. a zákona o kritickej infraštruktúre č. 367/2024 Z. z., doplnených vykonávacími vyhláškami NBÚ č. 226/2025 Z. z. o hláseniach a č. 227/2025 Z. z. o bezpečnostných opatreniach. Spolu s priamo uplatniteľným nariadením DORA tak vznikol komplexný vnútroštátny rámec kybernetickej a prevádzkovej odolnosti subjektov poskytujúcich základné a kritické služby.

Analýza potvrdila, že napriek formálnemu splneniu transpozičných povinností zostáva kľúčovou výzvou koordinácia viacerých regulačných režimov. Rámce NIS2/ZoKB, CER/KI a DORA sa prelínajú najmä v oblastiach riadenia rizík, incident reportingu, kontinuity činností a dohľadu, čo bez integrovaného prístupu vedie k duplicite povinností a fragmentácii bezpečnostných procesov.

Osobitné postavenie má nariadenie DORA ako lex specialis pre finančný sektor, ktoré sprísňuje požiadavky na riadenie ICT rizík, testovanie odolnosti a dohľad nad dodávateľským reťazcom, čím zvyšuje nároky na regulované subjekty aj dohľadové kapacity.

Rastúci význam nadobúda aj AI Act, ktorý rozširuje existujúce rámce o reguláciu algoritmických a rozhodovacích systémov. Prepojením s požiadavkami NIS2 a DORA posúva koncept odolnosti od ochrany technických infraštruktúr k ochrane rozhodovacích procesov v regulovaných sektoroch.

Úspech implementácie európskeho rámca odolnosti v Slovenskej republike preto nebude závisieť len od legislatívnej pripravenosti, ale najmä od koordinácie dohľadových orgánov, regulovaných subjektov a sektorov, od zdieľania informácií a od budovania jednotnej kultúry bezpečnosti. Integrovaný prístup k riadeniu kybernetickej, prevádzkovej a algoritmickej odolnosti predstavuje kľúčový predpoklad dlhodobej stability základných a kritických služieb.

Reference

[1] BERMAN, D., BUCZAK, A., CHAVIS, J., CORBETT, C., A survey of deep learning methods for cyber security. IEEE Communications Surveys & Tutorials, 2019. DOI: 10.1109/COMST.2019.2892762

[2] CONTI, M., DEHGHANTANHA, A., FRANKE, K., WATSON, S., Cyber Threat Intelligence: Challenges and Opportunities., Springer International Publishing, 2017

[3] CONTI, M., DEHGHANTANHA, A., FRANKE, K., WATSON, S., Cybersecurity and digital forensics: Challenges and opportunities., IEEE Computer, vol. 50, no. 12, pp. 14–17, 2017

[4] ENISA., Mapping of Security Requirements under NIS2, CER, and DORA., European Union Agency for Cybersecurity, 2023., Dostupné z: https://www.enisa.europa.eu

[5] ENISA., Good practices for cyber crisis management, European Union Agency for Cybersecurity, 2023., Dostupné z: https://www.enisa.europa.eu

[6] EUROPEAN PARLIAMENT AND THE COUNCIL., Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2)., Official Journal of the European Union, 2022., Dostupné z: https://eur-lex.europa.eu/eli/dir/2022/2555

[7] EUROPEAN PARLIAMENT AND THE COUNCIL., Directive (EU) 2022/2557 on the resilience of critical entities (CER)., Official Journal of the European Union, 2022., Dostupné z: https://eur-lex.europa.eu/eli/dir/2022/2557

[8] EUROPEAN PARLIAMENT AND THE COUNCIL., Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)., Official Journal of the European Union, 2022, Dostupné z: https://eur-lex.europa.eu/eli/reg/2022/2554

[9] NÁRODNÁ RADA SLOVENSKEJ REPUBLIKY., Zákon č. 366/2024 Z. z., ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti., Bratislava: NR SR, 2024

[10] NÁRODNÁ RADA SLOVENSKEJ REPUBLIKY., Zákon č. 367/2024 Z. z. o kritickej infraštruktúre, Bratislava: NR SR, 2024

[11] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD., Vyhláška č. 164/2018 Z. z. o kritériách určovania základnej služby, NBÚ SR, 2018

[12] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD., Vyhláška č. 166/2018 Z. z. o činnosti jednotiek CSIRT., NBÚ SR, 2018

[13] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD., Vyhláška č. 493/2022 Z. z. o audite kybernetickej bezpečnosti., NBÚ SR, 2022

[14] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD., Vyhláška č. 492/2022 Z. z. o znalostných štandardoch odborníkov v oblasti kybernetickej bezpečnosti, NBÚ SR, 2022

[15] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD., Vyhláška č. 226/2025 Z. z. o hláseniach a oznamovacích povinnostiach, NBÚ SR, 2025

[16] NÁRODNÝ BEZPEČNOSTNÝ ÚRAD., Vyhláška č. 227/2025 Z. z. o bezpečnostných opatreniach v oblasti kybernetickej bezpečnosti., NBÚ SR, 2025

[17] EUROPEAN PARLIAMENT AND THE COUNCIL., Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Official Journal of the European Union, 2024, Dostupné z: https://eur-lex.europa.eu

[18] EUROPEAN COMMISSION., The EU Artificial Intelligence Act – Impact and implementation overview. European Commission, 2024

[19] ENISA., Cybersecurity of AI and Machine Learning Systems, European Union Agency for Cybersecurity, 2024

Mediálny tréning pre príslušníkov Hasičského a záchranného zboru

Mária Pohanková Zahatlanová[1]

[1] Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva,
Univerzitná 1, 010 26 Žilina, maria.zahatlanova@gmail.com

Abstrakt:

Príspevok sa zaoberá problematikou mediálnej prípravy veliteľov zásahu v Hasičskom a záchrannom zbore. Hoci primárnu komunikáciu s médiami zabezpečujú hovorcovia, v praxi sú to často velitelia zásahov, ktorí poskytujú autentické informácie priamo z miesta udalosti. Článok popisuje vznik, štruktúru a ciele mediálneho kurzu, ktorý bol iniciovaný na Krajskom riaditeľstve Hasičského a záchranného zboru v Žiline a následne implementovaný do špecializovanej odbornej prípravy na Strednej škole požiarnej ochrany Ministerstva vnútra SR. Autor detailne rozoberá teoretickú časť školenia, zahŕňajúcu legislatívne pravidlá, zásady ustrojenosti, etické aspekty a obsahovú náplň mediálneho výstupu. Zároveň poukazuje na význam praktickej časti tréningu pre tvorbu mediálnych výstupov a tým aj budovanie profesionálneho imidžu a udržiavanie dôvery verejnosti voči Hasičskému a záchrannému zboru.

Kľúčové slová: hasičský a záchranný zbor, mediálny tréning, veliteľ zásahu, komunikácia s médiami, profesionálny imidž, etický kódex.

1 Úvod

Hasiči sú pre verejnosť symbolom pomoci, odvahy a profesionality. To, ako vystupujú v médiách, má priamy vplyv na dôveru spoločnosti voči nim. V krízových situáciách, ako sú požiare, dopravné nehody či živelné pohromy, očakáva verejnosť rýchle, presné a pokojné vyjadrenia. Slová majú moc. Jedna veta v médiách dokáže upokojiť tisíce ľudí, alebo naopak, vyvolať paniku.

Je dôležité, hasič vo svojom mediálnom výstupe pôsobil sebaisto, vecne a ľudsky zároveň. Mal by poznať základné princípy krízovej komunikácie, vedieť, ktoré informácie môže poskytnúť, a ktoré sú ešte predmetom zisťovania.

V neposlednom rade by mal hovoriť zrozumiteľne a jednoducho. Odbornosť je dôležitá, ale verejnosť nerozumie hasičskej terminológii a skratkám, preto informácie podávame primeraným spôsobom. Dôležité je verejnosti prostredníctvom médií vysvetliť, čo sa deje, prečo je zásah náročný, čo môžu ľudia očakávať, prípadne ako sa majú v podobných situáciách zachovať.

Médiá v dnešnej dobe pracujú rýchlo. Preto musia byť aj hasiči promptní, ale nie unáhlení. Správne pripravený výstup v médiách posilňuje dôveru verejnosti, podporuje transparentnosť a zvyšuje prestíž celého Hasičského a záchranného zboru.

2 Mediálny tréning

V Hasičskom a záchrannom zbore (ďalej HaZZ) je vytvorená pozícia hovorcu. Na Prezídiu Hasičského a záchranného zboru pôsobia aktuálne dve hovorkyne. Krajské riaditeľstvá Hasičského a záchranného zboru majú každé jedného hovorcu. V rámci organizačnej štruktúry Hasičského a záchranného zboru teda v súčasnosti pôsobí 10 hovorcov.

Hovorcovia však nie sú jediní príslušníci Hasičského a záchranného zboru, ktorí dostávajú priestor v médiách a televíziách. Informácie môže médiám poskytnúť prezident zboru, viceprezidenti zboru, riaditeľ odboru Prezídia HaZZ, príslušník na komunikačnom oddelení Prezídia HaZZ, riaditeľ krajského riaditeľstva, hovorca alebo poverený príslušník krajského riaditeľstva, veliteľ a riaditeľ zariadenia zboru, riaditeľ okresného riaditeľstva, operačný dôstojník, riadiaci dôstojník, veliteľ zásahu alebo osoba poverená veliteľom zásahu na mieste udalosti.

V praxi sú to najčastejšie velitelia zásahov, ktorí po skončení zásahu poskytujú prítomným médiám vyjadrenia o zásahu. V rámci ich odbornej prípravy (základnej, špecializovanej, cyklickej) od nástupu do Hasičského a záchranného zboru však nemali ucelené informácie, školenie alebo kurz zameraný na problematiku vystupovania pred kamerou.

Mnohí velitelia zásahov nechceli poskytovať médiám rozhovory. Necítili sa kompetentní, nevedeli, čo môžu povedať, čo nemôžu povedať, ani ako sa pri rozhovore tváriť. Mnohí z nich pred poskytnutím rozhovoru telefonicky kontaktovali hovorcu a konzultovali s ním jednotlivé vyjadrenia.

Práve táto potreba nás inšpirovala na vytvorenie mediálneho kurzu pre veliteľov zásahu. Uvedený mediálny kurz bol pôvodne určený pre veliteľov zásahu Krajského riaditeľstva Hasičského a záchranného zboru v Žiline. V mesiacoch september 2024 až január 2026 absolvovali mediálny kurz velitelia zásahu zo všetkých 7 okresných riaditeľstiev HaZZ v Žilinskom kraji. Neskôr sa mediálny kurz rozšíril aj na Strednú školu požiarnej ochrany, kde ho zaradili v dotácii dvoch vyučovacích hodín do špecializovanej odbornej prípravy príslušníkov HaZZ pre oblasť operatívne riadenie (veliteľské funkcie).

Mediálny tréning sa skladá z dvoch častí: teoretickej a praktickej. Na každú časť je vyčlenená jedna hodina.

2.1 Teoretická časť mediálneho tréningu

Teoretická časť mediálneho tréningu je v trvaní jednej vyučovacej hodiny. Formou prednášky a prezentácie sa poslucháči postupne oboznamujú s legislatívnym a teoretickým základom mediálnych výstupov. Obsahom prednášky je viacero tém.

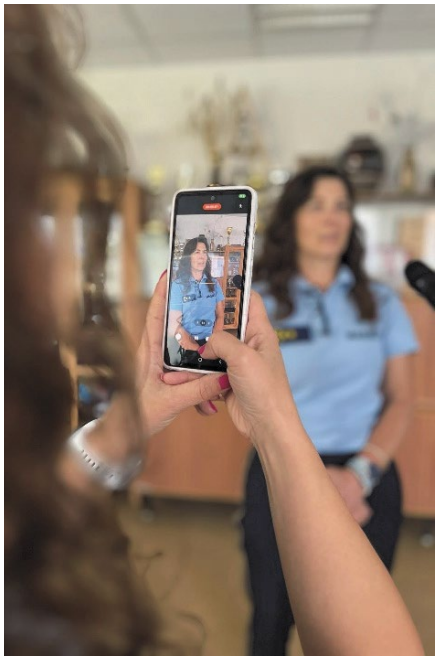
Médiá

Uvedením do mediálneho kurzu je časť o médiách. Ako ich delíme, ako fungujú a čo je ich úlohou a zámerom pri tvorbe reportáži s príslušníkmi Hasičského a záchranného zboru.

Médiá môžu byť našim spojencom a silným nástrojom na informovanie verejnosti o našej činnosti a prevencii pred požiarmi. Samozrejme, keď sa na reportáže pozrieme z pohľadu televízie, čím väčšia senzácia sa udeje, tým sledovanejšia bude reportáž. Samotní redaktori sa však snažia o získanie komplexných informácií z viacerých zdrojov. Keďže prvoradá je pre nich autentickosť, rozhovor s veliteľom zásahu priamo na mieste udalosti má pre nich väčšiu hodnotu, ako vyjadrenie hovorcu, ktorý sa na mieste nenachádzal a vyjadrenie poskytne s časovým oneskorením.

Reputácia

Pri každom mediálnom výstupe je potrebné si uvedomiť, že prezentujeme Hasičský a záchranný zbor, nie sami seba a svoj subjektívny názor (Obrázok 1).



Obrázok 1. Ilustračný záber, zdroj: Archív HaZZ

V čase, keď poskytujeme rozhovor do televízie, má už kameraman vytvorené svoje ilustračné zábery z miesta zásahu, na ktoré dosah nemáme. Stále však vieme ovplyvniť, čo televízny divák vidí, počuje a akú emóciu cíti počas nášho vyhlásenia. Je na nás, aby sme sa po dohode s redaktorom postavili tak, aby diváci nevideli nevhodné zábery a nepočuli nevhodné zvuky a nevyžiadané slová.

Neexistuje zásah bez emócií. Prejaviť ľútosť bez výrazných emocionálnych prejavov môže byť náročné. Každý divák však musí aj v ťažkých chvíľach vnímať našu profesionalitu a fyzickú a psychickú odolnosť. Obzvlášť počas mimoriadnych udalostí.

Zásady komunikácie s médiami

Základné pravidlá komunikácie s médiami upravuje Pokyn prezidenta Hasičského a záchranného zboru o poskytovaní informácií hromadným informačným prostriedkom č. 30/2021. V článku 3 sa hovorí, že veliteľ zásahu alebo osoba poverená veliteľom zásahu na mieste udalosti poskytuje informácie len o veciach *týkajúci sa bezprostredne vykonávania hasičských a záchranárskych postupov na mieste udalosti* a v priamej súvislosti s plnením služobných povinností. Neinformuje o príčinách vzniku udalosti a ani o záveroch vyšetrovania.

Poskytnutie informácií médiám má svoje zásady:

- informovať vždy transparentne a korektne,
- vyhýbať sa šíreniu mylných a neoverených informácií,
- dbať na obsahovú aj formálnu stránku prejavu,
- poskytovať informácie s maximálnou odbornosťou a objektivitou,

- poskytovať iba informácie súvisiace s bezprostredným výkonom hasičských a záchranárskych postupov na mieste udalosti a v priamej súvislosti s plnením služobných povinností,
- nevyjadrovať sa k činnostiam ostatných zložiek prítomných na zásahu.

Základné pravidlá mediálnych výstupov v HaZZ:

- Závažné údaje je pred zverejnením potrebné overiť u ďalšej osoby, prípadne ich konzultovať s nadriadeným.
- Spôsob podania citlivej informácie komunikovať s priamym nadriadeným alebo hovorcom.
- Neposkytovať médiám vlastné videozáznamy alebo fotografie.

Ustrojenosť príslušníka HaZZ

Ako príslušníci Hasičského a záchranného zboru máme predpísanú jednotnú uniformu a pravidlá ustrojenosti stanovené v Nariadení MV SR o rovnošate príslušníka Hasičského a záchranného zboru č. 54/2022. Tie dodržiavame počas celého výkonu služby a náš mediálny výstup nie je výnimkou, práve naopak.

Pred každým výstupom v médiách si nájdeme čas na vizuálnu kontrolu obrazu, ktorý vytvárame. Zameriavame sa predovšetkým na tieto body:

- *Jednotná uniforma* – nekombinujeme navzájom časti pracovnej rovnošaty vzor 1 (Obrázok 2), služobnej rovnošaty vzor 2, zásahový odev s civilným odevom a pod.
- *Prilba, resp. čiapka* je povinná súčasť uniformy – vo vonkajších priestoroch a pri zásahu je príslušná pokrývka hlavy povinnou súčasťou služobného odevu. Pri teplotách nad 25 °C môže príslušník na verejnosti a pri vykonávaní štátneho požiarneho dozoru chodiť bez čiapky.
- *Gombíky* – ak príslušník nosí bledomodrú polokošeľu, môže mať rozopnutý prvý vrchný gombík pri krku, nie však viac.
- *Slnečné okuliare* – príslušník môže na verejnosti nosiť slnečné okuliare, to neplatí pre zrkadlové okuliare, okuliare neštandardného tvaru a s neprimeranou veľkosťou skiel.

Obrázok 2. Uniforma príslušníka HaZZ, vzor 1

Obsahová stránka prejavu

Pri informovaní verejnosti o udalosti poskytujeme stručné a jasné vyjadrenia. Bez zbytočných príkras a umeleckých prostriedkov, no zároveň informačne výživné. Komplexné vyjadrenie poskytuje odpovede na všetky čiastkové otázky:

- KEDY sa udalosť stala?
- ČO sa stalo, resp. o aký typ udalosti sa jedná?
- KDE sa udalosť stala?
- KTO a s akou technikou na mieste zasahoval?
- AKO prebiehal zásah?

Pokiaľ máme počas vyjadrenia priestor, je žiaduce vyzdvihnúť prácu hasičov, napr. koľko osôb sa podarilo vďaka zásahu zachrániť, aké hodnoty uchrániť a pod.

Čo v mediálnych výstupoch nepovedať

„Mlčať je zlato“ platí aj pre mediálne výstupy hasičov. Čo povedať nemôžeme je niekedy ešte dôležitejšie ako to, čo povedať môžeme.

Na mediálnom kurze sa príslušníci dozvedia, že sa v reportážach nevyjadrujeme k nasledovným bodom:

- osobné údaje dotknutých osôb,
- identifikačné údaje (mená, adresy, názvy spoločností),
- informácie znižujúce ľudskú dôstojnosť,
- ekologické katastrofy,
- škodové udalosti na hasičskej technike,
- ujmy na zdraví zasahujúcich hasičov,
- zásahy, ktorých aktérmi sú hasiči a ich rodiny.

Formálna stránka prejavu

Mediálna prezentácia hasičov je významným nástrojom budovania dôvery. Rovnako dôležitá ako informácia, ktorú verejnosti oznámime, je aj forma, akou danú informáciu podáme. Práve forma predstavuje významný prvok profesionálneho imidžu hasičov a má priamy dopad na dôveru verejnosti v našu prácu.

V teoretickej časti kurzu rozoberáme, že postoj tela, tón hlasu, výraz tváre, ustrojenosť, sebavedomie a sebaovládanie – to všetko vnímajú diváci rovnako citlivo, ako obsahovú stránku vyjadrenia.

Každý z nás má svoje vlastné „ideálne tempo reči“. Nenechávame sa tlakom udalostí a médií dotlačiť do tempa, ktoré nám nie je prirodzené. Dôsledkom sú chyby vo vyjadrení a následná vlastná nespokojnosť s našim mediálnym výstupom.

Pri tvorbe spravodajstva sú uprednostňované stručné vyjadrenia. Preto sme vecní, tvoríme krátke a jednoduché vety. Pôsobia profesionálnejšie, navyše pomáhajú predchádzať rečníckym chybám.

Mediálne výstupy musia byť profesionálne, a to svojim obsahom aj formou. Preto je dôležité pracovať s vlastnými emóciami a ich intenzitou v mediálnom výstupe.

2.2 Praktická časť mediálneho tréningu

V druhej časti mediálneho kurzu si prakticky precvičujeme vedomosti, ktoré odzneli v teoretickej časti. Každý účastník kurzu si náhodným losovaním vyberá jednu z tém:

- Dopravná nehoda kamiónu a OMV bez zranenia;
- Dopravná nehoda 2 OMV so zranením;
- Technická pomoc – transport nadrozmerného pacienta;
- Požiar osobného automobilu;
- Požiar rodinného domu;
- Požiar chaty v neprístupnom teréne;
- Požiar bytového domu;
- Pátranie po utopenej osobe;
- Lesný požiar;
- Zranenie na skalách;
- Pomoc pri KPR s AED.

K vytvoreniu reálnej situácie využívame mikrofón a kameru. Vybraný respondent si vylosuje jednu z tém. Ostatní účastníci vytvoria presný scenár udalosti (čo sa stalo, na akej adrese, kedy sa to stalo, kto na mieste udalosti zasahuje, aká technika bola použitá pri zásahu, koľko je na mieste zranených a pod.).

Spolu s dobrovoľníkom vytvoríme reálnu situáciu, kedy jeho vyjadrenie snímame na kameru a respondent hovorí priamo do mikrofónu (Obrázok 3). Cieľom je vytvoriť reálny tlak, aký hasič pri mediálnom výstupe pociťuje a utvrdiť si získané teoretické vedomosti z prvej časti kurzu.

Po skončení mediálneho výstupu respondenta nasledujú pripomienky a postrehy ostatných účastníkov kurzu. Vyjadrujú sa k obsahovej stránke prejavu, t.j. či bolo povedané všetko, čo má vyjadrenie obsahovať a naopak, či respondent neprezradil niektorú z nepovolených informácií. Zároveň hodnotíme dodržanie všetkých formálnych náležitostí prejavu, ustrojenosti, očný kontakt s kamerou a i. Poslednou časťou praktickej skúšky je sebahodnotenie respondenta.

Obrázok 3. Praktická časť mediálneho tréningu pre príslušníkov HaZZ

3 Záver

Mediálny tréning sa ukázal ako potrebná súčasť odbornej prípravy veliteľov zásahu Hasičského a záchranného zboru. Kým teoretická časť tréningu poskytuje príslušníkom potrebný legislatívny rámec, zásady ustrojenosti a komunikačné pravidlá, praktický nácvik umožňuje tieto poznatky reálne pretaviť do profesionálneho vystupovania.

Práve praktická časť kurzu, simulujúca reálny stres pred kamerou a s mikrofónom, odbúrava u veliteľov počiatočnú neistotu a strach z médií. Prostredníctvom modelových situácií si účastníci osvojujú schopnosť jasne a vecne informovať verejnosť aj v emocionálne vypätých momentoch. Spätná väzba z nahrávok im umožňuje korigovať nielen verbálny prejav, ale aj reč tela a celkový vizuálny dojem, ktorý priamo vplýva na reputáciu celého zboru.

Zavedenie tohto kurzu do špecializovanej prípravy na Strednej škole požiarnej ochrany potvrdzuje, že mediálna gramotnosť už nie je len výsadou hovorcov, ale základnou kompetenciou moderného veliteľa zásahu alebo riadiaceho dôstojníka. Systematické vzdelávanie v mediálnej oblasti zabezpečuje, že Hasičský a záchranný zbor bude v očiach verejnosti aj naďalej vnímaný ako vysoko profesionálna, transparentná a dôveryhodná inštitúcia, ktorá dokáže komunikovať s maximálnou odbornosťou v každej situácii.

Referencie

[1] Pokyn prezidenta Hasičského a záchranného zboru o poskytovaní informácií hromadným informačným prostriedkom č. 30/2021

[2] Nariadenie MV SR o rovnošate príslušníka Hasičského a záchranného zboru č. 54/2022

[3] Rozkaz prezidenta Hasičského a záchranného zboru č. 9/2017 - Etický kódex príslušníka Hasičského a záchranného zboru

Security Incident Reporting in Hospitals and its Application in the Risk Management Process

Vladimír Pustay[1]

[1] Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva,
1. mája 32, 010 01 Žilina, vladimir.pustay@uniza.sk

Abstract:

Hospital facilities, as providers of essential services, constitute a specific category of critical infrastructure entities whose systemic disruption directly affects the continuity of healthcare delivery. Despite the emergence of new risk typologies and the escalation of security threats, a unified framework for the systematic reporting of security incidents remains absent in the context of the Slovak Republic. The objective of this study is to propose a conceptual methodological framework for the systematic recording, categorisation, and evaluation of security incidents in hospital settings, serving as a foundation for risk management and, in particular, for strengthening institutional resilience. Methodologically, the study is designed as a conceptual research endeavour based on the analysis of legislative and theoretical foundations, the systemic examination of hospital facilities as socio-technical systems, and expert assessment conducted by crisis management professionals. The primary output of the research is a typology of the most frequent incident patterns and the design of an incident reporting register that enables the transformation of qualitative incident descriptions into a semi-quantitative risk matrix based on the relationship $R = L \cdot I$. The proposed framework provides an analytical instrument for standardised data collection, comparable risk assessment, and decision-making support in the process of enhancing the resilience of hospital-based critical infrastructure entities.

Keywords: security incident reporting, healthcare sector, critical infrastructure, resilience, risk assessment.

1 Introduction

Pursuant to Section 14(3) of Act No. 367/2024 Coll., hospitals are designated as elements of the critical infrastructure of the Slovak Republic. [1] Any disruption to their security directly affects the continuity of healthcare provision at the local, regional, and national levels. As providers of essential services, they require a systematic and proactive approach to security management and resilience building. From a security management perspective, hospitals constitute a specific category of so-called soft targets. They are characterised by a high concentration of individuals, open-access regimes, continuous operation, and the presence of vulnerable patient populations. At the same time, they are highly dependent on the functionality of other critical infrastructure sectors, particularly energy supply, water management, and information and communication technologies. Disruptions within these interdependent systems may generate cascading effects with direct implications for healthcare delivery. Despite these risks, a unified and systematic framework for the reporting of security incidents within the hospital sector remains absent in the Slovak Republic. Existing reporting practices are fragmented and predominantly administrative in nature, limiting their analytical utility and reducing their effectiveness in supporting risk management processes. The objective of this paper is to propose a conceptual framework for the systematic reporting of security incidents in hospital facilities as critical infrastructure entities. The framework enables standardised data collection and the transformation of incident data into a semi-quantitative risk assessment model based on the relationship $R = L \cdot I$. The evaluated risks

are subsequently integrated into an adaptive incident and resilience management process, thereby supporting organisational learning and the continuous strengthening of systemic resilience.

2 Security Incidents in Hospitals as a Risk Management Challenge

Hospital facilities represent a specific category of critical infrastructure entities whose primary function is to ensure the continuity of healthcare delivery. [4] From a security management perspective, they are characterised by a combination of vulnerability factors, including a high concentration of individuals, open-access regimes, continuous operation, and the presence of vulnerable patient populations who cannot be readily evacuated in the event of an incident. Simultaneously, hospitals are significantly dependent on the functionality of external critical infrastructure systems, particularly energy supply, water management, and information and communication technologies. Disruptions within these interdependent systems may generate cascading effects with direct consequences for healthcare provision. Security incidents in hospital environments are inherently heterogeneous. From an analytical standpoint, they may be categorised into several principal groups. [5]

Violent incidents primarily involve verbal and physical aggression by patients or their relatives. Globally, this category represents one of the most prevalent types of incidents in the healthcare sector. The dominant impact is borne by healthcare personnel, particularly frontline staff. The absence of preventive and proactive measures may contribute to the cumulative psychological burden on staff, potentially resulting in increased absenteeism, staff turnover, and reduced workforce stability. Such effects may ultimately compromise the continuity and quality of healthcare delivery.

Operational and technical incidents include equipment failures (e.g., diagnostic devices or IT infrastructure), energy outages, and disruptions in the supply of medical materials and specialised equipment. Their primary impact is reflected in the impaired functionality of essential services.

Information and cyber incidents typically involve failures of information systems, loss of access, or reduced availability of critical data. These incidents significantly affect coordination, management processes, and outpatient care.

Internal organisational incidents arise from procedural violations or human error. Although often latent in nature, they may exert cumulative systemic effects over time.

Extraordinary and combined incidents are characterised by system-wide impacts on service continuity. They tend to exhibit cascading dynamics and multifactorial consequences, potentially resulting from natural, technical, or economic events, either independently or in combination.

The common denominator of these incident types is their potential to disrupt healthcare continuity and elevate systemic risk within hospitals as critical infrastructure entities. From a risk management perspective, however, the fundamental issue lies not in the mere existence of these risks, but in the manner in which they are recorded and analytically processed.

Within the healthcare system of the Slovak Republic, a unified and methodologically grounded framework for the systematic reporting of security incidents is lacking. Reporting practices are decentralised, and many institutions do not maintain a structured incident register. This situation leads to a significant disconnect between incident management at the operational level and strategic risk management processes. Incident data

are not standardised, which limits comparability across institutions and hinders the identification of trends, recurring patterns, and systemic vulnerabilities. [2]

A fragmented and predominantly reactive approach constrains the ability of hospitals to systematically identify, prioritise, and evaluate security risks. Without a unified reporting system and a methodology capable of transforming qualitative incident descriptions into analytically processable data, it is not possible to establish a consistent decision-support basis for the protection and resilience-building of hospital facilities.

These considerations highlight the need for a conceptual framework that enables standardised data collection as input for risk assessment, structured categorisation of incidents, and their subsequent transformation into a risk evaluation model. Such a framework has the potential to bridge the gap between the operational handling of individual incidents and the systematic management of security in hospital facilities as elements of critical infrastructure.

3 Methodology for the Design of the Security Incident Reporting Framework

The proposed framework for the systematic reporting of security incidents is conceived as a conceptual methodological model tailored to hospital facilities as critical infrastructure entities. Methodologically, it is grounded in the principles of risk management as defined in internationally recognised standards, particularly ISO 31000 and ISO 31010, while taking into account the specific characteristics of the healthcare environment and the limited availability of quantitative data.

3.1 Type of Research

The study is based on conceptual research incorporating elements of systems analysis. Its objective is not the empirical testing of hypotheses, but rather the development of a methodological instrument enabling the standardised collection of incident data, their categorisation, and the transformation of qualitative information into a semi-quantitative risk assessment model. The conceptual framework was developed through the synthesis of legislative and normative analysis, a comparative review of existing risk assessment approaches, expert evaluation from the perspective of security and crisis management professionals, and a systems-based examination of the hospital as a socio-technical system.

3.2 Systems Analysis of the Hospital Facility as a Critical Infrastructure Entity

Within the proposed model, the hospital facility is conceptualised as an open socio-technical system whose functionality depends on the stable operation of multiple interrelated subsystems and the continuous inflow of essential resources. The fundamental subsystems include, in particular, the technological subsystem and the organisational-process subsystem. Critical resource inputs comprise human resources as well as external dependencies, notably energy supply, water management, supply chains, and information and communication technologies. In this context, an incident is defined as an event that disrupts the stability of one or more subsystems, thereby threatening the continuity of healthcare delivery.

3.3 Architecture of Reporting Model

The methodology for designing the incident register was based on the identification of a minimum dataset required for subsequent analytical risk evaluation. Each reporting record must enable precise categorisation of the incident type, identification of the affected area or subsystem, determination of the underlying cause and mechanism of occurrence, documentation of consequences (operational, clinical, reputational, and economic), and assessment of the likelihood of recurrence.

3.4 Transformation of Incident Data Into the Risk Assesment Model

The input data for the risk assessment model are derived from the structured incident register (see Table 1), while the resulting risk levels are interpreted using the risk matrix (see Table 2). The proposed risk assessment model is based on a semi-quantitative approach in which qualitative characteristics of an incident are transformed into ordinal scales of likelihood of occurrence (L) and impact on system functionality (I). Numerical values within a defined range of 1–5 are assigned to each level of likelihood and impact. The resulting level of risk is determined by the relationship:

$$R = L \cdot I$$

The calculated value enables the identification of priority risks, the monitoring of trends over time, and informed decision-making regarding the allocation of security measures. The model does not constitute a fully quantitative risk analysis; rather, it serves as a decision-support instrument suitable for environments with limited availability of statistical data. [3]

3.5 Limitations of Methodology

The proposed framework is inherently dependent on the quality of input data and on the consistent methodological interpretation of the likelihood and impact scales. In the absence of clearly standardised evaluation criteria, a degree of subjectivity in risk scoring may arise. For this reason, the framework presupposes the methodological calibration of scales and internal training of evaluators to ensure consistency and comparability of assessments.

An additional limitation lies in the static nature of the risk matrix itself, which does not capture dynamic changes in the risk environment in real time. However, this characteristic is consistent with the conceptual objective of the study, which is to provide a structured decision-support instrument rather than a real-time monitoring system.

4 Results of the Proposed Reporting Model

The principal outcome of the study is the design of a systematic reporting framework for security incidents in hospital facilities, enabling the standardised collection of data and their transformation into a semi-quantitative risk assessment model:

1. **Structured incident register;**
2. **Defined scales of likelihood (*L*) and impact (*I*);**
3. **A risk matrix enabling the prioritisation of identified events.**

4.1 Architecture of the Security Incident Register

As illustrated in Table 1, the proposed register is designed to capture security incidents in a structured and consistent manner. Rather than serving only as a descriptive record, it organises key information about each incident, including its type, underlying cause, affected area, and resulting consequences. This structure makes it possible to move beyond simple documentation and to use incident data for basic analytical purposes, particularly in the context of risk assessment. By introducing a set of standardised variables, the register allows incidents to be compared across time and within different parts of the organisation. Compared to current practice, which is often fragmented and focused on administrative reporting, the proposed approach offers a more systematic way of working with incident data. It creates a foundation for identifying recurring issues and supports a more informed approach to managing risks in hospital environments.

Table 1. Security Incident Register

Category of data	Name of attribute	Definition and significance for risk assessment
Identification of incident	Type of incidents	Classification into category (violent, technical, organisational, cyber, extraordinary)
	ID of incidents	Classification into category (violent, technical, organisational, cyber, extraordinary)
Time and place	Time of origin and duration	Exact date and time (D/M/Y) for identifying frequency (*L*), duration of the incident
	Place of origin	Space identification (emergency department, data center, technical hub)
Cause analysis	Direction of incident	Threat identification (internal, external) and continuity disruption mechanism
	Affected area	Specification of whether the incident affected personnel, technology, data, infrastructure
Impact assessment	Disruption of continuity	Qualitative description of the impact on the provision of basic service (discomfort vs. life-threatening)
	Level of impact (*I*)	Quantification of severity on a scale of 1–5 (negligible/critical = total collapse)
Quantification	Likelihood (*L*)	Estimated frequency based on historical data (1–5)
	Resulting risk (*R*)	**The product *L* · *I*, determining the priority in implementing security measures**

As shown in Table 1, the register integrates identification, causal, and impact-related attributes, enabling the transformation of qualitative incident descriptions into structured data suitable for risk assessment.

4.2 Risk Matrix

The interpretation of the resulting risk levels and corresponding response measures is summarised in Table 2. It serves to calculate the level of risk based on the relationship $R = L \cdot I$, and to subsequently prioritise identified risks and allocate appropriate security measures to specific risk categories. In line with a proactive approach to strengthening the resilience of critical infrastructure, incidents classified at the highest impact level ($I = 5$) are categorised as critical risks irrespective of their likelihood, thereby requiring the immediate implementation of corrective or mitigating measures.

Table 2. Interpretation of the Resulting Risk Level

Value of *R*	**Risk level**	**Recommended response**
Green (1–4)	Low	Risk monitoring
Yellow (5–9)	Moderate	Preventive measures
Orange (10–16)	High	Priority risk management
Red (17+/ *I* = 5)	Critical	Immediate intervention

Table 2 enables the prioritisation of identified risks and supports decision-making regarding the implementation of appropriate security measures based on the calculated risk level.

4.3 Model Application

To demonstrate the functionality of the model, the procedure was applied to a hypothetical incident scenario.

Scenario: Repeated physical assaults against healthcare personnel working in the emergency department. The incident occurs several times per year (L = 4) and results in temporary disruption of healthcare delivery (I = 3). The overall operation of the hospital as a complex system remains unaffected.

Risk calculation: $R = 4 \cdot 3 = 12$

The incident is therefore classified as a high-level risk requiring prioritised and targeted risk management measures, such as strengthening physical security arrangements and providing staff training in conflict management and de-escalation techniques.

4.4 The Contribution of the Proposed Model

The proposed framework integrates operational incident reporting with strategic risk management. It enables the identification of recurring disruption patterns and supports informed decision-making regarding investments in security measures. Furthermore, it provides a structured foundation for strengthening the resilience of hospitals as critical infrastructure entities. The model is particularly suitable for environments with limited availability of quantitative data and represents an implementable and practice-oriented instrument for hospital settings.

5 Conclusion

Hospitals, as critical infrastructure entities, face a broad spectrum of security incidents that have the potential to disrupt the continuity of healthcare delivery. However, within the context of the Slovak Republic, a unified framework for their systematic reporting and analytical evaluation remains absent. This paper presents a conceptual reporting model that integrates a standardised incident register with a semi-quantitative risk assessment approach based on the relationship $R = L \cdot I$. The proposed framework enables the transformation of qualitative data into comparable analytical outputs, supports risk prioritisation, and provides a structured basis for decision-making in the processes of security management and resilience building in hospital settings. The model does not constitute a fully quantitative risk analysis; rather, it represents an implementable instrument suitable for environments with limited data availability. Future research should focus on its empirical validation and the calibration of evaluation scales within real-world hospital practice.

References

[1] ACT No. 367/2024 Coll. on Critical Infrastructure. Bratislava: Ministry of Justice of the Slovak Republic, 2024. § 14(3). [online]. [cit. 2026-02-22]. Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2024/367/20250101

[2] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 31000:2018 – Risk management – Guidelines [online]. Geneva: ISO, 2018. Available at: https://www.iso.org/standard/65694.html [cit. 2026-01-14]

[3] SLOVAK REPUBLIC. Ministry of Interior of the Slovak Republic. Strategy for the Resilience of Critical Entities in the Slovak Republic [online]. Government material No. UV-38268/2025, departmental reference No. KM-OPVA-2025/004878. Bratislava: Ministry of Interior, 2025. Available at: https://rokovania.gov.sk/RVL/Material/31491/1 [cit. 2026-01-12]

[4] WORLD HEALTH ORGANIZATION. Maintaining essential health services and systems [online]. Geneva: WHO, 2020. Available at: https://www.who.int/publications/i/item/WHO-2019-nCoV-essential-health-services-2020.1 [cit. 2026-01-12]

[5] SLOVAK REPUBLIC. Ministry of Interior of the Slovak Republic. Strategy for the Resilience of Critical Entities in the Slovak Republic – Annex 2 [online]. Bratislava: Ministry of Interior, 2025. Available at: https://rokovania.gov.sk/RVL/Material/31491/1 [cit. 2026-01-12]

Experimentálne stanovenie teploty vzplanutia a teploty vznietenia jaseňa štíhleho (Fraxinus excelsior) a smreku obyčajného (Picea abies)

Anna Mária Rajnohová[1], Linda Makovická Osvaldová[2]

[1] Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva,
1. mája 32, 010 26 Žilina, anna_maria.rajnohova@uniza.sk

[2] Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva,
1. mája 32, 010 26 Žilina, linda.makovicka@uniza.sk

Abstrakt:

Článok sa zameriava na experimentálne stanovenie teplôt vzplanutia a teplôt vznietenia dreva dvoch významných lesných drevín Slovenska – Jaseň štíhly (Fraxinus excelsior) a Smrek obyčajný (Picea abies) – so špecifickým dôrazom na posúdenie ich tepelnej a kinetickej stability. Problematika iniciácie horenia dreva predstavuje významný aspekt požiarnej bezpečnosti, najmä pri jeho využití ako konštrukčného alebo energetického materiálu. Experimentálna časť bola realizovaná v teplovzdušnej Setchkinovej peci v súlade s princípmi normy ISO 871, ktorá špecifikuje metodiku stanovenia teploty vzplanutia a vznietenia materiálov. Vzorky dreva boli pripravené vo forme kociek s rozmermi 2 × 2 cm a hmotnosťou približne 3 g. Pred samotným meraním boli vysušené pri teplote 100 °C s cieľom eliminovať vplyv vlhkosti a zabezpečiť hmotnostnú stabilitu. Po stabilizácii teploty pece boli vzorky vystavené definovaným teplotným podmienkam a zaznamenával sa indukčný čas do momentu vzplanutia alebo samovznietenia. Na základe nameraných údajov boli vypočítané aktivačné energie procesu. Pri smreku obyčajnom bola stanovená vyššia priemerná teplota vzplanutia (391,7 °C) aj vznietenia (496,4 °C) v porovnaní s jaseňom štíhlym (366,4 °C a 447,6 °C). Vyššie hodnoty aktivačnej energie pri smreku potvrdzujú jeho väčšiu energetickú bariéru iniciácie horenia. So zvyšujúcou sa teplotou prostredia sa pri oboch drevinách skracoval indukčný čas, čo potvrdzuje kinetický charakter procesu tepelného rozkladu. Výsledky poskytujú dôležité poznatky pre hodnotenie požiarneho rizika drevných materiálov a ich praktické využitie v technickej praxi.

Kľúčové slová: jaseň, smrek, vznietenie, vzplanutie.

1 Úvod

Drevo patrí medzi najvýznamnejšie prírodné materiály využívané človekom, pričom jeho vlastnosti sa líšia v závislosti od druhu dreviny, anatomickej stavby a chemického zloženia. Z hľadiska požiarnej bezpečnosti je dôležité poznať správanie jednotlivých drevín pri pôsobení zvýšenej teploty, najmä ich teplotu vzplanutia, teplotu vznietenia a kinetické parametre tepelného rozkladu. Tieto charakteristiky umožňujú lepšie posúdiť mieru požiarneho rizika a tepelnú stabilitu materiálu pri jeho praktickom využití.

Predmetom výskumu bolo porovnanie dvoch významných drevín rastúcich na území Slovenska – Jaseň štíhly (Fraxinus excelsior) a Smrek obyčajný (Picea abies).

Cieľom práce je experimentálne stanoviť teplotu vzplanutia, teplotu vznietenia, indukčné časy a aktivačnú energiu vybraných vzoriek týchto drevín a následne porovnať ich tepelnú a kinetickú stabilitu. Merania boli realizované pomocou teplovzdušnej pece podľa princípov normy STN ISO 871, pričom získané výsledky umožňujú komplexnejšie zhodnotenie ich správania pri tepelnom zaťažení.

Porovnanie listnatej a ihličnatej dreviny z hľadiska iniciácie horenia poskytuje dôležité poznatky pre oblasť požiarnej ochrany, lesného hospodárstva aj technickej praxe, kde je drevo využívané ako konštrukčný alebo energetický materiál.

2 Jaseň štíhly (Fraxinus excelsior)

Jednou z nami skúmaných drevín bol jaseň štíhly (Fraxinus excelsior), patriaci do čeľade olivovité (Oleaceae). Rod Fraxinus zahŕňa viac ako 60 známych druhov listnatých stromov, ktoré sú rozšírené predovšetkým v miernom pásme severnej pologule, najmä v Európe, Severnej Amerike a vo východnej Ázii vrátane Japonska. Zástupcovia tohto rodu sú významnou súčasťou lesných ekosystémov, kde plnia nielen ekologickú, ale aj hospodársku funkciu. Vyznačujú sa rýchlym rastom, kvalitným drevom a dobrou prispôsobivosťou rôznym stanovištným podmienkam. [1]

Na území Slovenskej republiky sa prirodzene vyskytujú najmä dva druhy jaseňa, a to jaseň mannový (Fraxinus ornus) a jaseň štíhly (Fraxinus excelsior). Oba druhy sa od seba odlišujú viacerými morfologickými aj ekologickými znakmi. Jaseň štíhly je mohutný strom dorastajúci do výšky 30 až 40 metrov, pričom vytvára priamy, valcovitý kmeň a vysoko nasadenú, pomerne riedku korunu. Jeho listy sú nepárno perovito zložené, zvyčajne tvorené 9 až 13 lístkami s jemne pílkovitým okrajom. Kôra mladých jedincov je hladká a sivá, s pribúdajúcim vekom tmavne a vytvára pozdĺžne brázdy. Typickým znakom sú aj čierne, nápadne sfarbené púčiky, ktoré predstavujú jeden z rozlišovacích znakov druhu. [2]

Naopak, jaseň mannový je výrazne menší strom alebo väčší ker, ktorý zvyčajne dorastá do výšky približne 6 až 8 metrov, výnimočne viac. Má hustejšiu, nižšie nasadenú korunu a jeho ekologické nároky sa mierne líšia – častejšie sa vyskytuje v teplejších a suchších oblastiach, najmä v južných častiach Slovenska. Charakteristickým znakom jaseňa mannového sú nápadné biele, voňavé súkvetia, ktoré sa objavujú na jar a majú význam aj z hľadiska produkcie tzv. manny (sladkej šťavy získavanej z poranenej kôry). [3]

Rozdiely medzi týmito dvoma druhmi sú zreteľné už na prvý pohľad, a to najmä v morfológii stromu – v celkovej výške, tvare a veľkosti koruny, ako aj v hrúbke a charaktere kmeňa. Kým jaseň štíhly je typickým predstaviteľom vyšších lesných porastov a často tvorí významnú zložku lužných či zmiešaných lesov, jaseň mannový sa uplatňuje skôr v teplomilných spoločenstvách. V dôsledku týchto výrazných morfologických a ekologických odlišností je zámena medzi uvedenými druhmi v prirodzených podmienkach málo pravdepodobná. [4]

Využitie jaseňa štíhlého

Jaseň štíhly patrí medzi cenné listnaté dreviny, a to z hľadiska kvality dreva aj ekologického významu. V lesnom hospodárstve sa zaraďuje medzi melioračné a spevňujúce dreviny, pretože jeho opad zlepšuje pôdne vlastnosti. Listy sa rýchlo rozkladajú, obohacujú pôdu o živiny, podporujú tvorbu humusu a prispievajú k zlepšeniu štruktúry a biologickej aktivity pôdy.

Hoci z hľadiska objemu produkcie dreva nepatrí medzi najvýznamnejšie hospodárske dreviny, jeho drevo je vysoko kvalitné. Anatomicky sa radí medzi kruhovito pórovité dreviny (podobne ako dub či agát). Jaseňové drevo je jadrové, pevné, tvrdé, ale zároveň pružné a húževnaté. Využíva sa na výrobu masívneho nábytku, krájaných dýh, parkiet a podlahových krytín. Pre svoju pružnosť je vhodné na násady náradia (napr. sekery), ale aj na výrobu hudobných nástrojov, napríklad tiel elektrických gitár. Uplatňuje sa aj v športovom priemysle, napríklad pri výrobe lyží, hokejok či lukov.

Okrem dreva sa využívajú aj listy, semená a kôra, ktoré obsahujú biologicky aktívne látky. V tradičnej medicíne sa používajú pri zápaloch, bolestiach kĺbov a reumatických ťažkostiach, pričom sa im pripisuje aj priaznivý vplyv na znižovanie hladiny cholesterolu.

Jaseň štíhly tak predstavuje drevinu s významným ekologickým aj praktickým využitím. [4,5]

3 Smrek obyčajný (Picea Abies)

Druhou skúmanou drevinou je smrek obyčajný (Picea Abies) významný ihličnatý strom patriaci do čeľade borovicovité (Pinaceae). Ide o jeden z najrozšírenejších a hospodársky najvýznamnejších ihličnanov v Európe, prirodzene sa vyskytujúci najmä v severnej, strednej a horskej časti kontinentu. Smrek obyčajný tvorí rozsiahle lesné porasty, najmä v horských a podhorských oblastiach, kde predstavuje dominantnú drevinu.

Smrek obyčajný je mohutný, vždyzelený strom, ktorý dorastá do výšky 50 až 60 metrov, pričom priemer kmeňa môže dosiahnuť až 150 cm. V priaznivých podmienkach sa bežne dožíva veku 200 až 300 rokov. [6]

Koruna smreka obyčajného má pravidelný kužeľovitý až stĺpovitý tvar, čo je typický znak najmä u jedincov rastúcich na voľnej ploche. Konáre vyrastajú v praslenoch, sú pomerne krátke a pevné; horné konáre smerujú šikmo nahor, zatiaľ čo spodné vetvy bývajú previsnuté. Tento charakteristický habitus prispieva k dobrej rozpoznateľnosti druhu v teréne.

Púčiky sú červenohnedej farby, približne 5 mm dlhé, s výrazne zašpicateným vrcholom. Ihlice sú 1 až 2,5 cm dlhé, tuhé, štvorhranného prierezu, čo je jeden z určujúcich znakov rodu Picea. Farba ihlíc sa pohybuje od svetlozelenej po tmavozelenú, pričom na ich povrchu možno pozorovať jemné biele bodkované línie spôsobené prítomnosťou prieduchov. [7]

Kôra smreka obyčajného je oranžovohnedá až hnedá, v mladosti pomerne hladká, neskôr sa odlupuje v tenkých šupinách. Drevo je svetlé, krémovobiele, mäkké a pomerne ľahko opracovateľné. [8]

Z ekologického hľadiska má smrek obyčajný významnú úlohu pri tvorbe horských lesných ekosystémov, kde ovplyvňuje mikroklímu, vodný režim a poskytuje životný priestor mnohým druhom rastlín a živočíchov. V súčasnosti je však tento druh v niektorých oblastiach vystavený stresovým faktorom, ako sú klimatické zmeny, sucho či napadnutie podkôrnym hmyzom, čo má významný dopad na stabilitu smrekových porastov. [9]

Využitie smreka obyčajného

Smrek obyčajný (Picea abies) patrí medzi najvýznamnejšie ihličnaté dreviny Európy, a to z hľadiska hospodárskeho aj ekologického významu. V podmienkach strednej Európy predstavuje základnú drevinu horských a podhorských lesov, kde plní dôležitú produkčnú aj mimoprodukčnú funkciu. Smrekové porasty významne ovplyvňujú vodný režim krajiny, znižujú eróziu pôdy a vytvárajú špecifickú mikroklímu lesného prostredia. Opad ihlíc sa rozkladá

pomalšie ako listnatý opad, čím sa podieľa na tvorbe surovejšieho humusu a ovplyvňuje chemické vlastnosti pôdy. [10]

Z hľadiska objemu produkcie dreva patrí smrek medzi najvýznamnejšie hospodárske dreviny na Slovensku aj v širšom európskom priestore. Jeho drevo je mäkké, ľahké, svetlé, s rovnomernou štruktúrou a bez výrazného jadra. Vyznačuje sa dobrým pomerom pevnosti k hmotnosti a veľmi dobrou opracovateľnosťou. Využíva sa predovšetkým v stavebníctve (konštrukčné rezivo, krovy, nosné prvky), v nábytkárstve a pri výrobe drevotrieskových a vláknitých dosiek. Významné je aj jeho uplatnenie v papierenskom priemysle, kde slúži ako dôležitá surovina na výrobu celulózy. [11]

Osobitné postavenie má smrekové drevo pri výrobe hudobných nástrojov, najmä rezonančných dosiek sláčikových nástrojov a klavírov, kde sa oceňujú jeho priaznivé akustické vlastnosti. Okrem toho sa využíva aj na výrobu obalového materiálu, paliet či energetickej štiepky.

Z ekologického hľadiska poskytujú smrekové porasty životný priestor mnohým druhom rastlín a živočíchov a plnia významnú krajinotvornú funkciu. V súčasnosti je však smrek obyčajný vystavený viacerým stresovým faktorom, ako sú klimatické zmeny, dlhodobé sucho a napadnutie podkôrnym hmyzom, čo ovplyvňuje stabilitu a zdravotný stav porastov.

Smrek obyčajný tak predstavuje drevinu zásadného hospodárskeho významu, ktorá má zároveň nezastupiteľnú ekologickú funkciu v lesných ekosystémoch strednej Európy. [12, 13]

4 Stanovenie teploty vzplanutia a vznietenia

Slovenská technická norma STN ISO 871 určuje laboratórnu metódu na stanovenie teploty vzplanutia a teploty vznietenia plastových materiálov pomocou teplovzdušnej pece. Táto norma je ekvivalentná medzinárodnej norme ISO 871:2022. Metóda patrí medzi viaceré postupy používané na hodnotenie reakcie materiálov na pôsobenie zdrojov zapálenia, avšak neposkytuje priamy údaj o horľavosti alebo rýchlosti horenia materiálu a neurčuje bezpečnú maximálnu prevádzkovú teplotu plastov. Z tohto dôvodu by sa nemala používať samostatne na hodnotenie reálneho požiarneho nebezpečenstva materiálov, výrobkov či konštrukcií. Výsledky merania však môžu byť súčasťou komplexného hodnotenia požiarneho rizika, ktoré zohľadňuje všetky relevantné faktory pre konkrétne použitie materiálu. Hoci je norma primárne určená pre plasty, rovnaké zariadenia umožňujú meranie teploty vzplanutia a vznietenia aj dreva či iných materiálov.

V rámci výskumu sme sa venovali skúmaniu teplôt vzplanutia a vznietenia kociek jaseňového dreva. Vzorky boli pripravené rezaním na pokosovej píle s rozmermi 2 × 2 cm a hmotnosťou približne 3 g každá. Pred samotným meraním boli kocky vysušené v sušiarni pri teplote 100 °C počas dvoch hodín, aby sa odstránila vlhkosť a zabezpečila reprodukovateľnosť výsledkov.

Experiment sme vykonávali na Setchkinovej peci, ktorá sa nachádza na Obrázku 1.

Pred začiatkom skúšky, bolo nutné pec predohriať na požadovanú teplotu a zabezpečiť stabilizáciu teplotního režimu. Následne bola vzorka vložená do pece a zaznamenávaal sa indukčný čas, teda čas od vloženia vzorky do momentu vzplanutia alebo vznietenia.

Teploty vzplanutia a vznietenia získané počas experimentu ú uvedené v Tabulkách 11 až 4.

Stanovené teploty vzplanutia a vznietenia pre jednotlivé druhy drevín sú dostupné v rôznych literárnych zdrojoch, odborných článkoch a iných vedeckých publikáciách. [14]

Obrázok 1. Setchkinova teplovzdušná pec

Súčasťou Setchkinovej pece sú dva termočlánky, prvý sa nachádza pod vzorkou a druhý nad ňou.

Teplota vzplanutia predstavuje najnižšiu teplotu, pri ktorej sa za presne definovaných podmienok skúšky uvoľní dostatočné množstvo horľavých plynov, na ktoré pôsobí zapaľovací plameň, čo spôsobí ich vzplanutie. Pred samotným meraním bolo potrebné nastaviť rýchlosť prietoku vzduchu na 25 mm.s^{-1} tak, že sa upraví skutočná rýchlosť prúdenia vzduchu q_v cez celý prierez vnútorného valca pri teplote pece na vypočítanú hodnotu v litroch za minútu podľa vzorca 1:

$$q_v = 6{,}62 \cdot \frac{293}{T} \tag{1}$$

Kde:

q_v rýchlosť prúdenia vzduchu (mm.s^{-1}),

T teplota (K).

Súčasťou stanovenia teploty vzplanutia a teploty vznietenia je aj výpočet aktivačnej energie, ktorý získame zo vzorca 2:

$$E = \ln\frac{\tau}{A} \cdot R \cdot T \tag{2}$$

Kde

E aktivačná energia (J.mol^{-1}),

t čas trvania reakcie,

A frekvenčný faktor,

R plynová konštanta,

T teplota (K).

Pri vykonávaní skúšky teploty vznietenia je rozhodujúce presné umiestnenie termočlánkov. Termočlánok TC1 slúži na meranie teploty samotnej vzorky a je umiestnený čo najbližšie k stredu jej hornej plochy, keď sa vzorka nachádza vo svojej polohe v peci. Vodič tohto termočlánku je upevnený na nosnej tyči, ktorá drží vzorku. Termočlánok TC2 zaznamenáva teplotu vzduchu prúdiaceho okolo vzorky. Je umiestnený vo vzdialenosti 10 mm ± 2 mm pod stredom misky, v ktorej je vzorka uložená, a je tiež vhodne pripevnený na nosnú tyč. Alternatívne môže byť inštalovaný cez otvor vyvŕtaný v strede uzáveru pod miskou. Termočlánok TC3 meria teplotu vykurovacej špirály a nachádza sa priamo pri nej, vedľa vykurovacieho telesa pece.

5 Výsledky merania

Výsledky experimentálneho merania teplôt vzplanutia a vznietenia jaseňového dreva sú uvedené v Tabuľkách 1 a 2. Tabuľka 1 prezentuje hodnoty teploty vzplanutia spolu s indukčnými časmi pri jednotlivých teplotách pece, zatiaľ čo Tabuľka 2 uvádza výsledky merania teploty vznietenia.

Z nameraných hodnôt vyplýva, že pri zvyšovaní teploty pece dochádza k postupnému skracovaniu indukčného času. Tento trend je typický pre procesy termického rozkladu organických materiálov a potvrdzuje kinetický charakter iniciácie horenia dreva.

Tabuľka 1. Vzplanutie vzoriek jaseňového dreva

	Teplota pece (°C)	**Indukčný čas (s)**	**Teplota vzplanutia (°C)**	**Teplota vzplanutia (K)**	**1/T (K^{-1})**
	320	490	335	608	0,00164474
	330	440	332	605	0,00165289
	340	380	352	625	0,0016
	350	294	365	638	0,0015674
	360	318	370	643	0,00155521
	370	323	367	640	0,0015625
	380	289	384	657	0,00152207
	390	278	375	648	0,00154321
	400	237	394	667	0,00149925
	410	253	390	663	0,0015083
Priemer	**365**	**330,2**	**366,4**	**639,4**	**0,00156556**

Aktivačná energia pri vzplanutí vzoriek jaseňového dreva bola vypočítaná na základe vzorca číslo 2 na 35 798 J.mol^{-1}.

Tabuľka 2. Vznietenie vzoriek jaseňového dreva

	Teplota pece (°C)	**Indukčný čas (s)**	**Teplota vznietenia (°C)**	**Teplota vznietenia (K)**	**1/T (K^{-1})**
	430	241	427	700	0,00142857
	440	217	429	702	0,0014245
	450	214	428	701	0,00142653
	460	171	450	723	0,00138313
	470	135	473	746	0,00134048
	480	119	465	738	0,00135501
	490	135	447	720	0,00138889
	500	104	475	748	0,0013369
	510	114	437	710	0,00140845
	520	112	445	718	0,00139276
Priemer	**475**	**156,2**	**447,6**	**720,6**	**0,00138852**

Aktivačná energia pri vznietení vzoriek jaseňového dreva bola vypočítaná na základe vzorca číslo 2 na 53 812 $J.mol^{-1}$.

Priemerná teplota vzplanutia jaseňového dreva bola stanovená na 366,4 °C, pričom priemerná teplota vznietenia dosiahla hodnotu 447,6 °C. Na základe experimentálnych údajov bola vypočítaná aj aktivačná energia procesu vzplanutia a vznietenia jaseňového dreva.

Výsledky merania teplôt vzplanutia a vznietenia smrekového dreva sú uvedené v Tabuľkách 3 a 4. Podobne ako pri jaseňovom dreve bolo možné pozorovať skracovanie indukčného času so zvyšujúcou sa teplotou pece.

Tabuľka 3. Vzplanutie vzoriek smrekového dreva

	Teplota pece (°C)	**Indukčný čas (s)**	**Teplota vzplanutia (°C)**	**Teplota vzplanutia (K)**	**1/T (K^{-1})**
	340	473	363	636	0,00157233
	350	340	373	646	0,00154799
	360	361	373	646	0,00154799
	370	329	385	658	0,00151976
	380	312	390	663	0,0015083
	390	265	395	668	0,00149701
	400	227	408	681	0,00146843
	410	241	396	669	0,00149477
	420	225	418	691	0,00144718
	430	242	416	689	0,00145138
Priemer	**385**	**301,5**	**391,7**	**664,7**	**0,00150551**

Aktivačná energia pri vzplanutí vzoriek smrekového dreva bola vypočítaná na základe vzorca číslo 2 na 44 984 $J.mol^{-1}$.

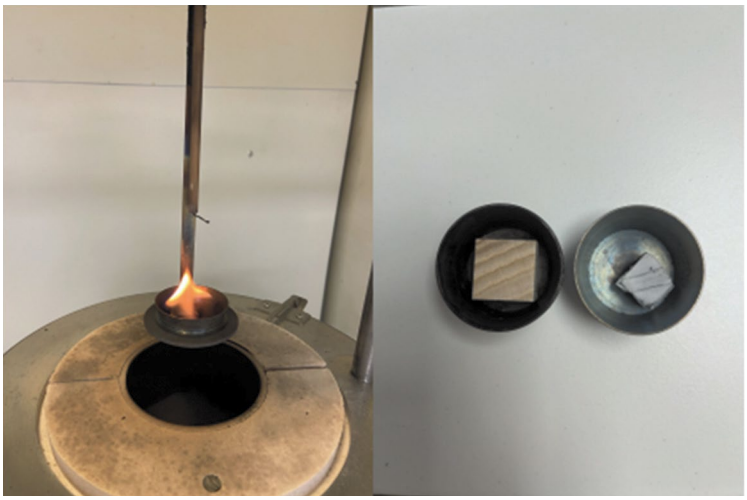
Tabuľka 4. Vznietenie vzoriek smrekového dreva

	Teplota pece (°C)	**Indukčný čas (s)**	**Teplota vznietenia (°C)**	**Teplota vznietenia (K)**	**1/T (K^{-1})**
	440	275	447	720	0,00138889
	450	211	495	768	0,00130208
	460	196	493	766	0,00130548
	470	161	483	756	0,00132275
	480	166	504	777	0,001287
	490	106	493	766	0,00130548
	500	105	510	783	0,00127714
	510	74	484	757	0,001321
	520	91	514	787	0,00127065
	530	64	541	814	0,0012285
Priemer	**485**	**144,9**	**496,4**	**769,4**	**0,0013009**

Aktivačná energia pri vznietení vzoriek smrekového dreva bola vypočítaná na základe vzorca číslo 2 na 67 166 $J.mol^{-1}$.

Pri smreku obyčajnom bola zistená priemerná teplota vzplanutia 391,7 °C, zatiaľ čo priemerná teplota vznietenia dosiahla hodnotu 496,4 °C.

Na Obrázku 2 je znázornený proces horenia vzorky a porovnanie stavu vzorky pred meraním a po skončení experimentu.



Obrázok 2. Proces horenia vzorky a porovnanie vzorky pred a po meraní

Na základe teplôt iniciácie aj hodnôt aktivačnej energie možno konštatovať, že smrek obyčajný vykazuje vyššiu tepelnú a kinetickú stabilitu než jaseň štíhly. Jaseň sa z hľadiska iniciácie horenia javí ako reaktívnejší materiál.

Rozdiely medzi smrekom obyčajným a jaseňom štíhlym môžu byť spôsobené kombináciou chemických, fyzikálnych a anatomických faktorov, ktoré ovplyvňujú priebeh tepelného rozkladu a tvorbu horľavých plynov.

6 Záver

Cieľom práce bolo experimentálne stanoviť teplotu vzplanutia, teplotu vznietenia, indukčné časy a aktivačnú energiu vybraných vzoriek jaseňa štíhleho a smreka obyčajného a následne porovnať ich tepelnú stabilitu.

Na základe vykonaných experimentov bolo zistené, že smrek obyčajný dosahuje vyššie hodnoty teploty vzplanutia aj teploty vznietenia než jaseň štíhly. Priemerná teplota vzplanutia smrekového dreva bola 391,7 °C a teplota vznietenia 496,4 °C, zatiaľ čo pri jaseňovom dreve boli tieto hodnoty 366,4 °C a 447,6 °C.

Vyššie hodnoty aktivačnej energie pri smrekovom dreve naznačujú vyššiu energetickú bariéru iniciácie horenia, a teda aj vyššiu tepelnú stabilitu tejto dreviny. So zvyšujúcou sa teplotou prostredia sa pri oboch drevinách skracoval indukčný čas, čo potvrdzuje kinetický charakter procesu tepelného rozkladu.

Získané výsledky prispievajú k lepšiemu poznaniu správania drevných materiálov a môžu byť využité pri hodnotení požiarneho rizika drevených konštrukcií alebo pri ďalšom výskume vlastností dreva pri pôsobení zvýšených teplôt.

V budúcnosti by bolo vhodné výskum rozšíriť aj o ďalšie druhy drevín a sledovať vplyv faktorov, ako sú vlhkosť dreva, hustota materiálu alebo aplikácia ochranných náterov, na proces iniciácie horenia.

Reference

[1] CIGÁŇOVÁ, S., 2018. Náchylnosť vybraných klonov jaseňov voči patogénnej hube [online]. [cit. 2025-04-27]. Dostupné na: https://vedanadosah.cvtisr.sk/priroda/zem/nachylnost-vybranych-klonov-jasenov-vocipatogennej-hube/

[2] WALKER, A., 2009. Dřevo. Praha: Grada Publishing. ISBN 978-80-247-2858-2

[3] Jaseň, 2013. Beliana – slovenská všeobecná encyklopédia [online]. [cit. 2025-04-27]. Dostupné na: https://beliana.sav.sk/heslo/jasen

[4] Jaseň štíhly, 2019. Lužný les [online]. [cit. 2025-04-27]. Dostupné na: https://www.luznyles.sk/sk/luzny-les/flora/jasen-stihly

[5] LEUGNEROVÁ, G., 2007. Fraxinus excelsior L. – jasan ztepilý / jaseň štíhly [online]. [cit. 2025-04-28]. Dostupné na: https://botany.cz/cs/fraxinus-excelsior/

[6] European ash, 2025. The Wood Database [online]. [cit. 2025-04-28]. Dostupné na: https://www.wood-database.com/european-ash/

[7] ECKENWALDER, J. E., 2009. Conifers of the World: The Complete Reference. Portland: Timber Press. ISBN 978-0-88192-974-4

[8] OECD, 2006. Safety Assessment of Transgenic Organisms. Vol. 2 of OECD Consensus Documents. Paris: OECD Publishing. ISBN 978-92-64-02958-7

[9] MITCHELL, A. F., 1974. A Field Guide to the Trees of Britain and Northern Europe. London: Collins. ISBN 978-0-00-219213-2

[10] HORGAN, T. et al., 2003. A Guide to Forest Tree Species Selection and Silviculture in Ireland. Dublin: National Council for Forest Research and Development (COFORD)

[11] SKRØPPA, T., 2003. EUFORGEN Technical Guidelines for Genetic Conservation and Use for Norway Spruce (Picea abies). Rome: International Plant Genetic Resources Institute

[12] JANSSON, G. et al., 2013. Forest tree breeding in Europe. In: PÂQUES, L. E., ed. Forest Tree Breeding in Europe. Dordrecht: Springer Netherlands. (Managing Forest Ecosystems; vol. 25)

[13] PRACIAK, A. et al., 2013. The CABI Encyclopedia of Forest Trees. Wallingford: CABI. ISBN 978-1-78064-236-9

[14] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2022. ISO 871:2022 Plastics – Determination of ignition temperature using a hot-air furnace. Geneva: ISO

Psychosociální rizika ve výrobním prostředí: Případová studie z automobilového průmyslu

Karolína Šablaturová[1], Hana Halíčková[2]

[1] VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství,
Lumírova 13, 700 30 Ostrava - Výškovice, karolina.sablaturova@vsb.cz

[2] VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství,
Lumírova 13, 700 30 Ostrava - Výškovice, hana.halickova@vsb.cz

Abstrakt:

Psychosociální rizika představují významnou oblast bezpečnosti a ochrany zdraví při práci, která je v automobilovém průmyslu umocněna vysokými pracovními požadavky, směnným provozem a centralizovanou organizační strukturou. Cílem studie bylo analyzovat psychosociální zátěž zaměstnanců ve vybraném podniku automobilového průmyslu pomocí kombinace kvantitativního dotazníku COPSOQ III a kvalitativních rozhovorů vedených se zaměstnanci středního managementu. Kvalitativní data byla zpracována v softwaru ATLAS.ti a identifikovala čtyři klíčová témata: strukturální nerovnost mezi výrobou a kanceláří, nedostatečnou komunikaci, snižování stavů a tlak na výkon, a pracovní podmínky spojené s únavou a vyčerpáním. Výsledky potvrzují, že psychosociální zátěž pramení především z kombinace organizačních a komunikačních faktorů, které se navzájem posilují. Studie zároveň poukazuje na význam otevřené komunikace, posílení autonomie a rozvoje wellbeing programů jako klíčových nástrojů pro zlepšení psychosociálního klimatu a kultury BOZP v automobilovém sektoru.

Klíčová slova: psychosociální rizika, automotive, rozhovor, kvalitativní analýza.

1 Úvod

Jedním z nejvýznamnějších problémů současnosti v oblasti bezpečnosti a ochrany zdraví při práci (BOZP) je podle EU-OSHA problematika psychosociálních rizik. Téměř 45 % evropských pracovníků udává, že se setkává s faktory, které mohou negativně ovlivnit jejich duševní zdraví, přičemž stres, úzkost a deprese představují druhý nejčastější zdravotní problém související s prací. Faktory, jako je nevhodná organizace a řízení práce a špatný sociální kontext mohou vést k nežádoucím psychickým i fyzickým dopadům na zdraví zaměstnanců. Mezi pracovní podmínky vedoucí k psychosociálním rizikům se řadí nadměrná pracovní zátěž, protichůdné nebo nejasné požadavky, nejistota zaměstnání, neúčinná komunikace nebo špatně řízená organizační změna. [1]

Základním předpisem v problematice psychosociálních rizik je rámcová směrnice 89/391/EHS ze dne 12. června 1989 o zavádění opatření pro zlepšení bezpečnosti a ochrany zdraví zaměstnanců při práci [2], která je do českého právního prostředí převedena v rámci zákona č. 262/2006 Sb., Zákoník práce [3]. V českém legislativním kontextu je dále v oblasti psychosociálních rizik klíčovým předpisem nařízení vlády č. 361/2007 Sb., které stanoví podmínky ochrany zdraví při práci [4] a vymezuje práci s psychickou zátěží. Ta zahrnuje činnosti spojené s monotonií, prací ve vnuceném pracovním tempu, v třísměnném či nepřetržitém provozu a práci vykonávanou pouze v noční době. Tyto faktory se v praxi často vyskytují právě v automobilovém průmyslu, který se vyznačuje vysokou intenzitou výroby, časovým tlakem, opakujícími se úkony a rostoucí automatizací. Tím dochází ke kumulaci fyzické i psychické zátěže pracovníků, což činí systematické hodnocení a prevenci psychosociálních rizik v tomto odvětví mimořádně významnými.

Hodnocení psychické zátěže, tak jak jej vyžaduje současná legislativa, zdaleka nereflektuje obsáhlost problematiky psychosociálních rizik. V České republice je tato oblast zatím řešena spíše dílčím způsobem, přestože mnoho nově vznikajících rizik vyžaduje komplexnější a systematičtější přístup. Efektivní řízení psychosociálních rizik má přitom přímý vliv nejen na ochranu zdraví zaměstnanců, ale také na výkonnost organizací. Přispívá ke snížení absence, fluktuace a chybovosti a zvyšuje kvalitu i produktivitu práce [1]. Cílem současného výzkumu probíhajícího v oblasti automobilového průmyslu je proto přispět k rozvoji metodik umožňujících systematickou identifikaci, hodnocení a prevenci těchto rizik v souladu s evropskými standardy.

V rámci probíhající studie bylo provedeno hodnocení psychosociálních faktorů pracovního prostředí prostřednictvím standardizovaného dotazníku Copenhagen Psychosocial Questionnaire (COPSOQ III) [5]. Výsledky tohoto šetření jsou v současné době zpracovávány, a proto nejsou součástí tohoto článku. Současně byla realizována doplňující kvalitativní část výzkumu formou polostrukturovaných rozhovorů se zaměstnanci, která umožňuje hlubší porozumění jejich zkušenostem a vnímání psychosociálních faktorů v pracovním prostředí. Tento článek se proto zaměřuje právě na prezentaci a interpretaci zjištění z této kvalitativní části studie.

2 Metodologie

Výzkumného šetření se zúčastnili zaměstnanci z výrobního podniku působícího v automobilovém průmyslu na území České republiky. Celkem bylo do výzkumu zahrnuto 70 respondentů (n = 70) zastupujících střední management na pozicích vedoucích týmů, údržby, skupin a junior leaderů. Věkové rozmezí bylo rozděleno do tří kategorií (< 31 let, 31–41 let, > 41 let), přičemž nejpočetnější skupinu tvořili zaměstnanci ve věku 31–41 let. Průměrná délka zaměstnání ve firmě činila více než 5 let u 92,7 % účastníků. Většina respondentů pracovala ve směnném provozu, což je pro automobilový sektor typické. Výběr účastníků proběhl ve spolupráci s personálním oddělením a bezpečnostními techniky, přičemž účast byla dobrovolná a anonymní.

Pro hodnocení psychosociálních faktorů pracovního prostředí byl použit standardizovaný dotazník COPSOQ III, který patří mezi nejrozšířenější nástroje pro identifikaci psychosociálních rizik na pracovišti [5]. Dotazník obsahoval 67 položek hodnocených pětibodovou Likertovou škálou (od „vždy“ po „nikdy“ nebo „zcela souhlasím“ po „zcela nesouhlasím“). Dotazníkové šetření tvořilo první fázi výzkumu, na kterou navázala kvalitativní část, zaměřená na hlubší pochopení identifikovaných problémů.

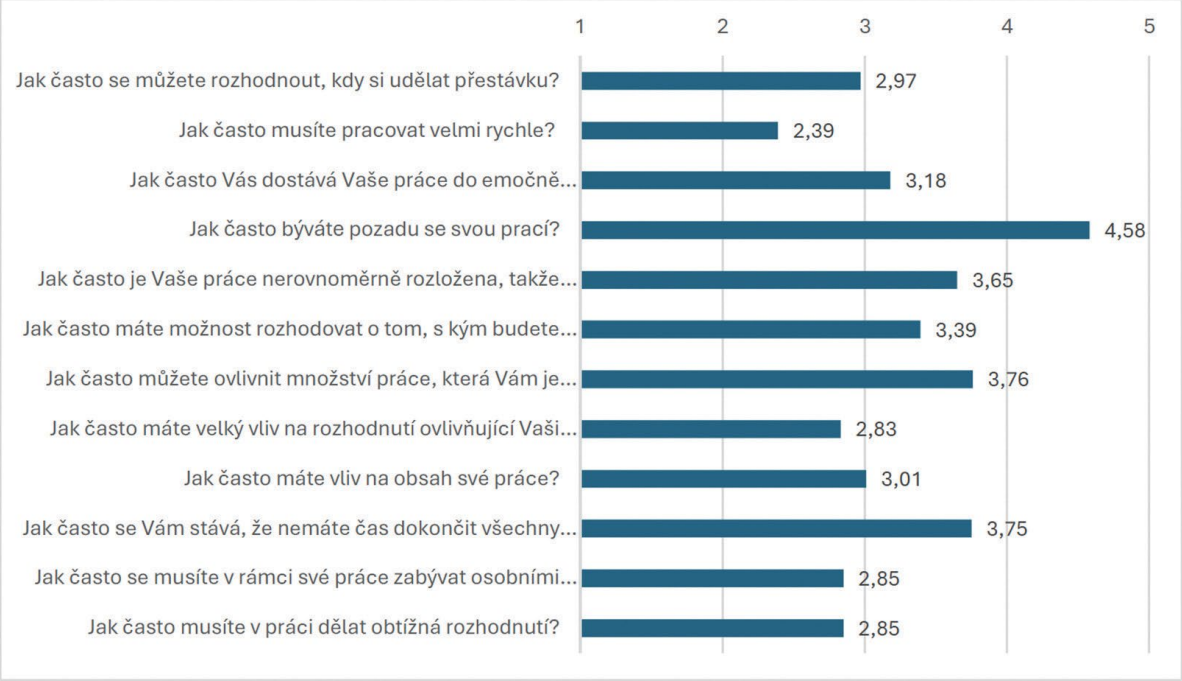
Za účelem hlubšího pochopení kontextu identifikovaných psychosociálních faktorů byly provedeny polostrukturované rozhovory typu „jeden na jednoho“. Rozhovory byly vedeny tazatelem a uskutečněny se všemi zaměstnanci středního managementu po vyplnění dotazníku. Každý rozhovor trval přibližně 30 minut a zaměřoval se na vnímání pracovního prostředí, mezilidských vztahů, pracovní zátěže, komunikace s nadřízenými a možností ovlivňovat pracovní podmínky. Po získání informovaného souhlasu byly rozhovory dokumentovány pomocí poznámek, které byly následně přepsány a analyzovány.

K analýze kvalitativních dat z rozhovorů byl využit software ATLAS.ti, který umožňuje systematické kódování a kategorizaci textových dat. Analýza probíhala metodou otevřeného a axiálního kódování s cílem identifikovat klíčová témata a významové kategorie. Tyto kategorie byly vytvářeny na základě opakujících se vzorců v datech a diskuse výzkumného týmu, což zajistilo validitu a transparentnost interpretace výsledků.

3 Výsledky

Na základě provedených polostrukturovaných rozhovorů se zaměstnanci středního managementu byla provedena kvalitativní analýza dat v softwaru ATLAS.ti. Tento postup umožnil identifikovat šest hlavních tematických oblastí, přičemž čtyři z nich se ukázaly jako klíčové pro pochopení psychosociální zátěže zaměstnanců v automobilovém průmyslu: (1) strukturální nerovnost mezi výrobou a kanceláří, (2) komunikační problémy a nízká důvěra ve vedení, (3) snižování stavů a tlak na výkon a (4) pracovní podmínky a vyčerpanost.

Tyto kvalitativní poznatky doplňuje i grafické znázornění vybraných položek dotazníkového šetření, které zachycuje subjektivní hodnocení některých aspektů práce souvisejících s pracovní autonomií, pracovním tempem, emoční zátěží a spokojeností s prací (Obrázek 1). U škály platí, že hodnota 1 znamená „vždy“ a hodnota 5 „nikdy“. Z grafu je patrné, že respondenti relativně častěji uváděli nutnost pracovat velmi rychle (2,39), obtížnost dokončit všechny pracovní úkoly včas (3,75) a určitou emoční zátěž spojenou s výkonem práce (3,18). Současně se ukazuje spíše omezená možnost ovlivnit některé aspekty vlastní práce, například rozhodování o přestávkách (2,97), důležitých pracovních rozhodnutích (2,83) nebo obsahu práce (3,01). Naopak nejvyšší hodnota byla zaznamenána u položky „Jak často býváte pozadu se svou prací?“ (4,58), což naznačuje, že respondenti se i přes vnímané pracovní zatížení většinou nepovažují za dlouhodobě nestíhající. Graf tak vhodně doplňuje kvalitativní zjištění a ukazuje, že psychosociální zátěž není tvořena jedním izolovaným faktorem, ale kombinací pracovního tempa, omezené autonomie a emočních nároků.



Obrázek 1. Vybrané položky dotazníkového šetření zaměřené na pracovní autonomii, pracovní tempo, emoční zátěž a spokojenost s prací (1 = vždy, 5 = nikdy)

Jedním z nejvýraznějších témat, které se objevovalo napříč rozhovory, byla vnímaná nerovnost mezi zaměstnanci z výroby a administrativy. Tato nerovnost se projevuje jak v možnostech rozhodování, tak v přístupu vedení k jednotlivým skupinám pracovníků. Zaměstnanci z výroby popisovali, že se cítí být na nižší úrovni hierarchie, jejich názory nejsou brány v potaz a nové návrhy bývají často odmítány. Tento pocit je posilován tím, že rozhodnutí přicházejí „shora“ bez dostatečné znalosti provozní reality. Časté byly výroky jako „nahoře pracují v bublině“ nebo „my děláme, oni si chodí na kafíčka“, které vyjadřují frustraci z nedostatku komunikace a uznání. Nerovnost

je vnímána i v praktické rovině – zaměstnanci uvádějí rozdílné podmínky v oblasti přestávek, benefitů či délky pracovních směn. Tento stav vede ke ztrátě motivace a oslabuje vztah zaměstnanců k firmě.

Druhé klíčové téma představuje komunikace mezi vedením a zaměstnanci. Rozhovory ukázaly, že tok informací je často jednostranný, zpožděný nebo nejasný. Změny v organizaci práce bývají oznamovány bez předchozí diskuse, což u zaměstnanců vyvolává nejistotu a pocit bezmoci. Zaměstnanci uváděli, že jejich připomínky nebo návrhy nejsou brány vážně, což oslabuje důvěru v management a podporuje rezignovaný postoj. Na druhé straně se objevují i pozitivní příklady. Jedná se především o přímé nadřízené, kteří se snaží udržet dobré mezilidské vztahy, řeší konflikty lidsky a podporují týmovou soudržnost. Právě tato úroveň řízení je vnímána jako klíčová pro udržení funkční komunikace a relativně stabilního pracovního klimatu.

Výrazným stresorem je podle respondentů dlouhodobé snižování počtu pracovníků ve výrobě při zachování nebo dokonce zvyšování výrobních plánů. Tento stav je popisován jako jeden z hlavních zdrojů psychické i fyzické zátěže. Zaměstnanci uváděli, že jsou často nuceni zastupovat chybějící kolegy, což zvyšuje pracovní tempo a omezuje možnost přestávek. Někteří zaměstnanci navíc popisovali, že místo své řídicí role musí pravidelně pracovat na lince, což vnímají jako degradující a demotivující. Nedostatek personálu se také promítá do napětí a častějších konfliktů na pracovišti. Zaměstnanci vyjadřovali obavy, že současné podmínky nejsou dlouhodobě udržitelné a zmiňovali zvýšený počet odchodů či úvah o změně zaměstnání. Zákaz přesčasů, který měl původně zlepšit pracovní podmínky, je naopak vnímán jako další stresor, protože omezuje flexibilitu plánování a snižuje výdělek pracovníků.

Téma pracovních podmínek se objevovalo napříč všemi rozhovory a představuje kombinaci fyzické i psychické zátěže. Zaměstnanci často popisovali únavu, nedostatek spánku a potíže se sladěním pracovního a osobního života, především kvůli třísměnnému provozu. Starší pracovníci uváděli, že adaptace na nové technologie je pro ně náročná a přispívá k vyšší psychické zátěži. Na některých pracovištích (např. chemická linka) byla opakovaně zmiňována vysoká fyzická náročnost, horko a nepříjemné pracovní podmínky. Zaznamenány byly i pozitivní změny. Jednalo se například o instalaci klimatizace a zavedení některých benefitů, které přispěly k částečnému zlepšení pracovního komfortu. Přesto převažuje pocit dlouhodobého vyčerpání a potřeby větší podpory ze strany vedení.

Analýza rozhovorů ukázala, že psychosociální zátěž zaměstnanců v automobilovém průmyslu má systémový charakter vyplývající z kombinace organizačních, komunikačních a provozních faktorů. Klíčovými rizikovými oblastmi jsou nedostatečná komunikace, strukturální nerovnost a vysoké pracovní tempo spojené s nižším počtem pracovníků. Tyto faktory se navzájem posilují a vedou k dlouhodobému stresu, pocitu nespravedlnosti a ztrátě motivace. Přesto výsledky ukazují, že zlepšení je možné. Respondenti pozitivně hodnotili otevřenější přístup přímých nadřízených, rozvoj benefitů a snahu o lepší pracovní podmínky. Pro udržitelné zlepšení psychosociálního klimatu je klíčové posílit transparentní komunikaci, spravedlivé rozdělení odpovědností a systematickou podporu wellbeing programů.

4 Diskuse

Výsledky kvalitativní analýzy potvrzují, že psychosociální zátěž zaměstnanců v automobilovém průmyslu pramení především z kombinace organizačních a komunikačních faktorů. Klíčovým zdrojem těchto problémů je silně centralizovaná rozhodovací struktura, v níž jsou pracovníci výroby a nižšího managementu jen omezeně zapojeni do plánování a realizace změn. Tento stav vede k pocitu bezmoci, nerovnosti a nízké důvěry ve vedení, které se dále promítají do poklesu motivace a celkové pracovní spokojenosti. Situaci umocňuje dlouhodobé snižování stavů, které zvyšuje pracovní tempo a snižuje prostor pro odpočinek, i neefektivní interní komunikace, jež je

často jednostranná a bez zpětné vazby. Kombinace těchto faktorů vytváří prostředí trvalého napětí a únavy, které může vést k fluktuaci a postupné ztrátě loajality k organizaci.

Zjištěné problémy jsou v souladu se závěry zahraničních studií [6,7], které v prostředí automobilového průmyslu popsaly obdobné fenomény, jako vysoké pracovní požadavky, nízkou kontrolu nad prací, nedostatek uznání a slabou podporu ze strany vedení. Tato shoda ukazuje, že psychosociální rizika v automobilovém sektoru mají mezinárodní a strukturální charakter, spíše než lokální příčiny. Silnou stránkou předložené studie je hloubka kvalitativních dat, která umožnila detailně zachytit subjektivní vnímání pracovního klimatu a identifikovat konkrétní organizační problémy. Naopak omezením zůstává velikost vzorku a jednorázový charakter výzkumu, který neumožňuje sledovat vývoj rizik v čase.

Na základě získaných poznatků lze doporučit opatření směřující ke zlepšení psychosociálního klimatu v podniku. Klíčová je především podpora obousměrné komunikace mezi vedením a zaměstnanci, posílení autonomie nižších manažerských pozic, rozvoj komunikačních a vůdčích dovedností vedoucích pracovníků a zavedení wellbeing programů zaměřených na prevenci stresu a podporu duševní pohody. Tato opatření mohou přispět ke zvýšení důvěry, spravedlnosti a sounáležitosti zaměstnanců, a tím i k dlouhodobé udržitelnosti a konkurenceschopnosti automobilového podniku.

5 Závěr

Zjištění z kvalitativní části výzkumu potvrzují, že psychosociální zátěž zaměstnanců v automobilovém průmyslu má komplexní charakter a je výsledkem vzájemného působení organizačních, komunikačních a provozních faktorů. Identifikovaná témata jako nerovnost mezi výrobními a administrativními pracovníky, nedostatečná komunikace, snižování stavů a tlak na výkon vytvářejí prostředí zvýšeného stresu a dlouhodobé psychické zátěže. Tato zjištění korespondují s výsledky zahraničních studií a v kombinaci s předběžnými výsledky kvantitativní části výzkumu realizované prostřednictvím dotazníku COPSOQ III poskytují komplexní pohled na problematiku psychosociálních rizik v průmyslovém prostředí.

Na základě provedeného šetření lze konstatovat, že systematické řízení psychosociálních rizik v automobilovém průmyslu je nezbytné nejen z hlediska ochrany zdraví zaměstnanců, ale také pro udržení efektivity a konkurenceschopnosti organizací. Doporučit lze zavedení pravidelného monitoringu pracovního klimatu, školení vedoucích pracovníků zaměřených na prevenci stresu a podporu duševní pohody a rozvoj mechanismů pro otevřenou komunikaci a zpětnou vazbu. Vhodným doplňkem jsou také programy podpory duševního zdraví a rovnováhy mezi pracovním a osobním životem.

Další výzkum by měl směřovat k rozšíření výzkumného vzorku na různé úrovně řízení a na více podniků automobilového průmyslu, případně provedení longitudinální studie sledující vývoj psychosociálních rizik v čase. Jako vhodné se jeví využití pokročilých analytických nástrojů, například využití umělé inteligence pro zpracování textových dat z rozhovorů, které by mohlo přinést detailnější vhled do dynamiky psychosociálních procesů v pracovním prostředí. Integrace těchto poznatků do systému řízení pracovních rizik představuje klíčový krok k posílení zdraví, spokojenosti a udržitelnosti pracovních týmů v automobilovém sektoru a k rozvoji kultury bezpečnosti.

Reference

[1] Psychosociální rizika a duševní zdraví při práci. Evropská agentura pro bezpečnost a ochranu zdraví při práci. Retrieved October 10, 2025, from https://osha.europa.eu/cs/themes/psychosocial-risks-and-mental-health

[2] SMĚRNICE RADY 89/391/EHS o zavádění opatření pro zlepšení bezpečnosti a ochrany zdraví zaměstnanců při práci (1989). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01989L0391-20081211

[3] Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů. (2006). Sbírka zákonů České republiky. Retrieved from https://www.zakonyprolidi.cz/cs/2006-262

[4] Nařízení vlády č. 361/2007 Sb. (2007). O stanovení podmínek ochrany zdraví při práci. Sbírka zákonů České republiky. Retrieved from https://www.e-sbirka.cz/sb/2007/361?zalozka=dalsiInformace

[5] T. S. Kristensen, H. Hannerz, A. Høgh, V. Borg. The Copenhagen Psychosocial Questionnaire-a tool for the assessment and improvement of the psychosocial work environment. Scand J Work Environ Health. 2005 Dec;31(6):438-49. doi: 10.5271/sjweh.948. PMID: 16425585

[6] R. Amiry, SS69-03 PSYCHOSOCIAL RISKS IN THE AUTOMOTIVE INDUSTRY IN TANGIER, Occupational Medicine, Volume 74, Issue Supplement_1, July 2024, Page 0, https://doi.org/10.1093/occmed/kqae023.0397

[7] K. Gyllensten, K. Torén, M. Hagberg, M. Söderberg. A sustainable working life in the car manufacturing industry: The role of psychosocial factors, gender and occupation. PLoS One. 2020 May 14;15(5):e0233009. doi: 10.1371/journal.pone.0233009. PMID: 32407358; PMCID: PMC7224489

Ekonomicko-sociální aspekty ergonomie v kontextu české legislativy: rámec pro vyčíslení přínosů ergonomických projektů

Dariusz Trachta[1]

[1] VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství,
17. listopadu 15, 708 00 Ostrava-Poruba, dariusz.trachta@vsb.cz

Abstrakt:

Ergonomie je v praxi často prezentována jako „měkké“ téma zaměřené na zdraví zaměstnanců, avšak řada studií ukazuje, že dobře vedené ergonomické projekty přinášejí měřitelné ekonomické i sociální efekty – vyšší produktivitu, stabilitu procesu, kvalitu, nižší absenci a fluktuaci a zároveň lepší dostupnost práce pro širší skupiny zaměstnanců. Cílem příspěvku je navrhnout praktický rámec pro vyčíslení přínosů ergonomických intervencí s důrazem na český právní kontext. Rámec kombinuje (i) obecně používané kategorie benefitů popsané v literatuře (náklady na WMSD, ztracený čas, kvalita, nábor a zaškolení, pojistné a compliance) a (ii) přímé mzdové a organizační dopady vyplývající z české legislativy – zejména bezpečnostní přestávky při překročení hygienických limitů fyzické, lokální svalové, polohové či zrakové zátěže a příplatek za práci ve ztíženém pracovním prostředí. Součástí je i stručné shrnutí důkazů o vlivu osvětlení a hluku na výkon a chybovost, protože právě tyto faktory mohou rozhodovat o klasifikaci práce jako ztížené nebo o nutnosti bezpečnostních přestávek. Výstupem je postup a soubor jednoduchých výpočtů (cost-of-constraints), které umožňují firmám rychle odhadnout roční úspory a dobu návratnosti a současně zviditelňují sociální přínosy ergonomie (participace, motivace, inkluze) jako součást udržitelného řízení práce. Rámec je ilustrován na modelových výpočtech pro rok 2026, kde lze minimální náklady vybraných legislativních požadavků přímo odvodit z hodinové minimální mzdy (např. minimální příplatek 10 % minimální mzdy za každý ztěžující vliv).

Klíčová slova: ergonomie, ekonomické hodnocení, ROI, bezpečnostní přestávky, ztížené pracovní prostředí, česká legislativa.

1 Úvod

Ergonomické projekty jsou v mnoha firmách stále vnímány primárně jako nástroj prevence pracovně souvisejících muskuloskeletálních poruch (WMSD). Současně však existuje rozsáhlá evidence, že ergonomie je schopna generovat přímé i nepřímé ekonomické přínosy, které lze kvantifikovat a využít při rozhodování o investicích [1–4].

Ekonomická zátěž WMSD je v Evropě dlouhodobě významná; dopady se projevují na úrovni jednotlivých zaměstnavatelů (absence, fluktuace, zhoršení kvality, omezená flexibilita plánování) i na úrovni společnosti (zdravotní a sociální systémy) [5–7]. To je v souladu s evropským rámcem BOZP, který ukládá zaměstnavatelům povinnost rizika hodnotit a snižovat, mimo jiné i v oblasti ruční manipulace s břemeny [8, 9].

Tento příspěvek navrhuje rámec pro vyčíslení přínosů ergonomických projektů s ohledem na český právní kontext. Vedle obecných nákladových kategorií (cost-of-illness, productivity, quality) se zaměřuje na dvě oblasti, kde české právo vytváří přímo ocenitelné „nákladové omezení“ (cost-of-constraints): (i) bezpečnostní přestávky při překročení hygienických limitů, (ii) příplatek za práci ve ztíženém pracovním prostředí a (iii) povinný příspěvek na zaměstnancův produkt spoření na stáří ve výši 4 % z vyměřovacího základu za rozhodné období.

2 Teoretické východisko

Literatura z oblasti „business case for ergonomics“ opakovaně ukazuje, že úspěšné projekty mají společné znaky: jasně definovaný problém, zapojení vedení, participaci pracovníků, měřitelné cíle a transparentní finanční vyhodnocení [1–4]. Hendrick [2] uvádí, že návratnost investic do ergonomie se typicky opírá o kombinaci úspor z nižší úrazovosti/WMSD, zkrácení času cyklu, redukce zmetkovitosti a snížení fluktuace.

V praxi se přínosy ergonomických projektů kumulují v několika opakujících se kategoriích, které lze převést do finančního vyjádření prostřednictvím výrobních, HR a BOZP dat. Níže uvádíme přehled typických položek a jejich logiky výpočtu (stručně) [1–7].

2.1 Ekonomické a organizační přínosy ergonomie

Ergonomické projekty a cílené ergonomické intervence mohou generovat měřitelné ekonomické i organizační přínosy prostřednictvím několika vzájemně provázaných mechanismů. V první řadě se jejich efekt často promítá do zvýšení produktivity práce, zejména díky zkrácení cyklového času, omezení neproduktivních intervalů (čekání, prostoje) a zlepšení plynulosti toku činností. V provozní praxi se tento dopad obvykle projeví buď nárůstem výstupu na směnu, nebo možností redukovat rozsah přesčasové práce při zachování požadovaného objemu výroby. Současně dochází ke zlepšení parametrů kvality, protože ergonomicky stabilnější úchopy, lepší viditelnost pracovního prostoru a nižší úroveň únavy snižují chybovost a riziko poškození výrobků při manipulaci. Výsledkem bývá pokles zmetkovitosti, omezení reworku a redukce reklamací, což má přímý dopad na náklady spojené s opravami, logistickými toky i zákaznickým servisem.

Důležitou oblast představují personální dopady, zejména snížení fluktuace zaměstnanců. Pokud ergonomická opatření vedou ke snížení fyzické náročnosti a souvisejících obtíží (např. bolestivosti či funkčních omezení), klesá podíl odchodů motivovaných náročností práce, roste stabilita týmů a snižují se ztráty provozního know-how. S tím úzce souvisí i nižší náklady na nábor a adaptaci pracovníků: menší počet volných pozic obvykle znamená méně náborových kampaní, nižší časovou zátěž mistrů a školitelů a menší rozsah adaptačních nákladů. Do těchto nákladů je vhodné zahrnovat nejen samotné zaškolení, ale i související položky, které se u nově nastupujících pracovníků standardně kumulují (např. osobní ochranné pracovní prostředky, administrativní úkony, pracovnělékařské prohlídky, základní výstroj a vybavení).

Z pohledu řízení rizik a nákladů lze přínosy ergonomie zachytit také v oblasti bezpečnosti práce a ochrany zdraví. Ergonomické projekty mohou snižovat pravděpodobnost pracovních úrazů a muskuloskeletálních onemocnění (WMSD), čímž se redukují jak přímé, tak nepřímé náklady. Mezi typické nákladové položky patří vyšetřování událostí, náklady na zastupitelnost, výpadky výroby, kompenzace, případně i reputační dopady. Pokles škodních událostí navíc může snižovat celkové náklady spojené s pojistnými plněními a u některých forem komerčního připojištění (např. úrazové či odpovědnostní pojištění) posilovat vyjednávací pozici zaměstnavatele při nastavování pojistných podmínek. Ergonomická optimalizace se dále může pozitivně projevit ve snížení nákladů na nástroje, přípravky a komponenty, protože redukce potřebných sil, rázů a neergonomických manipulací vede k menšímu mechanickému namáhání nástrojů i k nižší míře poškození dílů (např. pády výrobků, oděry nebo deformace), což je významné zejména v procesech s vysokou frekvencí manipulace.

V neposlední řadě je vhodné zohlednit i náklady a rizika spojené s uznáváním nemoci z povolání. Ergonomická opatření mohou snížit pravděpodobnost zahájení a průběhu administrativně i finančně náročných procesů, které zahrnují odborné posudky, šetření, dokumentaci, kompenzace a případné přeřazení zaměstnance, stejně jako navazující organizační dopady. V dlouhodobém horizontu může zlepšení ergonomických parametrů práce

přispět také k potenciálnímu snížení nákladů na dozor nad pracovním prostředím. Pokud dojde ke snížení expozice rizikovým faktorům a následně ke změně kategorizace práce, může klesnout rozsah a frekvence měření, odborných posudků a související administrativy (včetně dokumentace a komunikace s orgány ochrany veřejného zdraví).

2.2 Sociální přínosy a udržitelnost práce

Z hlediska sociálních aspektů ergonomie přesahuje ochranu zdraví: zvyšuje udržitelnost práce (pracovní schopnost v čase), podporuje inkluzi (možnost obsazovat pozice širším spektrem zaměstnanců), posiluje motivaci a percepci spravedlivých podmínek. Empirické studie ukazují, že participace zaměstnanců může pozitivně ovlivnit well-being i organizační výkon [16].

Konkrétní sociální dopady lze ilustrovat na dvou příkladech z praxe:

Příklad 1 (Slovensko – implementace průmyslového manipulátoru pro manipulaci s kuchyňskými dřezy): Ve výchozím stavu byla pracovní činnost charakterizována vysokou kumulativní manipulovanou hmotností, častým výskytem nefyziologických pracovních poloh a zvýšenou repetitivností pohybů. Tato kombinace faktorů vedla k vysokým nárokům na fyzickou kapacitu pracovníka a v praxi se promítala do omezené obsaditelnosti pracovního místa pouze na část pracovní populace, čímž se snižovala flexibilita personálního plánování směn. Zavedení účelového průmyslového manipulátoru vedlo k významné redukci fyzické zátěže (zejména mechanického zatížení při ruční manipulaci) a současně ke zvýšení „přístupnosti“ práce z hlediska požadavků na sílu a toleranci zátěže. Pracoviště se tak stalo obsaditelné širším spektrem pracovníků, včetně žen a osob se sníženou fyzickou kapacitou, což rozšířilo interní trh práce a snížilo riziko personálních výpadků a provozní zranitelnosti [22].

Příklad 2 (redukce lokální svalové zátěže prostřednictvím výměny kovového trnu za teflonový): Na pracovišti, kde operátor stahoval kabel z kovové tyče, bylo ve výchozím stavu vyžadováno opakované vyvíjení vysoké svalové síly oběma horními končetinami. Vysoký koeficient tření na rozhraní kabel-kovový trn determinoval zvýšené požadavky na sílu a vedl k výrazné lokální svalové zátěži, což dlouhodobě limitovalo obsazování pracovního místa převážně na pracovníky s vyšší svalovou kapacitou (v praxi zejména muže). Po nahrazení kovového trnu teflonovým došlo ke snížení třecího odporu a tím k významnému poklesu požadované síly, následně i k redukci lokální svalové zátěže. Z hlediska sociálních dopadů představovala intervence zvýšení inkluzivity pracovního místa a současně posílení stability personálního pokrytí směn, protože pracoviště bylo možné obsazovat širším spektrem pracovníků, včetně žen a osob s omezenou svalovou silou. Technická opatření a hodnocení rizik ve výrobě

V průmyslu se jako účinné intervence často uplatňují technická opatření (manipulátory, exoskeletony, úpravy pracovišť), která snižují biomechanickou zátěž při zachování produktivity [17]. V českých výrobních podnicích jsou ergonomická rizika stále častá a jejich systematické hodnocení je předpokladem pro cílené zásahy [18, 19].

3 Český legislativní rámec pro kvantifikaci přínosů

České právní předpisy významně chrání zdraví zaměstnanců tím, že vytvářejí různá opatření, která zaměstnavatele nutí ke zlepšování pracovních podmínek. Níže jsou uvedeny příklady takových opatření, která jsou specifická pro Českou republiku.

3.1 Bezpečnostní přestávky a režim práce

Český systém ochrany zdraví při práci stanovuje hygienické limity a organizační režimy práce zejména prostřednictvím nařízení vlády č. 361/2007 Sb. (podmínky ochrany zdraví při práci) [11]. Při překročení vybraných limitů (celková fyzická zátěž, lokální svalová zátěž, pracovní poloha, ruční manipulace s břemeny, monotónnost a vnucené tempo, zraková zátěž aj.) musí být práce přerušována bezpečnostními přestávkami typicky v trvání 5 až 10 minut nejpozději po každých 2 hodinách práce; poslední bezpečnostní přestávka se zařazuje nejpozději 1 hodinu před koncem směny [11].

Bezpečnostní přestávky se – na rozdíl od přestávky na jídlo a oddech – započítávají do pracovní doby, protože vyplývají ze zvláštních právních předpisů (zákoník práce, zákon č. 262/2006 Sb.) [10]. Z hlediska ekonomického hodnocení jde tedy o placený čas, který je nutné plánovat a který může snižovat disponibilní výrobní kapacitu, pokud není kompenzován reorganizací práce.

3.2 Příplatek za práci ve ztíženém pracovním prostředí

Druhou přímo ocenitelnou oblastí je příplatek za práci ve ztíženém pracovním prostředí. Pro zaměstnance odměňované mzdou stanoví nařízení vlády č. 443/2024 Sb., že příplatek činí za každý ztěžující vliv nejméně 10 % minimální mzdy [12]. Minimální mzda pro rok 2026 činí 134,40 Kč/h (22 400 Kč/měs.) [13], takže minimální příplatek představuje 13,44 Kč/h za každý ztěžující vliv. Pokud ergonomický projekt (např. snížení hluku pod hygienický limit, zlepšení mikroklimatu nebo eliminace expozice vibracím) odstraní podmínky pro klasifikaci „ztíženého pracovního prostředí“, lze tuto položku přímo zahrnout do roční úspory.

Vedle toho lze do hodnocení zahrnout i další legislativně podmíněné náklady, například požadavky na režim práce při zátěži teplem (střídání práce a bezpečnostní přestávky) či organizaci práce se zrakovou zátěží, kde kvalita osvětlení a oslňování mohou hrát významnou roli [11].

3.3 Povinný příspěvek na produkty spoření na stáří u rizikové práce

Od 1. 1. 2026 je účinný zákon č. 324/2025 Sb., který zavádí povinnost zaměstnavatele hradit zaměstnancům vykonávajícím vybrané rizikové práce povinný příspěvek na produkt spoření na stáří. Povinnost se vztahuje na práci zařazenou do 3. kategorie rizika (dle ochrany veřejného zdraví) pro faktory vibrace, zátěž chladem, zátěž teplem nebo celkovou fyzickou zátěž při dynamické práci velkými svalovými skupinami [20].

Výše příspěvku činí 4 % z vyměřovacího základu za rozhodné období (kalendářní měsíc), pokud zaměstnanec v daném měsíci odpracoval alespoň 3 směny rizikové práce [20]. Vedle přímého finančního dopadu je třeba uvažovat i organizační nároky: evidenci směn rizikové práce, informační povinnost vůči zaměstnancům a potvrzení o zaplaceném příspěvku [20]. Z pohledu ergonomického business case je tento mechanismus významný, protože ergonomická opatření, která sníží expozici a umožní přeřazení práce do nižší kategorie rizika, mohou u vybraných pracovišť eliminovat i tuto povinnou položku.

3.4 Náklady pracovnělékařských prohlídek

Další často opomíjenou nákladovou položkou jsou pracovnělékařské prohlídky (zejména vstupní, periodické, mimořádné a výstupní), které zaměstnavatel zajišťuje v návaznosti na rizikovost práce a její kategorizaci. V českých podmínkách se zařazení práce do kategorií a posouzení rizikových faktorů opírá o postupy a kritéria stanovená vyhláškou č. 432/2003 Sb. [22]. Z ekonomického hlediska je vhodné do kalkulace zahrnout nejen přímé náklady

(cena vyšetření/posudku, případná doplňková vyšetření), ale i nepřímé náklady (čas zaměstnance strávený na prohlídce v pracovní době, náklady na zastupitelnost či prostoje) a organizační náklady (administrativa, objednávání, evidence posudků, doprava). Ergonomické projekty, které vedou ke snížení expozice rizikovým faktorům a následně mohou podpořit změnu kategorizace práce, mohou v delším horizontu přispět ke snížení rozsahu navazujících povinností a tím i k omezení souvisejících nákladů na pracovnělékařské služby [22].

Níže je uveden přehled typických přínosů, které jsou výsledkem ergonomických projektů.

Tabulka 1. Přehled typických přínosů ergonomických projektů a zdrojů dat

Oblast přínosu	**Měřitelný ukazatel**	**Zdroj dat / opora**
Bezpečnostní přestávky	min / směna; plánovaná kapacita	NV 361/2007 Sb.; ZP 262/2006 Sb. [10, 11]
Ztížené pracovní prostředí	Kč / h; počet ztěžujících vlivů	NV 443/2024 Sb.; minimální mzda [12, 13]
WMSD a absence	DN (days lost), náklady/den	HR data; literatura o nákladech MSD [5–7]
Kvalita a zmetkovitost	% zmetků; rework; reklamace	Výroba/QA; interní náklady; literatura [1–4]
Fluktuace	odchody/rok; náklady na náhradu	HR; nábor/školení; literatura [2–6]
Sociální dopady	spokojenost; inkluze; participace	Dotazníky; participace a výkon [16]
Produktivita	čas cyklu; ks/směna; OEE	Výroba; průmyslové KPI; literatura [1–4]
Nábor a zaškolení	Kč/odchod; doba adaptace; OOPP	HR; interní kalkulace; literatura [2–6]
Úrazy a nemoci z povolání	počet událostí; DN; náklady na odškodnění	BOZP/HR; interní data; literatura [5–7]
Pojištění	pojistné události; plnění; komerční pojistné	Účetnictví; pojišťovna; interní data
Nástroje a komponenty	počet výměn; spotřeba; poškození dílů	Údržba; nákup; interní evidence
Dozor a kategorizace práce	náklady na měření; posudky; dokumentace	BOZP; OOVZ; NV 361/2007 Sb. [11]
Povinný příspěvek na spoření na stáří	4 % z vyměřovacího základu; směny rizikové práce	Zákon č. 324/2025 Sb. [20]
Pracovnělékařské prohlídky (vstupní/ periodické/mimořádné/výstupní)	přímé + nepřímé + organizační náklady	Vyhláška č. 432/2003 Sb. [22]

4 Metodický postup vyčíslení přínosů

Pro účely rychlé rozhodovací podpory doporučujeme využít kombinaci „top-down“ a „bottom-up“ přístupu. Top-down část vychází z účetních a HR ukazatelů (absence, fluktuace, kvalita) a bottom-up část z detailní ergonomické analýzy pracoviště (expozice, režim práce, počet pracovníků).

Metodický postup kvantifikace ekonomických přínosů ergonomické intervence lze strukturovat do několika na sebe navazujících kroků. Nejprve je nezbytné jednoznačně vymezit hodnocené pracoviště či výrobní úsek, včetně počtu dotčených zaměstnanců, směnnosti a organizačního kontextu. Současně je vhodné explicitně popsat výchozí stav (baseline) a definovat cílový stav po realizaci změny, aby bylo možné následně transparentně přiřadit pozorované či očekávané dopady konkrétní intervenci. V dalším kroku se provede ergonomické hodnocení pracovních podmínek s využitím relevantních standardů (např. ČSN/ISO) nebo ověřených observačních metod, přičemž klíčovým výstupem je identifikace rizikových faktorů a posouzení, zda dochází k překročení hygienických limitů a zda z toho vyplývá nárok na bezpečnostní přestávky [11, 20]. Na základě výsledků hodnocení se následně

určí přítomnost tzv. ztěžujících vlivů ve smyslu platné právní úpravy a vypočte se minimální příplatek za práci ve ztíženém pracovním prostředí jako součin počtu ztěžujících vlivů a 10 % minimální mzdy [12, 13]. Pokud je zároveň práce kategorizována jako riziková ve 3. kategorii u vybraných faktorů (např. vibrace, chlad, teplo nebo celková fyzická zátěž při dynamické práci), je vhodné do ekonomické bilance zahrnout také povinný příspěvek ve výši 4 % z vyměřovacího základu podle zákona č. 324/2025 Sb. a ověřit splnění podmínky alespoň tří směn rizikové práce v kalendářním měsíci u dotčených zaměstnanců [21].

V navazující fázi se kvantifikují klíčové dopadové oblasti, a to zejména časové dopady (např. bezpečnostní přestávky, neproduktivní čekání, doba manipulace), dopady na kvalitu (zmetkovitost, rework, reklamace) a personální dopady (absence, fluktuace, náklady na nábor a adaptaci včetně zaškolení) [1–7]. Tyto proměnné tvoří základ pro odhad ročních úspor a pro vyčíslení finančního efektu intervence v čase. Závěrečným krokem je stanovení nákladů samotné intervence, a to jak investičních (CAPEX), tak provozních (OPEX), přičemž je vhodné explicitně zohlednit realizační rizika (např. zpoždění implementace, potřeba dodatečných úprav, adaptační fáze) a definovat hodnoticí metriky, jako jsou roční úspory, návratnost investice (ROI), doba návratnosti a citlivost výsledků na klíčové předpoklady a vstupní parametry [2–4].

Základní výpočet roční úspory lze vyjádřit jako součet dílčích položek:

S = přestávky + příplatek + příspěvek + absence + úrazy + fluktuace + kvalita + produktivita + ostatní – náklady,

kde „příspěvek“ reprezentuje úsporu z povinného příspěvku na produkty spoření na stáří u vybraných rizikových prací [21], „úrazy“ zahrnuje přímé i nepřímé náklady úrazů a WMSD a „ostatní“ může zahrnout nábor/zaškolení, náklady na OOPP u nových pracovníků, spotřebu nástrojů/komponentů či náklady na dozor a měření pracovního prostředí.

Kde např. úspora z bezpečnostních přestávek (pokud odpadne povinnost jejich poskytování nebo se nahradí nerizikovou rotací) může být odhadnuta jako:

přestávky = $(\Delta t / 60) \cdot C \cdot N \cdot D$,

kde Δt je změna délky bezpečnostních přestávek na směnu (min), C je hodinová cena práce (mzda + odvody + režie), N je počet zaměstnanců na dané práci a D je počet směn/rok.

Analogicky úspora z příplatku za ztížené prostředí:

příplatek = $C \cdot H \cdot N \cdot V$,

kde C je minimální příplatek na hodinu (např. 13,44 Kč/h v roce 2026), H je počet odpracovaných hodin/rok, N počet zaměstnanců a V počet ztěžujících vlivů, které byly eliminovány [12, 13].

Analogicky lze ocenit povinný příspěvek na produkty spoření na stáří:

příspěvek = $0{,}04 \cdot VZ$,

kde VZ je součet vyměřovacích základů zaměstnanců, kterým v daném kalendářním měsíci vznikla povinnost příspěvku (odpracovali alespoň 3 směny rizikové práce) [20]. V ročním vyjádření lze uvažovat součet za všechny měsíce a všechny dotčené zaměstnance. Tato položka je pro rozhodování užitečná zejména tehdy, pokud ergonomické opatření umožní snížit kategorizaci práce (a tím nárok na příspěvek).

Pro ilustraci: při vyměřovacím základu 40 000 Kč za měsíc představuje povinný příspěvek 1 600 Kč na zaměstnance a měsíc, pokud jsou splněny podmínky zákona [20].

V modelové ilustraci: pokud má pracoviště 20 zaměstnanců v jednosměnném provozu (220 směn/rok), vznikají bezpečnostní přestávky 3 x 10 min na směnu a hodinová cena práce je 250 Kč, pak „náklad“ bezpečnostních přestávek představuje přibližně (30/60) x 250 x 20 x 220 = 550 000 Kč/rok. Pokud je zároveň vyplácen minimální příplatek za jeden ztěžující vliv, činí tato položka 13,44 x 8 x 20 x 220 = 473 088 Kč/rok. Takové výpočty umožňují rychle rámcově posoudit návratnost technických i organizačních ergonomických opatření.

Významné jsou i „měkké“ (hůře ocenitelné) efekty: zlepšení osvětlení a snížení hluku mohou snižovat únavu, chybovost a zvyšovat subjektivní spokojenost. Výzkumy z průmyslových pracovišť popisují mechanismy, jak změny osvětlení ovlivňují výkon (vizuální výkon, komfort, biorytmy, motivace) [14], a empiricky prokazují vztah mezi úrovní osvětlení, hluku a produktivitou [15].

5 Závěr

Navržený rámec ukazuje, že ergonomické projekty lze v českém prostředí hodnotit nejen prostřednictvím obecných ukazatelů (WMSD, produktivita, kvalita), ale také přes konkrétní legislativně podmíněné náklady, které jsou přímo vypočitatelné. Bezpečnostní přestávky podle nařízení vlády č. 361/2007 Sb., příplatek za práci ve ztíženém pracovním prostředí podle nařízení vlády č. 443/2024 Sb. a povinný příspěvek na produkty spoření na stáří u vybraných rizikových prací podle zákona č. 324/2025 Sb. tvoří praktické „kotvy“ pro business case, protože umožňují rychle převést zátěž pracovního systému do finančního vyjádření [11–13, 20].

Současně je třeba přínosy ergonomie vnímat i sociálně: participace, inkluze a udržitelnost práce podporují dlouhodobou výkonnost organizace a její atraktivitu na trhu práce [17]. Budoucí práce by měla ověřit rámec na souboru reálných českých projektů a doplnit jej o standardizované sběry dat pro citlivostní analýzy a benchmarking mezi odvětvími.

Reference

[1] BEEVIS, D. a SLADE, I. M. Ergonomics-costs and benefits. Applied Ergonomics. 2003, 34(5), 413–418. DOI 10.1016/S0003-6870(03)00061-9

[2] HENDRICK, H. W. Determining the cost-benefits of ergonomics projects and factors that lead to their success. Applied Ergonomics. 2003, 34(5), 419–427. DOI 10.1016/S0003-6870(03)00062-0

[3] SEELEY, P. A. a MARKLIN, R. W. Business case for implementing two ergonomic interventions at an electric power utility. Applied Ergonomics. 2003, 34(5), 429–439. DOI 10.1016/S0003-6870(03)00063-2

[4] DE LOOZE, M. P., VINK, P., KONINGSVELD, E. A. P., KUIJT-EVERS, L. a VAN RHIJN, G. J. W. Cost-effectiveness of ergonomic interventions in production. Human Factors and Ergonomics in Manufacturing & Service Industries. 2010, 20(4), 316–323. DOI 10.1002/hfm.20223

[5] BEVAN, S. Economic impact of musculoskeletal disorders (MSDs) on work in Europe. Best Practice & Research Clinical Rheumatology. 2015, 29(3), 356–373. DOI 10.1016/j.berh.2015.08.002

[6] DE KOK, J. aj. Work-related musculoskeletal disorders: prevalence, costs and demographics in the EU. EU-OSHA. Luxembourg, 2019. DOI 10.2802/66947

[7] QIU, K. aj. The global macroeconomic burden of musculoskeletal disorders. International Journal of Surgery. 2025, 111(11), 7857–7866. DOI 10.1097/JS9.0000000000003072

[8] COUNCIL DIRECTIVE 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work. EUR-Lex, CELEX 31989L0391

[9] COUNCIL DIRECTIVE 90/269/EEC of 29 May 1990 on the minimum health and safety requirements for the manual handling of loads where there is a risk particularly of back injury to workers. EUR-Lex, CELEX 01990L0269-20190726

[10] Zákon č. 262/2006 Sb., zákoník práce (v platném znění)

[11] Nařízení vlády č. 361/2007 Sb., kterým se stanoví podmínky ochrany zdraví při práci (v platném znění)

[12] Nařízení vlády č. 443/2024 Sb., o vymezení ztíženého pracovního prostředí a o výši příplatku ke mzdě za práci ve ztíženém pracovním prostředí (v platném znění)

[13] MINISTERSTVO PRÁCE A SOCIÁLNÍCH VĚCÍ. Minimální mzda v roce 2026 (informační leták). Praha: MPSV, 2025/2026

[14] JUSLÉN, H. T., WOUTERS, M. C. H. M. a TENNER, A. D. Mechanisms involved in enhancing human performance by changing the lighting in the industrial workplace. International Journal of Industrial Ergonomics. 2005. DOI 10.1016/j.ergon.2005.03.002

[15] AKBARI, J., DEHGHAN, H., AZMOON, H. a FOROUHARMAJD, F. Relationship between lighting and noise levels and productivity of workers in automotive assembly industry. Journal of Environmental and Public Health. 2013. DOI 10.1155/2013/527078

[16] URIBETXEBARRIA, U., GARMENDIA, A. a ELORZA, U. Does employee participation matter? An empirical study on the effects of participation on well-being and organizational performance. Central European Journal of Operations Research. 2021, 29, 1397–1425. DOI 10.1007/s10100-020-00704-7

[17] DE LOOZE, M. P., BOSCH, T., KRAUSE, F., STADLER, K. S. a O'SULLIVAN, L. W. Exoskeletons for industrial application and their potential effects on physical workload. Ergonomics. 2016, 59(5), 671–681. DOI 10.1080/00140139.2015.1081988

[18] HOKE, A., HEINZOVÁ, R., VESELÍK, P. a MARTINKOVÁ, M. Assessment of Ergonomic Risks in Manufacturing Enterprises in the Czech Republic. Management and Production Engineering Review. 2024, 15(4), 1–10. DOI 10.24425/mper.2024.153119

[19] TAKALA, E. P. aj. Systematic evaluation of observational methods assessing biomechanical exposures at work. Scandinavian Journal of Work, Environment & Health. 2010, 36(1), 3–24. DOI 10.5271/SJWEH.2876.

[20] Zákon č. 324/2025 Sb., o povinném příspěvku na produkty spoření na stáří a o změně souvisejících zákonů (v platném znění)

[21] TRACHTA, D., ŠABLATUROVÁ, K., KOCŮRKOVÁ, L. a ŠOŠKOVÁ, K. Ergonomic Risk Mitigation Through Task-Specific Assistive Technology: A Case Study from Slovak Industry. Manuskript (case study), 2026

[22] Vyhláška č. 432/2003 Sb. Vyhláška, kterou se stanoví podmínky pro zařazování prací do kategorií, limitní hodnoty ukazatelů biologických expozičních testů, podmínky odběru biologického materiálu pro provádění biologických expozičních testů a náležitosti hlášení prací s azbestem a biologickými činiteli (v platném znění)

Návrh riešenia rozdelenia poskytovateľov zdravotnej záchrannej služby na Slovensku

Lukáš Valla[1]

[1] Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva,
Univerzitná 1, 010 26 Žilina, lukas.valla@uniza.sk

Abstrakt:

Príspevok sa zaoberá analýzou organizačného modelu zdravotnej záchrannej služby (ZZS) v Slovenskej republike v komparácii so systémom fungujúcim v Českej republike. Cieľom je identifikovať systémové rozdiely v riadení, financovaní a rozložení kapacít a na základe štatistických údajov o výjazdovej činnosti za rok 2024 formulovať návrh optimalizácie organizačnej štruktúry ZZS na Slovensku. Analýza vychádza z porovnania počtu výjazdov, počtu obyvateľov a počtu posádok, pričom hodnotí najmä mieru vyťaženosti výjazdových skupín a regionálne disproporcie. Výsledky poukazujú na to, že slovenský model je charakteristický vyššou fragmentáciou poskytovateľov, čo môže komplikovať riadenie a koordináciu systému. Zároveň sa poukazuje aj na významné regionálne rozdiely. Na rozdiel od českého modelu, založeného na silných regionálnych subjektoch, slovenský systém vykazuje väčšiu pluralitu poskytovateľov pri centrálne určovanom rozmiestnení staníc. Na základe vykonanej analýzy je navrhnutý model troch regionálne organizovaných štátnych záchranných zdravotných služieb, ktoré by spravovali združené územia viacerých krajov, pričom by zostal zachovaný priestor pre participáciu súkromných subjektov prostredníctvom zmluvných vzťahov. Navrhované riešenie smeruje k vyrovnanejšiemu rozloženiu záťaže, zjednodušeniu riadiacich procesov, posilneniu medzikrajovej spolupráce a efektívnejšiemu využívaniu verejných zdrojov. Implementácia takéhoto modelu by mohla prispieť k zvýšeniu stability systému, transparentnosti financovania a k zlepšeniu kvality a dostupnosti prednemocničnej neodkladnej zdravotnej starostlivosti v podmienkach Slovenskej republiky.

Kľúčové slová: záchranná služba, prednemocničná starostlivosť, komparácia systémov, optimalizácia modelu.

1 Úvod

V poslednom období sa v mediálnom priestore Slovenskej republiky čoraz častejšie objavujú informácie týkajúce sa problematiky poskytovania zdravotnej záchrannej služby (ZZS). Pozornosť verejnosti i odbornej obce bola upriamená najmä na zrušenie verejného obstarávania na poskytovateľov ZZS, ktoré bolo pripravené podľa nových pravidiel. Otázky transparentnosti a zákonnosti jeho následného zrušenia vyvolali rozsiahlu diskusiu, avšak tieto aspekty nie sú primárnym predmetom tohto článku. Súčasne prebieha intenzívna odborná i spoločenská debata o navrhovanej zmene organizačného modelu fungovania zdravotnej záchrannej služby. Minister zdravotníctva Slovenskej republiky Kamil Šaško predstavil návrh, podľa ktorého by stanice ZZS mali byť na neurčitý čas organizačne začlenené pod nemocnice disponujúce urgentným príjmom. Tento návrh sa stretol s rezervovaným až kritickým postojom časti odbornej verejnosti, ako aj profesijných organizácií zastupujúcich zdravotníckych záchranárov. Významným problémom sa javí najmä skutočnosť, že návrh vznikol bez širšej odbornej diskusie so zástupcami profesijnej komunity, ktorých sa navrhovaná úprava bezprostredne dotýka. Hlavnou motiváciou pre spracovanie tohto článku je snaha identifikovať potenciálne optimálne riešenie organizačného modelu zdravotnej záchrannej služby na Slovensku, ktoré by umožnilo jej systematický rozvoj a stabilitu bez nadmernej závislosti od opakovane sa meniaceho okruhu poskytovateľov. Analýza vychádza najmä z komparácie so systémom zdravotnej záchrannej služby v Českej republike, kde je ZZS organizovaná na úrovni krajov. Tento model prináša

určité systémové výhody, ale aj identifikovateľné limity. V závere článku je prezentovaný návrh možného modelu fungovania zdravotnej záchrannej služby v podmienkach Slovenskej republiky, ktorý predpokladá kombináciu štátneho a súkromného sektora s cieľom zabezpečiť stabilitu, efektívnosť a odbornú kontinuitu poskytovania prednemocničnej neodkladnej zdravotnej starostlivosti.

2 Porovnanie súčasného stavu v Českej a Slovenskej republike

Druhá kapitola je zameraná na analýzu štatistických ukazovateľov výjazdovej činnosti zdravotnej záchrannej služby (ZZS) v Českej republike a Slovenskej republike. Pozornosť je sústredená predovšetkým na počet výjazdov ZZS k pacientom a na počet obyvateľov v referenčnom roku 2024. Tento rok bol zvolený zámerne, keďže za uvedené obdobie sú dostupné kompletné a porovnateľné údaje o počte výjazdov v Českej republike [1] aj v Slovenskej republike [2].

Do analytického spracovania boli zahrnuté tieto premenné: celkový počet výjazdov, počet obyvateľov a počet posádok ZZS. Na základe uvedených údajov bol vypočítaný koeficient výjazdov vo vzťahu k počtu obyvateľov (výjazdy na obyvateľov), ako aj priemerný počet výjazdov pripadajúci na jednu posádku za sledované obdobie. Tieto ukazovatele umožňujú objektívnejšie porovnanie zaťaženosti systému ZZS v oboch krajinách. Údaje o počte posádok vychádzajú zo zverejnených štatistík o výjazdoch v Českej republike a z interných dokumentov operačného strediska ZZS Slovenskej republiky.

Tabuľka 1. Štatistika výjazdov ZZS v Českej republike za rok 2024 [1]

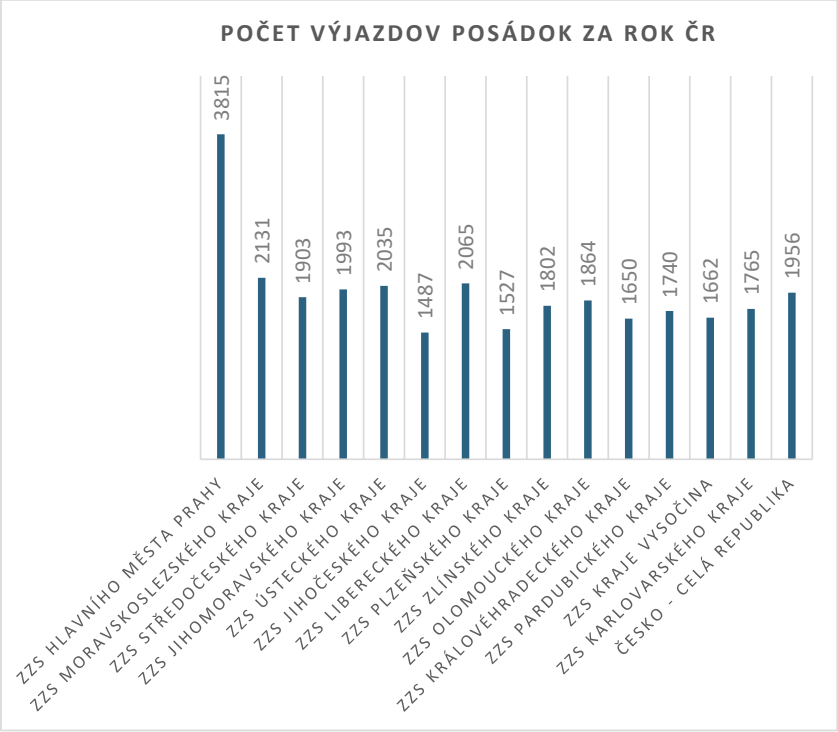
Kraj ČR	Počet výjazdov 2024	Počet obyvateľov	Počet posádok	Počet výjazdov/ počet obyvateľov	Počet výjazdov/ počet posádok
ZZS hlavního města Prahy	144 974	1 397 880	38	0,1037	3 815
ZZS Moravskoslezského kraje	138 487	1 182 613	65	0,1171	2 131
ZZS Středočeského kraje	163 632	1 466 215	86	0,1116	1 903
ZZS Jihomoravského kraje	107 647	1 229 343	54	0,0876	1 993
ZZS Ústeckého kraje	103 789	808 000	51	0,1285	2 035
ZZS Jihočeského kraje	83 290	654 000	56	0,1274	1 487
ZZS Libereckého kraje	66 076	449 000	32	0,1472	2 065
ZZS Plzeňského kraje	76 332	614 000	50	0,1243	1 527
ZZS Zlínského kraje	61 276	579 000	34	0,1058	1 802
ZZS Olomouckého kraje	59 656	631 000	32	0,0945	1 864
ZZS Královéhradeckého kraje	57 760	556 000	35	0,1039	1 650
ZZS Pardubického kraje	55 685	530 000	32	0,1051	1 740
ZZS Kraje Vysočina	49 865	518 000	30	0,0963	1 662
ZZS Karlovarského kraje	44 131	293 000	25	0,1506	1 765
Česká republika	1 212 600	10 908 051	620	0,1112	1 956

V Tabuľke 1 sú prezentované štatistické údaje o výjazdoch zdravotnej záchrannej služby (ZZS) v Českej republike, členené podľa jednotlivých krajov. Pri interpretácii týchto údajov je nevyhnutné zohľadniť špecifiká organizačného a riadiaceho modelu poskytovania prednemocničnej neodkladnej zdravotnej starostlivosti v Českej republike. Zdravotná záchranná služba je v Českej republike organizovaná na regionálnej úrovni, pričom jednotlivé kraje zodpovedajú za zriaďovanie, riadenie, financovanie a rozmiestnenie výjazdových skupín na svojom území. Každá krajská ZZS funguje ako samostatná príspevková organizácia kraja, čo jej poskytuje určitú mieru autonómie v oblasti plánovania kapacít, materiálno-technického zabezpečenia a personálneho

obsadenia. Hoci medzi jednotlivými krajmi existuje prepojenie najmä v oblasti informačných systémov a spolupráce pri riešení mimoriadnych udalostí, systém nie je úplne unifikovaný. Rozdiely sa môžu prejavovať v materiálno-technickom vybavení, liekovom zabezpečení, štandardných operačných postupoch, ako aj v ďalších organizačných a procesných aspektoch, ktoré si jednotlivé kraje upravujú prostredníctvom vlastných interných predpisov. Táto decentralizovaná štruktúra môže mať vplyv na interpretáciu regionálnych rozdielov v počte a charaktere výjazdov.

V Tabuľke 1 sú prezentované absolútne počty výjazdov zdravotnej záchrannej služby (ZZS) v Českej republike podľa jednotlivých krajov za rok 2024. Z údajov vyplýva, že najvyšší pomer počtu výjazdov na počet obyvateľov dosahuje Karlovarský kraj, nasledovaný Libereckým krajom. Tento ukazovateľ môže indikovať vyššiu mieru využívania prednemocničnej neodkladnej zdravotnej starostlivosti v uvedených regiónoch, pričom jeho interpretácia si vyžaduje zohľadnenie demografických, geografických a organizačných faktorov. Celkový počet výjazdových skupín ZZS v Českej republike predstavuje 620, pričom najväčšia koncentrácia výjazdových skupín je evidovaná v Stredočeskom a Moravskosliezskom kraji. V sledovanom období bol zaznamenaný celkový počet 1 212 600 výjazdov, čo poukazuje na vysokú záťaž systému prednemocničnej zdravotnej starostlivosti na celoštátnej úrovni.

Obrázok 1 znázorňuje komparáciu počtu výjazdov a počtu výjazdových skupín v jednotlivých krajoch. Toto porovnanie je z analytického hľadiska významné, keďže umožňuje stanoviť priemerný počet výjazdov pripadajúcich na jednu výjazdovú skupinu ako indikátor jej vyťaženosti. Na základe uvedeného ukazovateľa je možné identifikovať regióny s nadpriemernou záťažou a potenciálnou potrebou optimalizácie personálnych alebo materiálno-technických kapacít. Najvyššiu priemernú vyťaženosť vykazuje ZZS hlavného mesta Prahy, kde pri 38 výjazdových skupinách pripadá na jednu skupinu priemerne 3 815 výjazdov ročne, čo predstavuje viac ako 10 výjazdov denne. Tento údaj naznačuje výraznú intenzitu poskytovania zdravotnej starostlivosti v metropolitnom prostredí. Ostatné kraje vykazujú relatívne porovnateľné hodnoty, pričom najnižší priemerný počet výjazdov na jednu výjazdovú skupinu je evidovaný v Jihočeskom a Plzeňskom kraji.



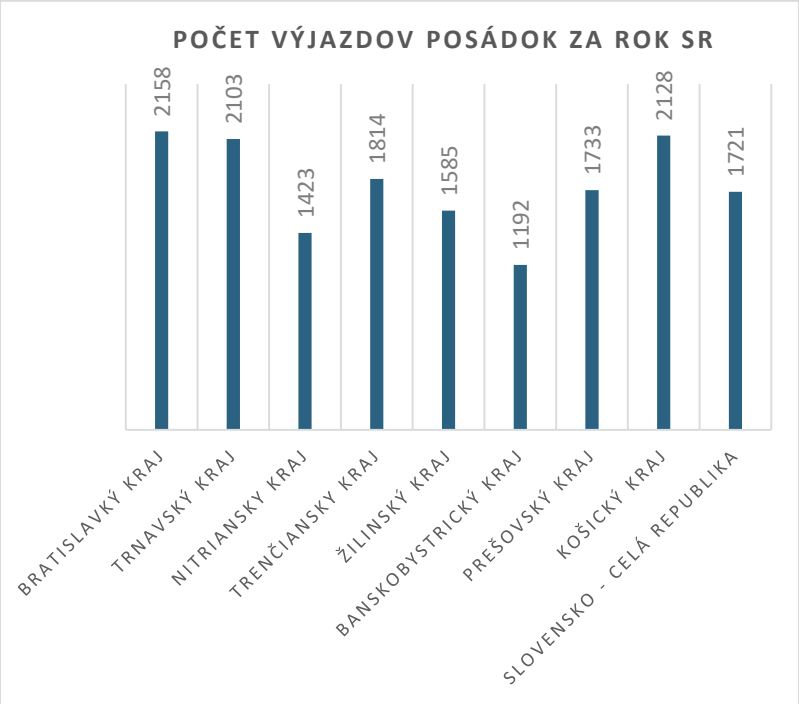
Obrázok 1. Počet výjazdov posádok v jednotlivých krajoch za rok 2024 v ČR

V Tabuľke 2 je prezentovaná štatistika výjazdov zdravotnej záchrannej služby (ZZS) v Slovenskej republike podľa jednotlivých krajov za rok 2024. Z analyzovaných údajov vyplýva, že s výnimkou Košického a Prešovského kraja neprekročil v žiadnom kraji celkový počet výjazdov hranicu 70 000 ročne. Uvedený fakt poukazuje na regionálne rozdiely v zaťažení systému prednemocničnej neodkladnej zdravotnej starostlivosti, ktoré môžu súvisieť s demografickou štruktúrou, zdravotným stavom populácie, ako aj so socioekonomickými a geografickými determinantmi. Osobitnú pozornosť si vyžaduje aj distribúcia výjazdových skupín, ktorá nie je medzi krajmi rovnomerná. Táto nerovnomernosť je podmienená nielen rozdielnou rozlohou krajov, ale aj variabilitou počtu obyvateľov a hustoty osídlenia. V porovnaní s Českou republikou je významným systémovým rozdielom spôsob určovania rozmiestnenia staníc ZZS. Kým v Českej republike je organizácia a sieť ZZS v kompetencii jednotlivých krajov, na Slovensku je rozmiestnenie staníc centrálne riadené Ministerstvom zdravotníctva SR prostredníctvom štátnej príspevkovej organizácie Operačné stredisko záchrannej zdravotnej služby SR (OS ZZS SR – linka 155). Ďalším podstatným rozdielom je štruktúra poskytovateľov. V Českej republike pôsobí v každom kraji spravidla jeden dominantný poskytovateľ ZZS, zatiaľ čo na Slovensku aktuálne pôsobí 14 poskytovateľov ZZS, z ktorých dvaja majú postavenie štátnych poskytovateľov (Bratislavská záchranná služba a Košická záchranná služba). Tento pluralitný model môže mať implikácie pre riadenie, financovanie aj koordináciu systému. Z hľadiska vzťahu medzi počtom výjazdov a počtom obyvateľov možno konštatovať, že väčšina krajov vykazuje relatívne vyrovnané hodnoty. Výraznejšiu disproporciu však zaznamenáva Košický kraj, kde je počet výjazdov v pomere k počtu obyvateľov vyšší v porovnaní s ostatnými regiónmi. Tento jav si vyžaduje podrobnejšiu analýzu s cieľom identifikovať potenciálne príčiny zvýšenej záťaže systému v danom regióne.

Tabuľka 2. Štatistika výjazdov ZZS v Slovenskej republike za rok 2024 [2]

Kraj SR	Počet výjazdov 2024	Počet obyvateľov	Počet posádok	Počet výjazdov/ počet obyvateľov	Počet výjazdov/ počet posádok
Bratislavský kraj (BA)	69 045	736 385	32	0,0938	2 158
Trnavský kraj (TT)	56 789	565 324	27	0,1005	2 103
Nitriansky kraj (NR)	59 785	671 508	42	0,0890	1 423
Trenčiansky kraj (TN)	56 231	582 567	31	0,0965	1 814
Žilinský kraj (ZA)	64 992	691 136	41	0,0940	1 585
Banskobystrický kraj (BB)	63 176	643 102	53	0,0982	1 192
Prešovský kraj (PO)	86 649	827 028	50	0,1048	1 733
Košický kraj (KE)	95 757	802 092	45	0,1194	2 128
Slovenská republika	552 424	5 519 142	321	0,1001	1 721

Obrázok 2 znázorňuje priemerný počet výjazdov pripadajúcich na jednu výjazdovú skupinu v roku 2024. Tento ukazovateľ predstavuje významný indikátor vyťaženosti posádok a umožňuje objektívnejšie porovnanie regionálnych rozdielov bez ohľadu na absolútny počet výjazdov či veľkosť kraja. Na celoštátnej úrovni sa priemerný počet výjazdov na jednu posádku pohybuje približne na úrovni 1 721 výjazdov ročne. Z regionálneho hľadiska je možné identifikovať významné rozdiely. V Banskobystrickom kraji je priemerný počet výjazdov na jednu posádku výrazne nižší než celoštátny priemer, čo však korešponduje s relatívne vyšším počtom výjazdových skupín dislokovaných v tomto kraji. Podobný trend možno pozorovať aj v Nitrianskom kraji, kde vyššia kapacitná základňa prispieva k nižšej individuálnej vyťaženosti posádok. Naopak, najvyššiu mieru vyťaženosti vykazujú Bratislavský, Trnavský a Košický kraj, ktoré dosahujú nadpriemerné hodnoty počtu výjazdov na jednu výjazdovú skupinu. V Bratislavskom kraji predstavuje priemerný počet výjazdov na jednu posádku približne šesť výjazdov denne, čo indikuje vysokú intenzitu poskytovania prednemocničnej neodkladnej zdravotnej starostlivosti v metropolitnom regióne. Uvedené rozdiely poukazujú na potrebu kontinuálneho hodnotenia efektívnosti rozmiestnenia kapacít a optimalizácie siete ZZS s ohľadom na regionálne špecifiká.



Obrázok 2. Počet výjazdov posádok v jednotlivých krajoch za rok 2024 v SR

3 Návrh riešenia spojenia krajov pod štátne záchranky

Druhá kapitola sa zameriavala na analýzu štatistických východísk relevantných pre formuláciu optimálneho modelu organizácie a fungovania zdravotnej záchrannej služby. Komparatívny pohľad poukazuje na zásadné rozdiely v systéme riadenia medzi Českou republikou a Slovenskou republikou. V Českej republike sú zdravotné záchranné služby zriaďované a spravované na úrovni jednotlivých krajov, pričom každý kraj vystupuje ako samostatný zriaďovateľ a zabezpečuje organizačné, personálne aj materiálno-technické podmienky poskytovania prednemocničnej neodkladnej zdravotnej starostlivosti. Na Slovensku je systém diverzifikovanejší. Poskytovanie zdravotnej záchrannej služby je zabezpečované kombináciou dvoch štátnych poskytovateľov a viacerých súkromných subjektov (spolu 12), medzi ktoré patria napríklad spoločnosti ZaMed Komárno, Life Star Emergency, RZP, a. s. so sídlom v Trenčíne, ako aj viaceré nemocničné záchranné služby, napríklad poskytovateľ prepojený s nemocnicou v Brezne. Bez ohľadu na právnu formu poskytovateľa sú všetky subjekty povinné spĺňať minimálne požiadavky na materiálno-technické vybavenie stanovené vo vestníku Ministerstva zdravotníctva Slovenskej republiky [3]. Tento normatívny rámec zabezpečuje základnú úroveň štandardizácie. Napriek tomu však v praxi dochádza k variabilite vo vybavení, keďže jednotliví poskytovatelia majú možnosť nad rámec povinného minima rozšíriť svoje technické a medicínske zabezpečenie podľa vlastných interných rozhodnutí a finančných možností. Určitým problémom sa javí aj oblasť vzájomnej spolupráce medzi poskytovateľmi, najmä v situáciách, keď dochádza k prekrývaniu kompetencií alebo k potrebe personálnej súčinnosti. Ako príklad možno uviesť fungovanie posádok typu RV (rendez-vous), kde lekár vyslaný na zásah v prípade potreby transportu pacienta do zdravotníckeho zariadenia často pokračuje v sprievode pacienta v sanitnom vozidle iného poskytovateľa. Takáto medzi-organizačná spolupráca môže byť z hľadiska kontinuity starostlivosti, zodpovednosti a administratívneho zabezpečenia komplikovaná a poukazuje na potrebu systematickejšieho nastavenia koordinačných mechanizmov v rámci celého systému.

Komparatívna analýza organizácie zdravotnej záchrannej služby v Českej republike a Slovenskej republike vytvára priestor pre formuláciu návrhu systémovej reformy fungovania zdravotnej záchrannej služby na Slovensku. Navrhované riešenie predstavuje kompromisný model medzi plne štátnym a pluralitným (kombinovaným) systémom poskytovateľov. Jeho ambíciou je posilniť koordinačnú a kontrolnú úlohu štátu, zvýšiť transparentnosť finančných tokov a zároveň zabezpečiť efektívnejšie využívanie verejných zdrojov s potenciálom vyššej návratnosti investícií v podobe stabilizácie systému a zvýšenia kvality poskytovanej starostlivosti. Podstatou návrhu je zriadenie troch regionálne organizovaných štátnych zdravotných záchranných služieb, ktoré by spravovali združené územia viacerých krajov. Model sa inšpiruje systémom fungujúcim v Českej republike, avšak s odlišnou teritoriálnou organizáciou – jednotlivé subjekty by nespravovali jeden kraj, ale väčšie, logicky previazané územné celky pozostávajúce z dvoch až troch krajov.

Navrhovaná štruktúra predpokladá existenciu troch štátnych poskytovateľov, pričom dva z nich už v súčasnosti pôsobia a tretí by bolo potrebné zriadiť. Konkrétne:

- Bratislavská záchranná zdravotná služba by zabezpečovala poskytovanie zdravotnej záchrannej služby v Bratislavskom, Trnavskom a Nitrianskom kraji.
- Banskobystrická záchranná zdravotná služba (novozriadená) by spravovala Trenčiansky, Žilinský a Banskobystrický kraj.
- Košická záchranná zdravotná služba by pôsobila v Prešovskom a Košickom kraji.

Takto koncipované rozdelenie by vytvorilo tri silné a organizačne stabilné subjekty s dostatočnou veľkosťou na efektívne riadenie, plánovanie a optimalizáciu siete staníc. Súčasne by sa posilnila horizontálna spolupráca medzi týmito subjektmi, keďže by išlo o organizácie v pôsobnosti štátu s jednotným strategickým riadením. Model zároveň počíta so zachovaním priestoru pre súkromných poskytovateľov. Každá zo štátnych záchranných služieb by mala možnosť rozhodnúť sa, že určitú stanicu nebude prevádzkovať vo vlastnej réžii, ale na základe zmluvného vzťahu poverí jej správou súkromného poskytovateľa. Takéto zmluvy by mohli byť uzatvárané na časovo ohraničené obdobie (napríklad dva roky) s možnosťou pravidelnej revízie podmienok vrátane finančných parametrov. V tomto modeli by súkromný subjekt nebol v priamom zmluvnom vzťahu s Ministerstvom zdravotníctva SR, ale s príslušnou štátnou záchrannou službou, ktorá by zodpovedala za financovanie a kontrolu výkonu služby. Tým by sa zjednodušila zmluvná architektúra systému a zvýšila operatívnosť riadenia. Významným prínosom navrhovaného modelu by bolo aj zefektívnenie komunikácie medzi Operačným strediskom tiesňového volania 155 a poskytovateľmi. V súčasnom fragmentovanom systéme je koordinácia zmien v rozmiestnení staníc či úprav prevádzky administratívne náročnejšia. Komunikácia s tromi štátnymi subjektmi by umožnila pružnejšie reagovať na demografické zmeny, sezónne výkyvy či mimoriadne udalosti a systematickejšie plánovať optimalizáciu siete. Navrhované riešenie má zároveň potenciál priniesť pozitívne efekty v oblasti kvality poskytovaných služieb. Väčšie, ekonomicky silnejšie subjekty by mohli efektívnejšie plánovať investície do obnovy vozového parku, modernizácie zdravotníckej techniky a implementácie inovatívnych technologických riešení (napr. telemedicínske prvky, digitálne systémy podpory rozhodovania). Centralizovanejšie riadenie by tiež umožnilo systematickejšie nastavenie personálnej politiky, vrátane transparentného odmeňovania, stabilizačných mechanizmov a kontinuálneho vzdelávania zdravotníckych pracovníkov. V konečnom dôsledku by takýto model mohol prispieť k vyššej stabilite systému, posilneniu jeho strategického riadenia a k zvýšeniu dostupnosti a kvality prednemocničnej neodkladnej zdravotnej starostlivosti pre obyvateľov Slovenskej republiky.

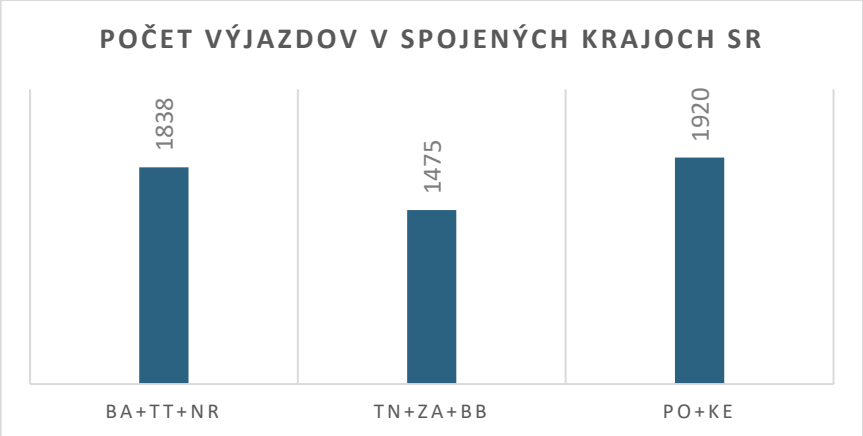
Z údajov uvedených v Tabuľke 3 vyplýva, že navrhovaná reorganizácia systému by nemala zásadný vplyv na celkový objem výjazdovej činnosti jednotlivých novovzniknutých subjektov. Počet výjazdov by sa v rámci zlúčených územných celkov relatívne stabilizoval, keďže by došlo k vyváženiu krajov s vyššou intenzitou zásahov s krajmi s nižším počtom výjazdov. Tento efekt priemerovania by prispel k rovnomernejšiemu rozloženiu pracovnej záťaže a k predvídateľnejšiemu plánovaniu kapacít. Z hľadiska organizačnej štruktúry by Banskobystrická záchranná

zdravotná služba spravovala 125 staníc zdravotnej záchrannej služby, Bratislavská záchranná zdravotná služba 101 staníc a Košická záchranná zdravotná služba 95 staníc. Takéto rozdelenie vytvára tri relatívne porovnateľné a manažérsky zvládnuteľné celky, ktoré disponujú dostatočnou veľkosťou na efektívne riadenie siete staníc, optimalizáciu rozmiestnenia posádok a strategické plánovanie rozvoja infraštruktúry. Navrhovaný model by zároveň umožnil zjednodušenie riadenia personálnych a technických kapacít, ako aj efektívnejšiu komunikáciu medzi jednotlivými poskytovateľmi. Koncentrácia riadiacich kompetencií do troch štátnych subjektov by mohla prispieť k väčšej transparentnosti rozhodovacích procesov, k jednotnejšiemu uplatňovaniu štandardov a k rýchlejšej implementácii systémových zmien. Súčasne by však zostala zachovaná možnosť participácie súkromných poskytovateľov prostredníctvom zmluvných vzťahov, čím by sa zabezpečila kontinuita ich pôsobenia v systéme a využitie ich regionálnych skúseností a kapacít.

Tabuľka 3. Štatistika výjazdov ZZS SR v prípade spojenia krajov

Kraj SR	Počet výjazdov 2024	Počet obyvateľov	Počet posádok	Počet výjazdov/ počet obyvateľov	Počet výjazdov/ počet posádok
BA+TT+NR	185 619	1 973 217	101	0,0941	1 838
TN+ZA+BB	184 399	1 916 805	125	0,0962	1 475
PO+KE	182 406	1 629 120	95	0,1120	1 920

Obrázok 3 ilustruje efekt vyrovnávania počtu výjazdov po zlúčení krajov do väčších územných celkov v rámci navrhovaného modelu. Z grafického znázornenia je zrejmé, že priemerný ročný počet výjazdov na úrovni novovzniknutých poskytovateľov sa stabilizuje. Tento efekt je dôsledkom spojenia krajov s vyššou intenzitou zásahov s krajmi, ktoré dlhodobo vykazujú nižší počet výjazdov. Výsledkom je rovnomernejšie rozloženie záťaže medzi jednotlivé organizačné jednotky a eliminácia výrazných regionálnych disproporcií. Takto nastavený model vytvára predpoklady pre efektívnejšie plánovanie personálnych a materiálno-technických kapacít, keďže výkyvy v počte zásahov sa rozložia v rámci väčšieho územného celku. Zároveň sa posilňuje medzikrajová spolupráca, pretože geograficky susediace kraje by boli spravované jednou zdravotnou záchrannou službou. Táto skutočnosť by mohla prispieť k pružnejšiemu presúvaniu posádok podľa aktuálnej potreby, k lepšej koordinácii pri riešení mimoriadnych udalostí a k jednotnejšiemu uplatňovaniu organizačných a odborných štandardov v rámci širšieho regiónu.



Obrázok 3. Počet výjazdov posádok v prípade spojenia krajov za rok 2024

4 Záver

Cieľom príspevku bolo analyzovať súčasný stav organizácie zdravotnej záchrannej služby v Slovenskej republike v komparácii so systémom fungujúcim v Českej republike a na základe získaných poznatkov formulovať návrh možnej optimalizácie organizačného modelu. Štatistická analýza výjazdovej činnosti za rok 2024 poukázala na rozdiely v miere vyťaženosti posádok, regionálnych disproporciách a v samotnej štruktúre poskytovateľov. Zatiaľ čo český model je založený na silných regionálnych subjektoch s jasne definovanou zodpovednosťou na úrovni krajov, slovenský systém je charakteristický vyššou fragmentáciou a pluralitou poskytovateľov, čo sa môže prejavovať v náročnejšej koordinácii a riadení. Navrhovaný model troch regionálne organizovaných štátnych záchranných zdravotných služieb predstavuje kompromisné riešenie, ktoré kombinuje prvky centralizovaného riadenia so zachovaním priestoru pre súkromných poskytovateľov. Zlúčenie krajov do väčších územných celkov by podľa vykonanej analýzy neviedlo k zásadnému nárastu či poklesu počtu výjazdov, ale naopak k vyrovnanejšiemu rozloženiu záťaže medzi jednotlivé organizačné jednotky. Stabilizácia priemerného počtu výjazdov na posádku vytvára predpoklady pre efektívnejšie plánovanie kapacít a racionálnejšie využívanie dostupných zdrojov. Významným prínosom navrhovaného riešenia je zjednodušenie riadiacich a komunikačných procesov. Koncentrácia zodpovednosti do troch štátnych subjektov by umožnila pružnejšiu koordináciu s operačným strediskom, systematickejšie plánovanie siete staníc a rýchlejšie prijímanie strategických rozhodnutí. Zároveň by sa posilnila medzikrajová spolupráca v rámci väčších územných celkov, čo by mohlo mať pozitívny vplyv najmä pri riešení mimoriadnych udalostí alebo dočasných výkyvov v zaťažení systému. Ekonomický rozmer navrhovaného modelu spočíva v možnosti efektívnejšieho hospodárenia s verejnými zdrojmi. Väčšie organizačné celky disponujú vyšším potenciálom pre plánovanie investícií do obnovy vozového parku, modernizácie zdravotníckej techniky a implementácie inovatívnych technologických riešení. Súčasne sa vytvárajú priaznivejšie podmienky pre stabilizáciu personálu prostredníctvom transparentnejšieho systému odmeňovania, systematického vzdelávania a dlhodobej personálnej stratégie. Navrhovaný model tak predstavuje realistickú alternatívu k aktuálnemu stavu, ktorá zohľadňuje špecifiká slovenského prostredia a zároveň využíva pozitívne prvky zahraničnej praxe. Jeho implementácia by mohla prispieť k zvýšeniu stability systému, k posilneniu strategického riadenia a v konečnom dôsledku k zlepšeniu dostupnosti a kvality prednemocničnej neodkladnej zdravotnej starostlivosti pre obyvateľov Slovenskej republiky.

Poďakovanie

Príspevok vznikol s podporou projektu KEGA 035ŽU-4/2025 Inovatívne modulárne vzdelávacie kurzy ako účinný nástroj na zvýšenie bezpečnosti v školách.

Referencie

[1] ASOCIACE ZDRAVOTNICKÝCH ZÁCHRANNÝCH SLUŽEB ČR. Statistika výjezdové činnosti ZZS ČR. 2024. [online]. Dostupné na: https://www.azzs.cz/dokumenty/zdravotnicke-zachranne-sluzby-v-cr-v-cislech/statistika-vyjezdove-cinnosti-zzs-cr

[2] OPERAČNÉ STREDISKO ZÁCHRANNEJ ZDRAVOTNEJ SLUŽBY SR. Výročná správa operačného strediska 155. 2024. [online]. Dostupné na: https://155.sk/subory/dokumenty/vyrocne_spravy/Vyrocna_sprava_OSZZSSR_2024.pdf

[3] MINISTERSTVO ZDRAVOTNÍCTVA SLOVENSKEJ REPUBLIKY. Vestník Ministerstva zdravotníctva SR č. 57–59. 2024. [online]. Dostupné na: https://www.health.gov.sk/Zdroje?/Sources/dokumenty/vestniky_mz_sr/2023/vestnik-2023-57-59.pdf

Effect of Physical Load on Physiological Parameters of Students During Patient Transport

Tatiana Verešová[1]

[1] University of Žilina, Faculty of Security Engineering,
1. mája 32, 010 26 Žilina, tatiana.veresova@uniza.sk

Abstract:

The aim of this study was to analyze the efficiency and physiological load of Emergency Services students during patient transport using the log-roll technique in simulated intervention scenarios. The study sample comprised 20 students, for whom basic anthropometric parameters (weight, height, waist circumference, BMI, ABSI) and physical activity levels were recorded. During the practical training, key physiological indicators were monitored, including heart rate, blood pressure, respiratory rate, oxygen saturation, and body temperature, with measurements taken before and immediately after patient transport. The results demonstrated that patient transport imposed a significant physical load, with respiratory and heart rates identified as the most sensitive indicators. Students with normal BMI and regular physical activity exhibited lower physiological stress and shorter transport times, whereas higher BMI was associated with increased cardiovascular load and prolonged patient handling. Oxygen saturation and body temperature remained relatively stable, indicating the maintenance of basic homeostatic mechanisms during short-term physical exertion. This study highlights the importance of body composition and physical fitness in managing practical training for emergency responders and provides a basis for optimizing training programs, enhancing transport safety, and improving team efficiency during real-life interventions.

Keywords: patient transport, log-roll, physiological load, BMI, emergency services, simulated intervention.

1 Introduction

Practical patient transport represents a key operational task for rescuers, requiring the integration of proper handling techniques, effective team coordination, and management of the physiological load on rescuers. The log-roll technique allows for the safe transfer of patients with suspected spinal injuries while minimizing the risk of secondary harm. The efficiency and safety of such transport depend on physical preparedness, body constitution, and the participants' ability to coordinate movement in spatially constrained environments, such as staircases in multi-story buildings.

The present study focused on evaluating the performance of students enrolled in the Rescue Services program during a simulated patient transport from the sixth floor, emphasizing time efficiency, procedural accuracy, physiological load, and the influence of body constitution (BMI) and physical fitness level. Physiological parameters, including heart rate, blood pressure, respiratory rate, oxygen saturation, and body temperature, were monitored before and after the transport, allowing a comprehensive analysis of the adaptive responses to the physical demands associated with practical training.

The aim of the research was to identify the relationship between physiological load and anthropometric characteristics of students, thereby contributing to the optimization of practical training methods for rescuers and enhancing patient safety during real interventions.

2 Patient Transport

Patient transport is one of the fundamental tasks of fire and rescue personnel and emergency medical services. It is a complex professional activity requiring adequate theoretical knowledge, practical skills, high physical fitness, and effective team collaboration. The quality and accuracy of transport significantly influence not only the patient's health status but also the safety of the rescuers and the overall efficiency of the intervention.

In the context of higher education focused on preparing future professionals in fire protection and rescue services, patient transport training constitutes an integral part of practical instruction. Students acquire principles of proper handling of injured or immobilized patients, transport techniques in various environments, and procedures for using transport devices such as stretchers, transfer sheets, spine boards, or vacuum mattresses. Physical fitness development is an essential component of the training, supporting safe and efficient execution of intervention tasks.

From a physiological perspective, patient transport imposes a complex load on the body, characterized by increased heart rate, arterial blood pressure, and oxygen consumption. The intensity of this load is influenced by multiple factors, including patient weight, transport distance and conditions, terrain, equipment used, and the rescuers' physical preparedness. Systematic monitoring of these parameters during training allows assessment of adaptive mechanisms to specific work stressors and identification of physical performance limits.

Objective assessment of workload is conducted through measurement of selected physiological indicators such as heart rate, blood pressure, oxygen saturation, and subjective perception of exertion. Analysis of these data enables comprehensive evaluation of the physical demands of different transport methods and comparison of their effectiveness, contributing to overload prevention and minimizing occupational injury risks.

Patient transport in rescue practice involves safely relocating injured, immobilized, or otherwise endangered persons from the incident site to a safe area or medical facility. It requires appropriate technical preparation, correct decision-making, and coordinated teamwork among multiple components of the integrated rescue system. The choice of transport method depends on the nature of the incident, the patient's condition, and environmental specifics [4] .

Proper use of transport equipment requires professional training focused on safe handling of loads, adherence to ergonomic principles, and coordinated team movements. Improperly executed transport may worsen the patient's condition or cause injury to rescuers. Therefore, training emphasizes simulation of scenario-based situations to practice technical procedures, team communication, and decision-making under increased physical and psychological stress.

In applied practice, patient transport often involves close cooperation among multiple components of the integrated rescue system. Firefighters work primarily with emergency medical services, which provide prehospital care and subsequent patient transport to medical facilities. In cases of traffic accidents or mass casualty incidents, the police secure the incident site. Effective coordination among these entities determines the speed, safety, and overall success of the intervention.

The transport process is systematic, comprising several consecutive phases. The initial step involves assessing the situation and securing the scene to eliminate potential hazards. This is followed by primary patient assessment to identify life-threatening conditions. Preparation for transport includes selecting appropriate equipment, immobilizing injured body parts, and assigning roles within the rescue team. The transport itself must be performed following ergonomic handling principles, continuously monitoring the patient's condition,

and maintaining clear communication among responders. Strict adherence to occupational safety and health guidelines is an inseparable part of the entire proces [1, 2] .

Integrating patient transport into practical education creates an opportunity to connect theoretical knowledge with empirical verification of physiological and performance parameters. Analysis of physiological responses and time-related indicators provides relevant data for optimizing training programs and enhancing the preparedness of future rescuers and firefighters.

3 Research Aim and Methodology

The primary aim of this study was to comprehensively analyze the performance and efficiency of Rescue Services students during practical training in the log-roll technique, a standardized method for coordinated patient transfer and subsequent fixation onto a transport board. The research focused on evaluating the accuracy of technique execution under simulated intervention conditions, assessing the physiological load experienced by students during the task, and identifying determinants affecting the quality, speed, and safety of the patient transport. Emphasis was placed on the precision of individual procedural steps, adherence to methodological guidelines, and the ability to perform coordinated teamwork.

An additional objective was to analyze the duration of patient transport by dividing the process into distinct phases: preparation, transfer and fixation onto the transport board, and actual patient transport. Identification of the most time-demanding segments allowed for an objective assessment of training efficiency and potential areas for improvement in practical preparation.

A key component of the study was the assessment of students' physiological responses to physical exertion during patient transport. Monitored parameters included cardiovascular and thermoregulatory indicators such as heart rate, blood pressure, oxygen saturation (SpO_2), and body temperature. Analysis of these measures enabled the quantification of workload and evaluation of the adaptive response of the organism to this specific type of physical activity.

The study also assessed safety and precision during patient handling, focusing on maintenance of a neutral spinal axis, head and trunk stability during transfer, and correct and secure fixation onto the transport board. These aspects are critical in preventing secondary injury to the patient.

Furthermore, the influence of selected anthropometric and training characteristics, especially Body Mass Index (BMI) and physical fitness level, on the speed and quality of patient transport was analyzed. The study also included evaluation of team cooperation and communication, as effective verbal and non-verbal coordination is essential for safe and smooth execution of the log-roll technique in real-world operational scenarios.

Training Methodology

The practical training aimed to verify the readiness of students for safe and effective patient transport under simulated intervention conditions. The exercise simulated a real-life scenario involving the transfer of an injured person from the sixth floor of a building, including stair navigation and handling of a patient with suspected spinal injury.

Organization and Course of Exercise

Training was conducted at the Faculty of Security Engineering, University of Žilina, within the "Tactics of Intervention Management" course. The sample consisted of 35 first-year Master's degree students in the Rescue Services program. Students were divided into seven four-member teams, each performing an identical transport scenario in two stages:

- Transfer of the patient onto a transport board using the log-roll technique.
- Transport of the patient from the sixth floor via stairs using transport equipment.

Standardized equipment, including a spine board, fixation straps, and a head stabilizer, was used. Each team worked with a mannequin simulating an unconscious patient with suspected spinal injury. Participants received safety instructions and wore personal protective equipment, including helmets and intervention clothing.

Physiological Measurements

Prior to training, anthropometric measurements were recorded (weight, height, waist circumference), and BMI and ABSI were calculated to characterize body constitution and its potential impact on physical workload. Participants also self-reported their physical activity level, with most engaging in regular sports (running, strength training, volleyball, motocross).

During training, physiological parameters were monitored to objectively assess workload and bodily response. Monitored variables included heart rate (HR; bpm), blood pressure (BP; mmHg), oxygen saturation (SpO_2; %), respiratory rate (RR; breaths/min), and body temperature (°C), measured in two phases:

- At rest after a five-minute seated recovery period.
- Immediately after patient transport (within 30 seconds of task completion).

Timing and Organizational Measures

Transport time was measured as an indicator of efficiency and team coordination, divided into three phases:

- Total transport time (t_1): from first contact with the patient to placement at the target location.
- Preparation time (t_2): from initial handling to lifting, including stabilization, transfer onto the board, and fixation.
- Actual transport time (t_3): from lifting to final placement.

Digital stopwatches with ± 0.01 s accuracy were used. Each team performed two repetitions under identical conditions. Technique accuracy was evaluated using a standardized protocol (1–5 scale), assessing spinal alignment, grip, synchronization, head and trunk stability, and fixation quality.

Safety and Physical Load Assessment

Safety was assessed regarding proper fixation, neutral body alignment, team communication quality, and adherence to ergonomic handling principles. Physical load was evaluated by comparing physiological parameters before and after exercise, providing an objective measure of cardiovascular and respiratory system activation.

Data Processing

Collected data were analyzed using descriptive and inferential statistics, including mean, standard deviation, minimum and maximum, median, and coefficient of variation.

Ethical Considerations

Training was conducted under professional supervision. All participants provided informed consent, and certified transport equipment and personal protective gear were used. Data were processed anonymously, ensuring compliance with ethical principles of scientific research.

4 Results

Patient transport was carried out under real operational building conditions. The route from the sixth floor led through an internal staircase. Team movement was limited by spatial constraints and obstacles, particularly vegetation placed on landings, which reduced maneuvering space and increased demands on precision handling. The most challenging segment of the transport involved rotating the spine board on the landings, requiring a high level of coordination, verbal communication, and synchronized movements among team members. In all cases, the transfer was completed smoothly, without significant disruption of carrying technique or the need to interrupt the activity.

Observations during the exercise confirmed that manipulation of the spine board in a multi-storey building represents both a physically and technically demanding task, especially in environments with restricted maneuvering space. Increased demands were particularly evident in maintaining patient stability, team coordination, and ergonomically correct posture during stair descent.

Basic Anthropometric Data of Participants

The research exercise involved 35 first-year Master's degree students enrolled in the Rescue Services study program within the course Tactics of Intervention Management. Prior to training, all participants provided basic identification data and signed informed consent for the processing of personal data, collection of physiological measurements, and documentation for scientific and educational purposes.

At the initial stage, basic anthropometric characteristics were recorded for all students, including body weight (kg), body height (m), and waist circumference (m). Based on these measurements, Body Mass Index (BMI) and A Body Shape Index (ABSI) were calculated.

BMI was interpreted according to the classification of the World Health Organization (WHO), with students categorized as underweight (< 18.5), normal weight (18.5–24.9), overweight (25.0–29.9), or obese (> 30.0). Four-member rescue teams were subsequently formed based on BMI to enable comparison of performance among groups with different body constitutions.

The average age of participants was 22.85 years. Mean anthropometric values of the research sample were as follows:

- Mean body height: 1.793 m;
- Mean body weight: 79.81 kg;
- Mean waist circumference: 0.85 m;

- Mean BMI: 24.85;
- Mean ABSI: 0.0744.

Anthropometric data of the students are presented in Table 1.

Table 1. Anthropometric Characteristics of the Study Participants

Group	No.	Sex	Age	Body Weight (kg)	Body Height (m)	Waist Circumference (m)	BMI	ABSI	Training Level
Š4-A	Š1	Male	23	87,9	1,85	0,97	25,683	0,082	
	Š2	Male	22	93,6	1,93	0,94	25,128	0,079	
	Š3	Male	23	91	1,87	0,96	26,023	0,080	
	Š4	Male	22	83,2	1,82	0,92	25,118	0,080	Fitness
Š4-B	Š5	Male	23	69,5	1,75	0,9	22,694	0,085	
	Š8	Male	24	75	1,89	0,88	20,996	0,084	
	Š6	Male	23	75,9	1,89	0,82	21,248	0,078	
	Š7	Male	24	79,1	1,86	0,88	22,864	0,080	running, fitness, motocross
Š4-E	Š21	Male	22	67,2	1,7	0,78	23,253	0,073	fitness, running
	Š19	Male	23	81,8	1,76	0,78	26,408	0,066	Fitness
	Š20	Male	23	75,4	1,67	0,79	27,036	0,068	Fitness
	Š18	Male	24	89	1,82	0,85	26,869	0,070	Fitness
Š4-F	Š22	Male	23	74,9	1,79	0,86	23,376	0,079	running
	Š24	Male	23	87	1,8	0,86	26,852	0,071	running
	Š23	Male	22	88,4	1,8	0,82	27,284	0,067	running
	Š27	Male	22	79,2	1,78	0,76	24,997	0,067	
Š4-G	Š28	Female	22	75,9	1,64	0,83	28,220	0,070	
	Š29	Female	23	74	1,8	0,76	22,840	0,070	
	Š30	Female	22	78	1,74	0,76	25,763	0,066	Fitness
	Š31	Female	24	70,1	1,7	0,79	24,256	0,072	

The study sample consisted of 20 students enrolled in the Rescue Services program, including 16 males (80 %) and 4 females (20 %). The average body height was 1.793 m, body weight 79.81 kg, waist circumference 0.85 m, BMI 24.85 kg/m², and ABSI 0.0744. According to the World Health Organization classification (2020), the mean BMI corresponds to the normal weight category, indicating adequate physical predispositions of the participants to cope with the workload during training. Half of the students (50 %) reported regular engagement in physical activity, with this subgroup exhibiting more favorable BMI and waist circumference values. ABSI values were within the reference range, suggesting a low risk of central obesity.

Physiological Parameters during Patient Transport

During the patient transport exercise, selected physiological indicators were systematically monitored in the students, including heart rate (HR), arterial blood pressure (BP), respiratory rate (RR), peripheral oxygen saturation (SpO_2), and body temperature (T). Data collection was conducted at two standardized time points – at rest before the practical training and immediately after its completion. The aim of the measurements was to objectively assess the acute physiological response to the workload induced by patient transport under simulated emergency conditions. Selected groups performed repeated transports from the 6th floor, allowing analysis of the dynamics of the monitored parameters under repeated physical exposure. Summary values of the measured indicators are presented in Table 2.

Table 2. Physiological Parameters of Students

		At the start – before transport					After transport				
Group	**No.**	**Blood Pressure**	**Heart Rate**	**Oxygen saturation**	**Respiratory Rate**	**Body Temperature**	**Blood Pressure**	**Oxygen saturation**	**Heart Rate**	**Respiratory Rate**	**Body Temperature**
Š4-A	Š1	153/95	108	97	16	36,1	129/88	97	84	18	35,9
	Š2	122/73	77	97	20	37,1	151/92	94	93	16	36,4
	Š3	169/74	78	98	16	37,4	140/83	97	97	20	36,4
	Š4	122/77	77	97	16	36,9	143/96	107	96	18	36,2
Š4-B	Š5	136/87	78	96	18	36,2	153/93	111	97	18	35,5
	Š8	139/75	76	96	16	36,3	150/85	91	92	20	37,4
	Š6	139/71	44	97	18	36,8	108/78	45	97	22	35,9
	Š7	132/74	89	96	24	36,7	145/78	84	97	14	35,8
Š4-E	Š21	117/58	67	97	16	36	147/75	99	122	24	35,7
	Š19	130/80	76	97	12	36,9	118/104	97	98	14	36,3
	Š20	154/86	75	98	12	36,9	150/87	98	112	14	36,7
	Š18	163/107	101	97	14	36,9	163/92	96	133	14	35,9
Š4-F	Š22	131/77	79	97	12	36,2	144/69	96	98	12	36
	Š24	113/80	81	99	10	36,5	130/90	97	102	24	36,6
	Š23	135/94	83	97	8	36,1	186/91	97	128	12	35,6
	Š27	128/79	66	97	13	36,5	117/82	96	97	14	36
Š4-G	Š28	139/75	94	95	20	36,7	139/80	98	122	41	36,6
	Š29	129/84	112	98	20	36,5	154/92	97	132	32	36,1
	Š30	130/89	96	97	8	35,2	134/91	97	133	18	35,9
	Š31	105/58	73	97	8	37	130/78	94	102	14	36,1
Š4-E	Š21	117/58	67	97	16	36	162/96	95	119	24	35,4
	Š19	130/80	76	97	12	36,9	122/70	97	64	24	36,2
	Š20	154/86	75	98	12	36,9	139/89	94	98	14	36,5
	Š18	163/107	101	97	14	36,9	143/95	95	115	20	35,6
Š4-F	Š22	131/77	79	97	12	36,2	154/84	96	93	16	35,8
	Š24	113/80	81	99	10	36,5	148/93	96	141	16	37
	Š23	135/94	83	97	8	36,1	166/89	92	135	12	35,8
	Š27	128/79	66	97	13	36,5	151/89	97	98	14	35,5
Š4-G	Š28	139/75	94	95	20	36,7	126/78	97	145	38	37,1
	Š29	129/84	112	98	20	36,5	124/88	96	140	32	36
	Š30	130/89	96	97	8	35,2	133/79	97	110	20	36,1
	Š31	105/58	73	97	8	37	149/90	97	155	24	35,9

Table 3 presents the basic statistical characteristics of the rescuers' physiological parameters before and after patient transport. For each monitored parameter (systolic and diastolic blood pressure, heart rate, oxygen saturation, respiratory rate, and body temperature), the mean, mode, median, standard deviation, coefficient of variation, minimum, and maximum values are reported.

Table 3. Basic Statistical Characteristics of Physiological Parameters

	At the start – before transport						After transport					
	Blood Pressure systolic	Blood Pressure diastolic	Heart Rate	Oxygen saturation	Respiratory Rate	Body Temperature	Blood Pressure systolic	Blood Pressure diastolic	Heart Rate	Oxygen saturation	Respiratory Rate	Body Temperature
Avarage	133,13	80,00	82,28	97,06	14,06	36,51	142,13	86,38	110,78	94,91	19,78	36,12
Mode	139,00	58,00	76,00	97,00	16,00	36,90	151,00	78,00	97,00	97,00	14,00	35,90
Median	130,50	79,50	78,50	97,00	13,50	36,50	143,50	88,50	102,00	97,00	18,00	36,00
Standard deviation	15,85	12,22	14,81	0,88	4,44	0,50	16,20	7,95	20,81	10,06	7,36	0,48
Coefficient of variation	11,91	15,28	18,00	0,90	31,54	1,36	11,40	9,21	18,78	10,60	37,21	1,33
Min	105,00	58,00	44,00	95,00	8,00	35,20	108,00	69,00	64,00	45,00	12,00	35,40
Max	169,00	107,00	112,00	99,00	24,00	37,40	186,00	104,00	155,00	111,00	41,00	37,40

Blood Pressure: The average systolic blood pressure before transport was 133.1 mmHg, with a median of 130.5 mmHg and a mode of 139 mmHg, while the diastolic pressure averaged 80 mmHg. After patient transport, the average systolic pressure increased to 142.1 mmHg and the diastolic to 86.4 mmHg. The increase in systolic mode from 139 mmHg to 151 mmHg indicates heightened cardiovascular activity of the student rescuers due to the physical exertion during patient transport. The standard deviation remained relatively stable, with a slight decrease in diastolic variability, which may reflect a more homogeneous physiological response within the observed group. The changes in systolic and diastolic blood pressure before and after transport are illustrated in Figure 1.

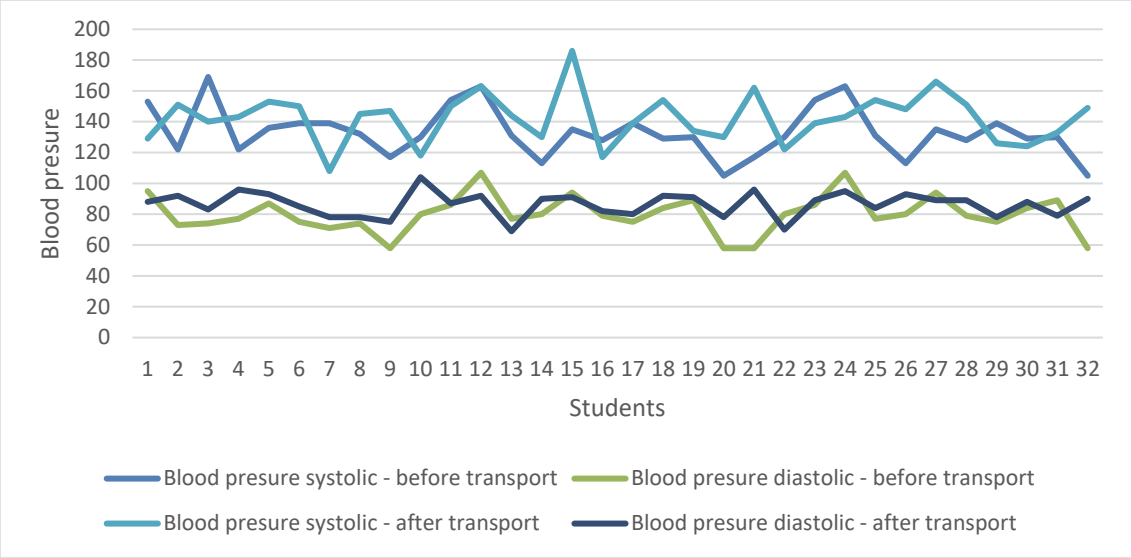


Figure 1. Graph of Blood Pressure Changes Before and After Transport

Heart Rate: The average heart rate before transport was 82.3 beats/min, increasing to 110.8 beats/min after transport. The rise in standard deviation (14.8 → 20.8) and shifts in mode and median confirm the significant impact of physical exertion on the cardiovascular system of the student rescuers.

Figure 2 illustrates the heart rate of rescuers before and after patient transport. The results show a marked increase from pre-transport to post-transport. The elevated heart rate reflects sympathetic activation of the cardiovascular system as an adaptive response to the physical load associated with patient transport.

The graph clearly visualizes this upward trend, confirming the substantial physiological impact of the exertion involved in handling and moving the patient.

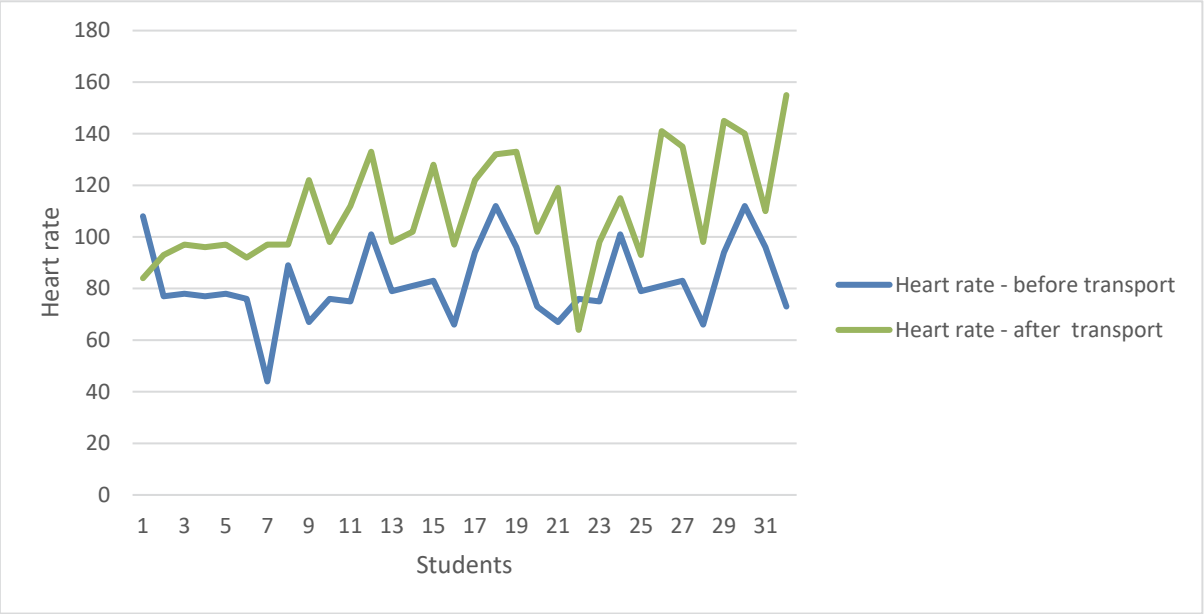


Figure 2. Graph of Students' Heart Rate before and after Patient Transport

Oxygen saturation: The average oxygen saturation (SpO_2) before the transport was 97.1 %, which slightly decreased to 94.9 % after the transport. The increase in variability may reflect individual differences in ventilation and the body's adaptation to physical exertion. Figure 3 illustrates the SpO_2 values of students before and after patient transport. The mean saturation decreased only slightly post-transport, while the standard deviation increased (SD 0.88 → 10.06), indicating varied respiratory responses among participants during physical stress. This visualization provides not only the average trend but also the extreme values, minimum, and maximum, offering a comprehensive overview of students' physiological adaptation to the exertion associated with patient transport. The relatively minor decrease in average saturation suggests that baseline oxygenation remained largely preserved, with the increased variability likely due to individual differences in ventilatory response and physiological adaptation to the workload.

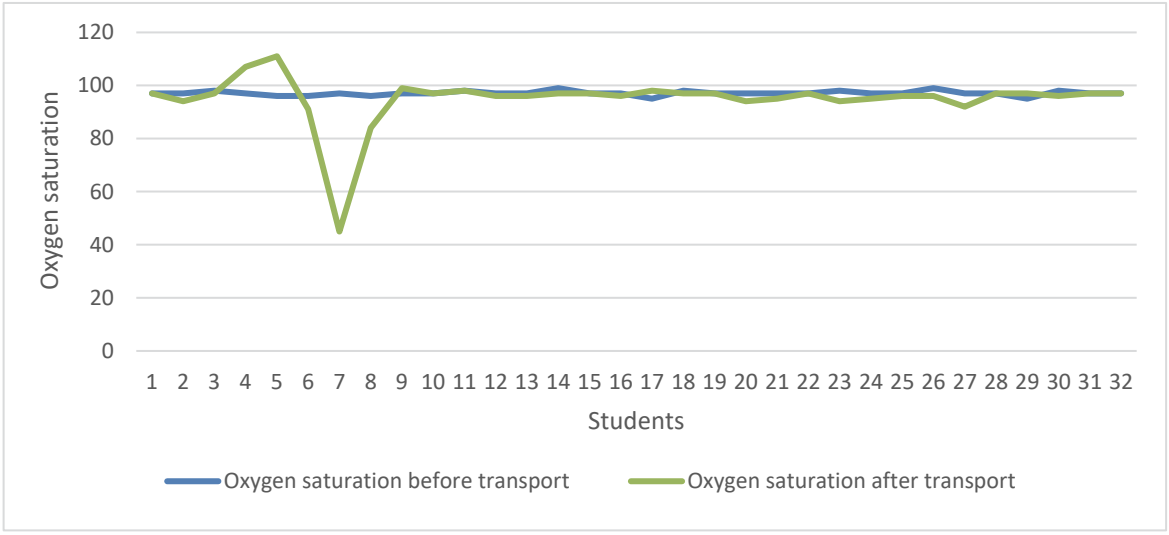


Figure 3. Graph of Students' Oxygen Saturation

Respiratory Rate: The average value increased from 14.1/min to 19.8/min, with the standard deviation rising from 4.4 to 7.36 and the coefficient of variation from 31.5 % to 37.2 %. The elevated respiratory rate and variability indicate adaptive ventilation in response to the increased energy demand during patient transport. Figure 4 illustrates the respiratory rate of students before and after the physical exertion associated with patient transport. Visualization of all data, including minimum and maximum values, allows assessment of the range of respiratory system adaptation in individual students. The increase in respiratory rate represents a typical physiological response to heightened energy requirements and increased muscle activity during physical load, confirming patient transport as a significant physical stressor.

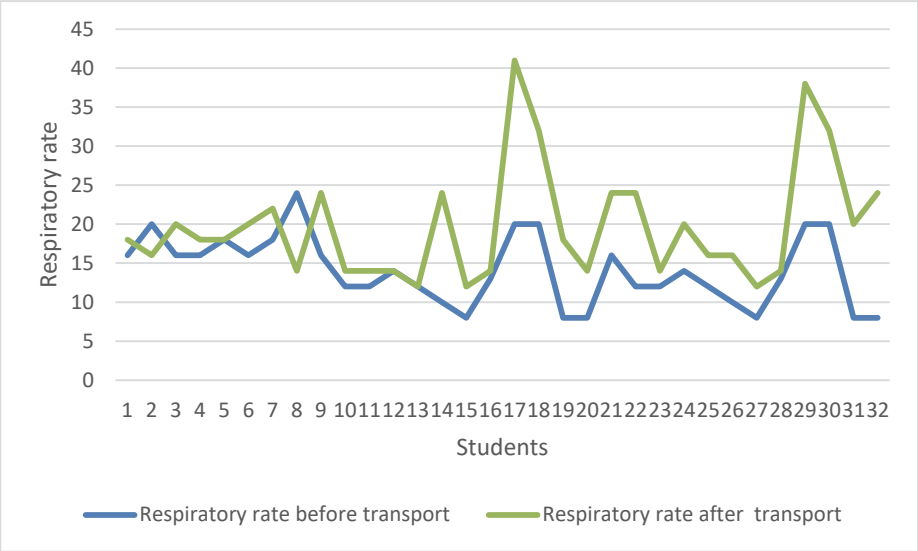


Figure 4. Respiratory Rate of Students before and after Patient Transport

Body Temperature: The average body temperature of the students before transport was 36.51 °C and decreased slightly to 36.12 °C after transport, with low variability in the recorded values. This parameter remained relatively stable, indicating the preservation of thermoregulatory mechanisms during the physical load associated with patient transport. However, potential methodological factors affecting measurement accuracy should be considered: the temperature was measured using a non-contact digital thermometer on the forehead, and after physical activity, the students' skin was sweaty. The presence of sweat may have caused localized cooling of the skin surface, leading to slight underestimation of the measured values. Such systematic bias is important to consider when interpreting body temperature results obtained with a non-contact method.

Patient transport represented a significant physical load for the students, reflected by increases in blood pressure, heart rate, and respiratory rate. Oxygen saturation and body temperature remained relatively stable. The greatest variability was observed in respiratory rate and heart rate, reflecting individual differences in physiological response to physical exertion.

4.1 Influence of Physical Fitness and BMI on Transport Performance

The analysis showed that students with a normal BMI (18.5–24.9) and regular physical activity achieved lower heart rates after the task and shorter transport times. A Spearman correlation analysis was conducted to examine the relationship between students' BMI and patient transport time. Results indicated a moderate positive correlation ($\rho = 0.378$), suggesting that students with higher BMI tended to perform the transport slightly more slowly. This correlation aligns with the expectation that higher body weight may increase the physical demands of handling a patient, thereby prolonging transport time.

Correlation analysis of the physiological parameters measured before and after patient transport allowed the exploration of relationships between individual variables. Pearson correlation was used due to the continuous nature of the data. The analysis revealed that respiratory rate exhibited the highest moderate positive correlation with other monitored parameters ($r = 0.481$), indicating that respiratory rate may serve as a relatively consistent indicator of physiological activity before and after transport and is partially associated with other physiological variables, such as heart rate and blood pressure.

Heart rate showed another moderate positive correlation ($r = 0.350$), suggesting that higher heart rates were partially associated with increased respiratory rates and slight variations in diastolic blood pressure. Diastolic blood pressure ($r = 0.313$) demonstrated a weaker, but still observable, positive correlation, indicating it may modestly reflect individual physiological differences prior to physical exertion. In contrast, systolic blood pressure ($r = 0.042$) and SpO_2 ($r = 0.008$) exhibited very weak or negligible correlations with other parameters, suggesting that these indicators do not significantly reflect variability in physiological responses among students at baseline or after transport. Body temperature ($r = 0.278$) showed a weak positive correlation, indicating only a minor influence on other physiological measures.

Overall, these results indicate partial interrelations among the measured physiological parameters, with the most significant and persistent correlations observed between respiratory rate and heart rate. Weak correlations for systolic blood pressure, oxygen saturation, and temperature suggest that these parameters are not sensitive indicators of individual differences in standardized simulated training conditions.

4.2 Physiological Changes During Transport

To assess physiological load during the practical patient transport training, percentage changes (Δ%) were calculated for systolic and diastolic blood pressure, heart rate, respiratory rate, SpO_2, and body temperature. Percentage changes allow comparison of individual responses regardless of baseline values. The percentage changes are presented in Table 4.

Table 4. Percentage Physiological Changes in Students

Δ%

Group	No.	Blood presure systolic	Blood presure diastolic	Oxygen saturation	Heart rate	Respiratory rate	Body temperature
Š4-A	Š1	-15,69	-7,37	-22,22	0,00	12,50	-0,55
	Š2	23,77	26,03	20,78	-3,09	-20,00	-1,89
	Š3	-17,16	12,16	24,36	-1,02	25,00	-2,67
	Š4	17,21	24,68	24,68	10,31	12,50	-1,90
Š4-B	Š5	12,50	6,90	24,36	15,63	0,00	-1,93
	Š8	7,91	13,33	21,05	-5,21	25,00	3,03
	Š6	-22,30	9,86	120,45	-53,61	22,22	-2,45
	Š7	9,85	5,41	8,99	-12,50	-41,67	-2,45
Š4-E	Š21	25,64	29,31	82,09	2,06	50,00	-0,83
	Š19	-9,23	30,00	28,95	0,00	16,67	-1,63
	Š20	-2,60	1,16	49,33	0,00	16,67	-0,54
	Š18	0,00	-14,02	31,68	-1,03	0,00	-2,71
Š4-F	Š22	9,92	-10,39	24,05	-1,03	0,00	-0,55
	Š24	15,04	12,50	25,93	-2,02	140,00	0,27
	Š23	37,78	-3,19	54,22	0,00	50,00	-1,39
	Š27	-8,59	3,80	46,97	-1,03	7,69	-1,37
Š4-G	Š28	0,00	6,67	29,79	3,16	105,00	-0,27
	Š29	19,38	9,52	17,86	-1,02	60,00	-1,10
	Š30	3,08	2,25	38,54	0,00	125,00	1,99
	Š31	23,81	34,48	39,73	-3,09	75,00	-2,43
Š4-E	Š21	38,46	65,52	77,61	-2,06	50,00	-1,67
	Š19	-6,15	-12,50	-15,79	0,00	100,00	-1,90
	Š20	-9,74	3,49	30,67	-4,08	16,67	-1,08
	Š18	-12,27	-11,21	13,86	-2,06	42,86	-3,52
Š4-F	Š22	17,56	9,09	17,72	-1,03	33,33	-1,10
	Š24	30,97	16,25	74,07	-3,03	60,00	1,37
	Š23	22,96	-5,32	62,65	-5,15	50,00	-0,83
	Š27	17,97	12,66	48,48	0,00	7,69	-2,74
Š4-G	Š28	-9,35	4,00	54,26	2,11	90,00	1,09
	Š29	-3,88	4,76	25,00	-2,04	60,00	-1,37
	Š30	2,31	-11,24	14,58	0,00	150,00	2,56
	Š31	41,90	55,17	112,33	0,00	200,00	-2,97

Blood Pressure: Systolic blood pressure showed percentage changes (Δ%) ranging from -22.3 to 41.9, while diastolic pressure varied between -14.0 and 65.5 %. This range highlights substantial variability among participants. Some students experienced a decrease in blood pressure after patient transport, while others showed an increase. These differences reflect individual cardiovascular adaptations to physical exertion and the ability to efficiently manage coordinated patient transfer. The overall trend indicates a slight increase in diastolic pressure, consistent with the expected physiological response to mild-to-moderate physical effort associated with patient handling.

Heart Rate: Percentage changes in heart rate (Δ%: -53.6 to 15.6) indicate variability in student responses. Most participants showed a slight increase or stable heart rate, suggesting that the physical load was appropriate and did not trigger a significant cardiac stress response. The extreme value of -53.6 % may result from individual variability, measurement deviation, or short-term adaptive mechanisms. Overall, heart rate proved to be a relatively stable indicator of physiological load during short-term patient transport.

Respiratory Rate: Analysis of percentage changes in respiratory rate demonstrated the most pronounced response to physical exertion, with Δ% reaching up to 200 %. This parameter clearly reflects the physical effort during patient transport and highlights substantial individual differences in physical fitness and coordination ability. The average increase confirms the expected physiological adaptation to exertion, while extreme values indicate variations in endurance, respiratory capacity, or technique. This demonstrates that respiratory rate is a sensitive and suitable parameter for assessing physical demands in practical training.

SpO_2 Saturation: Percentage changes in SpO_2 ranged from -22.2 to 120.4 %. Most changes were slightly positive, indicating that patient transport did not induce clinically significant hypoxia. Extreme values likely reflect measurement errors or short-term monitoring variations rather than true physiological distress. Overall, these results indicate that patient transport under simulated conditions was safe with regard to oxygenation.

Body Temperature: Percentage changes in body temperature were minimal (Δ%: -3.0 to 3.0), suggesting stable thermoregulation even during increased physical effort associated with patient handling. This parameter appears to be the least sensitive indicator of physiological load during short-term transport, consistent with expectations for practical training performed at room temperature over a brief period.

A line chart (Fig. 5) illustrates the percentage changes (Δ%) of physiological parameters during the practical patient transport training. The X-axis represents individual students, and the Y-axis shows Δ% values for each parameter: systolic and diastolic blood pressure, heart rate, respiratory rate, SpO_2, and body temperature. Each line represents the change pattern of one parameter across all students.

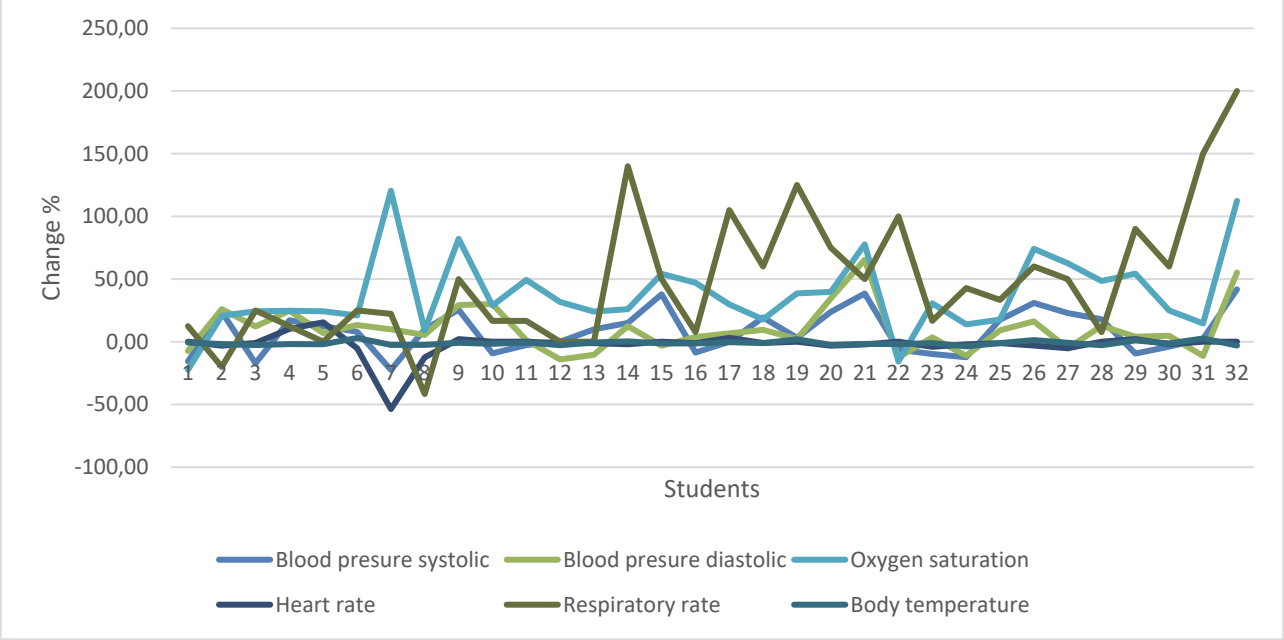


Figure 5. Graph of Changes in Students' Physiological Parameters

The graph supports the conclusion that the most sensitive indicator of students' physical workload during patient transport is respiratory rate, while the other parameters serve as supplementary indicators of the body's physiological adaptation. The graph also highlights the need to monitor individual differences among students during practical training and when assessing intervention safety.

Effect of BMI on physiological response during patient transport

Analysis of physiological changes during practical patient transport showed that participants' body composition, expressed by BMI, significantly affects cardiovascular and respiratory responses. Students with higher BMI tended to exhibit higher heart rates and increased systolic and diastolic blood pressure at the same level of physical effort, reflecting greater cardiovascular load associated with moving a weight combining the patient's mass and their own body weight. In contrast, participants with normal BMI and regular physical activity demonstrated lower heart rates and shorter transport times, indicating more efficient physiological adaptation and higher work efficiency.

Higher BMI was also associated with an increase in respiratory rate, reflecting elevated energy demands and ventilation during physical exertion. Correlation analysis confirmed a moderately strong positive relationship between BMI and patient transport time (ρ = 0.378), suggesting that higher body weight may prolong task completion due to greater physical effort and more challenging movement coordination.

Parameters such as oxygen saturation (SpO_2) and body temperature remained relatively stable and independent of BMI, indicating that these indicators are less sensitive to body composition during short-term transport. BMI had the most pronounced impact on heart rate and respiratory rate, which proved to be the most sensitive indicators of physiological workload during simulated intervention.

Overall, the results suggest that BMI is a significant factor determining individual physiological responses to physical effort and the efficiency of practical patient transport. Participants with normal BMI and regular physical activity displayed more favorable physiological profiles, supporting their ability to perform rescue tasks safely and effectively.

5 Discusion

The results of this study clearly indicate that patient transport represents a physically demanding activity for students, as evidenced by significant changes in physiological parameters. Heart rate showed a marked increase from an average of 82.3/min before transport to 110.8/min after completion, with the standard deviation rising from 14.8 to 20.8, reflecting individual differences in response to physical exertion [5]. Similarly, blood pressure increased-systolic from 133.1 mmHg to 142.1 mmHg and diastolic from 80.0 mmHg to 86.4 mmHg-indicating hemodynamic activation of the sympathetic nervous system in response to physical effort. Oxygen saturation exhibited a slight decrease in average value (97.1 % → 94.9 %), with increased variability among participants pointing to differences in respiratory adaptation to physical load. Despite this, saturation remained relatively stable, suggesting preservation of baseline tissue oxygenation even during physically demanding performance [3].

These findings are consistent with previous studies on physiological responses to exertion in rescuers and athletes, which demonstrated increases in cardiovascular and ventilatory parameters during intense physical aktivity [6]. The rise in heart rate and blood pressure, along with a slight decrease in SpO_2, confirms that patient transport is physiologically demanding, with individual differences potentially influenced by physical fitness level, BMI, and the body's adaptation to exertion.

6 Conclusion

The research results confirmed that patient transport using the log-roll technique represents a significant physical load, primarily manifested by an increase in heart rate and respiratory rate, along with a moderate rise in blood pressure. Oxygen saturation and body temperature remained relatively stable, indicating the preservation of basic homeostatic mechanisms even during physical exertion under simulated conditions.

Analysis of the influence of body constitution showed that students with higher BMI exhibited greater cardiovascular strain and slightly longer transport times, whereas students with normal BMI and regular physical activity achieved more favorable physiological responses and higher efficiency in handling. Correlation analysis between respiratory and heart rates confirmed that these parameters are the most sensitive indicators of physical load during practical patient transport.

Overall, the study highlights the importance of physical fitness and optimal body weight for the safe and effective performance of rescue tasks. The findings provide a basis for optimizing training scenarios, setting the intensity of physical exertion, and individualizing training procedures to maximize patient safety and intervention efficiency.

Acknowledgement

This contribution was supported by the project "KEGA 048ŽU-4/2025 Centre for Practical Education for the Study Programme Emergency Medical Services."

Reference

[1] Hignett, S. (2003). Intervention strategies to reduce musculoskeletal injuries associated with handling patients: A systematic review. Occupational and Environmental Medicine, 60(9), 9–14. https://doi.org/10.1136/oem.60.suppl_1.i9

[2] Knapik, J. J., Hauret, K. G., & Jones, B. H. (2011). Primary prevention of injuries in emergency medical technicians: A systematic review. Journal of Emergency Medical Services, 36(3), 44–50

[3] Wielemborek, K., 2005. The blood pressure response to physical exertion in adults: a preliminary survey results. (2006). Journal of Physical Activity and Health. Retrieved from PubMed: https://pubmed.ncbi.nlm.nih.gov/16521919/

[4] Pavkovičová, A., 2014. Preparedness of the Integrated Rescue System Components for Mass-Casualty Incidents in the Slovak Republic. Master's Thesis. 125 s. České Budějovice, 2014

[5] KARLSSON, K. a kol., 2011. Heart rate as a marker of stress in ambulance personnel: a pilot study of the body's response to the ambulance alarm. Prehospital and Disaster Medicine. 2011, 26(1), 21–26. DOI: 10.1017/S1049023X10000129

[6] TREMBLAY, M. a kol., 2020. Physiological responses during paramedics' simulated driving tasks. Work: A Journal of Prevention, Assessment & Rehabilitation. 2020, 66(2), 445–460. DOI: 10.3233/WOR-203184

Možnosti numerického modelovania indukovaných rázových vĺn vo vybraných softvérových nástrojoch

Sebastián Vojtáš[1], Miroslav Mynarz[2], Juraj Sinay[3]

[1] VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství,
Lumírova 13, 700 30 Ostrava, sebastian.vojtas@vsb.cz

[2] VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství,
Lumírova 13, 700 30 Ostrava, miroslav.mynarz@vsb.cz

[3] VŠB – Technická univerzita Ostrava, Fakulta bezpečnostního inženýrství,
Lumírova 13, 700 30 Ostrava, juraj.sinay@vsb.cz

Abstrakt:

V kontexte aktuálnych vojenských konfliktov a technologických procesov používajúcich výhradne látky s výbušnými vlastnosťami, je kladený zvýšený dôraz na analýzu rizík. Na analýzu je možné využiť viacero prístupov, napríklad experimentálne alebo analytické, empirické alebo numerické metódy. Tieto prístupy výpočtu metódy sa vzájomne dopĺňajú, ale použitím len jedného typu výpočtu môže riešiteľ dostať skresľujúce výsledky. Pre validáciu numerických modelov je preto odporúčané overiť výsledky na základe experimentálnych meraní, ak to nie je možné tak alespoň empirickými metódami. Numerické prostredie Autodyn alebo LS-Dyna používajú pre výpočty stavovú rovnicu podľa Jones Wilkins Leeho (ďalej JWL), ktorá bola primárne používaná pre popis expanzie produktov detonácie výbušnín. Prvé kroky numerických modelov smerovali k použitiu 1D modelu šírenia rázovej vlny a následným porovnaním s hodnotami nameranými na experimentálnych meraniach. Druhý model bol zameraný na použitie 2D modelu, ktorý bol tiež následne porovnaný s experimentálnymi dátami ale aj s prvým modelom. Podklad pre validáciu boli brané experimentálne merania prebiehajúce pod záštitou Fakulty bezpečnostního inženýrství. Po validácii výsledkov boli následne použité komplexnejšie geometrie, kde bola sledovaná aj interakcia s prekážkami. Model mestskej zástavby, po iniciácií 50 kg TNT bol jeden z najväčších. Model dvojposchodovej budovy zase detailnejší. Bolo overené použitie testovanej prekážky BALBAR pre zvýšenie ochrany jednotiek Integrovaného záchranného systému. Výsledkom použitia matematických modelov bolo úspešná validácia výsledkov a overenie účinnosti bariéry. Odchýlky od experimentálnych meraní dosahovali hodnoty v jednotkách percent a analýza potvrdila útlm okamžitého tlaku za bariérou o takmer 80 %.

Klíčová slova: matematické modely, indukované rázové vlny, výbuchový materiál, interakcia rázových vĺn s prekážkami, validácia experimentu s numerickými modelmi.

1 Úvod

Numerické modelovanie rýchlych dynamických dejov predstavuje významný nástroj pri analýze rizík spojených s výbuchovými procesmi. V praxi sa pri hodnotení krízových scenárov často využívajú empirické metódy, ktoré však vzhľadom na svoje zjednodušenia neumožňujú analýzu komplexných geometrických interakcií [1]. Alternatívou je použitie matematických modelov založených na metódach CFD, ktoré umožňujú detailné sledovanie šírenia rázových vĺn v priestore.

Analýza výbuchových javov a šírenia indukovaných rázových vĺn predstavuje významnú súčasť hodnotenia rizík v technických a priemyselných systémoch. Výbuchy horľavých plynných zmesí alebo výbušnín môžu viesť k vzniku tlakových vĺn s výraznými deštrukčnými účinkami na stavebné konštrukcie, technologické zariadenia aj

ľudský organizmus. Z tohto dôvodu je dôležité venovať pozornosť nielen experimentálnemu skúmaniu týchto javov, ale aj numerickému modelovaniu, ktoré umožňuje analyzovať rôzne havarijné scenáre a predikovať ich možné dôsledky [2, 3].

Experimentálne merania predstavujú základný pilier pri validácii matematických modelov výbuchových dejov. Poskytujú reálne údaje o časovom priebehu tlaku, vrcholných pretlakoch a dynamike šírenia rázových vĺn. Na druhej strane však experimentálne skúšky bývajú finančne náročné, časovo limitované a často nie je možné nimi pokryť všetky potenciálne scenáre havarijných udalostí. Z tohto dôvodu sa čoraz viac využívajú numerické modely, ktoré umožňujú simulovať šírenie rázových vĺn v komplexných geometriách a analyzovať ich interakciu s okolitým prostredím alebo konštrukciami [4, 5].

Významným problémom pri modelovaní výbuchov horľavých plynov je správny opis fyzikálnych a chemických procesov prebiehajúcich počas iniciácie a šírenia reakčného frontu. Empirické prístupy, napríklad modelovanie pomocou ekvivalentu TNT, umožňujú rýchly odhad tlakových účinkov, avšak často nedokážu zachytiť komplexnú dynamiku šírenia rázovej vlny ani vplyv geometrie prostredia [8, 10]. Presnejšie výsledky je možné dosiahnuť použitím pokročilých numerických metód, ktoré explicitne zohľadňujú chemickú kinetiku horľavých zmesí a interakciu rázovej vlny s konštrukčnými prvkami [8, 10]. Príkladom takéhoto prístupu je numerické modelovanie výbuchu vodíkovo-vzdušnej zmesi s využitím CESE riešiča implementovaného v prostredí LS-DYNA, kde bola analyzovaná interakcia rázovej vlny s betónovou bariérou. Výsledky štúdie ukázali, že zahrnutie redukovanej chemickej kinetiky umožňuje presnejšie zachytiť priebeh tlakovej vlny a jej interakciu s prekážkami v porovnaní so zjednodušenými prístupmi založenými na ekvivalente TNT [9].

Numerické modelovanie výbuchových javov je dnes realizované pomocou špecializovaných softvérových nástrojov, medzi ktoré patria napríklad ANSYS AUTODYN alebo LS-DYNA. Tieto programy umožňujú simulovať šírenie rázových vĺn v prostredí s prekážkami, analyzovať dynamickú odozvu konštrukcií a hodnotiť účinnosť ochranných prvkov proti výbuchovému zaťaženiu. Po úspešnej validácii základných modelov je možné simulácie rozšíriť aj na komplexné scenáre, napríklad modely mestského prostredia alebo interiéru budov, kde dochádza k viacnásobným odrazom rázových vĺn a ich interakcii s konštrukčnými prvkami [7,13].

Cieľom tohto príspevku je predstaviť možnosti numerického modelovania indukovaných rázových vĺn vo vybraných softvérových nástrojoch a analyzovať ich presnosť pri porovnaní s experimentálnymi meraniami. Osobitná pozornosť je venovaná vplyvu výpočtovej siete, voľbe materiálových modelov a správnemu nastaveniu okrajových podmienok na výslednú presnosť simulácií.

2 Metodika

Základná metodika bola založená na analýze dát zaznamenaných z experimentálnych meraní uskutočnených na Fakulte bezpečnostního inženýrství. Dáta z týchto meraní slúžili ako podklady pre stanovenie okrajových podmienok modelu a určenie citlivosti výpočtovej siete.

2.1 Numerické prostredie a typ riešiča

Explicitné riešiče Autodyn a LS-Dyna sú obidva softvéry založené na matematickom modelovaní a teda sú vhodné pre analýzu šírenia indukovaných rázových vĺn. Autodyn je vyslovene softvér pre analýzu explózií, kde sa dajú veľmi vhodne analyzovať rázové vlny v prostredí s prekážkami. Za určitých okolností pri správnom nastavení okrajových podmienok modelu je možné analyzovať aj deštrukciu či ohyb prekážok. LS-Dyna sa používa hlavne pre analýzu crash testov áut, prúdenia tekutín, výbuch airbagov ale aj vo vojenskom priemysle (streľba zo zbrane,

výbuch mín pod autom, pády dronov). LS-Dyna má vhodnejšie zobrazenie deformácií konštrukcií po zaťažení rázovými vlnami, ako v softvéri Autodyn. Podľa dostupných informácií nebol v poslednom období vývoj softvéru AUTODYN rozšírený o zásadné nové funkcie, čo môže predstavovať obmedzenie pri riešení niektorých typov úloh. Analýza šírenia indukovaných rázových vĺn po iniciácií náloží je vhodná, ale šírenie rázových vĺn horľavých plynných zmesí je značne obmedzená. Pre zjednodušené výpočty v prostredí s tekutinami sa používajú Euler metódy. Pre komplexnejšie modely a analýzu deformácie tuhého skupenstva je určená Lagrange metóda (Crash testy, airbagy s figurínami). Spojenie Euler a Lagrange metódy v analýzu jedného modelu je nevyhnutné pre analýzu interakcie tuhého a kvapalného/plynného skupenstva. V prostredí LS-Dyna je možné nájsť túto metódu pod skratkou ALE (Arbitrary Lagrange Euler).

2.2 Materiálový model výbušniny (JWL)

Stavová rovnica JWL bola použitá na popis expanzie produktov detonácie pri explicitných dynamických dejoch, kde umožňuje presné zachytenie tlakovo-objemových vzťahov počas šírenia rázovej vlny [2]. Tvar výslednej rovnice JWL je nasledovný:

$$P = A\left(1 - \frac{\omega}{R_1 V}\right)e^{-R_1 V} + B\left(1 - \frac{\omega}{R_2 V}\right)e^{R_2 V} + \frac{\omega E}{V} \tag{1}$$

Detonačná energia *E* obsahuje energiu chemickej väzby, spolu s kinetickou energiou spojenou s hybnosťou toku a udáva sa v jednotkách [kJ/dm^3]. *A*, *B*, *C* sú koeficienty tlaku väčšinou v jednotkách [GPa]. *R*1 a *R*2 sú veličiny bez jednotiek a *ω* je zlomková časť normálneho adiabatického exponentu Taitovej rovnice. Objem vo vzorci *V* je špecifický objem vychádzajúci zo vzorca *V* = *v*/*v*0 (9), kde špecifický objem *v*0 je inverzná hodnota k počiatočnej hustote výbušniny a špecifický objem *v* je nezávislá premenná.

$$B_T = \frac{1}{\rho}\left(\frac{\partial \rho}{\partial T}\right) = \frac{1}{\left[1 - C ln[(P+B)/(P_0+B)]\right]} \cdot \frac{C}{P+B} \tag{2}$$

ρ je hustota, *P* je tlak, *ρ*0 a *P*0 sú hustota a tlak na počiatku merania. Veličiny *B* a *C* závisia od teploty skúmanej látky. Úpravou vzorca 14 je možné získať veličinu izotermickú stlačiteľnosť látky B_T. Ak je známa hustota materiálu a izotermická stlačiteľnosť za určitej teploty, tak jedinou neznámou v aplikácií Taitovej stavovej rovnici je závislosť teploty na parametri *B*. Na zistenie týchto parametrov bola použitá škála zodpovedajúcich rámcov (Corresponding states framework - CS). Tieto zodpovedajúce rámce majú použitie hlavne pri polárnych tekutinách, nie len vtedy ak závisia na zredukovanej teplote (*T*/*Tc*) a zredukovanom tlaku (*P*/*Pc*) ale aj na treťom parametre. Týmto parametrom je akcentrický faktor *ω*. [15]

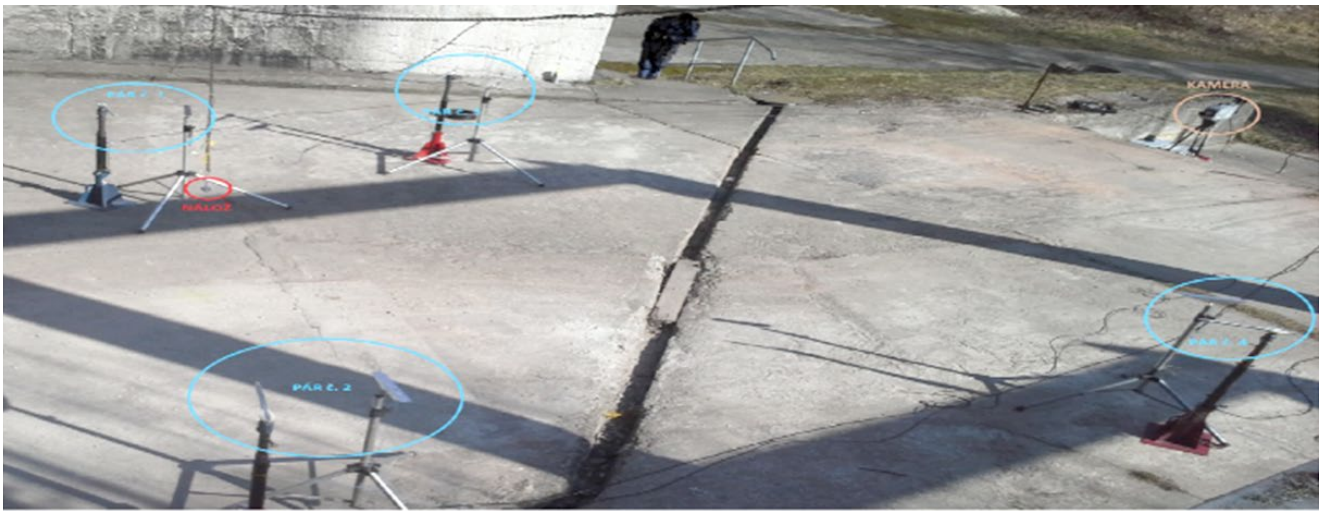
Použitie stavovej rovnice JWL v prostredí AUTODYN bolo úspešne validované aj v práci [12], kde numerické simulácie rázových vĺn generovaných viacvrstvovými náložami vykazovali dobrú zhodu s experimentálnymi meraniami, pričom odchýlky maximálneho pretlaku sa pohybovali približne do 20 %.

2.3 Okrajové podmienky

Výpočtová doména bola navrhnutá tak, aby zabezpečovala dostatočný priestor pre voľnú propagáciu rázovej vlny bez ovplyvnenia výsledkov okrajovými efektmi. Na hraniciach domény boli použité okrajové podmienky umožňujúce ďalšie šírenie vlny mimo modelu (outflow). Podložie bolo definované s úplnou reflexiou tlakovej vlny. Meracie body boli umiestnené v rovnakých vzdialenostiach ako pri experimentálnych meraniach za účelom overenia vhodnosti matematického modelu. Vlastnosti vzduchu boli zvolené pre štandardné atmosférické podmienky. Materiálové parametre TNT boli prevzaté z databázy výrobcu softvéru.

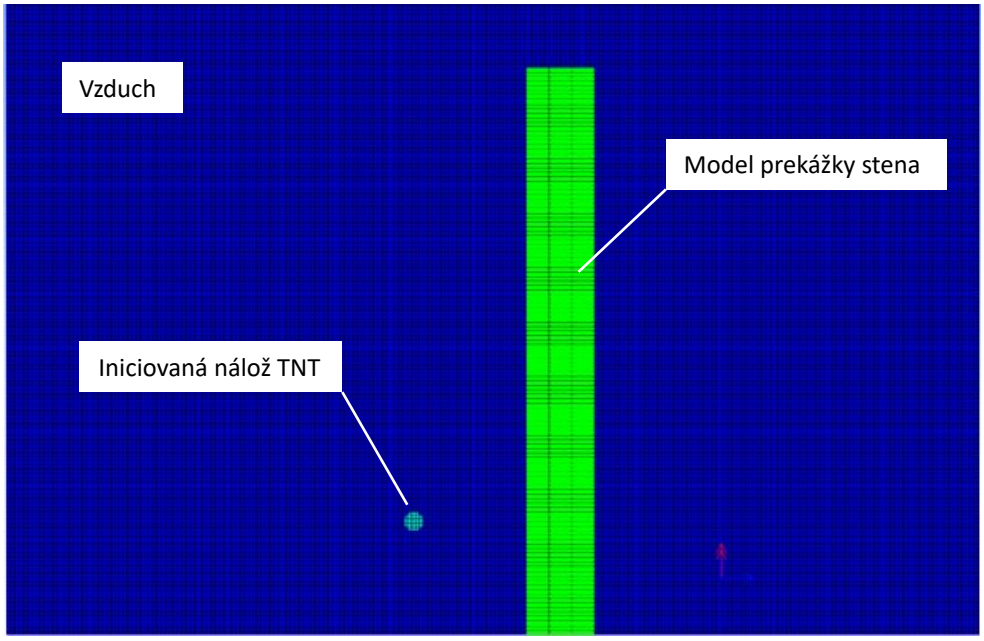
3 Výsledky a diskusia

Pre overenie numerických modelov boli použité dáta z diplomových prác zameraných na šírenie rázových vĺn za pomoci piezoelektrických čidiel pre rôzne nálože (napr. TNT, Semtex 10-SE). Experimentálna zostava je zobrazená na Obrázku 1. Priebeh bol taktiež zaznamenaný na vysokorýchlostnú kameru viditeľnú na obrázku.



Obrázok 1. Príprava experimentu na záznam priebehu okamžitých tlakov indukovanej rázovej vlny [15]

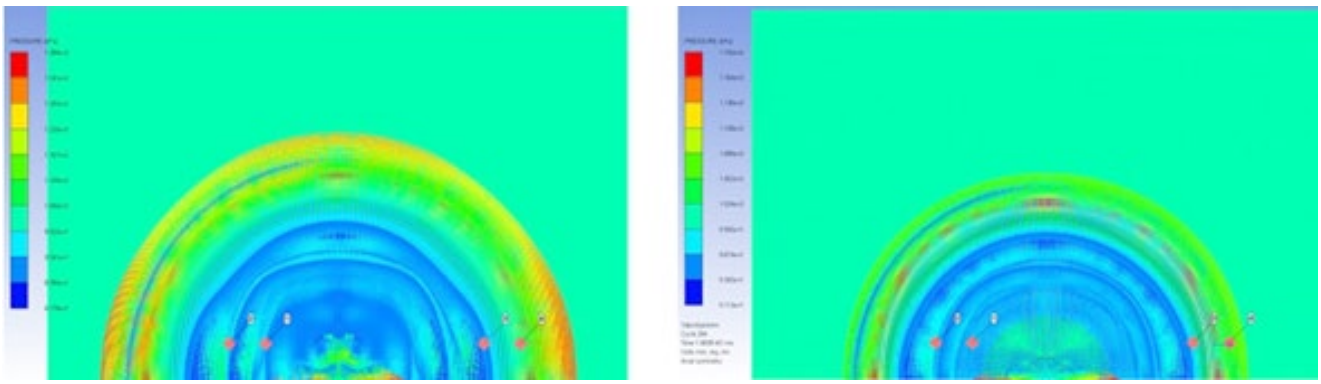
Numerické modelovanie nepozostáva len z určenia materiálových vlastností alebo návrhu geometrie. Dôležitý faktor výrazne ovplyvňujúci výsledné dáta je výpočtová sieť, ktorá je zložená zo súboru jednotlivých buniek. Celkový výpočtový čas pre model je lineárne závislý na počtu použitých buniek. Pri malom počte použitých buniek môžu byť výsledky skreslené, ale výpočet modelu neprebieha tak zdĺhavo. Naopak pri príliš veľkom počte buniek výpočet trvá príliš dlho a výsledky prestávajú vykazovať významné zlepšenie vzhľadom na výpočtový čas (numerická saturácia). Na Obrázku 2 je zobrazené prostredie Autodyn so zobrazenou výpočtovou sieťou. Obrázok 2 predstavuje model prekážky steny s náložou.



Obrázok 2. Zobrazenie prostredia Autodyn so zapnutou funkciou zobraziť „výpočtovú sieť“

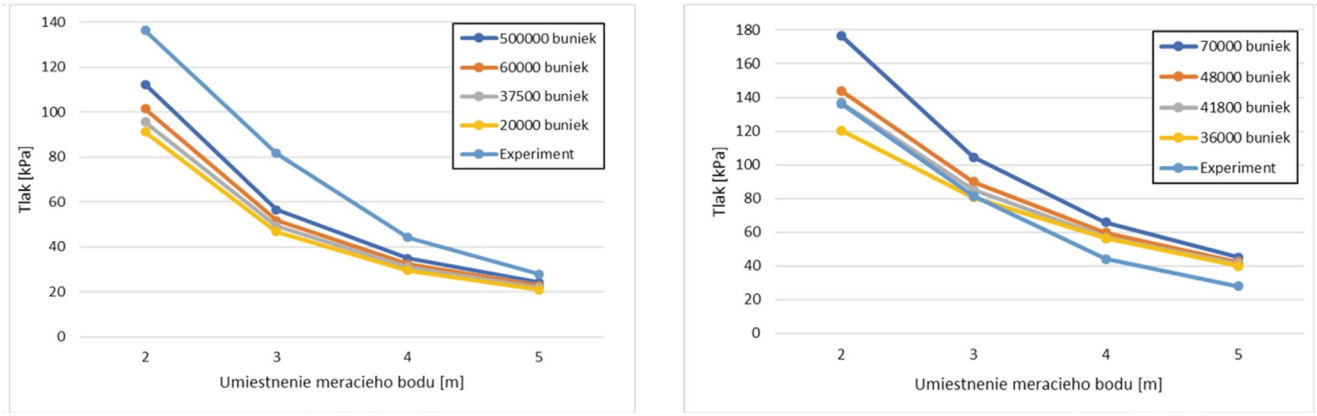
3.1 Štúdia citlivosti siete

Bola sledovaná odlišná veľkosť jednotlivých buniek siete, a jej vplyv na výsledky priebehu okamžitého tlaku pri zvolení dvoch odlišných postupov. Prvý postup nazvaný ako 2D kvázi axisymetrický model, bol vytvorený za pomocí 1D klínu v ktorom bola iniciovaná nálož. Po dokončení výpočtu, bol celý model následne vložený do 2D prostredia „vzduchu“. Druhý postup bol zložený z 2D axisymetrického modelu do ktorého bola umiestnená nálož. Na Obrázku 3 je zobrazené vizuálne porovnanie jednotlivých modelov. Na obrázkoch je možné si všimnúť aj meracie body (na obrázkoch červené značky), ktoré boli umiestnené v rovnakých vzdialenostiach ako pri experimentálnych meraniach.



Obrázok 3. Porovnanie výsledkov za použitia rozdielnych postupov (naľavo 2D model a napravo 2D-kvázi model)

Bol zistený výrazný vplyv podľa veľkosti výpočtovej siete na okamžitý tlak zaznamenaný v meracích bodoch. Pri každom zvolenom postupe bol tento vplyv odlišný. Ako je možné vidieť na Obrázku 4.



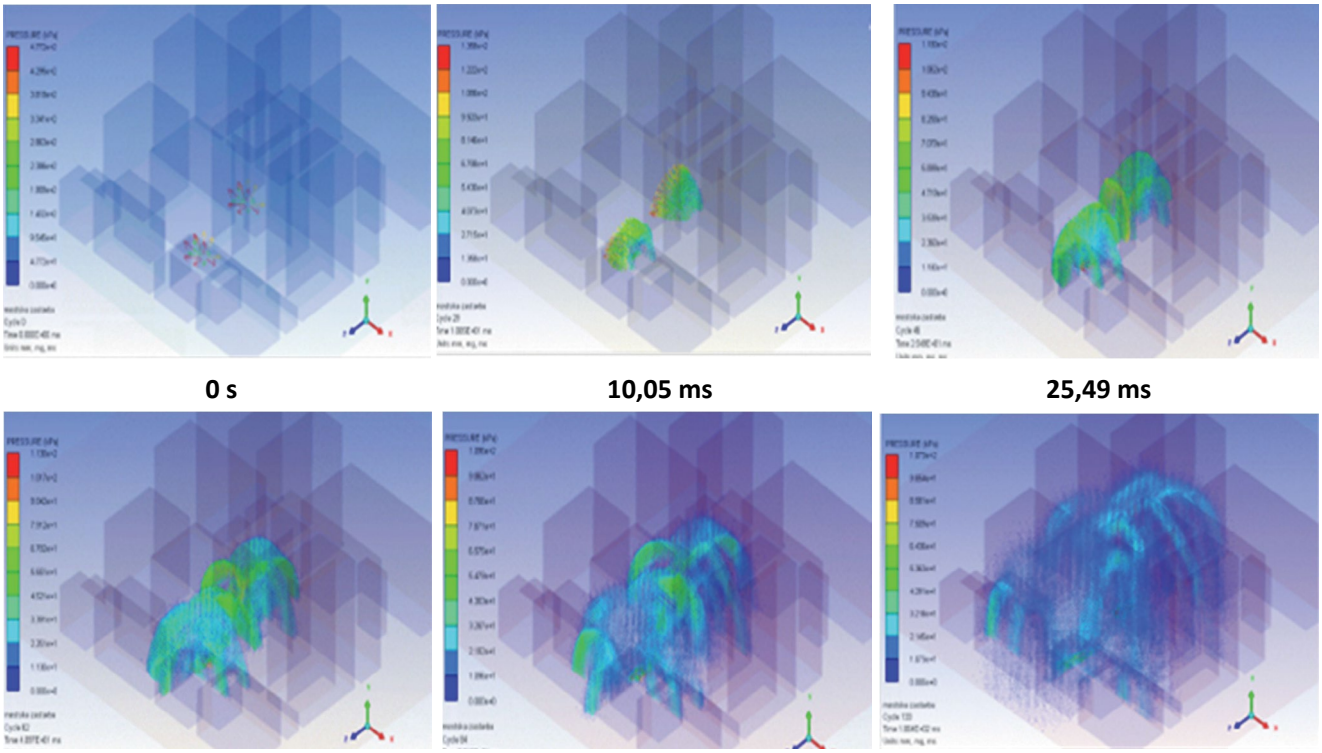
Obrázok 4. Závislosť počtu buniek v sieti na vrcholnom pretlaku pri použití odlišného postupu výpočtu v porovnaní s dátami z experimentu (naľavo 2D kvázi model, napravo 2D model)

3.2 Validácia modelu

V práci [13] bol použitý model s 1D klínom, kde bola odchýlka od experimentálneho merania v jednom prípade v priemere 5 % a v druhom prípade 11 % [13]. Pri použití postupov spomenutých v odseku vyššie, boli odchýlky vyššie, kde sa v priemere odlišovali necelých 22 % [14]. Pre posudzovanie zložitejších scenárov, je však nevyhnutné použitie 2D axisymetrického modelu alebo 3D izometrického modelu. Vyššie odchýlky pri 2D modeloch sú spôsobené kompromisom medzi presnosťou a výpočtovou náročnosťou, pričom pre praktické aplikácie je potrebné voliť rozlíšenie siete s ohľadom na dostupný výpočtový výkon.

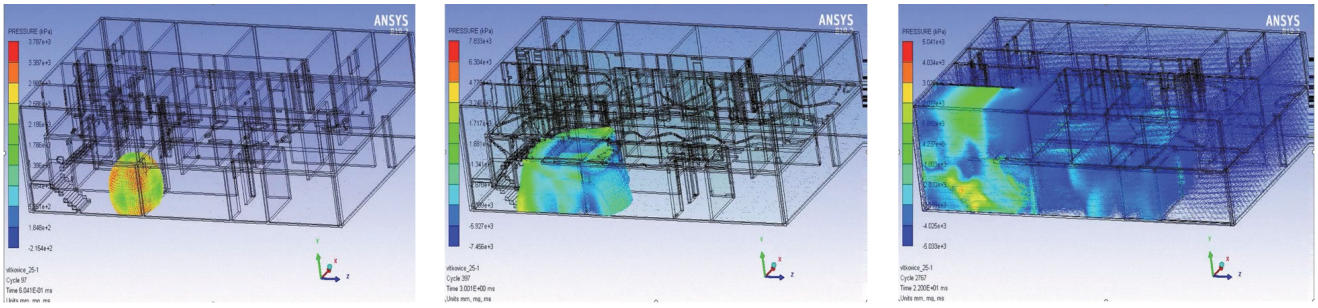
3.3 Komplexné scenáre

Po overení presnosti numerického modelu na jednoduchých geometriách (1D/2D modeloch) bol ďalší postup zameraný na simulácie komplexných scenárov, ktoré lepšie reprezentujú reálne podmienky šírenia rázovej vlny v zastavanom prostredí. Model zmenšeného mesta bol inšpirovaný po vykonaných teroristických útokoch v rámci západného sveta. Bol kladený dôraz na úzke uličky a nereagujúce prekážky (tzv. Rigid bodies). Pre iniciáciu boli použité dve nálože TNT o hmotnosti 50 kg jednotlivo [3]. To môže byť takisto ekvivalent nálezu starej nevybuchnutej munície z druhej svetovej vojny, ktorý sa stále občas vyskytne v našom prostredí Českej a Slovenskej republiky. Na Obrázku 5 je možné si všimnúť numerický model mesta a priebeh šírenia rázovej vlny medzi prekážkami (budovami).



Obrázok 5. Priebeh šírenia rázovej vlny v namodelovanom prostredí mesta

Analýza šírenia indukovaných rázových vĺn bola overená aj na komplexnej geometrii interiéru dvojpodlažnej stavby na Obrázku 6. Vďaka projektovej dokumentácií bol vytvorený matematický model budovy v ktorej bolo iniciovaných 10 kíl nálože TNT.

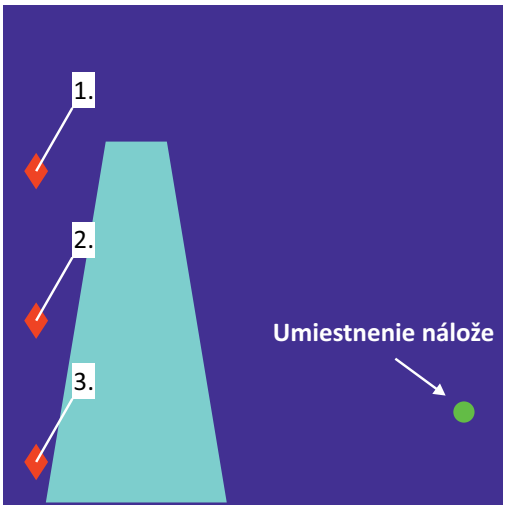


Obrázok 6. Priebeh šírenia indukovaných rázových vĺn v prostredí dvojpodlažnej budovy

Posledný posudzovaný model je zameraný na analýzu poklesu okamžitého tlaku v prostredí s prekážkou BALBAR. Táto balistická bariéra bola vyvinutá pre ochranu osôb pred účinkami rázovej vlny, fragmentácie či dokonca účinkami sálavého tepla pri požiari. Autori BALBAR otestovali efekt ochrany pred účinkami rázovej vlny za pomoci 1 kg trhaviny (TNT), a použitia figuríny. Zostava pokusu je viditeľná na Obrázku 7.

Obrázok 7. Pokus výrobcu BALBAR s figurínou [14]

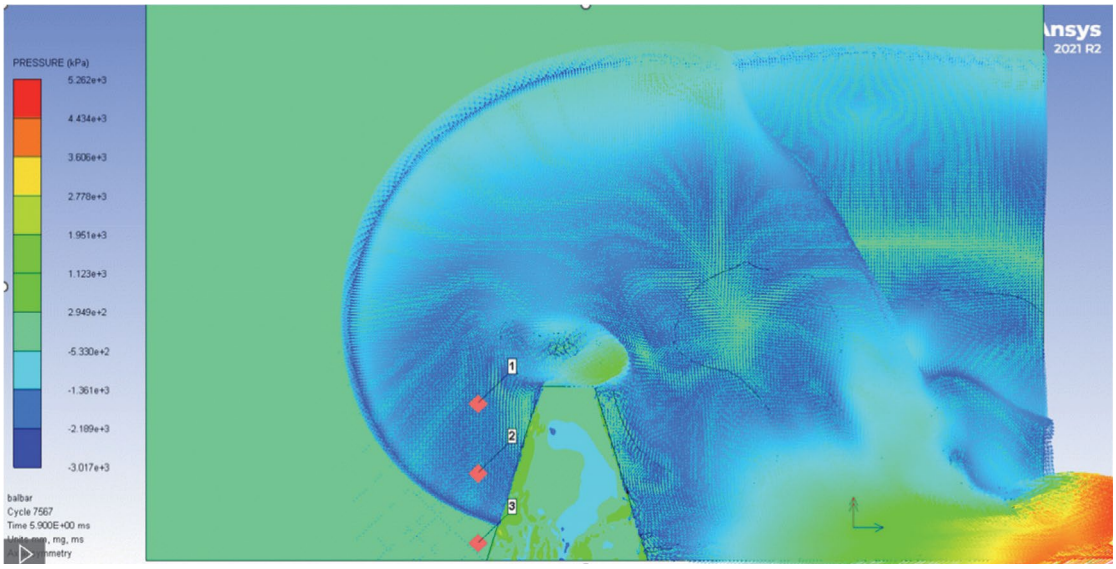
Vytvorením matematického modelu je možné získať priebeh okamžitého tlaku za balistickou bariérou. Okamžitý tlak je potom možné porovnať so šírením rázovej vlny s a bez prekážky. Na Obrázku 8 je zobrazený model pred iniciáciou. Iniciovaná nálož bola umiestnená 2 metre od prekážky BALBAR a 0,5 metra nad zemou (červený bod). Boli použité 3 meracie body (oranžové body) v troch rôznych vzdialenostiach. Prvý merací bod je vo vzdialenosti 1,8 metra nad zemou, druhý merací bod je vo vzdialenosti 1 meter nad zemou a tretí merací bod bol umiestnený 0,2 metra nad zemou. V tabuľke umiestnenej na hornej časti obrázku je porovnanie zaznamenaných okamžitých tlakov pri odlišných výškach od zeme.



Merací bod číslo [-]	**1**	**2**	**3**
Maximálny pretlak – s prekážkou [kPa]	141,68	88,51	227,83
Maximálny pretlak – bez prekážky [kPa]	551,68	861,68	1170,78
Rozdiel pretlaku [%]	74,32	89,73	80,54

Obrázok 8. Numerický model bariéry BALBAR a porovnanie maximálnych pretlakov rázovej vlny v meracích bodoch (bod 1. = 1,8 m; bod 2. = 1,0 m; bod 3. = 0,2 m)

Na základe získaných hodnôt bol zaznamenaný pokles maximálneho pretlaku v rozsahu 74–90 %, čo potvrdzuje vysokú účinnosť bariéry BALBAR pri ochrane osôb pred účinkami rázovej vlny. Obrázok 9 zobrazuje interakciu rázových vĺn s prekážkou BALBAR.



Obrázok 9. Šírenie rázových vĺn v interakcii s prekážkou BALBAR

Na Obrázku 9 je znázornené šírenie indukovanej rázovej vlny v interakcii s prekážkou BALBAR v čase 5 ms od iniciácie nálože. Zobrazené tlakové pole poukazuje na odraz rázovej vlny od prekážky a na zmenu jej propagácie v priestore za bariérou. Farebná škála zobrazuje okamžitý tlak v jednotkách kPa.

4 Záver

V príspevku boli analyzované možnosti numerického modelovania indukovaných rázových vĺn s využitím rôznych výpočtových postupov a softvérových nástrojov. Z porovnania jednotlivých prístupov vyplynulo, že 1D model založený na klínovej geometrii vykazoval najlepšiu zhodu s experimentálnymi meraniami, pričom odchýlky maximálnych pretlakov dosahovali jednotky percent. Naopak, kvázi 2D a 2D modely vykazovali vyššie odchýlky, čo poukazuje na výrazný vplyv zvolenej hustoty výpočtovej siete a numerickej formulácie na presnosť výsledkov.

Výsledky potvrdili, že voľba veľkosti výpočtovej siete predstavuje kľúčový kompromis medzi presnosťou a výpočtovou náročnosťou. Pri nedostatočnom rozlíšení siete dochádza k podhodnoteniu alebo nadhodnoteniu vrcholných pretlakov, zatiaľ čo pri príliš jemnej sieti už nedochádza k významnému zlepšeniu výsledkov vzhľadom na exponenciálny nárast výpočtového času. Z tohto dôvodu je nevyhnutné pristupovať k návrhu siete individuálne pre každý typ modelu a účel simulácie.

Po úspešnej validácii základných modelov bolo možné rozšíriť simulácie na komplexnejšie geometrie reprezentujúce reálne scenáre, ako sú zastavané mestské prostredie, interiér viacpodlažnej budovy a ochranné bariéry. Tieto simulácie preukázali schopnosť numerických nástrojov zachytiť nelineárne interakcie rázových vĺn s prekážkami a ich opakované odrazy, ktoré nie je možné spoľahlivo analyzovať pomocou empirických vzťahov.

Osobitná pozornosť bola venovaná analýze účinnosti balistickej bariéry BALBAR, kde numerické modelovanie potvrdilo výrazný útlm maximálneho pretlaku za bariérou v rozsahu približne 74–90 %. Tieto výsledky korešpondujú s experimentálnymi pozorovaniami a poukazujú na vysoký potenciál využitia numerických simulácií pri návrhu ochranných prvkov pre zložky integrovaného záchranného systému.

Z porovnania použitých softvérových nástrojov vyplýva, že prostredie ANSYS AUTODYN je vhodné najmä na analýzu šírenia rázových vĺn v otvorenom priestore a na rýchlu vizualizáciu tlakových polí, zatiaľ čo LS-DYNA poskytuje širšie možnosti pre modelovanie interakcie rázovej vlny so stavebnými konštrukciami a ich deformáciou. Open-source riešenia založené na OpenFOAM predstavujú perspektívnu alternatívu, avšak ich praktické využitie je v súčasnosti limitované vyššou náročnosťou nastavenia a absenciou komplexnej používateľskej podpory.

Do budúcna je vhodné zamerať ďalší výskum na rozšírenie validácie numerických modelov pre výbuchy plynných zmesí, detailnejšie zohľadnenie termodynamických a chemických procesov a na systematické porovnanie komerčných a open-source riešení z hľadiska presnosti, výpočtovej náročnosti a použiteľnosti v inžinierskej praxi.

Poďakovanie

Tento příspěvek vznikl za podpory projektu [ev. č. VK01030175] s názvem "Bezpečnostní koncept vodíkových technologií pro chytrá města a regiony" podpořeného Ministerstvem vnitra České republiky.

Reference

[1] Autodyn Theory manual: Explicit software for Nonlinear dynamics. 4.3. Ansys, 2005

[2] Gan, E. C. J., Remennikov, A., Mohotti, D., Huang, Z., Senarathna, W., & Wijesooriya, K. (2025). Characterising blast environment and structural loading from large-scale unconfined hydrogen explosions. International Journal of Hydrogen Energy, 128, 264–278. https://doi.org/10.1016/j.ijhydene.2025.04.200

[3] Bao, Q., Fang, Q., Yang, S., Zhang, Y., Xiang, H., Chen, L., & Li, Z. (2016). Experimental investigation on the deflagration load under unconfined methane-air explosions. Fuel, 185, 565–576. https://doi.org/10.1016/j.fuel.2016.07.126

[4] Liang, Y., Clouthier, T., & MacCoy, R. (2019). The simulation and analysis of leakage and explosion risk associated with hydrogen refueling stations (International Journal of Hydrogen Energy). https://doi.org/10.1016/j.ijhydene.2019

[5] Li, X., Xu, Y., Li, X., Jin, Z., & Qian, J. (2021). Effect of wind condition on unintended hydrogen release in a hydrogen refueling station. International Journal of Hydrogen Energy, 46(7), 5537–5547. https://doi.org/10.1016/j.ijhydene.2020.11.036

[6] Yang, Z., Chen, Z., Han, X., Chen, G., & Wang, X. (2025). Numerical and experimental studies on the evolution characteristics of high-pressure hydrogen leakage and explosion accidents in hydrogen refueling stations. International Journal of Hydrogen Energy, 142, 580–595. https://doi.org/10.1016/j.ijhydene.2025.04.420

[7] Lee, H., & Seo, J. (2025). Dynamic structural response of a corrugated blast wall under hydrogen blast loads. Applied Sciences, 15(15), 8237. https://doi.org/10.3390/app15158237

[8] Hallquist, J.O. (2013). FSI with the detailed chemistry and their applications in LS-DYNA R/Cese compressible solver (Technical Paper). ANSYS, Inc. https://lsdyna.ansys.com/wp-content/uploads/attachments/fsi-with-the-detailed-chemistry-and-their-applications-in-ls-dyna-r-cese-compressible-solver.pdf

[9] Rokhy, H., & Mirzababaie Mostofi, T. (2023). Tracking the explosion characteristics of the hydrogen-air mixture near a concrete barrier wall using CESE IBM FSI solver in LS-DYNA incorporating the reduced chemical kinetic model. International Journal of Impact Engineering, 172, 104401. https://doi.org/10.1016/j.ijimpeng.2022.104401

[10] Chen, D., Wu, C., & Li, J. (2023). Assessment of modeling methods for predicting load resulting from hydrogen-air detonation. Process Safety and Environmental Protection, 180, 752–765. https://doi.org/10.1016/j.psep.2023.10.051

[11] BAUDIN, Gérard. Review of Jones-Wilkins-Lee equation of state. In EPJ Web of Conferences, 2010, vol. 10, pp. 00021. New Models and Hydrocodes for Shock Wave Processes in Condensed Matter (NMH2010), Paris, France, May 24–28 2010

[12] LI, Jun-bao; LI, Wei-bing; WANG, Xiao-ming. Numerical investigation on characteristics of the shock wave generated by an annular nested charge. Journal of Applied Mechanics and Technical Physics, 2024, vol. 65, No. 3, pp. 401–413. DOI: 10.1134/S0021894424030027

[13] VOJTÁŠ, Sebastián and MYNARZ, Miroslav, 2023. Analýza pôsobenia výbuchového zaťaženia na stavby. Bakalárska práca. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava

[14] VOJTÁŠ, Sebastián and MYNARZ, Miroslav, 2025. Analýza správania sa a šírenia rázových vĺn v interakcii s prekážkami. Diplomová práca. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava

[15] SYBLÍK, Jan. Vliv působení výbuchového zatížení na stavby. Online, Diplomová práce. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, 2022. Dostupné z: http://hdl.handle.net/10084/147218. [cit. 2024-11-23]

Investície do bezpečnosti železničnej infraštruktúry a ochrana života

Drahoslav Vyšný[1,2], Martin Flodr[3,4]

[1] Žilinská Univerzita v Žiline, Fakulta bezpečnostného inžinierstva,
Univerzitná 8215, 010 26 Žilina, drahoslav.vysny@gmail.com

[2] Dopravný úrad,
Letisko M. R. Štefánika, 823 05 Bratislava

[3] Žilinská Univerzita v Žiline, Fakulta bezpečnostného inžinierstva,
Univerzitná 8215, 010 26 Žilina, flodr@qem.sk

[4] QEM, s.r.o.,
J. Janošku 3, 031 01 Liptovský Mikuláš

Abstrakt:

Článok analyzuje ekonomickú primeranosť modernizácie technických bezpečnostných systémov železničných staníc v kontexte ochrany kritickej infraštruktúry a prevencie rizík spojených s mäkkými cieľmi. Cieľom je aplikovať prístup hodnotenia nákladov životného cyklu (Life Cycle Costing – LCC) na modelový koridor Bratislava – Košice a posúdiť finančnú efektívnosť navrhovaných opatrení vo vzťahu k investičnému rámcu správcu infraštruktúry a regulačným požiadavkám na odolnosť kritických subjektov. Štúdia systematicky kvantifikuje investičné a prevádzkové náklady integrovaných bezpečnostných systémov a identifikuje dominantné nákladové faktory ovplyvňujúce dlhodobú udržateľnosť riešenia. V tomto kontexte článok implicitne otvára otázku ekonomického vyjadrenia hodnoty ochrany ľudského života v podmienkach verejnej dopravy a skúma mieru proporcionality medzi finančnými vstupmi a bezpečnostným prínosom. Výsledky poskytujú analytický rámec pre hodnotenie proporcionality bezpečnostných investícií a prispievajú k diskusii o ekonomickej racionalite preventívnych opatrení v železničnej doprave.

Kľúčové slová: ochrana mäkkých cieľov, kritická infraštruktúra, železničné stanice, zlepšenie ochrany.

1 Úvod

Železničná doprava patrí medzi základné prvky dopravného systému štátu a zabezpečuje mobilitu obyvateľstva, prepravu tovarov a kontinuitu hospodárskych procesov. Železničné stanice ako uzlové body infraštruktúry koncentrujú vysoký počet osôb, technologických zariadení a riadiacich systémov, čím sa stávajú citlivými prvkami z hľadiska bezpečnosti a prevádzkovej kontinuity.

Na úrovni Európskej únie je zvyšovanie odolnosti subjektov poskytujúcich základné služby upravené smernicou Európskeho parlamentu a Rady (EÚ) 2022/2557 o odolnosti kritických subjektov (CER), ktorá zdôrazňuje povinnosť identifikovať riziká a prijímať primerané technické, bezpečnostné a organizačné opatrenia [1]. Paralelne dochádza k prepojeniu fyzickej a kybernetickej bezpečnosti, čo reflektuje smernica (EÚ) 2022/2555 (NIS2) o zabezpečení vysokej úrovne kybernetickej bezpečnosti v Únii [2]. V slovenskom právnom prostredí je ochrana kritickej infraštruktúry upravená zákonom č. 367/2024 Z. z. o kritickej infraštruktúre, ktorý stanovuje rámec identifikácie kritických subjektov, hodnotenia rizík a prijímania ochranných opatrení [3].

Výskum v tejto oblasti sa v posledných rokoch zameriava najmä na optimalizáciu bezpečnostných procesov a riadenie zdrojov v železničných staniciach, napríklad prostredníctvom modelov dynamického plánovania bezpečnostných kapacít založených na predikcii toku cestujúcich a metódach hlbokého učenia [4]. Tieto prístupy však primárne riešia operatívnu optimalizáciu zdrojov, zatiaľ čo komplexné finančné hodnotenie modernizácie bezpečnostných systémov zostáva menej rozpracované.

Cieľom článku je navrhnúť metodický rámec finančného hodnotenia modernizácie technických bezpečnostných systémov železničných staníc v kontexte ochrany kritickej infraštruktúry a dlhodobej prevádzkovej udržateľnosti. Štúdia sa zameriava na identifikáciu a kvantifikáciu investičných (CAPEX) a prevádzkových (OPEX) nákladov integrovaných bezpečnostných riešení a na posúdenie ich finančnej efektívnosti počas životného cyklu systému.

2 Materiály a metódy

2.1 Klasifikácia kritickej infraštruktúry

V európskom rámci sa ochrana kritickej infraštruktúry posúva od „ochrany objektov“ k odolnosti kritických subjektov, t. j. k schopnosti predchádzať incidentom, odolávať im, reagovať na ne a obnoviť poskytovanie základných služieb. Problematiku rieši zákon č. 367/2024 Z. z. o kritickej infraštruktúre.

Klasifikácia kritickej infraštruktúry sa v praxi opiera o sektorový prístup (napr. doprava, energia, voda, zdravotníctvo) a o hodnotenie kritickosti na základe dopadových kritérií (dopad na život a zdravie, hospodárske škody, narušenie verejného poriadku, dostupnosť služieb). CER zároveň pracuje s konceptom základných služieb a požaduje, aby opatrenia reflektovali relevantné hrozby (prírodné, technologické, úmyselné ľudské konanie).

2.2 Špecifikácia železničnej dopravy

Železničná doprava sa vyznačuje vysokou mierou prevádzkovej previazanosti (trať – stanica - zabezpečovacie a informačné systémy – energetické napájanie), čo znamená, že incident v uzle môže spôsobiť kaskádové dopady na rozsiahle územie (meškania, odklony, zníženie kapacity siete). Stanice sú zároveň priestormi s vysokou koncentráciou cestujúcich a s kombináciou „verejných“ a „poloverejných/technologických“ zón (nástupištia, podchody, technologické miestnosti, serverovne, dispečing), čo zvyšuje nároky na zónovanie, prístupový režim a monitoring.

Špecifickou črtou je aj tlak na súčasné plnenie dvoch cieľov: bezpečnosť a komfort cestujúcich. V železničnom sektore sa čoraz viac uplatňujú prístupy zamerané na optimalizáciu bezpečnostných kapacít v závislosti od dynamiky pohybu cestujúcich, s cieľom minimalizovať čakacie doby a zároveň zvyšovať efektívnosť využívania dostupných zdrojov.

2.3 Riziká a hrozby

Bezpečnostný profil železničných staníc je typicky multihrozbový (multi-hazard). Kľúčové sú najmä úmyselné hrozby [5]:

1) **Sabotáž a úmyselné narušenie prevádzky:** zásahy do technológií, poškodenie kritických prvkov stanice, narušenie prevádzkových procesov. CER výslovne pracuje so širokým spektrom hrozieb vrátane hybridných a úmyselných aktérov, čo zvyšuje požiadavky na preventívne a detekčné opatrenia.

2) **Vandalizmus a kriminalita:** poškodzovanie majetku (kamerové body, osvetlenie, vstupné prvky), graffiti, krádeže a incidenty vo verejných priestoroch stanice. Praktické aspekty manažmentu bezpečnosti staníc (vrátane vandalizmu) zdôrazňuje aj sektorová metodika UIC pre staničné prostredie.
3) **Terorizmus a násilné útoky:** stanice ako „soft targets“ s vysokou koncentráciou osôb vyžadujú vrstvenú ochranu (detekcia, dohľad, kontrola prístupu do vybraných zón, koordinácia s IZS). UIC upozorňuje, že bezpečnosť staníc nie je iba o protiteroristických opatreniach, ale aj o každodennej ochrane osôb a prevádzky.
4) **Kybernetické riziká:** moderné stanice majú integrované dohľadové, prístupové, požiarne a komunikačné systémy napojené na IT/OT infraštruktúru. NIS2 posilňuje požiadavky na riadenie kybernetických rizík a incident reporting pre subjekty v sektore dopravy (podľa rozsahu a klasifikácie subjektu v národnej transpozícii) [5].

2.4 Integrované bezpečnostné systémy

V praxi sa ochrana železničnej stanice realizuje ako integrovaný bezpečnostný systém (ďalej len „IBS“), ktorý prepája detekciu, verifikáciu, reakciu a dokumentáciu udalostí [6]. Integrácia je dôležitá z hľadiska:

- rýchlosti reakcie,
- minimalizácie falošných poplachov,
- koordinácie zložiek,
- efektívnej prevádzky (OPEX).

Odborné vymedzenie bežných subsystémov používaných aj v staničnom prostredí je uvedené v nasledujúcej časti:

- EZS (elektrický zabezpečovací systém) – systém na detekciu neoprávneného vniknutia a poplachových stavov, typicky navrhovaný podľa požiadaviek radu noriem EN 50131 (stupeň zabezpečenia, triedy prostredia, požiadavky na komponenty a prepojenia).
- TPS (tiesňový poplachový systém) – slúži na úmyselné vyvolanie poplachového stavu v tiesni alebo nebezpečenstve. Môže byť kombinovaný s elektrickým zabezpečovacím systémom – EZS/TPS.
- EPS (elektrická požiarna signalizácia) – systém včasnej detekcie požiaru a vyhlásenia poplachu, viazaný na normový rad EN 54 (komponenty, riadiace jednotky, signalizačné prvky, zásady funkcií systému).
- VSS/VSSS – kamerové dohľadové systémy pre bezpečnostné aplikácie, pri návrhu a prevádzke sa opierajú o požiadavky a odporúčania IEC/EN 62676 (minimálne systémové požiadavky a aplikačné usmernenia pre plánovanie, inštaláciu, údržbu a testovanie).
- SKV (systém kontroly vstupu) – riadenie prístupu do zón podľa identity/autorizačných pravidiel (dvere, turnikety, brány), vrátane prevádzkových požiadaviek na plánovanie, uvedenie do prevádzky a údržbu podľa IEC/EN 60839-11 (aplikačné usmernenia a systémové požiadavky).
- MPPC/PCO (pult centrálnej ochrany) – Monitorovacie a poplachové prijímacie centrum/pult centralizovanej ochrany - centralizované monitorovanie poplachov a udalostí (EZS/TPS/EPS/SKV/VSS), verifikácia udalostí a eskalácia zásahu (SBS, polícia, IZS). Z prevádzkového hľadiska je PCO kľúčové pre nastavenie procesov reakcie, SLA, režimov servisu a pre vyčíslenie OPEX [6, autori].
- PPS (poplachový prenosový systém) je zariadenie a sieť používané na prenos informácií týkajúcich sa stavov jedného alebo viacerých poplachových systémov (EZS/TPS/EPS/SKV/VSS) na MPPC/PCO.

Funkčný systém ochrany majetku možno definovať ako taký bezpečnostný systém, pri ktorom je celkový čas potrebný na realizáciu útoku dlhší než čas detekcie a následnej reakcie systému, pričom do tohto času sa započítava aj doba potrebná na prekonanie mechanických zábranných prvkov a čas pohybu narušiteľa v chránenom priestore [7].

Integračný prínos integrovaného bezpečnostného systému je možné chápať ako „vrstvenú ochranu". EZS/SKV rieši neoprávnený prístup, VSS verifikuje a dokumentuje, EPS rieši požiarne riziká a PCO zabezpečuje kontinuálny dohľad a koordináciu reakcie. Z hľadiska ekonomiky modernizácie je integrácia dôležitá aj preto, že môže znižovať prevádzkové náklady (napr. efektívnejšia obsluha udalostí, centralizácia monitoringu), ale zvyšuje nároky na interoperabilitu, kybernetickú bezpečnosť a životný cyklus technologických komponentov [8]. Integráciu jednotlivých systémov (EZS/TPS/EPS/SKV/VSS) rieši norma EN 50398 Kombinované a integrované poplachové systémy.

3 Súčasný stav a výzvy v oblasti riadenia a plánovania bezpečnostných zdrojov

Súčasný výskum v oblasti riadenia a plánovania bezpečnostných zdrojov v dopravnej infraštruktúre sa primárne sústreďuje na prostredie letísk a systémov metra. V oboch prípadoch ide o dopravné uzly s vysokou koncentráciou osôb a významnými nárokmi na bezpečnostnú kontrolu, pričom výskumné aktivity sú orientované najmä na optimalizáciu alokácie bezpečnostných zdrojov, zvyšovanie priepustnosti kontrolných bodov a minimalizáciu čakacích dôb cestujúcich [9].

V prostredí metra sa výskum zameriava predovšetkým na dynamické riadenie toku cestujúcich počas dopravných špičiek, ktoré sa vyznačujú výraznými časovými a cyklickými výkyvmi. Počet cestujúcich môže v špičke dramaticky narásť, čo vytvára tlak na bezpečnostné kontrolné systémy. Empirické výskumy realizované na staniciach pekinského metra identifikovali viaceré faktory ovplyvňujúce trvanie bezpečnostnej kontroly, pričom medzi najvýznamnejšie patrili typ batožiny a technológia detekčných zariadení. Modelovanie procesov bezpečnostnej kontroly pomocou zovšeobecnených stochastických Petriho sietí (GSPN) umožnilo identifikovať úzke miesta systému a vytvoriť analytický základ pre jeho optimalizáciu [9].

V letiskovom sektore sa výskum plánovania bezpečnostných zdrojov opiera najmä o aplikáciu teórie radenia, simulačných modelov diskrétnych udalostí a metód operačného výskumu. Integrácia simulačných a optimalizačných modulov umožnila redukovať prevádzkové náklady aj mieru nepohodlia cestujúcich. Ďalšie štúdie preukázali, že vhodné nastavenie paralelných a sériových bezpečnostných systémov môže významne zvýšiť efektívnosť počas dopravnej špičky, pričom optimalizácia konfigurácie viedla k skráteniu času obsluhy o viac ako 30 % [9].

Osobitnú pozornosť si zasluhujú prístupy založené na inteligentnom riadení bezpečnostných pruhov a diferenciácii cestujúcich podľa rizikových profilov. Dynamické prideľovanie pruhov podľa typu batožiny alebo využívanie dátových profilov cestujúcich umožňuje efektívnejšiu alokáciu zdrojov a zníženie preťaženia systému [9].

Napriek pokročilým modelovacím a optimalizačným prístupom však aplikačná prax poukazuje na limity implementácie týchto opatrení. Ilustratívnym príkladom je situácia v Pekingskom metre, kde zavedenie rozsiahlych bezpečnostných kontrol porovnateľných s letiskovým režimom viedlo podľa medializovaných informácií k výrazným kolapsovým stavom počas dopravnej špičky [10]. Tento prípad poukazuje na riziko neprimeraného zavádzania bezpečnostných opatrení bez adekvátneho kapacitného plánovania, priestorovej optimalizácie a systémovej integrácie.

Z uvedeného vyplýva, že efektívne plánovanie bezpečnostných zdrojov si vyžaduje interdisciplinárny prístup, ktorý integruje architektonické riešenie priestoru, modelovanie toku cestujúcich, technologické parametre detekčných systémov a behaviorálne faktory. Zároveň možno konštatovať, že hoci sú letiská a metro predmetom rozsiahleho výskumu, porovnateľná hĺbka analýzy v oblasti železničných staníc, najmä vysokorýchlostných terminálov, je zatiaľ limitovaná, čo predstavuje relevantnú výskumnú medzeru.

4 Aktuálny stav železničných staníc na Slovensku a možnosti zlepšenia

Železničná sieť Slovenskej republiky patrí svojím rozsahom medzi významné dopravné systémy v regióne strednej Európy. Správu infraštruktúry zabezpečuje spoločnosť Železnice Slovenskej republiky (ďalej len „ŽSR“), ktorá eviduje približne 3 629 km železničných tratí a takmer 300 železničných staníc. Napriek postupnej modernizácii vybraných úsekov však značná časť staníc dlhodobo vykazuje znaky technickej a morálnej zastaranosti [11].

Odborné analýzy aj mediálne hodnotenia poukazujú na existenciu výrazného investičného dlhu v oblasti železničnej infraštruktúry, ktorý sa prejavuje v stave budov, nástupíšť, podchodov a technologických zariadení. Modernizácia bola v posledných rokoch realizovaná predovšetkým na koridorových tratiach spolufinancovaných z fondov EÚ (napr. modernizácia úsekov Bratislava – Žilina – Košice), pričom komplexná obnova staníc mimo hlavných ťahov postupuje pomalšie [11].

Najväčšou aktuálnou investíciou do železničnej infraštruktúry je modernizácia železničného uzla Žilina, ktorá zahŕňa rekonštrukciu koľajiska, nástupíšť, zabezpečovacích zariadení a prestavbu staničnej budovy. Napriek týmto projektom však väčšina regionálnych staníc nedisponuje modernými informačnými systémami, integrovanými bezpečnostnými technológiami ani adekvátnym architektonickým riešením podporujúcim bezpečnosť a komfort cestujúcich.

Z pohľadu ochrany mäkkých cieľov predstavujú železničné stanice vysoko exponované verejné priestory s otvoreným prístupom a vysokou koncentráciou osôb. Ich súčasný stavebný a technologický stav často nezodpovedá požiadavkám na moderné bezpečnostné riadenie rizík. Koncepčné dokumenty Ministerstva vnútra SR v oblasti ochrany mäkkých cieľov zdôrazňujú potrebu aplikácie preventívnych opatrení, najmä situačnej prevencie kriminality a princípov CPTED (Crime Prevention Through Environmental Design), ktoré majú znižovať zraniteľnosť verejných priestorov prostredníctvom vhodného urbanistického a architektonického riešenia [12].

Pri modernizácii železničných staníc je preto vhodné uplatňovať integrovaný prístup zahŕňajúci:

- rekonštrukciu stavebných objektov s dôrazom na prehľadnosť, osvetlenie a elimináciu slepých zón,
- implementáciu inteligentných monitorovacích systémov (CCTV, analytika obrazu, detekcia pohybu),
- optimalizáciu pohybu cestujúcich prostredníctvom jasného zónovania a riadenia tokov,
- zvýšenie technologickej odolnosti zabezpečovacích a informačných systémov.

Inšpirácia zahraničnými modelmi modernizácie staníc je žiadúca, avšak ich nekritická aplikácia môže viesť k nežiaducim efektom. Príkladom je situácia v Pekingskom metre, kde zavedenie rozsiahlych bezpečnostných kontrol porovnateľných s letiskovým režimom spôsobilo problémy [10].

Preto je potrebné, aby modernizácia slovenských železničných staníc vychádzala z princípu proporcionality medzi bezpečnosťou a prevádzkovou efektívnosťou. Opatrenia musia byť systémovo integrované do riadenia dopravnej infraštruktúry a založené na analýze rizík, nie iba na mechanickom preberaní zahraničných bezpečnostných modelov.

5 Finančné aspekty modernizácie bezpečnostných systémov železničných staníc

Táto časť sa zameriava na ekonomické hodnotenie modernizácie bezpečnostných systémov železničných staníc v kontexte investičného rámca železničnej infraštruktúry v Slovenskej republike. Cieľom je porovnať finančnú náročnosť implementácie integrovaných bezpečnostných technológií na vybraných staniciach hlavného dopravného koridoru Bratislava – Košice s celkovými investíciami do železničnej infraštruktúry a posúdiť ich ekonomickú primeranosť, efektívnosť a potenciálny bezpečnostný prínos pri ochrane verejných priestorov železničných staníc ako typických mäkkých cieľov.

5.1 Porovnanie investícií do modernizácie bezpečnostných systémov staníc v kontexte investičného rámca ŽSR za rok 2024

Podľa Výročnej správy ŽSR za rok 2024 predstavovali celkové investície do železničnej infraštruktúry objem 406 020 000,- EUR [11]. Tieto investície smerovali najmä do modernizácie tratí, zabezpečovacích zariadení, trakčného vedenia a obnovy objektov.

Z ekonomického hľadiska ide o investície s výrazne nižšou kapitálovou náročnosťou v porovnaní s traťovými modernizáciami, avšak s vysokým bezpečnostným multiplikačným efektom. Modernizácia subsystémov ako kamerový dohľad (VSS), kontrola vstupu do technologických zón (SKV), detekcia neoprávneného vstupu (EZS) a požiarna signalizácia (EPS) umožňuje zvýšiť úroveň situačného povedomia, skrátiť reakčný čas zásahu a znížiť prevádzkové riziká. Systém PCO a zásah SBS zároveň predstavujú organizačný prvok, ktorý zabezpečuje okamžitú reakciu na incident [6].

Z právneho hľadiska je možné tieto investície odôvodniť najmä povinnosťou prevádzkovateľa infraštruktúry zabezpečiť ochranu kritickej infraštruktúry a kontinuitu poskytovania základnej služby v zmysle smernice CER, ako aj vnútroštátnej legislatívy o kritickej infraštruktúre. Železničné stanice ako verejne prístupné priestory spĺňajú charakteristiky zraniteľných objektov s vysokou koncentráciou osôb, čo zvyšuje požiadavku na primerané preventívne opatrenia.

Z hľadiska postupného zvyšovania ochrany mäkkých cieľov je možné navrhnúť implementáciu modelu v koridore Bratislava – Košice, ktorý predstavuje hlavný dopravný ťah štátu a zároveň časť siete TEN-T. V prvej fáze by bolo možné:

1. Centralizovať dohľad (PCO) pre celý koridor, čím sa znížia jednotkové prevádzkové náklady.
2. Zjednotiť štandard VSS a EPS na uzlových staniciach (AOD).
3. Zaviesť jednotnú architektúru integrácie systémov (IBS).
4. Uprednostniť technologické riešenia pred čisto personálnym zabezpečením, čím sa z dlhodobého hľadiska stabilizuje OPEX.
5. Realizovať pilotný projekt v najväčších uzloch (Bratislava, Žilina, Košice) a následne ho replikovať na regionálne stanice.

Takýto prístup umožňuje relatívne nízkym podielom z celkového investičného rámca ŽSR (v porovnaní s traťovými stavbami) dosiahnuť výrazné zvýšenie úrovne fyzickej ochrany verejných priestorov, pričom je v súlade s deklarovanými cieľmi revitalizácie staníc do roku 2030.

5.2 Ekonomická efektívnosť ochrany mäkkých cieľov v porovnaní s traťovými investíciami

Investičný rámec ŽSR v roku 2024 dosiahol 406 020 000,- EUR [10], pričom dominantná časť prostriedkov smerovala do modernizácie tratí, zabezpečovacích zariadení, trakčného vedenia a obnovy infraštruktúrnych objektov.

V rámci tejto štúdie bol navrhnutý a aplikovaný modelový modernizačný plán zavedenia bezpečnostných systémov na vybrané železničné stanice situované na hlavnom dopravnom koridore Bratislava – Košice. Tento koridor predstavuje kľúčovú os železničnej siete Slovenskej republiky, je súčasťou medzinárodného dopravného systému a siete TEN-T a zároveň koncentruje najvyšší objem osobnej dopravy v rámci štátu. Výber koridoru preto slúži ako reprezentatívny modelový prípad na overenie ekonomických a bezpečnostných aspektov navrhovanej modernizácie. Do tejto štúdie boli pre účely výskumu zahrnuté železničné stanice zaradené do kategórií AOD a BOD podľa oficiálnej kategorizácie dopravných bodov pre osobnú dopravu v systéme ŽSR [13].

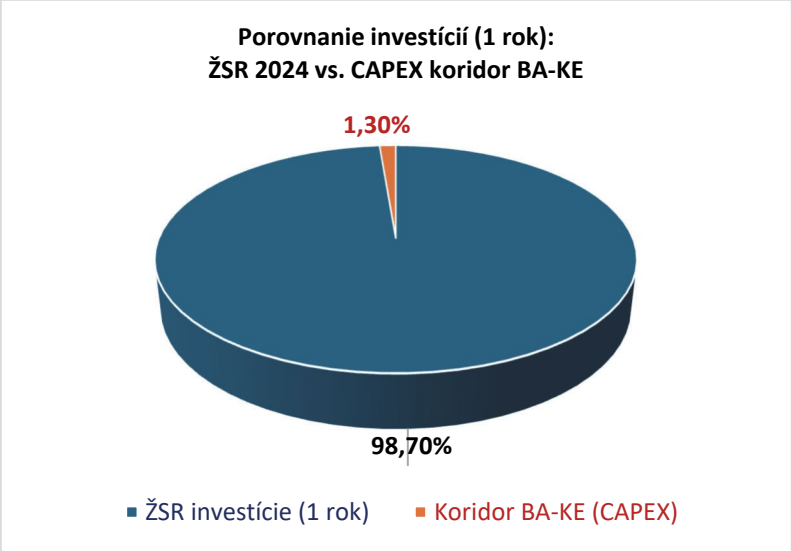
Tabuľka 1. Capex a Opex vybraných železničných staníc, cenová ponuka od spoločnosti QEM, s.r.o., J. Janošku 900/3, 031 01 Liptovský Mikuláš, Slovensko, Autori [15]

Stanica	**Kategória**	**Hodnota**	**CAPEX**	**OPEX**
Bratislava	BOD	2	454 920,- €	78 000,- €
Bratislava-Vinohrady	BOD	1	227 460,- €	39 000,- €
Trnava	AOD	2	454 920,- €	78 000,- €
Trenčín	BOD	1	227 460,- €	39 000,- €
Púchov	AOD	2	454 920,- €	78 000,- €
Považská Bystrica	BOD	1	227 460,- €	39 000,- €
Žilina	AOD	2	454 920,- €	78 000,- €
Vrútky	AOD	2	454 920,- €	78 000,- €
Kraľovany	BOD	1	227 460,- €	39 000,- €
Ružomberok	BOD	1	227 460,- €	39 000,- €
Liptovský Mikuláš	BOD	1	227 460,- €	39 000,- €
Štrba	BOD	1	227 460,- €	39 000,- €
Poprad-Tatry	AOD	2	454 920,- €	78 000,- €
Spišská Nová Ves	BOD	1	227 460,- €	39 000,- €
Margecany	BOD	1	227 460,- €	39 000,- €
Kysak	BOD	1	227 460,- €	39 000,- €
Košice	AOD	2	454 920,- €	78 000,- €
SPOLU			**5 459 040,- €**	**936 000,- €**

Kategorizácia dopravných bodov pre osobnú dopravu na sieti ŽSR je založená na bodovom hodnotení vybraných ukazovateľov, ktoré odrážajú technickú, dopravnú a prevádzkovú úroveň stanice [13]. Medzi hodnotené kritériá patrí najmä kategória trate, počet nástupiskových hrán, spôsob prístupu k vlakom (úrovňový alebo mimoúrovňový), rozsah krytia nástupíšť, existencia parkovísk a stojísk pre bicykle, vybavenosť budov (vestibuly, čakárne), informačné zariadenia, technologické operácie, vybavenie pre imobilných cestujúcich a technické zabezpečenie stanice. Každému ukazovateľu je priradený bodový rozsah, pričom maximálny možný počet bodov je 30. Na základe súčtu bodov sa dopravné body zaraďujú do troch kategórií: AOD (26–30 bodov), BOD (13–25 bodov) a COD (0–12 bodov). Kategória AOD teda predstavuje stanice s najvyššou technickou, infraštruktúrnou a prevádzkovou úrovňou, typicky umiestnené na hlavných tratiach s vysokým

dopravným významom a rozsiahlym vybavením pre cestujúcich. Kategória BOD zahŕňa stanice so strednou úrovňou vybavenosti a dopravného významu, ktoré síce spĺňajú základné štandardy osobnej dopravy, avšak nedosahujú komplexnosť a technickú úroveň staníc kategórie AOD. Predmetná kategorizácia vytvára objektívny rámec pre hodnotenie významu staníc v rámci siete ŽSR a zároveň predstavuje vhodný základ pre ekonomické modelovanie investičnej náročnosti ich modernizácie. Takto zvolený súbor následne umožňuje modelovať nákladovosť modernizácie v rôznych prevádzkových podmienkach a vytvoriť reprezentatívny ekonomický obraz implementácie bezpečnostných opatrení na celom koridore [13].

Výber staníc reflektuje ich dopravnú funkciu, intenzitu osobnej dopravy a strategický význam v rámci národnej železničnej infraštruktúry. Z hľadiska ochrany mäkkých cieľov ide o priestory s vysokou koncentráciou cestujúcich a otvoreným režimom prístupu, čo zvyšuje požiadavky na implementáciu integrovaných bezpečnostných systémov.

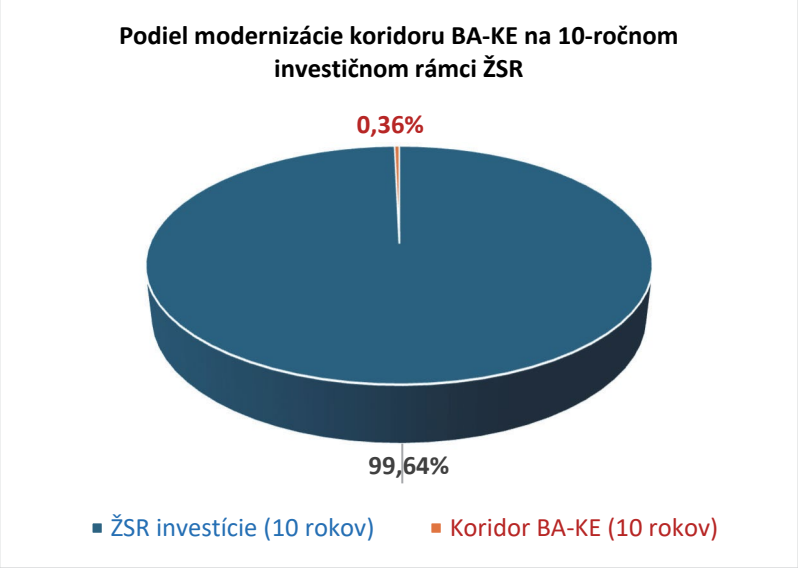


Obrázok 1. Porovnanie investícií ŽSR s investičnými nákladmi bezpečnostných systémov, Autor

V tomto kontexte predstavuje modernizácia bezpečnostných systémov staníc v koridore Bratislava – Košice investíciu vo výške približne 5 459 040,- EUR, čo zodpovedá 1,3 % ročných investícií.

Investičný plán bol modelovaný v desaťročnom horizonte z dôvodu zohľadnenia typickej technickej a morálnej životnosti bezpečnostných technológií používaných v železničnom prostredí. Elektronické zabezpečovacie systémy, kamerové dohľadové systémy, systémy kontroly vstupu aj riadiace jednotky požiarnej signalizácie sa v praxi navrhujú s predpokladanou prevádzkovou životnosťou približne 8 až 12 rokov, pričom po uplynutí tohto obdobia je spravidla potrebná ich modernizácia alebo technologická obnova.

Desaťročný horizont preto predstavuje primerané časové obdobie na hodnotenie celkových nákladov životného cyklu systému, keďže umožňuje zachytiť nielen počiatočné investičné výdavky, ale aj kumulatívne prevádzkové náklady a potrebu budúcej obnovy. Takto zvolený rámec poskytuje realistický pohľad na ekonomickú udržateľnosť navrhovaných opatrení a zároveň reflektuje štandardné plánovacie obdobia v oblasti verejných infraštruktúrnych investícií.



Obrázok 2. Porovnanie investícií ŽSR s nákladmi na prevádzku bezpečnostných systémov, Autor

Obrázok 2 znázorňuje porovnanie kumulatívnych investičných výdavkov ŽSR v desaťročnom horizonte pri zachovaní investičnej úrovne roku 2024 s celkovými nákladmi modernizácie bezpečnostných systémov železničných staníc na koridore Bratislava – Košice (CAPEX + 10 x OPEX).

Pri zachovaní ročného investičného objemu 406 002 000,- EUR dosahujú desaťročné investície ŽSR približne 4,06 mld. EUR. Naopak, celková nákladovosť modernizácie bezpečnostných systémov v rovnakom období predstavuje 14 819 040,- EUR, čo zodpovedá približne 0,36 % desaťročného investičného rámca.

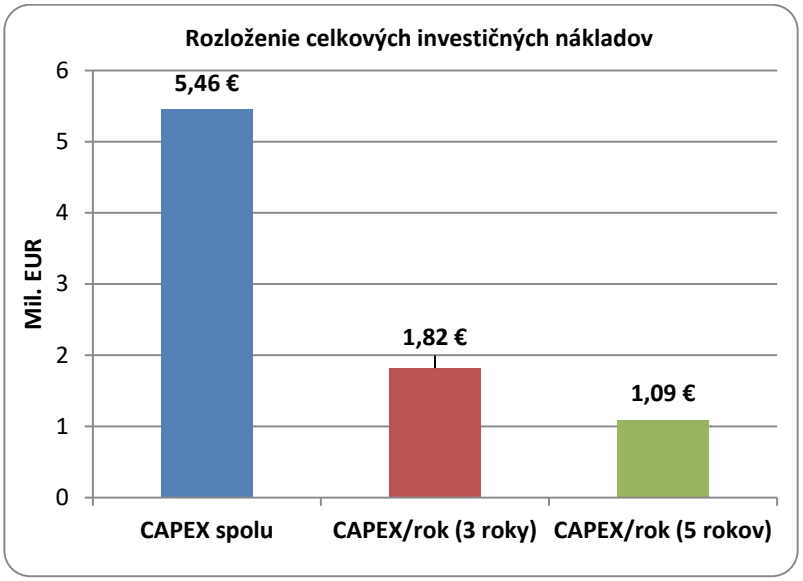
Z grafického porovnania vyplýva výrazná disproporcia medzi objemom systémových investícií do železničnej infraštruktúry a relatívne nízkou finančnou náročnosťou ochrany mäkkých cieľov. Výsledok poukazuje na skutočnosť, že zvýšenie úrovne bezpečnosti staníc v hlavnom dopravnom koridore je možné realizovať bez zásadného dopadu na celkovú investičnú bilanciu podniku.

Z hľadiska strategického riadenia ide o investíciu s nízkou relatívnou finančnou záťažou a potenciálne vysokým bezpečnostným a spoločenským prínosom.

Z ekonomického hľadiska ide o investíciu s vysokým pomerom bezpečnostného prínosu k objemu kapitálu. Na rozdiel od traťových modernizácií, ktorých primárnym cieľom je zvýšenie traťovej rýchlosti, kapacity alebo interoperability, investície do systémov PCO, EZS/TPS, EPS, VSS a SKV/MZP priamo zvyšujú úroveň ochrany osôb a majetku v exponovaných verejných priestoroch. Železničné stanice ako mäkké ciele sú charakterizované vysokou koncentráciou osôb a otvoreným režimom prístupu, čo zvyšuje ich zraniteľnosť voči bezpečnostným incidentom.

Relatívne nízky podiel investícií (≈1,3 %) naznačuje, že zvýšenie ochrany mäkkých cieľov nevyžaduje zásadnú reštrukturalizáciu investičného plánu, ale skôr jeho doplnenie o systematický bezpečnostný komponent. Vzhľadom na strategické ciele ŽSR do roku 2030, ktoré zahŕňajú revitalizáciu staníc a modernizáciu zabezpečovacích zariadení, je možné konštatovať, že implementácia integrovaných bezpečnostných systémov na hlavnom koridore je finančne realizovateľná bez významného narušenia investičnej rovnováhy podniku.

Z hľadiska efektívnosti verejných výdavkov tak ide o opatrenie s nízkou relatívnou finančnou náročnosťou a potenciálne vysokým spoločenským prínosom, najmä v oblasti prevencie incidentov, skrátenia reakčného času zásahu a zvýšenia subjektívneho pocitu bezpečia cestujúcich.



Obrázok 3. Rozloženie celkových investičných nákladov, Autor

Obrázok 3 prezentuje model rozloženia celkových investičných nákladov (CAPEX = 5 459 040,- EUR) na modernizáciu bezpečnostných systémov železničných staníc koridoru Bratislava – Košice do časového horizontu 3 a 5 rokov. Cieľom analýzy je posúdiť finančnú realizovateľnosť projektu pri rôznych implementačných scenároch.

V prípade 3-ročnej realizácie predstavuje ročná investičná záťaž približne 1 819 680,- EUR, zatiaľ čo pri 5-ročnom horizonte ide o 1 091 808,- EUR ročne. V porovnaní s ročným investičným objemom ŽSR za rok 2024 (406 020 000,- EUR) ide o podiel približne 0,45 % pri trojročnom a 0,27 % pri päťročnom scenári.

Z ekonomického hľadiska obe alternatívy potvrdzujú, že modernizácia bezpečnostných systémov je realizovateľná bez zásadného narušenia existujúceho investičného rámca. Rozdiel medzi scenármi spočíva najmä v dynamike implementácie a rýchlosti dosiahnutia plnej úrovne ochrany. Kratší horizont umožňuje rýchlejšie zvýšenie bezpečnostnej úrovne koridoru, avšak s vyššou krátkodobou finančnou koncentráciou. Naopak, päťročná etapizácia predstavuje konzervatívnejší model s nižšou ročnou záťažou, no pomalším nábehom bezpečnostného efektu.

Z pohľadu riadenia verejných investícií ide o flexibilný projekt, ktorého časové rozloženie je možné prispôsobiť aktuálnym rozpočtovým možnostiam bez zásadného vplyvu na jeho celkovú ekonomickú efektívnosť.

5.3 Bezpečnosť ako zanedbateľná položka rozpočtu, no kľúčová hodnota systému

Analýza ukázala, že komplexná modernizácia bezpečnostných systémov staníc na hlavnom železničnom koridore Bratislava – Košice predstavuje investíciu vo výške 5 459 040,- EUR a ročné prevádzkové náklady 936 000,- EUR. V prepočte na celkový počet cestujúcich v Slovenskej republike (73 345 000 osôb ročne) znamená zvýšenie úrovne ochrany približne 1 cent na cestujúceho ročne [14].

- Ročný náklad na jedného cestujúceho:

$$x = \frac{\text{OPEX}}{\text{počet cestujúcich za rok}} = \frac{936\,000}{73\,345\,000} \approx 0{,}0127616061\ EUR\ (\approx 1{,}3\ centa)$$

- 10 ročný náklad na jedného cestujúceho (CAPEX + 10 · OPEX):

$$\text{ϰ} = \frac{\text{CAPEX} + 10 \cdot \text{OPEX}}{\text{počet cestujúcich za rok} \cdot 10} = \frac{5\,459\,040 + 10 \cdot 936\,000}{73\,345\,000 \cdot 10} \approx 0{,}0202045675\ EUR\ (\approx 2\ centy)$$

Na vyjadrenie ekonomickej primeranosti modernizácie bol vypočítaný ukazovateľ nákladov v prepočte na jedného cestujúceho. Ročný prevádzkový náklad (OPEX) vo výške 936 000 EUR pri ročnom počte 73 345 000 cestujúcich predstavuje približne 0,0128 EUR na osobu, teda približne 1,3 centa ročne. Tento údaj znamená, že ochrana ľudského života a zvýšenie bezpečnostnej úrovne železničných staníc je z pohľadu jednotlivca realizovaná za sumu približne jeden cent ročne.

Pri zohľadnení desaťročného horizontu vrátane investičných nákladov (CAPEX) a kumulatívnych prevádzkových výdavkov dosahuje celkový náklad približne 0,0202 EUR na cestujúceho, teda približne dva centy na osobu za celé hodnotené obdobie. Aj po započítaní investičnej fázy tak zostáva jednotková cena ochrany ľudského života v železničnej doprave vyjadrená v centových hodnotách. Z ekonomického hľadiska ide o mimoriadne nízku individuálnu záťaž, ktorá je v zjavnom nepomere k potenciálnym spoločenským, reputačným a finančným dôsledkom závažného bezpečnostného incidentu. Výsledky preto podporujú záver o vysokej nákladovej efektívnosti preventívnych opatrení v oblasti ochrany mäkkých cieľov v železničnej infraštruktúre.

Otázka ochrany ľudského života a zdravia má však nielen ekonomický, ale aj právny a spoločenský rozmer. Prevádzkovateľ kritickej infraštruktúry je povinný prijímať primerané opatrenia na minimalizáciu rizík a zabezpečenie kontinuity základnej služby. Skutočnosť, že v minulosti nedošlo na území Slovenskej republiky k významnému útoku na železničnú infraštruktúru, nepredstavuje garanciu budúcej bezpečnosti. Riziko nízkej pravdepodobnosti, no vysokého dopadu, je typickým znakom mäkkých cieľov. Prevencia preto nemôže byť založená výlučne na retrospektívnom hodnotení incidentov.

6 Záver

Cieľom článku bolo navrhnúť metodický rámec finančného hodnotenia modernizácie bezpečnostných systémov železničných staníc v kontexte požiadaviek na ochranu kritickej infraštruktúry a dlhodobú prevádzkovú udržateľnosť. Analýza potvrdila, že investície do ochrany tzv. mäkkých cieľov v železničnej doprave predstavujú z makroekonomického hľadiska relatívne nízku finančnú záťaž, pričom ich bezpečnostný a spoločenský význam je výrazný.

Celkové investičné náklady modernizácie vybraného koridoru Bratislava – Košice dosahujú 5 459 040,- EUR a ročné prevádzkové náklady 936 000,- EUR. V desaťročnom horizonte predstavuje celková nákladovosť systému približne 14 819 040,- mil. EUR, čo zodpovedá približne 0,36 % desaťročného investičného rámca ŽSR pri zachovaní úrovne investícií roku 2024. V prepočte na jedného cestujúceho ide o približne jeden cent ročne, čo predstavuje zanedbateľnú jednotkovú hodnotu v porovnaní s potenciálnymi dôsledkami bezpečnostného incidentu.

Analýza štruktúry nákladov zároveň ukázala, že dominantnú časť nákladov životného cyklu netvorí samotná investícia (CAPEX), ale dlhodobé prevádzkové náklady (OPEX). Z tohto pohľadu je kľúčové, aby rozhodovanie o modernizácii nebolo orientované výlučne na minimalizáciu vstupnej investície, ale na optimalizáciu celkových nákladov životného cyklu systému. Integrovaný prístup k bezpečnostným technológiám (EZS, TPS, EPS, VSS, SKV, MPPC/PCO) umožňuje dosiahnuť vyššiu úroveň detekcie, verifikácie a reakcie pri relatívne nízkom podiele na celkových investíciách do železničnej infraštruktúry.

Z legislatívneho hľadiska modernizácia prispieva k napĺňaniu požiadaviek smernice CER a zákona o kritickej infraštruktúre, ktoré kladú dôraz na identifikáciu rizík, prijímanie primeraných opatrení a zabezpečenie kontinuity základných služieb. Skutočnosť, že Slovenská republika doteraz nečelila rozsiahlemu útoku na železničnú infraštruktúru, nemôže byť interpretovaná ako dôkaz dostatočnej odolnosti systému. Prevencia v oblasti kritickej infraštruktúry musí byť založená na princípe predvídania rizík a proporcionality opatrení, nie na retrospektívnom hodnotení incidentov.

Výsledky potvrdzujú, že zvýšenie úrovne ochrany železničných staníc je ekonomicky realizovateľné bez zásadného narušenia investičnej rovnováhy podniku. Investícia vo výške približne jedného centa na cestujúceho ročne predstavuje minimálnu finančnú záťaž, avšak významný príspevok k ochrane života, zdravia a dôvery verejnosti v železničnú dopravu. V tomto kontexte možno konštatovať, že otázka modernizácie bezpečnostných systémov nie je primárne otázkou finančnej únosnosti, ale otázkou strategického rozhodnutia o úrovni ochrany kritickej infraštruktúry v podmienkach meniaceho sa bezpečnostného prostredia.

Ďalší výskum by sa mal zamerať na aplikáciu modelov nákladov životného cyklu zohľadňujúcich časovú hodnotu peňazí (LCC), na analýzu vplyvu vývoja prevádzkových nákladov a na porovnanie alternatívnych technologických scenárov s cieľom presnejšie kvantifikovať ekonomickú efektívnosť modernizačných opatrení.

Referencie

[1] EURÓPSKY PARLAMENT A RADA EÚ. Smernica (EÚ) 2022/2557 o odolnosti kritických subjektov (CER). Úradný vestník Európskej únie, L 333, 27.12.2022

[2] EURÓPSKY PARLAMENT A RADA EÚ. Smernica (EÚ) 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v celej Únii (NIS2). Úradný vestník Európskej únie, L 333, 27.12.2022

[3] Zákon č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov

[4] LI, M.; SUN, Y.; XU, C.; DU, C.; SHAO, W. Research on the Model of High-Speed Railway Station Security Resource Scheduling Based on Dynamic Passenger Flow Prediction. Applied Sciences. 2024, roč. 14, č. 11634

[5] INTERNATIONAL UNION OF RAILWAYS (UIC). Station Security for Station Business – Handbook [online]. Dostupné na: https://uic.org/IMG/pdf/station_security_for_station_business_handbook_2.pdf [cit. 2026-02-27]

[6] LOVEČEK, T.; REITŠPÍS, J. Projektovanie a hodnotenie systémov ochrany objektov. Žilina: EDIS – vydavateľstvo ŽU, 2011. 280 s. ISBN 978-80-554-0457-8

[7] KAMPOVÁ, K.; LOVEČEK, T. Modelovanie systémov ochrany objektov a ich optimalizácia. Žilina: EDIS – vydavateľstvo ŽU, 2021. 280 s. ISBN 978-80-554-1753-0

[8] LOVEČEK, T.; VEĽAS, A.; ĎUROVEC, M. Bezpečnostné systémy: poplachové systémy. Žilina: EDIS – vydavateľstvo ŽU, 2015. 230 s. ISBN 978-80-554-1144-6

[9] LI, M.; SUN, Y.; XU, C.; DU, C.; SHAO, W. Research on the Model of High-Speed Railway Station Security Resource Scheduling Based on Dynamic Passenger Flow Prediction [online]. Dostupné na: https://www.researchgate.net/publication/386997103 [cit. 2026-02-27]

[10] ŽELEZNICE SLOVENSKEJ REPUBLIKY. Výročná správa ŽSR 2024 [online]. Dostupné na: https://www.zsr.sk/files/o-nas/vyrocne-spravy/vyrocna-sprava-zsr-2024.pdf [cit. 2026-02-27]

[11] CPTED INTERNATIONAL. Crime Prevention Through Environmental Design (CPTED) [online]. Dostupné na: https://www.cpted.net/ [cit. 2026-02-27]

[12] ŽELEZNICE SLOVENSKEJ REPUBLIKY. Zoznam dopravných bodov pre osobnú dopravu – Príloha 2.3.3.A Podmienok používania železničnej infraštruktúry [online]. Dostupné na: https://www.zsr.sk/files/dopravcovia/zeleznicna-infrastruktura/podmienky-pouzivania-zel-infrastruktury/ppzs-2026/priloha-2_3_3_a-zoznam_db_pre-od-11-2025.pdf [cit. 2026-02-27]

[13] ŠTATISTICKÝ ÚRAD SLOVENSKEJ REPUBLIKY. Datacube – železničná osobná doprava [online]. Dostupné na: https://datacube.statistics.sk/ [cit. 2026-02-27]

[14] QEM, s.r.o. Technologické riešenia bezpečnostných systémov [online]. Dostupné na: https://www.qem.sk/ [cit. 2026-02-27]

Manažment rizík technickej kompatibility pri implementácii technologických zmien v priemyselnom procese

Alžbeta Žerebáková[1]

[1] Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva,
1. mája 32, 010 26 Žilina, alzbeta.zerebakova@uniza.sk

Abstrakt:

Implementácia technologických zmien vo výrobných systémoch je spravidla motivovaná snahou o zvýšenie efektívnosti a výkonnosti procesov. Súčasne však môže viesť k vzniku nových operačných rizík, najmä v prípadoch, keď dochádza k technickej nekompatibilite medzi nadväzujúcimi výrobnými uzlami. Príspevok sa zameriava na posudzovanie rizika technickej kompatibility v konkrétnom priemyselnom procese spracovania papiera, kde rozdielne technické parametre jadier medzi výrobným uzlom a tlačovým zariadením podmieňovali existenciu medzistupňovej adaptácie materiálu. Táto adaptácia predstavovala dodatočné mechanické rozhranie zvyšujúce procesnú komplexnosť a citlivosť systému na dynamické odchýlky. Posudzovanie rizika bolo realizované v súlade s princípmi normy ISO 31000 s využitím analytického rámca FMEA a semi-kvalitatívnej rizikovej matice založenej na kombinácii pravdepodobnosti výskytu a závažnosti dôsledku. Analýza identifikovala mechanické rozhranie adaptácie jadra ako dominantný zdroj vysokého rizika z hľadiska kontinuity a stability výrobného procesu. Následná implementácia technického opatrenia založeného na eliminácii zdroja poruchového stavu viedla k redukcii počtu mechanických rozhraní a k zmene rizikového profilu procesu. Výsledky potvrdzujú význam systematického hodnotenia rizík technickej kompatibility ako nástroja zvyšovania robustnosti, spoľahlivosti a dlhodobej stability priemyselných výrobných systémov.

Kľúčové slová: manažment rizík, priemyselné procesy, implementácia zmien, technická kompatibilita.

1 Úvod

Technologické zmeny vo výrobných systémoch predstavujú významný nástroj zvyšovania efektívnosti a výkonnosti podnikov. Súčasne však môžu generovať nové operačné riziká, najmä v prípade technickej nekompatibility medzi jednotlivými výrobnými uzlami. Zvýšená procesná komplexnosť a rastúci počet technologických rozhraní sú v literatúre identifikované ako faktory negatívne ovplyvňujúce spoľahlivosť a prevádzkovú výkonnosť výrobných systémov [1]. Podobne aj výskumy v oblasti hodnotenia operačného rizika vo flexibilných výrobných sieťach poukazujú na citlivosť systémov na kvalitu technologických interakcií medzi jednotlivými prvkami [2]. Identifikácia a hodnotenie takýchto rizík si vyžaduje systematický metodický prístup. V praxi sa často využíva analýza FMEA a jej moderné dátovo orientované modifikácie, ktoré umožňujú štruktúrovanú identifikáciu poruchových stavov a ich následkov v technických systémoch [3, 4]. Zároveň sa zdôrazňuje potreba transparentne definovaných kritérií hodnotenia rizika a jeho integrácie do širšieho rámca podnikového riadenia rizík. Cieľom príspevku je identifikovať a systematicky vyhodnotiť riziko technickej kompatibility v konkrétnom priemyselnom procese a posúdiť vplyv implementovaného technického opatrenia na zmenu rizikového profilu výrobného systému.

2 Analýza výrobného procesu a identifikácia problému

Analýza výrobného procesu bola iniciovaná na základe opakujúcich sa prevádzkových odchýlok v nadväznosti medzi papierenským výrobným uzlom PM19 a tlačovým zariadením CRYSTAL. Výstup z PM19 bol navíjaný na jadro s vnútorným priemerom 100 mm, zatiaľ čo tlačové zariadenie CRYSTAL je konštrukčne prispôsobené pre upínanie rolí s jadrom 70 mm. Tento rozdiel v technických parametroch vytváral nesúlad medzi výrobnými uzlami a znemožňoval priamy technologický prechod materiálu. Pre zabezpečenie kompatibility bolo do procesu zaradené medzistupňové prevíjanie materiálu na jadro s požadovaným priemerom pred vstupom do tlačového zariadenia a následne ďalšia prevíjacia operácia po realizácii tlače, aby bol výstup prispôsobený požiadavkám ďalšej manipulácie. Proces tak obsahoval dve operácie, ktoré nevytvárali pridanú hodnotu z hľadiska kvality produktu, ale slúžili výlučne na kompenzáciu technickej nekompatibility.

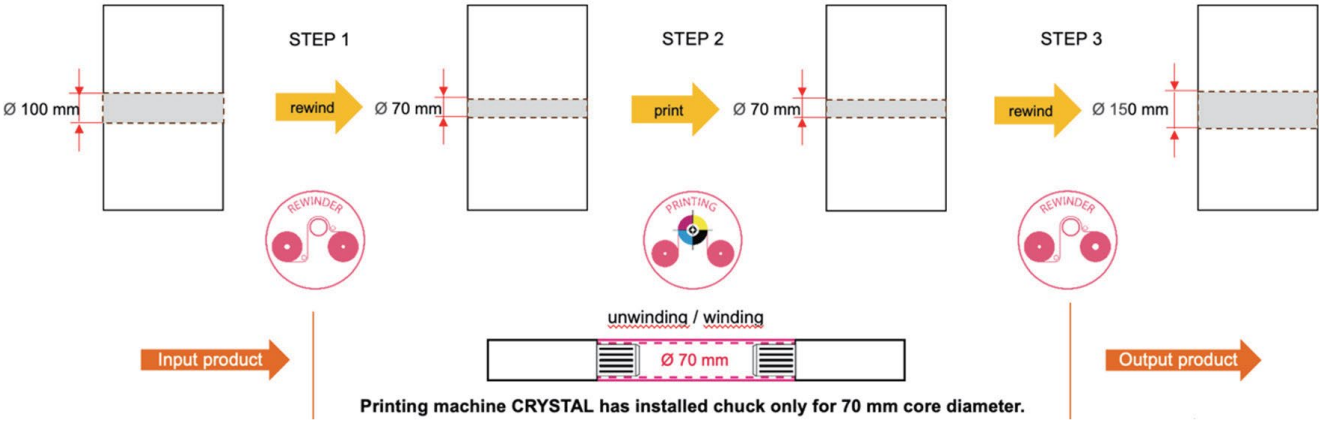
Identifikácia problému prebehla prostredníctvom procesného mapovania, sledovania toku materiálu a analýzy technologických rozhraní medzi zariadeniami. Kritické bolo najmä mechanické rozhranie zabezpečujúce adaptáciu rozdielnych priemerov jadier prostredníctvom redukčného prvku. Počas skúšobnej prevádzky boli zaznamenané nasledovné prejavy nestability:

- preklz redukcie voči hnaciemu hriadeľu navíjacej jednotky,
- kolísanie ťahového napätia pásu,
- nerovnomerné navíjanie materiálu,
- zvýšená potreba zásahov obsluhy,
- aktivácia bezpečnostného zastavenia zariadenia pri prekročení tolerancií.

Tlačové zariadenie CRYSTAL pracuje s presne definovanými parametrami synchronizácie navíjacej a odvíjacej jednotky. Stabilita jadra a osové zarovnanie adaptéra sú preto kritickými technickými parametrami ovplyvňujúcimi dynamiku procesu. Akékoľvek mechanické odchýlky sa priamo premietajú do stability navíjania a kontinuity výroby. Z pohľadu systémovej spoľahlivosti predstavujú technologické rozhrania medzi nekompatibilnými prvkami systému významné zdroje operačného rizika [2]. Rastúca procesná komplexnosť a vyšší počet mechanických prechodov medzi zariadeniami zvyšujú pravdepodobnosť poruchových stavov a znižujú robustnosť výrobného systému [1]. Identifikovaná potreba dvojitého prevíjania tak nepredstavovala len otázku organizačnej efektívnosti, ale predovšetkým faktor zvyšujúci citlivosť procesu na mechanické odchýlky.

Na základe uvedených zistení bol problém formulovaný ako riziko technickej kompatibility medzi výrobnými uzlami PM19 a CRYSTAL, ktoré sa prejavovalo:

- zvýšením počtu mechanických rozhraní v procese,
- zvýšenou citlivosťou systému na geometrické a dynamické odchýlky,
- nárastom pravdepodobnosti poruchových stavov,
- potenciálnym narušením kontinuity výroby.



Obrázok 1. Schéma pôvodného výrobného procesu s medzistupňovým prevíjaním materiálu [autor]

3 Regulačný a normatívny rámec riadenia rizík technologických procesov

Riadenie rizík technologických procesov v priemyselných podnikoch je determinované nielen internými postupmi organizácií, ale aj širším regulačným a normatívnym rámcom upravujúcim návrh, integráciu a prevádzku technických zariadení. Implementácia technologických zmien vo výrobných systémoch môže vytvárať nové technické rozhrania medzi jednotlivými výrobnými uzlami, ktoré predstavujú potenciálny zdroj prevádzkových odchýlok alebo poruchových stavov. Z tohto dôvodu je systematické posudzovanie rizík technologických procesov súčasťou širšieho regulačného rámca zabezpečujúceho bezpečnú a spoľahlivú prevádzku priemyselných zariadení.

Na úrovni Európskej únie je problematika návrhu a integrácie technologických zariadení upravená najmä Smernicou Európskeho parlamentu a Rady 2006/42/ES z 17. mája 2006 o strojových zariadeniach a o zmene smernice 95/16/ES (prepracované znenie), ktorá stanovuje základné požiadavky na bezpečnosť a ochranu zdravia pri navrhovaní, konštrukcii a uvádzaní strojových zariadení na trh [5]. Jednou z jej kľúčových požiadaviek je systematické posudzovanie rizík počas celého životného cyklu zariadenia, pričom osobitná pozornosť sa venuje identifikácii rizík vyplývajúcich z integrácie jednotlivých technologických komponentov do komplexných výrobných systémov. Smernica zároveň zdôrazňuje potrebu zohľadniť interakciu jednotlivých komponentov technologických systémov a identifikovať riziká vyplývajúce z ich vzájomnej integrácie.

V kontexte technologického rozvoja a rastúcej úrovne automatizácie priemyselných procesov bol regulačný rámec doplnený novým právnym aktom Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1230 z 14. júna 2023 o strojových zariadeniach, ktoré reflektuje aktuálny vývoj v oblasti digitalizácie, automatizácie a inteligentných výrobných systémov [6]. Cieľom tohto nariadenia je modernizovať existujúci regulačný rámec a posilniť požiadavky na bezpečnosť a spoľahlivosť technologických zariadení, pričom osobitný dôraz sa kladie na systematické posudzovanie rizík pri integrácii strojových zariadení do komplexných technologických celkov.

Významnú úlohu pri posudzovaní rizík technologických zariadení zohrávajú aj technické normy a medzinárodné štandardy poskytujúce metodický rámec pre identifikáciu nebezpečenstiev a hodnotenie rizík. Norma ISO 12100:2010 Safety of machinery – General principles for design – Risk assessment and risk reduction definuje základné princípy identifikácie nebezpečenstiev a systematického hodnotenia rizík pri návrhu a integrácii strojových zariadení. Norma zdôrazňuje potrebu analyzovať potenciálne zdroje rizika vyplývajúce nielen z konštrukčných vlastností zariadenia, ale aj z jeho interakcie s ďalšími technologickými prvkami výrobného procesu [7].

V širšom kontexte riadenia rizík v organizáciách poskytuje metodický rámec norma ISO 31000:2018 Risk management – Guidelines, ktorá zdôrazňuje potrebu systematického prístupu k identifikácii, analýze a hodnoteniu rizík v rôznych oblastiach činnosti podniku [8]. Implementácia princípov tejto normy umožňuje organizáciám integrovať proces riadenia rizík do rozhodovacích procesov súvisiacich s implementáciou technologických zmien a optimalizáciou výrobných procesov.

Uvedené regulačné a normatívne požiadavky sa v praxi premietajú do potreby systematicky analyzovať technologické rozhrania medzi jednotlivými výrobnými uzlami výrobného systému. V analyzovanom prípade technologického prepojenia výrobného uzla PM19 a tlačového zariadenia CRYSTAL bola identifikovaná technická nekompatibilita jadier ako faktor zvyšujúci citlivosť výrobného systému na dynamické odchýlky. Systematické hodnotenie takýchto rizík umožňuje identifikovať kritické miesta technologického procesu a prijať technické opatrenia smerujúce k zvýšeniu stability a spoľahlivosti výroby.

4 Metodika posudzovania rizika technickej kompatibility

Identifikované riziko technickej nekompatibility medzi výrobnými uzlami PM19 a zariadením CRYSTAL bolo následne podrobené systematickému hodnoteniu. Cieľom zvoleného metodického postupu bolo overiť významnosť identifikovaného mechanického rozhrania z hľadiska stability procesu a určiť jeho relatívnu rizikovosť v rámci celého výrobného toku. Posudzovanie rizík vychádzalo z princípov normy ISO 31000:2018 Risk Management - Guidelines, ktorá definuje riziko ako kombináciu pravdepodobnosti výskytu udalosti a jej dôsledku na stanovené ciele [8]. Tento prístup je v podmienkach podnikového riadenia rizík považovaný za základný rámec systematického rozhodovania o technických a organizačných opatreniach [6]. Na identifikáciu potenciálnych poruchových stavov bola využitá logika analýzy FMEA (Failure Mode and Effects Analysis), ktorá predstavuje štandardizovaný nástroj identifikácie spôsobov zlyhania a ich dôsledkov v technických systémoch [3], [4]. Metodika FMEA bola v tomto prípade použitá ako identifikačný rámec pre štruktúrované určenie rizikových miest, pričom samotné hodnotenie významnosti rizika bolo realizované prostredníctvom kvalitatívnej rizikovej matice založenej na parametroch pravdepodobnosti (P) a dôsledku (D).

Metodický postup zahŕňal:

- procesné mapovanie technologických rozhraní medzi výrobnými uzlami,
- identifikáciu potenciálnych spôsobov zlyhania na jednotlivých mechanických rozhraniach,
- analýzu technických príčin nestability,
- posúdenie dôsledkov zlyhania na kontinuitu výroby,
- zaradenie rizika do príslušnej kategórie pomocou rizikovej matice.

V centre hodnotenia sa nachádzalo mechanické rozhranie zabezpečujúce adaptáciu rozdielnych priemerov jadier prostredníctvom redukčného prvku. Analýza sa zamerala najmä na mechanickú stabilitu redukcie, osové zarovnanie medzi jadrom a hnacím hriadeľom, stabilitu ťahového napätia pásu a dynamickú citlivosť systému na odchýlky.

Pravdepodobnosť výskytu poruchy bola stanovená na päťstupňovej škále na základe prevádzkových prejavov a frekvencie výskytu odchýlok. Dôsledok vyjadroval mieru narušenia kontinuity výrobného procesu, pričom najvyšší stupeň predstavoval prerušenie procesu alebo aktiváciu bezpečnostného zastavenia zariadenia. Úroveň rizika bola určená kombináciou hodnôt P a D a následne interpretovaná prostredníctvom rizikovej matice.

Pravdepodobnosť (P)	**5**	**Veľmi vysoká**	5	10	15	20	25
	4	**Vysoká**	4	8	12	16	20
	3	**Stredná**	3	6	9	12	15
	2	**Nízka**	2	4	6	8	10
	1	**Veľmi nízka**	1	2	3	4	5
			Zanedbateľný	**Nízky**	**Stredný**	**Významný**	**Kritický**
			1	**2**	**3**	**4**	**5**
			Dôsledok (D)				

Obrázok 2. Matica rizík pre proces posudzovania rizík [upravené podľa 10]

Tabuľka 1. Posúdenie rizík technickej kompatibility [autor]

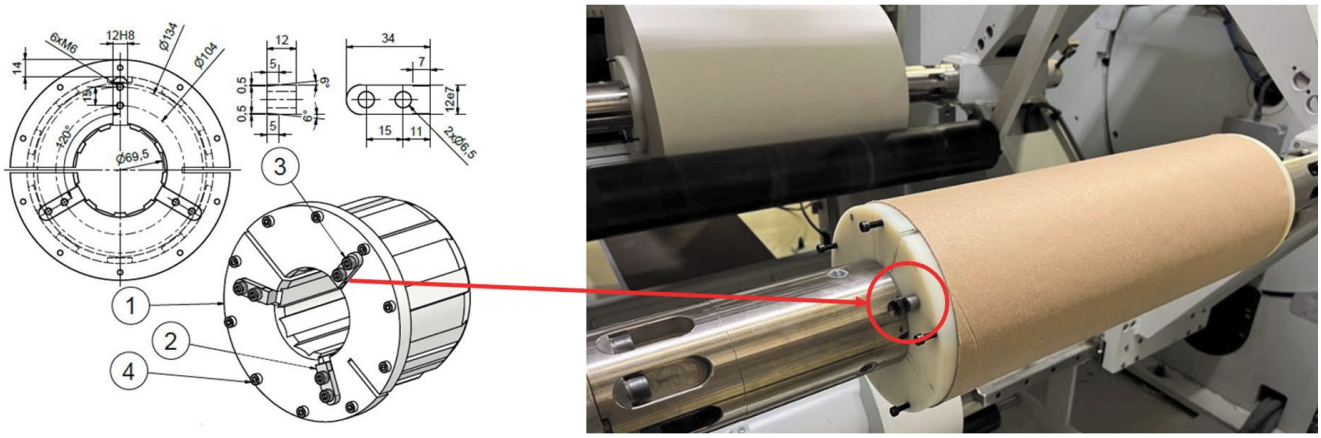
Riziko	**Technická príčina**	**Pravdepodobnosť (P)**	**Dôsledok (D)**	**Úroveň rizika (P · D)**	**Interpretácia**
Preklz redukčného prvku	Nedostatočné mechanické zaistenie voči hnaciemu hriadeľu	4	4	16	Riziko s vysokou pravdepodobnosťou a významným dopadom na kontinuitu výroby; vyžaduje prioritné technické opatrenie.
Odchýlka osového zarovnania	Geometrická nepresnosť adaptéra	3	4	12	Hraničná hodnota stredného rizika; potenciál prerušenia procesu pri dynamických odchýlkach.
Nestabilita navíjania	Kolísanie ťahového napätia pásu	3	5	15	Faktor zvyšujúci citlivosť systému; vyžaduje kontrolné opatrenia a technickú stabilizáciu.
Dynamická nestabilita výstupu	Zmena zotrvačných pomerov pri prevíjaní	2	3	6	Riziko s obmedzeným dopadom na stabilitu procesu; postačuje monitorovanie.

Výsledky hodnotenia potvrdili, že redukčný prvok predstavuje rozhranie s vysokou citlivosťou na mechanické odchýlky. Vzhľadom na dynamický charakter navíjacieho procesu a požiadavky na presnú synchronizáciu tlačového zariadenia CRYSTAL sa aj malé odchýlky v osovom zarovnaní alebo stabilite uloženia prejavovali zvýšenou nestabilitou systému. Technologické rozhrania medzi nekompatibilnými prvkami sú pritom v literatúre identifikované ako významné zdroje operačného rizika v komplexných výrobných systémoch [2]. Na základe metodického hodnotenia možno konštatovať, že redukcia medzistupňovej adaptácie jadier predstavuje opatrenie smerujúce k zníženiu počtu mechanických rozhraní a k redukcii procesnej komplexnosti, čo je v súlade so zisteniami o vzťahu medzi komplexnosťou systému a jeho spoľahlivosťou [1].

5 Implementácia opatrenia a zmena úrovne rizika technickej kompatibility

Na základe výsledkov analýzy rizík bolo identifikované mechanické rozhranie zabezpečujúce adaptáciu jadra 100/70 mm ako dominantný zdroj operačného rizika. Hodnotenie pomocou rizikovej matice preukázalo vysokú úroveň rizikovosti pri poruchových stavoch súvisiacich s preklzom redukčného prvku a nestabilitou navíjania. Tieto zistenia vytvorili podklad pre návrh technického riešenia zameraného na odstránenie príčiny rizika, nie iba jeho následkov.

Navrhované opatrenie vychádzalo z princípu zníženia procesnej komplexnosti elimináciou medzistupňovej adaptácie jadier. Technické riešenie spočívalo v konštrukčnej úprave systému navíjania, ktorá umožnila stabilné mechanické spojenie bez potreby redukčného prvku. Úpravou došlo k odstráneniu jedného mechanického rozhrania a k redukcii počtu prevíjacích operácií v procese. Konštrukčné riešenie implementované s cieľom eliminovať identifikovaný zdroj rizika je znázornené na Obrázku 3.



Obrázok 3. Implementované konštrukčné riešenie mechanického rozhrania navíjacieho systému [autor]

Z pohľadu riadenia rizík predstavuje eliminácia zdroja rizika najvyššiu úroveň preventívneho opatrenia v hierarchii manažmentu rizík podľa ISO 31000 [8]. Odstránením redukčného prvku došlo k:

- zníženiu počtu mechanických prechodov medzi zariadeniami,
- stabilizácii osového zarovnania jadra a hnacieho hriadeľa,
- zníženiu citlivosti systému na dynamické odchýlky,
- zníženiu potreby zásahov obsluhy,
- zvýšeniu kontinuity výrobného procesu.

Výsledky implementácie potvrdili významnú zmenu rizikového profilu analyzovaného procesu. Pôvodne identifikované vysoké riziko (P x D ≥ 15) bolo po odstránení zdroja poruchového stavu redukované na úroveň stredného až nízkeho rizika. Elimináciou redukčného prvku ako kritického mechanického rozhrania došlo k odstráneniu samotnej príčiny preklzu, čím bola pravdepodobnosť výskytu poruchy zásadne znížená. Implementačný zásah nepredstavoval iba lokálnu stabilizáciu mechanického prvku, ale štrukturálnu zmenu procesu vedúcu k redukcii počtu technologických rozhraní. Tým sa znížila procesná komplexnosť, ktorá je v literatúre dlhodobo identifikovaná ako faktor zvyšujúci zraniteľnosť výrobných systémov [5]. Implementované opatrenie tak priamo prispelo k zvýšeniu robustnosti procesu a k stabilizácii jeho dynamického správania.

Získané výsledky zároveň demonštrujú, že systematická aplikácia princípov riadenia rizík podľa ISO 31000 v kombinácii s analytickým rámcom FMEA umožňuje identifikovať a eliminovať skryté zdroje technickej nekompatibility ešte pred ich plnou manifestáciou v podobe opakovaných poruchových stavov. Riadenie rizík technickej kompatibility tak možno považovať za integrálnu súčasť optimalizácie technologických procesov v priemyselnom prostredí.

6 Záver

Príspevok sa zameral na posúdenie rizika technickej nekompatibility medzi výrobnými uzlami v konkrétnom priemyselnom procese. Analýza preukázala, že rozdielne technické parametre jadier a existencia medzistupňovej adaptácie vytvárali dodatočné mechanické rozhranie, ktoré významne zvyšovalo citlivosť systému na odchýlky a generovalo operačné riziko. Aplikácia princípov manažmentu rizík podľa ISO 31000 v kombinácii s logikou analýzy FMEA umožnila systematicky identifikovať kritické miesto procesu a objektivizovať jeho úroveň rizikovosti prostredníctvom rizikovej matice. Hodnotenie potvrdilo vysokú úroveň rizika súvisiacu s mechanickou nestabilitou redukčného prvku. Implementované technické opatrenie, založené na eliminácii zdroja rizika a redukcii počtu mechanických rozhraní, viedlo k zníženiu procesnej komplexnosti a k významnej zmene rizikového profilu výrobného systému. Výsledky potvrdzujú, že riadenie rizík technickej kompatibility môže predstavovať efektívny nástroj zvyšovania stability a robustnosti priemyselných procesov. Zistenia poukazujú na význam systematického posudzovania technologických rozhraní pri implementácii zmien vo výrobných systémoch. Integrácia manažmentu rizík do procesu technických rozhodnutí umožňuje nielen minimalizovať pravdepodobnosť poruchových stavov, ale aj optimalizovať štruktúru výrobného procesu z hľadiska jeho spoľahlivosti a prevádzkovej udržateľnosti.

Poďakovanie

Publikácia tohto článku bola podporená Grantovou agentúrou Ministerstva školstva, vedy, výskumu a mládeže Slovenskej republiky – VEGA 1/0743/25 Zvyšovanie udržateľnosti a hodnoty podnikov prostredníctvom riadenia procesných rizík.

Referencie

[1] CARIDI, M., CRIPPA, L. a PEREGO, A. Impact of manufacturing complexity on operational performance. International Journal of Production Economics. 2010, 125(2), 289–302. DOI: https://doi.org/10.1016/j.ijpe.2010.01.009

[2] WANG, X., KE, Y., CAI, Z. a YE, Z. Operation risk assessment of Flexible Manufacturing Networks subject to quality-reliability coupling. Reliability Engineering & System Safety. 2024, 250, 110282. DOI: https://doi.org/10.1016/j.ress.2024.110282

[3] EL-AWADY, S. M. M. Failure mode and effects analysis in risk assessment: a systematic review. Processes. 2023, 11(5), 1483. DOI: https://doi.org/10.3390/pr11051483

[4] ERVURAL, B. C., ZERENLER, M. a YILDIRIM, N. A data-driven FMEA framework for risk assessment in manufacturing systems. Reliability Engineering & System Safety. 2023, 236, 109247. DOI: https://doi.org/10.1016/j.ress.2023.109247

[5] HUDÁKOVÁ, M. a BUGANOVÁ, K. Integrated risk management in industrial enterprises. Management Systems in Production Engineering. 2018, 26(4), 220–224. DOI: https://doi.org/10.2478/mspe-2018-0035

[6] EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE. Smernica Európskeho parlamentu a Rady 2006/42/ES z 17. mája 2006 o strojových zariadeniach a o zmene smernice 95/16/ES (prepracované znenie). Úradný vestník Európskej únie. 2006. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32006L0042

[7] EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE. Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1230 z 14. júna 2023 o strojových zariadeniach. Úradný vestník Európskej únie, 2023. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32023R1230

[8] EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE. Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1230 z 14. júna 2023 o strojových zariadeniach. Úradný vestník Európskej únie. 2023. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32023R1230

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 31000:2018 Risk management – Guidelines. Geneva: ISO, 2018. Dostupné z: https://www.iso.org/standard/65694.html

[10] COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). Enterprise Risk Management – Integrating with Strategy and Performance [online]. New York: COSO, 2017. Dostupné z: https://www.coso.org/erm-framework