KRÍZOVÝ MANAŽMENT
CRISIS MANAGEMENT

Ročník 24 Číslo 2/2025

Vedecký časopis
FAKULTY BEZPEČNOSTNÉHO INŽINIERSTVA ŽILINSKEJ UNIVERZITY V ŽILINE

Scientific Journal
OF FACULTY OF SECURITY ENGINEERING AT UNIVERSITY OF ŽILINA

ŽILINSKÁ UNIVERZITA
V ŽILINE

HR EXCELLENCE IN RESEARCH

ŽILINSKÁ UNIVERZITA V ŽILINE
Fakulta bezpečnostného
inžinierstva

Moderné vzdelávanie pre vedomostnú spoločnosť/
Projekt je spolufinancovaný zo zdrojov EÚ
Tento projekt sa realizoval vďaka podpore z Európskeho sociálneho fondu a Štátneho rozpočtu SR v rámci Operačného programu Vzdelávanie
Systematizácia transferu pokrokových technológií a poznatkov medzi priemyselnou sférou a univerzitným prostredím ITMS 26110230004

PREDHOVOR

Vážení čitatelia, vedúci pracovníci a krízoví manažéri orgánov verejnej správy a zainteresovaných právnických osôb, kolegovia z akademického prostredia, vedeckí pracovníci, doktorandi a študenti vysokých škôl, predkladáme Vám druhé číslo 24. ročníka vedeckého časopisu, Fakulty bezpečnostného inžinierstva UNIZA, **Krízový manažment**.

Ďakujem všetkým domácim a zahraničným autorom, že venovali svoj čas a vypracovali pestré spektrum článkov. Oponentom ďakujem za ich kritické posúdenie článkov systémom „Double-blind peer review“. V tomto čísle sa autori venujú viacerým zaujímavým a inšpiratívnym problematikám.

Predkladané číslo časopisu je inovované prostredníctvom rozšírených článkov, resp. rozšírených posterov, z našej tohtoročnej konferencie s medzinárodnou účasťou, Riešenie krízových situácii v špecifickom prostredí 2025, v Žiline na Žilinskej univerzite. Z dôvodu nového formátu tejto konferencie, kde boli príspevky prezentované formou posterovej prezentácie a tak priestor na podrobnejšie vysvetlenie poskytujeme prostredníctvom nášho časopisu.

Rád by som dal do pozornosti internetové stránky časopisu, zvýšenie podielu článkov v anglickom jazyku a jeho propagáciu v domácom a zahraničnom prostredí. Náš časopis prešiel je registrovaný v medzinárodnej databáze ERIH plus a jednotlivé články sú tiež registrované v databáze Google Scholar a majú priradené DOI, čím zvyšujeme nie len kvalitu časopisu, ale aj dosah informácii, ktoré umožňujeme prezentovať.

Aj v budúcnosti radi privítame Vaše články zo všetkých oblastí teórie a praxe krízového manažmentu, civilnej ochrany, záchranných služieb, ochrany osôb a majetku, ochrany kritickej infraštruktúry a ďalších oblastí občianskej bezpečnosti. Články prijímame vo forme vedeckých príspevkov, odborných štúdií a skúseností, ako aj informácií o konferenciách, projektoch a nových publikáciách, počas celého roka. Vzor článku sa nachádza na posledných stranách časopisu, ako aj na web stránke časopisu.

Náš časopis je voľne dostupný v elektronickej podobe aj na stránke fbi.uniza.sk (https://fbi.uniza.sk/stranka/casopis-krizovy-manazment).

Budem veľmi rád za Vaše prípadné podnety a pripomienky, zaslané e-mailom na adresu Jozef.Ristvej@fbi.uniza.sk alebo vyslovené osobne na pôde Žilinskej univerzity v Žiline.

Prajem vám zaujímavé čítanie

Jozef Ristvej
predseda redakčnej rady

KRÍZOVÝ MANAŽMENT
Časopis pre pracovníkov zaoberajúcich sa otázkami bezpečnosti, rizík, krízovým manažmentom a krízovým plánovaním. Vychádza 2x ročne. Nevyžiadané rukopisy nevraciame. Kopírovanie a verejné rozširovanie povolené len so súhlasom vydavateľa. Články sú posúdené redakčnou radou a nezávislými oponentmi systémom „Double-blind peer review“. Časopis je evidovaný v medzinárodnej databázach ERIH plus a Google Scholar.

Vydáva Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, Univerzitná 8215/1, 010 26 Žilina, SR
IČO: 00397563
tel.: 041/ 513 67 04, fax: 041/ 513 66 20
e-mail: Jozef.Ristvej@uniza.sk
Tlač EDIS, vydavateľstvo UNIZA
Registrácia MK SR zo dňa 8.3.2009
pod číslom EV 3481/09 (tlačené vydanie)
Registrácia MK SR zo dňa 15.12.2022
pod číslom EV 45/22/EPP (online)
DOI 10.26552/krm.J.2025.2
ISSN 1336-0019 (tlačené vydanie)
ISSN 2730-0544 (online)
Dátum vydania: december 2025
Grafická úprava obálky
doc. Ing. Mária Hudáková, PhD.

VEDECKÉ ČLÁNKY

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.6-11
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

VYUŽITIE GEOGRAFICKÝCH INFORMAČNÝCH SYSTÉMOV V RÁMCI CYKLU KRÍZOVÉHO RIADENIA

THE USE OF GEOGRAPHIC INFORMATION SYSTEMS WITHIN THE CRISIS MANAGEMENT CYCLE

JOZEF RISTVEJ, JOZEF KUBÁS, BORIS KOLLÁR, DANIEL CHOVANEC

ABSTRACT: *The spatial nature of crisis events requires the use of specialised tools that allow visualisation of their manifestations and, at the same time, more advanced analyses for informed decision-making. Geographic information systems enable the handling of spatial data and therefore represent one of the most appropriate tools for this purpose. Crisis management is a complex system whose phases form a continuous circle. The aim of this paper is to analyse and describe the use of geographic information systems within the whole cycle of crisis management. The analysis of domestic and foreign literature has allowed a clear summarisation and visualisation of their use within the entire crisis management cycle. The results also allow to discuss the shortcomings in their use in the field of crisis management in the conditions of the Slovak Republic.*

KEYWORDS: *Crisis Management, Civil Protection, Crisis Management Cycle, Geographic Information Systems.*

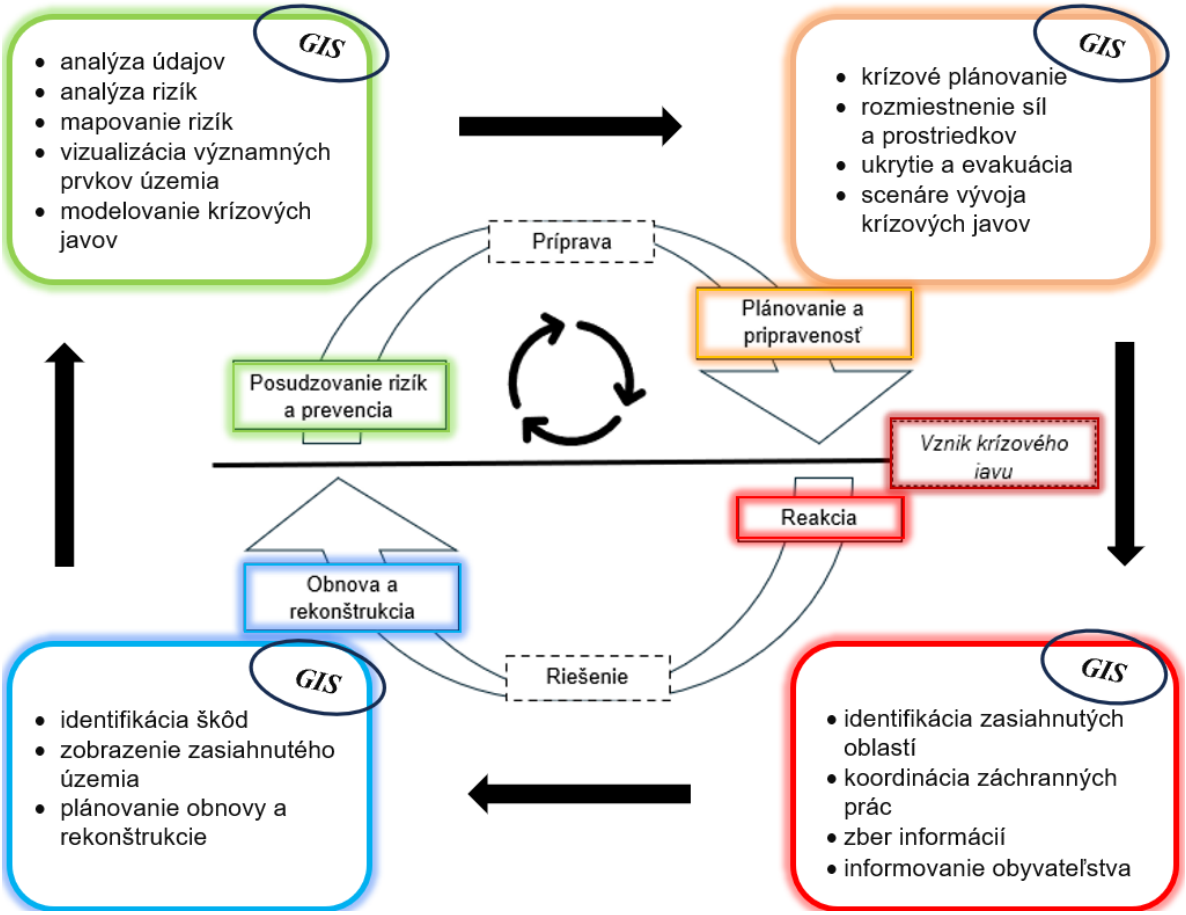
ÚVOD

Krízové riadenie je súbor aktivít a opatrení inštitúcií, ktorých hlavnou úlohou je predchádzanie a riešenie krízových javov s cieľom ochrany obyvateľstva a majetku. Tento súbor aktivít zahŕňa najmä monitorovanie rizikových činiteľov, prevenciu, plánovanie, koordináciu síl a prostriedkov a kontrolu činností zameraných na predchádzanie a samotné riešenie krízových javov (Bezpečnostná rada SR, 2017). V snahách o pochopenie krízového riadenia ako celku je možné vychádzať z jeho modelov, ktoré členia krízové riadenie na fázy. V podmienkach Slovenskej republiky (ďalej len SR) sa modelom krízového riadenia venovali Šimák (2015) a Ristvej (2018). Súhrnnej charakteristike modelov krízového riadenia, popisu ich fáz a činností, ktoré sú ich súčasťou, sa v ostatnom období venuje vo svojej práci Kollár (2024).Posudzovanie rizík ako samostatná fáza krízového riadenia alebo súčasť fázy prevencie predstavuje významný prvok pre podporu rozhodovania v krízovom riadení. Tento proces je všeobecne charakterizovaný technickou normou ISO 31 000:2018 Manažérstvo rizika. Zároveň je súčasťou oblasti záujmu viacerých domácich a zahraničných autorov (Hudáková a kol., 2021), (Šimák, 2015), (Pursiainen, 2017).

Hlavný prínos procesu posudzovania rizík v oblasti krízového riadenia s dôrazom na možný vznik krízových javov vychádza z jednotlivých fáz. Vo všeobecnosti ide o identifikáciu rizík, ktoré môžu nastať v konkrétnom prostredí, analýzu ich dopadov a konečné hodnotenie rizika podľa modelov. Priestorový charakter rizík a prvkov územia (Krömer, 2010) si vyžaduje využitie nástrojov, ktoré umožnia ich vizualizáciu a analýzu pomocou informačných technológií. Nevyhnutnou súčasťou posudzovania rizík územia je tiež údajová dostupnosť, pričom celý proces si vyžaduje zber, transformáciu a využitie širokého spektra údajov z rôznych zdrojov a od rôznych poskytovateľov a prevádzkovateľov. Geografické informačné systémy (ďalej len GIS) sú ucelený systém pozostávajúci z hardvéru, softvéru a údajov priestorového a nepriestorového charakteru (Ďuračiová, 2014). Práve GIS sú najvhodnejším nástrojom pre proces posudzovania rizík. Okrem vizualizácie zdrojov rizika, prvkov územia a rozsahu ich pôsobenia umožňujú vytváranie ďalších údajov, ktoré sú potrebné v modeloch hodnotenia rizík. Príkladom využitia GIS sú výpočty počtu ohrozených objektov, infraštruktúry a obyvateľov, ktoré vstupujú do modelu hodnotenia vybraných rizík na vnútroštátnej úrovni (Jánošíková a kol., 2013). Využitiu GIS v rámci posudzovania rizík, ale i v ďalších fázach cyklu krízového riadenia, sa venuje vo svojej práci viacero autorov. Na základe identifikovaných možností ich aplikácie poskytuje tento príspevok v ďalšom texte súhrnný prehľad ich využitia v podmienkach krízového riadenia, s možnosťami využitia nie len na Slovensku, ale aj s aplikáciou v zahraničí, najmä v členských štátoch Európskej únie.

1. VYUŽITIE GIS VO FÁZACH CYKLU KRÍZOVÉHO RIADENIA

Prepojenie problematík cyklu krízového riadenia, posudzovania rizík územia a geografických informačných systém umožňuje identifikovať oblasti ich vzájomnej aplikácie v systéme krízového riadenia. Prehľadná sumarizácia zároveň umožní komparáciu s aktuálnym stavom ich využitia v podmienkach krízového riadenia Slovenskej republiky. GIS je možné využiť v procese posudzovania rizík, ako aj v ostatných fázach krízového riadenia. Vzájomné prepojenie výsledkov ich aplikácie v jednotlivých fázach zobrazuje nasledujúci obrázok 1.



Obrázok 1 Možnosti využitia GIS v rámci cyklu krízového riadenia (vlastné spracovanie)

Posudzovanie rizík a prevencia

Hlavné využitie GIS v tejto fáze cyklu krízového riadenia vychádza najmä z prípravy a tvorby podporných materiálov pre rozhodovanie a ďalšie fázy tohto cyklu. Po načítaní potrebných údajov môžeme prekryť vektorové vrstvy a vypočítať potrebné štatistiky. Využitím rastrových údajov môžeme pomocou analýz identifikovať rizikové oblasti alebo vypočítať údaje potrebné pre ďalšie výpočty.

S využitím možností priestorových analýz je ďalej možné komplexné analyzovanie rizík. Príkladom môže byť prekrytie obalovej zóny okolo ciest, vypočítanej pre potenciálny únik nebezpečnej látky, s prvkami územia, ako sú objekty, vodné zdroje a pod. Výstupom budú počty ohrozených prvkov územia, ich identifikácia alebo počty ohrozených obyvateľov s využitím ďalších údajov.

Využitím výstupov z analýzy údajov a komplexných analýz rizík je možné pomocou GIS vytvárať prehľadné mapy rizík sledovaného územia pre podporu rozhodovania osôb s rozhodovacou právomocou. GIS umožňujú tiež vizualizovať zraniteľné oblasti a prvky územia (Singh, 2024).

Plánovanie a pripravenosť

Výstupy využitia GIS vo fáze posudzovania rizík a prevencie ďalej slúžia pre fázu plánovania a prípravy. Táto fáza zahŕňa najmä krízové plánovanie. Ide napríklad o plánovanie evakuačných trás pomocou sieťových analýz, ktoré sú súčasťou jednotlivých GIS (Kubás a kol., 2025). Ďalším príkladom môže byť využitie GIS pre plánovanie vhodného rozmiestnenia úkrytov, ako tiež návrh evakuačných trás k týmto úkrytom (Rodríguez-Espíndola a kol., 2016), (Chelariu a kol., 2022). S prepojením všetkých doposiaľ získaných a spracovaných údajov pomocou GIS je možné v tejto fáze modelovať rôzne scenáre vývoja krízových javov (Tomaszewski, 2015).

Reakcia

Z časového hľadiska delenia cyklu krízového riadenia, nachádza GIS využitie tiež vo fáze reakcie. Odborníci na GIS môžu krízovým manažérom posyktnúť cenné informácie integráciou údajov v reálnom čase. S využitím týchto údajov je možné mapovať reálnu situáciu a následky krízového javu, čo umožní efektívnejšie rozloženie síl a prostriedkov (Singh, 2024).

GIS má vo fáze reakcie uplatnenie tiež v oblasti informovania obyvateľstva. Vizualizáciou pôsobenia krízových javov a tvorbou prehľadových máp je možné zdieľať požadované informácie prostredníctvom hromadných médií (Roche a kol., 2011).

Obnova a rekonštrukcia

Geografické informačné systémy zohrávajú významnú úlohu aj v etape obnovy po krízových javoch, kde slúžia ako podpora pre rozhodovanie a koordináciu rekonštrukčných činností. Pomáhajú najmä pri vizuálnom zobrazení poškodených oblastí a infraštruktúry, ako aj pri porovnávaní situácie pred udalosťou a po nej, čo uľahčuje hodnotenie dopadov a plánovanie ďalších krokov (Jánošíková a kol., 2018). GIS sa v tejto fáze využíva aj na identifikáciu poškodených trás a návrh alternatívnych ciest pre zásobovanie a záchranné operácie, čo je kľúčové pri odstraňovaní následkov katastrof (Tomaszewski, 2015). Celkovo predstavuje GIS nástroj, ktorý umožňuje efektívne riadiť obnovu územia na základe aktuálnych a priestorovo presných údajov.

2. MOŽNOSTI VYUŽITIA GIS V PODMIENKACH KRÍZOVÉHO MANAŽMENTU NA SLOVENSKU

Praktickým príkladom využitia GIS v jednotlivých fázach cyklu krízového riadenia sú napríklad mapy riečneho povodňového ohrozenia v globálnom meradle. Tieto údaje sú vo formáte GEOTIFF a sú spracované pre povodne rôzneho rozsahu. Ide o hydrodynamické a hydrologické modely, ktoré vychádzajú z klimatologických údajov systémov včasného varovania EFAS a GloFAS služby krízového riadenia Copernicus (Baugh, 2024). Ďalším príkladom využitia GIS je plánovanie vhodných evakuačných miest pre prípad povodní v Rumunsku. Pomocou GIS boli vypočítané vhodné zóny, ktoré sa nenachádzajú v ohrozenej oblasti. Zároveň boli vypočítané najkratšie evakuačné trasy aj s časom trvania evakuácie (Chelariu a kol., 2022). Príkladom využitia GIS vo fáze reakcie je ONOVA GIS HUB. Ide o platformu poskytujúcu informácie o poškodených zariadeniach na Ukrajine vplyvom vojny a ich technickom stave. Platforma umožňuje sledovať stav poškodených nemocničných, administratívnych alebo športových zariadení prostredníctvom mapy a dashboardov. Tieto informácie slúžia najmä na sledovanie rozsahu škôd a následné plánovanie obnovy (ONOVA, 2025).

Uvedené praktické príklady využitia GIS, ako tiež možnosti využívania GIS v jednotlivých fázach cyklu krízového riadenia popísané v domácej a zahraničnej literatúre, poukazujú na ich širokú aplikovateľnosť. Možnosti využitia GIS v krízovom riadení priamo poukazujú na ich prínos pre podporu rozhodovania. V podmienkach Slovenskej republiky bol v oblasti krízového riadenia a civilnej ochrany k dispozícii informačný systém CIPREGIS, ktorý umožňoval vizualizáciu vybraných prvkov a ohrození na mape. Tento systém však v súčasnosti už nie je k dispozícii. V rámci krízového riadenia je pracovníkom

v oblasti integrovaného záchranného systému k dispozícii informačný systém s podporou GIS. Ide napríklad o systém CoordCom, ale aj ďalšie obdobné systémy. Tento systém umožňuje správu údajov a vizualizáciu lokácie síl a prostriedkov. V oblasti varovania obyvateľstva má SR k dispozícii systém SEHIS, ktorý umožňuje diaľkové ovládanie sirén a vizualizáciu ich lokácie a dosahu. Priamo pre krízové riadenie a civilnú ochranu nemá SR k dispozícii žiadne informačné systémy s podporou GIS (Bíbelová, 2024). V oblasti hospodárskej mobilizácie je k dispozícii aplikačný softvér EPSIS, ktorý má k dispozícii GIS rozhranie pre vizualizáciu vybraných prvkov (Schultz, 2025). Podrobný popis jednotného informačného systému hospodárskej mobilizácie a aplikačného softvéru EPSIS popisuje Ristvej a kol. (2017).

Pracovníci odboru krízového riadenia na okresných úradoch v sídle kraja sa v rámci prieskumu ohľadom spracovania dokumentu Analýza územia a procesu posudzovania rizík vyjadrili, že aktuálne absentuje dostatočné technické a softvérové vybavenie pre jednotlivé úlohy a požadované výstupy. Ďalším z identifikovaných problémov je údajová dostupnosť a rozptýlenosť zdrojov dostupných údajov. Absencia GIS v krízovom riadení neumožňuje využitie aktuálne dostupných údajov a vykonávanie požadovaných analýz, pričom práve GIS sú nevyhnutné pre spracovanie požadovaných výstupov v oblasti dokumentu Analýza územia a posudzovania rizík územia.

Podľa Šofranka (2014) je práca s údajmi a ich geografické znázorňovanie neoddeliteľnou súčasťou krízového riadenia a krízového plánovania. Keďže v podmienkach SR neexistuje komplexný informačný systém s podporou GIS pre krízové riadenie, je možné využiť voľne dostupné alebo komerčné produkty. V prípade komerčných GIS nástrojov je možné využiť ArcGIS od spoločnosti Esri, Inc. alebo napríklad AutoCAD Map a ďalšie, ktoré spĺňajú takmer všetky požiadavky komplexných riešení pre krízové riadenie. K dispozícii sú však aj nekomerčné nástroje, ktorých príkladom je geografický informačný systém QGIS. Pomocou QGIS a jednotlivých nástrojov, ktoré poskytuje, je možné napríklad filtrovať údaje zo súborov, vykresľovať vybrané údaje, pracovať, analyzovať a vytvárať nové rastrové a vektorové vrstvy a pod. (Šofranko, 2015).

Problémom využívania či už komerčných alebo voľne dostupných nástrojov môže byť počiatočná technická náročnosť pre pracovníkov odboru krízového riadenia. Využívanie týchto nástrojov by si vyžadovalo spracovanie metodiky, školenia a implementáciu týchto nástrojov do pracovných procesov. Ďalším problémom môže byť práve identifikovaná rozptýlenosť zdrojov potrebných údajov, ich agregácia a v neposlednom rade ich dostupnosť. Preto by sa ako vhodnejšie riešenie javilo vytvorenie komplexného informačného systému s podporou GIS, ktorý budú spravovať špecializovaní pracovníci so vzdelaním v oblasti informačných technológií a odbornou znalosťou v oblati krízového manažmentu. Tento informačný systém by zároveň musel disponovať prívetivým užívateľským rozhraním, pričom samotní pracovníci odboru krízového riadenia by podávali podnety na toto rozhranie v súvislosti s ich pracovnými postupmi a procesmi.

ZÁVER

Komplexnosť sytému krízového riadenia si v súčasnosti vyžaduje implementáciu moderných informačných technológii. GIS je jednoznačne možné považovať za pokročilú technnológiu s presahom do krízového riadenia. Využívanie GIS v rámci cyklu krízového riadenia má široké uplatnenie na Slovensku, ale najmä v zahraničných podmienkach. Z odbornej literatúry, ale i reálnych príkladov využitia, je zrejmé, že ide o komplexný nástroj s uplatnením najmä v podpore rozhodovania krízových manažérov. Široké uplatnenie GIS v krízovom riadení v zahraničí však doposiaľ nebolo prenesené do podmienok krízového riadenia SR. Z prieskumu medzi pracovníkmi na odboroch krízového riadenia okresných úradov v sídle kraja vyplýva, že okrem nedostupnosti GIS nástrojov v podmienkach ministerstva je problémom najmä rozptýlenosť zdrojov údajov a ich samotná dostupnosť. Jedným z riešení je využitie komerčných alebo voľne dostupných GIS, čo si však vyžaduje praktické skúsenosti používateľov. Dostupnosť údajov sa aj podľa odborníkov z rámca Sendai najlepšie zabezpečuje právnou úpravou. Rozptýlenosť údajov je možné vyriešiť nastavením systému dátového manažmentu a vytvorením jednej spoločnej databázy alebo dátového skladu.

POĎAKOVANIE

Táto práca bola podporená Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-24-0153. Článok bol spracovaný aj 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“.

LITERATÚRA

Baugh, C., Colonese, J., D'Angelo, C., Dottori, F., Neal, J., Prudhomme, C., & Salamon, P. (2024). *River flood hazard maps for Europe and the Mediterranean Basin region* [Dataset]. European Commission, Joint Research Centre (JRC). https://doi.org/10.2905/1D128B6C-A4EE-4858-9E34-6210707F3C81

Bezpečnostná rada Slovenskej republiky. (2017). *Terminologický slovník krízového riadenia a zásady jeho používania* [Online]. https://www.reserves.gov.sk/wp-content/uploads/2019/10/Terminologick%C3%BD-slovn%C3%ADk-kr%C3%ADzov%C3%A9ho-riadenia.pdf

Bíbelová, B. (2024). Informácia o dostupnosti IS v KR SR [elektronická pošta]. Správa pre: Boris Kollár. 2024-04-07 (cit. 2024-07-15). Osobná komunikácia.

Chelariu, O.-E., Iațu, C., & Minea, I. (2022a). A GIS-Based Model for Flood Shelter Locations and Pedestrian Evacuation Scenarios in a Rural Mountain Catchment in Romania. *Water*, *14*(19), Article 19. https://doi.org/10.3390/w14193074

Ďuračiová, R. (2014). *Databázové systémy v GIS* (1st ed.). Slovenská technická univerzita v Bratislave.

Hudáková, M., Buganová, K., Míka, V. T., & Masár, M. (2021). *Integrovaný systém manažmentu rizík v podniku* (1st ed.). Žilinská univerzita v Žiline – EDIS.

Jánošíková, G., & Hudecová, D. (2013). *Metodika hodnotenia vybraných rizík na vnútroštátnej úrovni* [Online document]. Ministerstvo vnútra Slovenskej republiky. https://www.minv.sk/?Dokumenty_na_stiahnutie_CO

Jánošíková, M., Ristvej, J., & Lacinák, M. (2018). Possible use of a geographical information system within crisis management simulations. *CBU International Conference Proceedings, 6*, 218–222. https://doi.org/10.12955/cbup.v6.1159

Kollár, B. (2024). Význam posudzovania rizík v rámci cyklu krízového riadenia. Mladá veda, 12(3), 78-89. https://www.mladaveda.sk/casopisy/2024/03/03_2024_08.pdf

Krömer, A., Musial, P., & Folwarczny, L. (2010). *Mapování rizik* (1st ed.). Sdružení požárního a bezpečnostního inženýrství.

Kubás, J., Ristvej, J., Kollár, B., Petrlová, K., Trličíková, A., Blažková, K. (2025). Evacuation Transport Provision Design Using Network Analysis with GIS Support. Communications- Scientific letters of the University of Zilina, DOI: 10.26552/com.C.2025.044

ONOVA GIS Hub helps Ukraine with war recovery and reconstruction. (n.d.). Retrieved 15 July 2025, from https://www.esri.com/en-us/lg/industry/electric-and-gas/onova-case-study

Pursiainen, C. (2017). *The crisis management cycle* (1st ed.). Routledge.

Ristvej, J., Sokolová, L., Starackova, J., Ondrejka, R., & Lacinak, M. (2017). Experiences with implementation of information systems within preparation to deal with crisis situations in terms of crisis management and building resilience in the Slovak Republic. *2017 International Carnahan Conference on Security Technology (ICCST)*, 1–6. https://doi.org/10.1109/CCST.2017.8167821

Ristvej, J., Ondrejka, R., & Jánošíková, M. (2018). *Crisis management II - 2nd part: Application software in crisis management* (1st ed.). University of Žilina.

Roche, S., Propeck-Zimmermann, E., & Mericskay, B. (2013). GeoWeb and crisis management: Issues and perspectives of volunteered geographic information. *GeoJournal*, *78*(1), 21–40. https://doi.org/10.1007/s10708-011-9423-9

Rodríguez-Espíndola, O., Albores, P., & Brewster, C. (2016). GIS and Optimisation: Potential Benefits for Emergency Facility Location in Humanitarian Logistics. *Geosciences*, *6*(2), Article 2. https://doi.org/10.3390/geosciences6020018

Schultz, O. (2025). Konzultácia k JIS HM EPSIS [elektronická pošta]. Správa pre: Boris Kollár. 2025-04-28. (cit. 2025-07-15). Osobná komunikácia.

Singh, R. (2024). The role of geographic information systems (GIS) in disaster management and planning. *International Journal of Geography, Geology and Environment*, *6*(2), 195–205. https://doi.org/10.22271/27067483.2024.v6.i2c.305

Šimák, L. (2015). *Krizový manažment vo verejnej správe* (2nd rev. ed.). Žilinská univerzita v Žiline, EDIS.

Šofranko, P. (2014). Mapový klient ZBGIS: úvod do problematiky GIS. Revue civilnej ochrany, 16(5), 40-43. https://www.minv.sk/swift_data/source/civilna_ochrana/dokument_skr/revue_co/Revue_CO_5_2014_web_verzia.pdf

Šofranko, P. (2015). Geografický informačný systém- QGIS. Revue civilnej ochrany, https://www.minv.sk/swift_data/source/civilna_ochrana/dokument_skr/revue_co/revue_co_2015/revue_CO_4_2015_pre_web.pdf

Tomaszewski, B. (2015). *Geographic information systems (GIS) for disaster management* (1st ed.). CRC Press – Taylor & Francis Group.

Jozef Ristvej - prof. Ing., PhD, EMBA

Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, Katedra krízového manažmentu, Univerzitná 8215/1, 01026 Žilina, Slovensko

e-mail: jozef.ristvej@uniza.sk

Jozef Kubás – doc. Ing., PhD.

Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, Katedra krízového manažmentu, Univerzitná 8215/1, 01026 Žilina, Slovensko

e-mail: jozef.kubas@uniza.sk

Boris Kollár – Ing.

Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, Katedra krízového manažmentu, Univerzitná 8215/1, 01026 Žilina, Slovensko

e-mail: boris.kollar@uniza.sk

Daniel Chovanec – Ing.

Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, Katedra krízového manažmentu, Univerzitná 8215/1, 01026 Žilina, Slovensko

e-mail: daniel.chovanec@uniza.sk

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.12-25
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

ASSESSING WATER CONSUMPTION AND WASTEWATER QUALITY IN UNDERGRADUATE CHEMISTRY AND PHARMACY LABORATORIES: IMPLICATIONS FOR SUSTAINABLE WATER RESOURCE MANAGEMENT AND OCCUPATIONAL HEALTH AND SAFETY

SIPHUMZE BANI, ROMAN TANDLICH

ABSTRACT: *Academic institutions play a crucial role in fostering skills development, advancing environmental sustainability, and addressing global socio-economic challenges, including those outlined in the Sustainable Development Goals (SDGs). A key factor ensuring the effective functioning of universities is the consistent availability and reliable access to clean water. This is especially critical in the face of increasing climate variability. In particular, droughts, which are caused by climate change, pose a significant threat to institutional resilience, operations, and academic continuity. This study focused on quantifying water usage and wastewater generation during Chemistry and Pharmacy undergraduate practical sessions conducted over four weeks. Among the sessions analysed, the highest average consumption of distilled water occurred in Pharmaceutics 4, amounting to 96.50 ± 1.60 L. While Pharmaceutical Chemistry 3 generated the highest average volume of wastewater at 128.70 ± 3.05 L. The most heavily polluted wastewater was recorded in Pharmaceutics 3. The observed average values for key contamination indicators were Total Bacteria of 3.75×10⁴ ± 1.07×10⁴ CFU/100 mL, Chemical Oxygen Demand of 6050.00 ± 450.92 mg/L, Electrical Conductivity of 0.77 ± 0.43 mS/cm, pH of 8.20 ± 0.29, Surface Tension of 39.75 ± 2.99 mN/m, Total Suspended Solids of 273.00 ± 47.81 mg/L, and Turbidity of 263.50 ± 54.71 NTU. The continuation of this research is essential. It will enhance the understanding of water-related risks in academic institutions and contribute significantly to disaster risk management, resource planning, and promoting environmentally sustainable practices in higher education.*

KEYWORDS: *Academic institutions. Climate change. Drought. Water usage and wastewater quality. Water resource management.*

INTRODUCTION

Universities are important in developing a skilled workforce and significantly affect the sustainability of the environment, for instance, impact on achieving the SDGs (Mukwevho & Togo, 2020; Bovea & Valls-Val, 2021; Galvao *et al.,* 2024; Nyambiya *et al.,* 2024). Water is one of the most consumed resources on university campuses because it is essential for health, well-being and daily business functioning (Broering *et al.,* 2024; Galvao *et al.,* 2024). Specifically, in Chemistry and Pharmacy undergraduate laboratories with more students, high volumes of water are used for experiments, cleaning, and equipment maintenance. The wastewater from these laboratories is contaminated with chemical and pharmaceutical pollutants, which are posing public health and environmental health risks. Water management is challenged by climate change impacts (i.e. drought and floods), exponential population growth, and improper waste management. The challenges, such as higher water demand and inconsistent supply, show the need for efficient water usage and wastewater treatment and reuse practices in all sectors, including higher education institutions (Arriga-Medina & Piedra-Miranda, 2021; Gherhes & Cernicova-Buca, 2025). At the same time, universities have conducted surveys on drinking water and implemented various sustainable water resource management initiatives (Espinosa-Garcia *et al.,* 2015; Siruma *et al.,* 2015; Mahler, 2018; Azaki & Rivett, 2020; Mahmood *et al.,* 2024; Tshivhase & Bisschoff, 2024; Alnasrawy and Ali, 2025; Al-Sumati *et al.,* 2025; Hashim *et al.,* 2025; Kalumba *et al.,* 2025). Limited research focuses on water consumption patterns and wastewater quality in specific academic settings, such as Chemistry and Pharmacy undergraduate laboratories.

1. WATER SCARCITY IS A DISASTROUS CHALLENGE IN ACADEMIC INSTITUTIONS

Water scarcity and quality concern environmental and public health and are pressing disaster risks, particularly in academic institutions, as they rely primarily on water for educational, operational, and safety functions. The management in academic institutions and laboratories tends to underestimate institutional disaster preparedness planning, such as sustainable water resources and wastewater management. Many universities' science laboratories are designed without water-saving and recycling systems. Designing and operating efficient water-saving, treatment, recycling systems, and efficient distributing infrastructure is important to ensure sustainable water management and use (Assi *et al.,*

2021; Val *et al.,* 2021; Ferreante *et al.,* 2024). Apart from the impactful natural disasters such as earthquakes, tsunamis, tropical cyclones (floods), and tornadoes (Abedin & Shaw, 2015; Georges *et al.,* 2017), prolonged drought can also severely affect functioning in academic institutions (Dzvimbo *et al.,* 2022; Luttik & Maters, 2023).

Unsustainable water supply can result in academic disruption, compromised safety, and improper sanitation and hygiene (Afiatun *et al.,* 2019). For instance, Barreiros *et al.* (2023) reported that the amount of water needed per person on campus ranges from 1.8 to 23.5 litres per day. Although safety observations, equipment and procedures are provided in laboratory settings, fire and explosion accidents have been reported to be frequent and cause an alarming number of deaths (Schroder *et al.,* 2016; Sonawane *et al.,* 2022; Wu *et al.,* 2023; Yang *et al.,* 2023; Zhao *et al.,* 2024; Liu *et al.,* 2025). In addition to the risk assessments and suggestions on safety protocols and management in university laboratories (Payne *et al.,* 2020; Li *et al.,* 2021; Wang *et al.,* 2021; Ezenwa *et al.,* 2022; Kuzmina *et al.,* 2022; Li *et al.,* 2022; Tziakou *et al.,* 2023; Zhao *et al.,* 2023; Zhong *et al.,* 2023; Lin *et al.,* 2024; Abedsoltan & Shiflett, 2024), consistent water supply is also essential because emergency fire extinguishing requires high volumes of water (Van Zyl & Haarhoff, 1997; Kondashov *et al.,* 2023; Ilemobade, 2023). During periods of drought and extended municipal water cut-offs, laboratory activities are restricted or completely stopped, resulting in ineffective delivery and assimilation of the information and research outcomes. Additionally, institutions struggle to maintain adequate functional, sanitation and hygiene standards, resulting in practices that compromise human and environmental health and academic integrity. For instance, inadequate sanitation and hygiene can lead to evolving and spread of diseases (Alwan *et al.,* 2023). At the same time, insufficient water availability in laboratories can result in improper dilution and disposal of hazardous reagents, leading to highly concentrated pollutants in wastewater networks (Gadipelly *et al.,* 2014; Munzhelele *et al.,* 2024). This increases environmental health risks and regulatory non-compliance (Foster, 2005; Gomes *et al.,* 2023).

Therefore, concerning water scarcity as a disaster risk in academic institutions gives insights and plans such as sustainable water resource and wastewater management, resilience building and preparedness. Practical approaches for executing these insights and plans include quantifying water consumption and wastewater quality in undergraduate laboratories and designing water-saving and wastewater treatment systems. These approaches are essential for preparedness and resilience during long drought conditions caused by unpredicted climate change (Dzvimbo *et al.,* 2022). Continuous analysis of laboratory wastewater quality is also important for tracking environmental impacts.

WATER CONSUMPTION AND WASTEWATER QUALITY IN UNDERGRADUATE LABORATORIES

The design and setting of the Chemistry and Pharmacy undergraduate laboratories are mainly for hands-on activities requiring significant amounts of water for preparing reagents, conducting experiments and cleaning the glassware before and after use. The water for laboratory operation is sourced from the Municipality reservoir. The water used to prepare the reagents is distilled/deionised, treated and obtained from ultrafiltration systems such as the Millipore Milli-Q Direct 16 Water Purification System. The washing of the hands and glassware and preparation of the water baths are done using tap water. The amount of water that is used in these activities is not metered or monitored. Hence, there is a shortage of data on water usage in these laboratories. The lack of water quantification systems in undergraduate laboratories results in inefficiency in water usage. The quantification of water consumption is an essential step towards designing and implementing water-saving systems within the undergraduate laboratory setting. Additionally, continuous assessment of water usage in undergraduate laboratories is aligned with the sustainable water resource management strategy in academic institutions.

The quality of wastewater from the Chemistry and Pharmacy laboratories comprises hazardous constituents such as heavy metals, inorganic/organic solvents, and pharmaceutical compounds. Laboratory wastewater poses high health risks to the public and environment because it can contaminate tap water distribution networks via pipe leakage and affect aquatic ecosystems through

disposal to surface water such as rivers (Madikizela & Ncube, 2022; Udebuani *et al.,* 2023; Paiga & Delerue-Matos, 2024; Newman *et al.,* 2024). Alarming concentrations of chemical and pharmaceutical contaminants have been reported to be present in surface waters, wastewater and effluent networks and subsequently in municipal taps (Madikizela *et al.,* 2022; Ogunlaja *et al.,* 2022; Oluwalana *et al.,* 2022; Archer *et al.,* 2023; Manyepa *et al.,* 2024; Nsibande *et al.,* 2024; Netshithothole *et al.,* 2024; Netshithothole and Madikizela, 2024; Sihlahla & Mngadi, 2024; Munzhelele *et al.,* 2024; Olaoluwa *et al.,* 2024; Mazhundu & Mashifana, 2024). Disposal of wastewater with high concentrations of chemical and pharmaceutical residues is also a risk of regulatory violation. Hence, performing quality wastewater analysis throughout undergraduate practical sessions is important. The knowledge of the composition of wastewater from different experiments/practical sessions is important for designing and implementing treatments, such as adsorption-filtering systems within the undergraduate laboratory drainage network (Ajiboye *et al.,* 2024; Sihlahla & Mngadi, 2024). This would be a sustainable approach to decrease the chemical and pharmaceutical contamination load that is deposited to the general wastewater network, thereby reducing public and environmental health risks (Letsoalo *et al.,* 2023; Manyepa *et al.,* 2024; Inarmal & Moodley, 2025).

SUSTAINABLE WATER RESOURCE MANAGEMENT IN ACADEMIC INSTITUTIONS

Sustainable water resource management in academic institutions refers to the implementation of strategies that encourage water conservation, efficient usage, and effective wastewater treatment and reuse. These strategies are implemented and practised through the aid of research centres because they are essential for alleviating climate change impacts such as prolonged drought, which turns out to be disastrous. Over the years, efforts on sustainable water resource management have been put by different universities across South Africa and globally (Gleick, 2010; Ilemobade *et al.,* 2011; Powell & Larsen, 2012; Marinho *et al.,* 2014; Crow-Miller *et al.,* 2016; Afiatum & Gustria, 2019); Barreiros *et al.,* 2023; Chowdhury *et al.,* 2024). These efforts include implementing rainwater harvesting systems, underground water abstraction and treating greywater from student residences and academic buildings (Ilemobade *et al.,* 2011; Malapane *et al.,* 2012; Chivenge *et al.*, 2024). The higher education institutes have also created a network and engagement with communities to emphasise awareness of efficient water usage and continuous quality assessment (Malapane *et al.,* 2012; Saito *et al.,* 2012; Siruma *et al.,* 2015). The key pillars to support the universities include policies and strategies such as the National Water Act of 1998, National Water Resource Strategy (NWRS), Integrated Water Resource Management (IWRM), Resource Directed Measures (RDMS) and Source Directed Controls (SDCs), Water Conservation and Water Demand Management (WC/WDM) Strategy, and Drought Management Plan (DMP).

The quantification of water usage and wastewater quality analysis from undergraduate science laboratories is rarely performed. It is a crucial approach to encouraging sustainable water resource management and managing drought disasters. Quantifying water usage in undergraduate laboratory sessions is a preparedness strategy because sufficient volumes of water can be predicted and supplied for catering practical sessions or experiments during drought seasons, particularly when municipal water supply is stopped. This would then mitigate the impact of drought disasters on academic progress. Quality analysis of wastewater generated during the experiment sessions is also a proactive approach that informs the design and formulation of wastewater treatment systems that can be built or retrofitted within the laboratory drainage systems. This would reduce concentrations of chemical and pharmaceutical residues that potentially contaminate municipal tap water and surface waters. Additionally, treated laboratory wastewater can be recovered and preserved for reuse in toilet flushing and emergency firefighting. This approach aligns with the above policies and strategies and the SENDAI Framework for Disaster Reduction 2015-2030 (2018).

Therefore, this study aims to assess the water consumption patterns and wastewater quality in undergraduate Chemistry and Pharmacy laboratories at Rhodes University. The objectives include the quantification of the water that is used and the analysis of the microbiological and physicochemical quality of wastewater generated during specific practical sessions. The findings of this study will provide valuable insights into the water usage and wastewater quality in university laboratories, informing the

ongoing development of policies and practices that promote sustainable water resource management and preparedness for drought disasters in higher education institutions.

2. METHODOLOGY

This project was conducted during the second term of the 2025 academic year. Data and observations were collected over four-weeks from the practical sessions in Chemistry Extended/Foundation studies, Pharmaceutical Chemistry 3, and Pharmaceutics 3 and 4. Lecturers, laboratory demonstrators, and technicians responsible for each session were asked to report the number of attending students and provide information about the experiment titles/topics and protocols. The data collection focused on the number of students attending each practical session, the titles and protocols of the experiments, the types and quantities of glassware and reagents used, the volume of distilled water used to prepare experimental solutions, and the volume of water used for rinsing and washing glassware before and after the experiments. To collect wastewater samples, six pairs of students were instructed to place stoppers in their sinks to prevent drainage during rinsing and washing. The resulting wastewater was aseptically collected for microbiological and physicochemical analysis.

QUANTIFICATION OF WATER CONSUMPTION

In the practical sessions, distilled/Milli-Q water was supplied by an ultrafiltration system (Millipore Milli-Q Elix, Merck) and provided in 25-liter barrels. Students accessed the water via taps on the barrels to prepare their solutions (Figure 1). The amount of distilled/Milli-Q water used was calculated using Equation 1.

Figure 1 Supply and access of distilled/deionised water for preparing solutions

$$Wu\ (L) = Vi - Vf \quad (1)$$

where: *Wu (L)*– water used in litres,
Vi – Initial volume before the practical session
Vf – Final volume after the practical session

The amount of water used for rinsing and washing glassware before and after experiments was quantified using laboratory sink dynamics and calculated based on Equation 2.

$$V\ (L) = \frac{L\ .\ W.\ D}{1000} \quad (2)$$

where: *V (L)*– Volume in litres,
L – Lenght in cm
W – Widht in cm
D- Depth in cm

The dynamics varied between sinks due to differences in laboratory design. In these calculations (Equation 2), Depth was treated as the dependent variable, as it represented the actual water level in the closed sink during measurements (Figure 2). The total water usage was calculated by summing the volume of water used to prepare solutions and the volume used for rinsing and washing glassware. The water consumption/usage per student during practical sessions was then determined using Equation 3.

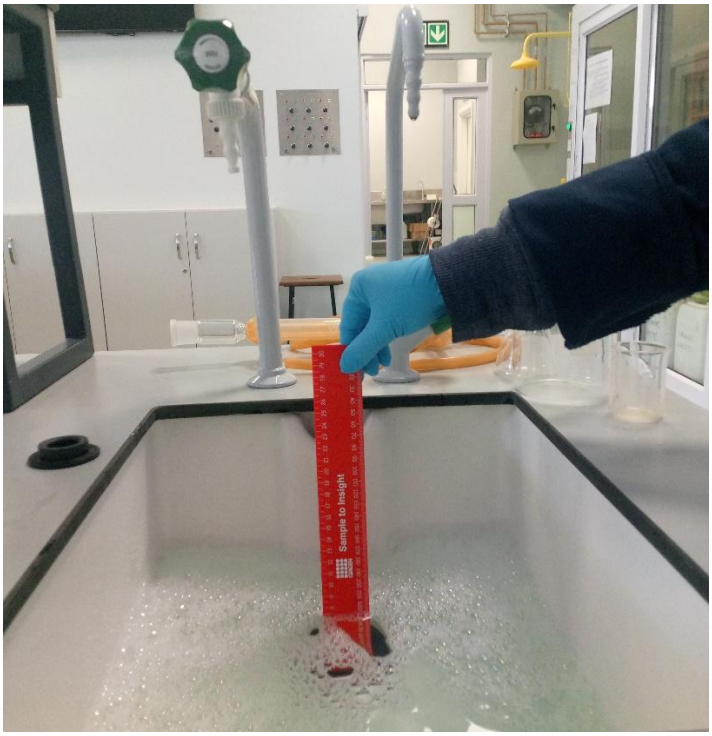


Figure 2 Measurement of generated wastewater after rinsing and washing of the glassware

$$Wups\ (L) = \frac{Wt}{Ns} \quad (3)$$

where: *Wups (L)*– Water used per student in litres,
Wt– Total water used in litres
Ns – Number of students in a practical session

QUANTIFICATION OF WATER CONSUMPTION

Wastewater generated from rinsing and washing glassware was collected in the sinks and aseptically sampled using sterile 500 mL Schott bottles, which had been autoclaved using an Equitron autoclave. The samples were immediately transported to the laboratory for microbiological (Total Bacteria and Faecal Coliforms) and physicochemical analyses, which included Chemical Oxygen Demand (COD), Electrical Conductivity (EC), pH, Surface Tension (ST), Total Suspended Solids (TSS), and Turbidity.
Total bacterial analysis was conducted by spread plating 100 µL of the wastewater sample onto Nutrient Agar plates (NEOGEN culture media). The number of colony-forming units per 100 mL (CFU/100 mL) for both Total Bacteria and Faecal Coliforms was calculated using Equation 4.

$$CFU = \frac{Nc \,.\, Df}{Vp} . 100 \quad (4)$$

where: *CFU* – Colony Forming Units per 100 ml,
Nc– Number of colonies
Df- Dillution factor
Vp – Volume platted in ml

The analysis of Faecal Coliforms, COD, EC, pH, TSS, and Turbidity was performed according to the methods described by Bani *et al.* (2024a, b). Surface tension (ST) was measured at room temperature using a KRÜSS tensiometer, with distilled water and 0.05 M sodium lauryl sulphate used as standards.

DATA ANALYSIS AND PRESENTATION

The average ± standard deviation (n=4) amount of distilled/Milli-Q water used, generated wastewater, and water used per student over the four weeks in all the practical sessions are presented in a bar graph (Figure 3). The significance of the difference across all the practical sessions on the amount of distilled/Milli-Q water used, generated wastewater, and water used per student is calculated using one-way ANOVA statistics. Figure 3 and ANOVA (p-value) statistical analysis are used to evaluate the level and significance of the difference in the consumption of water across the observed practical sessions.

The average ± standard deviation (STDEV) (n=4) of the wastewater quality in all the practical sessions over four weeks is presented in Table 1. The microbiological quality parameters (Total bacteria and Faecal Coliforms are presented as Geometric mean ± STDEV). The significance of the difference (one-way ANOVA statistics) of the wastewater quality parameters across all the practical sessions is also presented in Table 1. The calculations of the average, geometric mean, STDEV, and one-way ANOVA statistics were performed using Excel (Microsoft Office Professional Plus 2019).

3. RESULTS AND DISCUSSION

The analysis of the results obtained from each practical session reports contributing factors to the observed differences. Variations in the consumption of distilled or Milli-Q water is associated with the number of students attended and the specific experimental protocols conducted during each practical session. Also, the variation in the volume and quality of wastewater generated is influenced by the capacity of the laboratory sinks, the number, type and degree of contamination of the used glassware. The level of contamination of the glassware and subsequently wastewater is linked to the used reagents and complexity of the experiments conducted, which vary across practical sessions.

WATER CONSUMTPTION IN THE PRACTICAL SESSIONS

Over four weeks, the average levels of distilled water consumption, wastewater generation, and water usage per student during Chemistry and Pharmacy practical sessions are presented in Figure 3. A statistically significant difference in distilled water usage was observed between the practical sessions (p-value = 5.03×10^{-14}), with Chemistry sessions consuming lower volumes. The Chemistry practical sessions focused on introductory scientific concepts and methods. The experiments included identifying inorganic substances, determining vinegar concentration using volumetric analysis, and applying Le Chatelier's Principle to study the solubility of acids and bases in water and Soap formulation. Across the Chemistry experiments, distilled water consumption by 30 pairs of students ranged from 5.00 ± 1.00 to 10.00 ± 2.00 L, with an average of 6.50 ± 2.00 L. The laboratory sink capacity, calculated based on measured dimensions (length = 31 cm, width = 25 cm, depth = 14.5 cm), was 11.24 L. The wastewater generated by the same group over four weeks ranged from 69.00 ± 0.50 to 93.00 ± 3.10 L, with an average of 76.00 ± 2.22 L. The water usage per student over the four weeks ranged from 1.22 ± 1.71 to 1.74 ± 3.80 L, with an average of 1.40 ± 2.28 L.
In the Pharmaceutical Chemistry 3 practical sessions, the experiments that were performed over four weeks included the Isolation of red pigment from paprika, the Synthesis of local anaesthetic benzocaine, the Synthesis of Sulphanilamide, and the Synthesis of 4-cholestene-3-one from cholesterol. Across these experiments, the distilled water consumption by 42 students ranged from 42.00 ± 2.00 to 46.00 ±

1.45 L, with an average of 43.25 ± 1.56 L. According to the measured dimensions (length = 42.5 cm, width = 32 cm, depth – 22.5 cm), the laboratory sink capacity was found to be 30.6 L, and the wastewater generated by 42 students over four weeks ranged from 114.24 ± 1.56 to 199.50 ± 2.21 L, with an average of 160.55 ± 2.34 L. The water usage per student over the four weeks ranged from 3.76 ± 4.12 to 5.75 ± 3.52 L, with an average of 8.85 ± 4.72 L. Distilled water consumption was due to refluxing which was essential step experiments, while elevated wastewater generation was caused by multiple rinsing and washing of the glassware (round bottom flasks, Erlenmeyer flasks, reflux condensers, beakers, and watch glasses) before and after the experiments.

The Pharmaceutics 3 practical sessions were based on an assessment of suppositories, which included examination of their external appearance, weight, internal appearance, and disintegration test using 0.3 L of 37 °C distilled water per suppository. The following experiments involved the formulation of suppositories using different dye/base combinations, which included Amaranth, Sudan III Red, Macrogol, and Theobroma oil. Each formulated suppository was placed in beakers containing 0.3 L of 37 °C distilled water to observe the rate and behaviour of dye release. Across these experiments, the distilled water consumption by 57 students (29 pairs) ranged from 17.40 ± 3.21 to 26.10 ± 0.56 L, with an average of 21.75 ± 1.82 L. The laboratory sink capacity (length =34.5 cm, width = 24.5 cm, depth = 15 cm) was found to be 12.68 L, and the wastewater generated by 29 pairs of students over four weeks ranged from 61.28 ± 5.67 to 196.10 ± 1.23 L, with an average of 128.70 ± 3.05 L. The water usage per student over the four weeks ranged from 3.76 ± 4.12 to 5.75 ± 3.52 L, with an average of 2.64 ± 2.60 L. Low values of distilled water were consumed in the Pharmaceutics 3 compared to the Pharmaceutical Chemistry 3 practical sessions. The washing of glassware stained with Sudan III Red and Theobroma oil resulted in a high generation of wastewater from these experiments.

The experiments performed in Pharmaceutics 4 practical sessions included quantifying the active pharmaceutical ingredient (API), which was done by producing a calibration curve of paracetamol in water using a UV-VIS spectrophotometer. The second experiment focused on chemical kinetics, which was mainly on the evaluation of the pH stability of a drug by dissolving in water (about 0.1 L) to produce a calibration curve. The third experiment was based on releasing an API from two suppository formulations, which consume 1.00 L of 37 °C distilled water as a dissolution medium. The fourth experiment focused on releasing an API from 3 tablet formulations, which consumes 3.00 L of 37 °C of distilled water as a dissolution medium. Across these experiments, the consumption of distilled water by 31 students (16 pairs) over four weeks ranged from 93.00 ± 1.03 to 99.00 ± 2.10 L, with an average of 96.50 ± 1.60 L. The laboratory sink capacity (length = 30 cm, width = 25.5 cm, depth= 17.5 cm) was found to be 13.39 L, and the wastewater generated by 16 pairs of students ranging from 85.20 ± 3.20 to 109.54 ± 2.10 L, with an average of 89.93 ± 2.05 L. the water demand or water usage per student in these experiments ranged from 5.56 ± 3.21 to 6.53 ± 1.54 L, with an average of 6.01 ± 2.14 L. Amongst the observed practical sessions, Pharmaceutics 4 consumed high volumes of distilled water and this is due to the dissolution experiments. The rinsing and washing of dissolution beakers before and after the experiments resulted in high volumes of wastewater from the Pharmaceutics 4 practical sessions. The laboratory sink capacity, which was found to be high in Pharmaceutical Chemistry 3, impacts wastewater generation; students tend to rinse the glassware several times.

Although the quantification of water usage and wastewater generation in university laboratories is rarely conducted or reported, it is evident that water consumption mainly depends on the nature of the experiments. The observed demand for distilled water and the volume of wastewater shows the need for reliable and sustainable water access in academic laboratories. Therefore, ongoing data collection and observation of water usage during practical sessions are essential to effective and sustainable water resource management. Additionally, the volumes of generated wastewater show the potential for treatment and reuse for non-portable purposes to alleviate the impacts of drought disasters in higher education institutes.

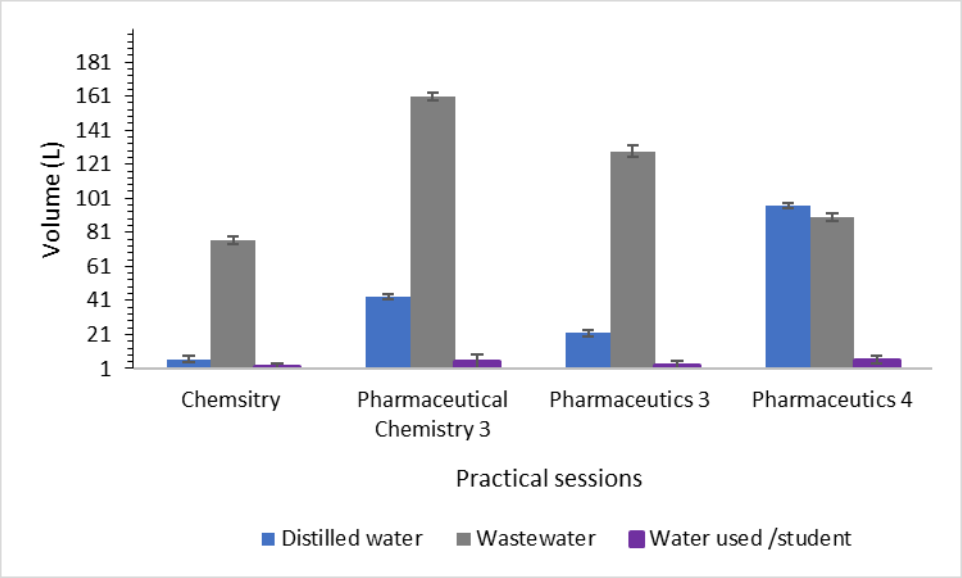


Figure 3 Levels of distilled water consumption, wastewater generation and water used per student in Chemistry and Pharmacy practical sessions

QUALITY OF WASTEWATER GENERATED FROM THE PRACTICAL SESSIONS

As shown in Table 1, the wastewater samples from the Chemistry, Pharmaceutical Chemistry 3, and Pharmaceutics 4 practical sessions contained Total Bacteria and Faecal Coliforms in the range below 0 CFU/10 ml (designated as TFTC in further text of the article) and, therefore, insignificant in representing microbial concentration. In contrast, the Total Bacteria count in the Pharmaceutics 3 wastewater was significantly higher, measured at $3.75 \times 10^4 \pm 1.07 \times 10^4$ CFU/100 ml. The low bacterial counts in Chemistry, Pharmaceutical Chemistry 3, and Pharmaceutics 4 practical sessions are likely due to the presence of residual reagents and the use of detergents during glassware washing, which disinfected the microorganisms in the wastewater. However, in the case of Pharmaceutics 3, the use of warm water for washing, combined with the presence of recalcitrant reagent residues such as Theobroma oil and Sudan Red III dye, have promoted microbial proliferation rather than inhibition.

Among the physicochemical contaminants analysed,COD levels were found to be high in the wastewater from Pharmaceutics 3, Pharmaceutical Chemistry 3, and Pharmaceutics 4. In contrast, the Chemistry wastewater showed low COD concentrations due to the lower quantities of reagents and salts used in the experiments, as well as minimal detergent use during glassware cleaning. The differences in EC and pH values across all practical sessions were found to be statistically insignificant. However, ST was highest in the Chemistry wastewater, suggesting limited use of detergent, while lower ST values in the other sessions indicate more extensive detergent use. High TSS and Turbidity levels were also observed in the Pharmaceutical Chemistry 3 wastewater. This was primarily due to the presence of Theobroma oil aggregates and Sudan Red III dye, which contributed to brownish colouration. Among all the practical sessions, Pharmaceutics 3 generated the most contaminated wastewater due to the nature and intensity of the experiments conducted over four weeks.

The analysis of laboratory wastewater quality has important implications for public health and environmental safety. It informs the profiling and mitigation of health risks, supports environmental protection efforts, and guides decisions regarding appropriate treatment for reuse or safe discharge (Reed, 2006). Notably, the evaluation of wastewater from Pharmaceutics 3 practical sessions revealed issues such as microbial regrowth and residual reagents. These factors not only pose direct health risks but also contribute to the emergence of antimicrobial-resistant strains in surface waters and wastewater treatment plants (Odjadjare and Olaniran, 2015; Olaniran *et al.,* 2015; Pillay & Olaniran, 2016; Booth *et al.,* 2020; Holton *et al.,* 2022) Additionally, elevated COD levels show the concentration of organic and inorganic pollutants which are hazardous to surface water bodies, as they lead to oxygen depletion,

which results in disruption of aquatic ecosystems and threaten livestock and biodiversity (Mamba *et al.,* 2009; Wilhelm, 2009; Chigor *et al.,* 2013; Li and Liu, 2019; Han *et al.,* 2022).In addition to these concerns, the quality of wastewater generated across all practical sessions indicates the potential for efficient on-site treatment. Adsorbent-filter-based systems show promise for integration into existing laboratory plumbing networks to reduce pollutant loads before discharge or reuse (Nondlazi *et al.,* 2017; Bani *et al.,* 2024a, b). Implementing laboratory wastewater treatment technologies addresses contamination concerns and supports strategies for sustainable water resource management. This approach is important in academic institutions vulnerable to water scarcity and drought conditions.

Table 1 Microbiological and Physicochemical quality of wastewater generated from the Practical sessions

	Microbiological quality		**Physicochemical quality**					
	Geometric mean ± STDEV		**Average ± STDEV**					
Practical session	**Total Bacteria (CFU/100 ml)**	**Faecal Coliforms (CFU/100 ml)**	**COD (mg/l)**	**EC (mS/cm)**	**pH**	**ST (mN/m)**	**TSS (mg/l)**	**Turbidity (NTU)**
Chemistry	TFTC	TFTC	128.25 ± 7.37	0.75 ± 0.24	8.10 ± 0.28	68.25 ± 1.71	47.00 ± 17.40	37.50 ± 17.46
Pharmaceutical Chemistry 3	TFTC	TFTC	4000.00 ± 509.90	0.87 ± 0.23	8.35 ± 0.44	35.00 ± 3.92	54.75 ± 8.73	46.50 ± 6.86
Pharmaceutics 3	$3.75x10^4$ ± $1.07x10^4$	TFTC	6050.00 ± 450.92	0.77 ± 0.43	8.20 ± 0.29	39.75 ± 2.99	273.00 ± 47.81	263.50 ± 54.71
Pharmaceutics 4	TFTC	TFTC	2575.00 ± 403.11	1.04 ± 0.15	8.00 ± 0.34	41.75 ± 4.50	53.00 ± 12.75	48.25 ± 13.91
ANOVA (p-value)	-	-	$6.48x10^{-10}$	$4.64x10^{-1}$	$5.44x10^{-1}$	$4.58x10^{-8}$	$8.05x10^{-8}$	$2.90x10^{-7}$

CONCLUSION

Overall, this study has emphasized the important role of academic institutions as centres for human skill development, environmental sustainability, and contributions to global socio-economic objectives, including the SDGs. The effective functioning of universities relies on various resources, among which water is particularly critical. However, climate change impacts such as droughts and floods increasingly contribute to water scarcity via reduced rainfall or siltation of water reservoirs. Among natural disasters,

prolonged droughts have a particularly disruptive effect on academic institutions. Consequences include operational interruptions, intense anxiety among staff and students, compromised health and safety conditions, and increased vulnerability to emergencies such as laboratory fires. Reliable water access is essential for maintaining safe and efficient operations in science laboratories and supporting the broader delivery of knowledge and skills.

The quantification of water usage and wastewater generation in Chemistry, Pharmaceutical Chemistry, and Pharmaceutics 3 and 4 practical sessions provide valuable insights into sustainable water resource management within universities. Moreover, analysing laboratory wastewater quality provides a foundation for designing and integrating efficient treatment technologies. Such approaches enable safer discharge into wastewater systems or reuse for non-potable applications such as toilet flushing and firefighting, thus supporting sustainability and disaster preparedness.

Future phases of this research will involve continued data collection and observation of additional practical sessions during the 2025 second semester. Additional analysis is recommended, including identification of bacterial strains and pharmaceutical residues in the wastewater. These efforts will enhance the impact and details of the study and association with local and international disaster management strategies and policies.

ACKNOWLEDGEMENTS

The authors would like to thank the Henderson Prestigious Scholarship for funding of this study. Rhodes University for the platform and support.

REFERENCES

Abedin M.A & Shaw R. (2015). The Role of university networks in disaster risk reduction: Perspective from coastal Bangladesh. International Journal of Disaster Risk Reduction. 13. 381-389. 10.1016/j.ijdrr.2015.08.001.

Abedsoltan H & Shiflett M.B. (2024). Mitigation of Potential Risks in Chemical Laboratories: A focused Review. ACS Chemical Health and Safety. 31(2). 104-120.10.1021/acs.chas.3c00097.

Afiatun E, Wahyuni S, & Gustria N. (2019). Study on fluctuation of water consumption at education activity building (Universitas Pendidikan Indonesia as a case study). IOP Conf. Series: Earth and Environmental Science 245. :10.1088/1755-1315/245/1/012032.

Ajiboye T.O, Oladoye P.O, & Omotola E.O. (2024). Adsorptive reclamation of pharmaceuticals from wastewater using carbon-based materials: A review. Kuwait Journal of Science. 51(3). 10.1016/j.kjs.2024.100225.

Alnasraywy S.T & Ali H.A.M. (2025). Exploring the Perspectives of Iraqi College Students on the Causes and Suggested Remedies for Water Scarcity: An In-Depth Analysis. Journal of Environmental Engineering (United Sates). 151(5). 10.1061/JOEEDU.EEENG-7905.

Al-Sumati A.S, Ali-Ali R.S, Saini V.K, Al-Saif N, & Kumar R. (2025). Evaluating drivers of water-energy use: Insights from a selected Higher Education University in Abu Dhabi, UAE. Sustainable Futures. 9. 10.1016/j.sftr.2025.100446.

Alwan N, Safwan J, Kerek R, & Ghach W. (2023). Hand hygiene during the spread of COVID-19: a cross-sectional study of awareness and practices among academic institutions in Lebanon. Frontiers in Public Health. 11. 10.3389/fpubh.2023.1256433.

Archer E, Holton E, Fida J, Kasprzyk-Hordern B, Carstens A, Brocker L, Kjeldsen T.R, & Wolfaardt G.M. (2023). Occurrence of contaminants of emerging concern in the Eerste River, South Africa: Towards the optimisation of an urban water profiling approach for public- and ecological health risk characterisation. Science of the Total Environment. 859. 10.1016/j.scitotenv.2022.160254.

Arriaga-Medina J.A & Piedra-Miranda. (2021). Water consumption practices in university campuses. The experience of the National Autonomous University of Mexico. Water Science and Technology. 84 (5): 1125–1135. 10.2166/wst.2021.306.

Assi R.A, Ng T.F, Tang J.R, Hassan M.S, & Chan S.Y. (2021). Statistical analysis of green laboratory practice survey: Conservation on non-distilledwater from distillation process. Water (Switzerland). 13(15). 10.3390/w13152018.

Azaki J.I & Rivett U. (2020). Persuasive information campaign to save water in Universities: An option for water-stressed areas? COMPASS 2020 - Proceedings of the 2020 3rd ACM SIGCAS Conference on Computing and Sustainable Societies. 279-283. 10.1145/3378393.3402238.

Bani S, Limson J, Zuma B, & Tandlich R. (2024b). Short Communication: Potential of Biochar and Clays as Sorbents for Treatment of Greywater and related Wastewaters in South Africa. Journal of Solid Waste Technology and Management. 50(2); 577-589. 10.5276/jswtm/iswmaw/502/2024.577.

Bani S, Matambo C, Limson J, Zuma B, & Tandlich R. (2024a). Operation and Performance of the Lab and Pilot-scale Greywater Treatment Systems: Biochar and Gravel use in South Africa. Journal of Solid Waste Technology and Management. 50(1); 458-478. 10.5276/JSWTM/ISWMAW/501/2024.458.

Booth A, Aga D.S, & Wester A.L. (2020). Retrospective analysis of the global antibiotic residues that exceed the predicted no effect concentration for antimicrobial resistance in various environmental matrices. Environmental International. 141. 10.1016/j.envint.2020.105796.

Broering L.A, Michel J, Henning E, Kalbusch A, & Konrath A.C. (2024). An investigation into water consumption by university students: actions, beliefs and perceptions. 4. 10.1007/s43832-024-00176-9.

Chigor V.N, Sibanda T, & Okoh A.I. (2013). Variations in the physicochemical characteristics of the Buffalo River in the Eastern Cape Province of South Africa. Environmental Monitoring and Assessment. 185(10). 8733-8747. 10.1007/s10661-013-3208-1.

Chivenge M, Chirisa I, & Moyo T. (2024). Decentralised Wastewater Treatment Plant for University of Zimbabwe Technical Staff Housing, Hatcliffe Harare: A Site Analysis. Urban Book Series. 161-179. 10.1007/978-3-031-45568-1_9.

Chowdhury S, Ren Z, Rouhana F, Wang J, & Zhu J. (2024). Exploring Sustainability in Resource Management: Implementation of a Water-Energy-human Nexus Framework at University Campus. ASCE Library. 150(10). 10.1061/JCEMD4.COENG-13609.

Crow-Miller B, Chang H, Stoker P, & Wentz E.A. (2016). Facilitating collaborative urban water management through university-utility cooperation. Sustainable Cities and Society. 27. 475-483. 10.1016/j.scs.2016.06.006.

Espinosa-Garcia A.C, Diaz-Avalos C, Gonzalez-Vilarreal F.J, Val-Segura R.V, Malvaez-Oroco V, & Mazari-Hiriart M. (2015). Drinking Water Quality in a Mexico City University Community: Perception and Preferences. 12. 88-97.

Ezenwa S, Talpade A.D, Ghanekar P, Joshi R, Devaraj J, Ribeiro F.H, & Mentzer R. (2022). Toward Improved Safety Culture in Academic and Industrial Chemical Laboratories: An Assessment and Recommendation of Best Practices. ACS Chemical Health and Safety. 29(2). 202-213. doi.org/10.1021/acs.chas.1c00064.

Ferrante M, Rogers D, Mugabi J, & Franscesco C. (2024). A Laboratory Investigation on the Effects of Intermittent Water Supply and Remedial Measures. Water Resource Research. 60(2). 10.1029/2023WR035282.

Foster B.L. (2005). The Chemical Inventory Management System in academia. Chemical and Safety. 12(5). 21-25. 10.1016/j.chs.2005.01.019.

Gadipelly C, Perez-Gonzalez A, Yadav G.D, Ortiz Inmaculada, Ibanez R, Rathod V.K, & Marathe K.V. (2014). Pharmaceutical Industry Wastewater: Review of the Technologiesfor Water Treatment and Reuse. 11571-11872. org/10.1021/ie501210j.

Galvao A, Matos C, Durao A, Mourato S, Mateus D, Araujo I, Neves L, & Barreiros A. (2024). Water Efficiency Perception Among Higher Education Students. ICoWEFS 2024 Sustainability Proceedings. 10.1007/978-3-031-80330-7_15.

Georges C.B, Brown L, & Carlin E. (2017). Strengthening the Disaster Resilience of the Biomedical Research Community: Protecting the Nation's Investments. Impacts of Prior Disasters on the Academic Biomedical Research Community. The National Academy Press. Washington, DC. 10.17226/24827.

Gherhes V & Cernicova-Buca M. (2025). Reducing Water Consumption on a Student Campus Through Communication Campaigns. Sustainability. 17(2). 10.3390/su17020680.

Gleick P.H. (2010). Roadmap for sustainable water resources in southwestern North America. Sustainability Science. 107 (50) 21300-21305. 10.1073/pnas.1005473107.

Gomes L.P, Caetano M.O, Brand S.M, Dai-Pra L.B, & Pereira B.N. (2023). Maintenance of an environmental management system based on ISO 14001 in a Brazilian private university, seeking sustainable development. International Journal of Sustainability in Higher Education. 24(2). 361-381. 10.1108/IJSHE-07-2021-0298.

Han X, Chen X, Ma J, Chen J, Xie B, Yin W, Yang Y, Jia W, Xie D, & Huang F. (2022). Discrimination of Chemical Oxygen Demand Pollution in Surface Water Based on Visible Near-Infrared Spectroscopy. Water. 14(19). 10.3390/w14193003.

Hashim N.S.B, Malek M.B.A, Latif S.D, Alsubih M, ElShafie A, & Ahmed A.N. (2025). Water Footprint Assessment to Map and Quantify Water Consumption and Water Pollution Incurred: A Case Study of Malaysia. Water, Air, and Soil Pollution. 236(3). 10.1007/s11270-025-07786-6.

Hilton E, Archer E, Fidal J, Kjeldsen T, Wolfaardt G, & Kasprzyk-Horden B. (2022). Spatiotemporal urban water profiling for the assessment of environmental and public exposure to antimicrobials (antibiotics, antifungals, and antivirals) in the Eerste River Catchment, South Africa. Environmental International. 164. 10.1016/j.envint.2022.107227.

Ilemobade A, Olanrewaju O, & Griffioen M. (2011). Experiences of greywater reuse for toilet flushing within a university academic and residential building. Urban Water Management: Challenges and Oppurtunities - 11th International Conference on Computing and Control for the Water Industry, CCWI. 1.

Ilemobade A. (2023). The status of water for firefighting in South Africa. Journal of the South African Institution of Civil Engineering. 65(3). doi.org/10.17159/2309-8775/2023/v65n3a2.

Inarmal N & Moodley B. (2023). Selected pharmaceutical analysis in a wastewater treatment plant during COVID-19 infection waves in South Africa. Environmental Science: Water Research and Technology. 9(6). 1566-1576. 10.1039/d3ew00059a.

Inarmal N & Moodley B. (2025). Removal efficiencies and environmental risk assessment of selected pharmaceuticals and metabolites at a wastewater treatment plant in Pietermaritzburg, South Africa. Environemntal Monitoring and Assessment. 197(1). 10.1007/s10661-024-13515-z.

Kondashov A.A, Bobrinev E.V, Udavtsova E.Y, & Ryumina S.I. (2023). Analysis of Water Consumption during Fire Extinguishing at Objects of Different Functional Fire Hazard Classes. Safety of Technogenic and Natural systems. 10.23947/2541-9129-2023-7-4-30-39.

Kulumba A.M, Afuye G.A, Mazinyo S.P, Zhou L, Adom R.K, Simatele M.D, & Das D.K. (2025). Spatial assessment of climate change, water resource management, adaptation and governance in South Africa. Frontiers in Water. 7. 10.3389/frwa.2025.1376943.

Kuzmina O, Hartrick E, Marchant A, Edwards E, Brandt J.R, & Hoyle S. (2022). Chemical Management: Storage and Inventory in Research Laboratories. ACS Chemical Health and Safety. 29(1). 62-71. 10.1021/acs.chas.1c00086.

Letsoalo M.R, Sithole T, Mufamadi S, Mazhandu Z, Sillapaa M, Kaushik A, & Mashifana T. (2023). Efficient detection and treatment of pharmaceutical contaminants to produce clean water for better health and environmental. Journal of Cleaner Production. 387. 10.1016/j.jclepro.2022.135798.

Li D & Liu S. (2019). Detection of River Water Quality. Basis, Technology and Case Studies: Water Quality Monitoring and Management. 211-220. 10.1016/B978-0-12-811330-1.00007-7.

Li X, Zhang L, Zhang R, Yang M, & Li H. (2021). A semi-quantitative methodology for risk assessment of university chemical laboratory. Journal of Loss Prevention in the Process Industries. 72.10.1016/j.jlp.2021.104553.

Li Y, Shi J, Fan Y, Liang T, & Meng Z. (2022). Research on Safety Risk Assessment and Management System Construction of University Laboratory Based on Structural Equation Model. International Journal of Social Science and Education Research. 5(9). 135-146.10.6918/IJOSSER.292209_5(9).0020.

Lin Y, Li Y, Liao Z, & Deng M. (2024). Analysis and Management of Laboratory Safety Causes in Universities: A Case Study of j University. Advances in Applied Sociology. 14(2).10.4236/aasoci.2024.142006.

Luttik J & Maters E. (2023). Water Management to Cope with the Effects of Climate Change Best practices in Water Management at Wageningen University & Research. IOP Conference Series: Earth and Environmental Science. 10.1088/1755-1315/1194/1/012015.

Madikizela L.M & Ncube S. (2022). Health effects and risks associated with the occurrence of pharmaceuticals and their metabolites in marine organisms and seafood. Science of the Total Environment. 837. 10.1016/j.scitotenv.2022.155780.

Mahler R.L. (2019). University Science-Based Education Positively ImpactsCollege Student Views of Water Issues. Natural Science Education. 48. 10.4195/nse2018.11.0020.

Mahmood R, Hassan N, Chamseddine A, Rangarajan R, & Yassoub R. (2024). Examining Drinking Water Preferences among University Students: A Comparative Assessment. 21(10):1271.10.3390/ijerph21101271.

Malapane T.A, Hackett C, Netshandama V, & Smith J. (2012). Ceramic water filter for point-of-use water treatment in Limpopo province, South Africa. 2012 IEEE Systems and Information Engineering Design Symposium, SIEDS 2012. 10.1109/SIEDS.2012.6215150.

Mamba B.B, Krause R.W, Matsebula B, & Haarhoff J. (2009). Monitoring natural organic matter and disinfection by-products at different stages in two South African water treatment plants. Water SA. 35(1). 121-128.

Manyepa P, Gani K.M, Seyam M, Banoo I, Genthe B, Kumari S, & Bux F. (2024). Removal and risk assessment of emerging contaminants and heavy metals in a wastewater reuse process producing drinkable water for human consumption. Chemosphere. 361. 10.1016/j.chemosphere.2024.142396.

Marhino M, Goncalves M.S, & Kiperstok A. (2014). Water conservation as a tool to support sustainable practices in a Brazilian public university. Journal of Cleaner Production. 62. 98-106. 10.1016/j.jclepro.2013.06.053.

Mazhaundu Z & Mashifana T. (2024). Active pharmaceutical contaminants in drinking water: myth or fact? DURA Journal of Pharmaceutical Sciences. 32(2). 925-945. 10.1007/s40199-024-00536-9.

Mukwevho E.E & Togo M. (2020). Comparative Analysis of Sustainable Practices/Innovations Between University of Pretoria, Gauteng and University of Venda, Limpopo. World Sustainability Series. 585-599. 10.1007/978-3-030-30306-8_35.

Munzhelele E.P, Mudzielwana R, Ayinde W.B, & Gitari W.M. (2024). Pharmaceutical Contaminants in Wastewater and Receiving Water Bodies of South Africa: A Review of Sources, Pathways, Occurrence, Effects, and Geographical Distribution. Water (Switzerland). 16(6). 10.3390/w16060796.

Netshithothole R & Madikizela L.M. (2024). Occurrence of Selected Pharmaceuticals in the East London Coastline Encompassing Major Rivers, Estuaries, and Seawater in the Eastern Cape Province of South Africa. ACS Measurement Science Au. 4(3). 283-293. 10.1021/acsmeasuresciau.4c00004.

Netshithothole R, Managa M, Botha T.L, & Madikizela L.M. (2024). Occurrence of selected pharmaceuticals in wastewater and sludge samples from wastewater treatment plants in Eastern Cape province of South Africa. South African Journal of Chemistry. 78(1).7-14. 10.17159/0379-4350/2024/v78a02.

Newman B.K, Velayudan A, Petrovic M, Alvarez-Munoz D, Celic M, Ndungu K, Madikizela L.M, Chmuka L, & Richards H. (2024). Occurrence and potential hazard posed by pharmaceutically active compounds in coastal waters in Cape Town, South Africa. Science of the Total Environment. 949. 10.1016/j.scitotenv.2024.174800.

Nondlazi S, Ngqwala N.P, Zuma B, & Tandlich R. (2017). Investigating the viability and performance of the pilot scale fly ash/lime filter tower for onsite greywater treatment. Desalination and Water Treatment. 91. 349-364. 10.5004/dwt.2017.21461.

Nsibande L.R, Lehutso R.F, Thwala M, Mzimela H.M.M, Seopela M, & Masikane N.F. (2024). Occurrence of contaminants of emerging concern in the uMhlathuze and uThukela river systems, KwaZulu-Natal, South Africa. African Journal of Aquatic Science. 49(3). 262-274. 10.2989/16085914.2024.2388557.

Nyambiya I, Chapungu L, & Maoela M.A. (2024). Localization of sustainable development goals among non-teaching staff in higher education: the status quo dynamics at great Zimbabwe university. Frontiers in Education. 9. 10.3389/feduc.2024.1389817.

Odjadjare E.C & Olaniran A.O. (2015). Prevalence of antimicrobial resistant and virulent Salmonella spp. in treated effluent and receiving aquatic milieu of wastewater treatment plants in Durban, South Africa. International Journal of Environmental Research and Public Health. 12(8). 9692-9713. 10.3390/ijerph120809692.

Olaniran A.O, Nzimande S.B.T, & Mkize N.G. (2015). Antimicrobial resistance and virulence signatures of Listeria and Aeromonas species recovered from treated wastewater effluent and receiving surface water in Durban, South Africa. BMC Microbiology. 15(1). 10.1186/s12866-015-0570-x.

Olaoluwa A.O, Onu M.A, Ameh V.I, & Ayeleru O.O. (2024). Detection of pharmaceutical pollutants in wastewater. Smart Nanomaterials for Environmental Applications. 405-422. 10.1016/B978-0-443-21794-4.00033-8.

Oluwalana A.E, Musvuugwa T, Sikwila S.T, Sefadi J.S, Whata A, Nindi M.M, & Chaukura N. (2022). The screening of emerging micropollutants in wastewater in Sol Plaatje Municipality, Northern Cape, South Africa. Environmental Pollution. 314. 10.1016/j.envpol.2022.120275.

Paiga P & Delerue-Matos C. (2024). Tracing Pharmaceuticals in Water Systems: Focus on Neurodegenerative and Psychiatric Treatments. Journal of Xenobiotics. 14(4). 1807-1825. 10.3390/jox14040096.

Payne M.K, Nelson A.W, Humphrey W.R, & Straut C.M. (2020). The Chemical Management System (CMS): A Useful Tool for Inventory Management. Journal of Chemical Education. 97(7). 1795-1798. 10.1021/acs.jchemed.9b00905.

Pillay L & Olaniran A.O. (2016). Assessment of physicochemical parameters and prevalence of virulent and multiple-antibiotic-resistant Escherichia coli in treated effluent of two wastewater treatment plants and receiving aquatic milieu in Durban, South Africa. Environmental Monitoring and Assessment. 188(5). 10.1007/s10661-016-5232-4.

Powell N & Larsen R.K. (2012). Integrated water resource management: a platform for higher education institutions to meet complex sustainability challenges. Environmental Education Research. 19(4). 10.1080/13504622.2012.704898.

Reed R. (2006). Waste handling in the brewing industry. Brewing: New Technologies. Woodhead Publishing Series in Food Science, Technology and Nutrition. 335-357. 10.1533/9781845691738.335.

Saito L, Fiedler F, Cosens B, & Kauneckis D. (2012). A vision of interdisciplinary graduate education in water and environmental resources in 2050. Toward a Sustainable Water Future: Visions for 2050. 196-206. 10.1061/9780784412077.

Schronder I, Huang D.Y.Q, Ellis O, Gibson J.H, & Wayne N.L. (2016). Laboratory safety attitudes and practices: A comparison of academic, government, and industry researchers. Journal of Chemical Health and Safety. 12-23. 10.1016/j.jchas.2015.03.001.

SENDAI Framework for Disaster Risk Reduction 2015-2030. (2018). Implementation Guide for Addressing Water-Related Disaster and Transboundary Cooperation: Integrating disaster risk management with water management and climate change adaptation. United Nations, New York.

Sihlahla M & Mndadi S. (2024). A review of occurrence of emerging contaminants and the advanced analytical techniques used for detection and removal of these pollutants in wastewater. Detection and Treatment of Emerging Contaminants in Wastewater. 203-226. 10.2166/9781789063752_0203.

Sihlahla M & Mngadi S. (2024). A review of occurrence of emerging contaminants and the advanced analytical techniques used for detection and removal of these pollutants in wastewater. Detection and Treatment of Emerging Contaminants in Wastewater. 203-226. 10.2166/9781789063752_0203.

Siruma A, Tandlich R, Hornby D, & Srinivas C.S. (2015). Role of higher education institution and community engagement in disaster management in South Africa. International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management, SGEM. 2(5). 783-789. 153979.

Sonawane S.L, Patil V.J, & Tigaa R.A. (2022). Evaluating and Promoting Chemical Safety Awareness in the Chemical Sciences. Journal of Chemical Education. 100(2).469-478. 10.1021/acs.jchemed.2c00102.

Tshivhase M.L & Bisschoff C.A. (2024). Investigating green initiatives at South African public universities. Nurture. 18(2). 245-263. 10.55951/nurture.v18i2.599.

Tziakou E, Fragkaki A.G, & Platis A.N. (2023). Identifying risk management challenges in laboratories. Accreditation and Quality Assurance. 28:167-179.10.1007/s00769-023-01540-3.

Udebuani A.C, Pereao O, Akharame M.O, Fatoki O.S, & Opeolu B.O. (2023). The potential ecological risk of veterinary pharmaceuticals from swine wastewater on freshwater aquatic environment. Water Environment Research. 95(1). 10.1002/wer.10833.

Val L.J, Wisniewski R, & Kallesoe C.S. (2021). Smart water infrastructures laboratory: Reconfigurable test-beds for research in water infrastructures management. Water (Switzerland). 13(13). 10.3390/w13131875.

Valls-Val & Bovea M.D. (2021). Carbon footprint in Higher Education Institutions: a literature review and prospects for future research. Clean Technologies and Environmental Policy. 23(9). 2523-2542. 10.1007/s10098-021-02180-2.

Van Zyl J.E & Haarhoff J. (1997). South African fire water guidelines and their impact on water supply system cost. SAICE Journal. 39(1). 16-22.

Wang D, Pan C, & Wang L.C. (2021). Design and Practice of an Organic ANALYSIS Laboratory to Enhance Laboratory Safety. Journal of Chemical Health and Safety. 28(4). 238-243.10.1021/acs.chas.1c00008.

Wilhelm F.M. (2009). Pollution of Aquatic Ecosystems 1. Encyclopedia of Inland Waters: Reference Module in Earth Systems and Environmental Sciences. 110-119. 10.1016/B978-012370626-3.00222-2.

Wu G, Yang Y, & Xu C. (2023). Determination of University Students' Laboratory Safety Awareness: A Cross Sectional Study. Journal of Chemical Education. 100(9). 3402-3409. 10.1021/acs.jchemed.3c00305.

Yang Q-Z, Deng X-L, & Yang S-Y. (2023). Laboratory Explosion Accidents: Case Analysis and Preventative Measures. ACS Health and Safety. 30(2). 72-82. 10.1021/acs.chas.2c00083.

Zhao A.Y, DeSousa N.E, Henriksen H.C, May A.M, Tan X, & Lawrence D.S. (2024). An Assessment of Laboratory Safety Training in Undergraduate Education. Journal of Chemical Education. 101(4). 1626-1634.10.1021/acs.jchemed.3c01299.

Zhao J, Cui H, Wang G, Zhang J, & Yang R. (2023). Risk assessment of safety level in university laboratory using questionnaire and Bayesian network. Journal of Loss Prevention in the Process Industries.10.1016/j.jlp.2023.105054.

Zhong S, Du J, & Jiang X. (2023). Analysis of Energy Laboratory Safety Management in China Based on the System-Theoretic Accident Model and Processes/System Theoretic Process Analysis STAMP/STPA Model. Sustainability. 15(15). 10.3390/su151511505.

Siphumze Bani - 1, PhD candidate

Contact information (Faculty of Phamarcy, Rhodes University Artillery Road, P.O. Box 94, Makhanda 6140, South Africa)

e-mail:siphumzebani@gmail.com

Roman Tandlich - 2, Associate Professor

Contact information (Disaster Management Programme, Stenden South Africa, 1 Grand Street, Port Alfred 6170, South Africa)

e-mail:roman.tandlich@gmail.com

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.26-31
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

ROZVOJ TRANSVERZÁLNYCH ZRUČNOSTÍ ŠTUDENTOV KRÍZOVÉHO MANAŽMENTU POMOCOU PRÍSTUPU ESP

DEVELOPING TRANSVERSAL SKILLS AMONG CRISIS MANAGEMENT STUDENTS USING THE ESP LANGUAGE APPROACH

KATARÍNA SMOLKOVÁ

ABSTRACT: As crisis management evolves into a more interdisciplinary and high-stakes profession, English for Specific Purposes (ESP) training must adapt with innovative strategies that extend beyond linguistic accuracy. This paper analyses the incorporation of soft skills training into English for Specific Purposes education for students prepared for professions in crisis management. Emphasizing the growing demand for communication, teamwork, critical thinking, and leadership abilities, the study draws on graduate profile descriptors from a selected university faculty and data from the National System of Occupations to identify key competencies required by the labour market. The paper outlines language learning activities designed to foster these soft skills within the ESP classroom and highlights the importance of aligning language instruction with real-world professional expectations. A student questionnaire is introduced as a self-assessment tool, providing insights into learners' awareness and perceived proficiency in specific soft skills. The findings endorse a redefined ESP model that actively facilitates the comprehensive development of future crisis managers.

KEYWORDS: Crisis Management, English for Specific Purposes, Transferable skills, Education, Self-assessment

ÚVOD

V kontexte súčasného pracovného prostredia, charakterizovaného dynamickými zmenami, nástupom technológií umelej inteligencie a globalizačnými procesmi, čelia budúci absolventi vysokých škôl viacerým výzvam prameniacim z ich obmedzenej pripravenosti v oblasti praktických skúseností a profesijných zručností. Medzi ďalšie aspekty, ktoré si zasluhujú pozornosť, je aj vysoká miera konkurencie na trhu práce, finančná neistota a iné systémové obmedzenia. Efektívna reakcia na tieto výzvy si vyžaduje cieľavedomé nadobúdanie a rozvíjanie relevantných zručností, ako aj schopnosť adaptácie na aktuálne trendy a požiadavky trhu práce (Almonte, 2022).

Anglický jazyk predstavuje v súčasnosti dominantný komunikačný nástroj v oblastiach vzdelávania, obchodu, vedy a technológií. Jeho kompetentné ovládanie a používanie výrazne napomáha študentom v prístupe k odborným informáciám, sledovaniu aktívnych vývojových trendov na medzinárodnom trhu práce, pričom zvyšuje ich konkurencie schopnosť v rámci profesijného uplatnenia sa. Hlavný cieľ výučby anglického jazyka ako cudzieho jazyka prestavuje získanie komunikačnej kompetencie, ktorá pozostáva zo štyroch čiastkových kompetencií – gramatickej, sociolingvistickej, diskurzívnej a strategickej (Hymes, 1972). Výučba anglického jazyka v súčasnom kontexte do veľkej miery presahuje tradičné zameranie sa na najmä gramatickú kompetenciu.

1. ANALÝZA POTRIEB A METODOLÓGIA

S cieľom reagovať na dynamicky sa meniace požiadavky súčasného trhu práce, predstavuje výučba angličtiny ako cudzieho jazyka na UNIZA (ÚCV – Zameranie, 2025) zameraná na výučbu angličtiny pre špecifické účely (ang. ESP – English for Specific Purposes), teda prakticky orientovaný didaktický prístup. Prispôsobením jazykového vzdelávania konkrétnym odborným a komunikačným potrebám študenta daného odboru ESP zabezpečuje, že učiaci sa si osvojujú nielen jazykové kompetencie (schopnosti, ktoré charakterizuje vynikajúci výkon v niektorej oblasti činnosti) (Hrmo &Turek, 2003), ale

aj schopnosť efektívne sa uplatniť v autentických profesionálnych situáciách. Z toho vyplýva, že prístup k výučbe cudzieho jazyka podľa ESP v oblasti krízového manažmentu rozvíja vyššie uvedené čiastkové kompetencie nasledovne:

- Gramatická kompetencia – teda schopnosť používať správne gramatické štruktúry, syntax, grafémy a výslovnosť. Tento prístup umožňuje krízovým manažérom presne a jasne komunikovať príkazy, protokoly a technické informácie, čím sa znižuje pravdepodobnosť nesprávneho výkladu v kritických situáciách.
- Sociolingvistická kompetencia – inými slovami schopnosť vhodne používať jazyk v daných sociálnych a kultúrnych situáciách. V oblasti krízového riadenia je táto schopnosť nevyhnutná pre komunikáciu s rôznymi zainteresovanými stranami, napr. miestne obyvateľstvo, zahraniční partneri alebo záchranné zložky štátu.
- Diskurzívna kompetencia – predstavuje schopnosť produkovať a interpretovať koherentné a súdržné jazykové prejavy v ústnej a písomnej forme. V oblasti krízovej komunikácie zohráva diskurzívna kompetencia zásadnú úlohu pri tvorbe prehľadných a logicky usporiadaných brífingov, správ a operačných hlásení. Efektívna krízová komunikácia si vyžaduje nie len vecnú presnosť, ale aj zrozumiteľnú štruktúru výkladu, ktoré napomáhajú recipročnému porozumeniu medzi účastníkmi komunikácie.
- Strategickú kompetencia – označuje schopnosť zvládať komunikačné zlyhanie a optimalizovať efektívnosť interakcie v rôznych kontextoch. V krízových situáciách, najmä v prostredí charakterizovanom neistotou, je táto strategická kompetencia mimoriadne dôležitá. Odborníci v oblasti krízového manažmentu musia byť schopní flexibilne prispôsobiť svoje vyjadrenia, objasniť prípadné nedorozumenia a uplatňovať kompenzačné stratégie, napr. re-formulácia výpovedí, prispôsobenie jazykových prostriedkov recipientovi alebo použitie efektívnych vizuálnych a gestikulárnych náznakov – s cieľom zachovať funkčnosť a zrozumiteľnosť komunikácie aj v podmienkach obmedzených jazykových zdrojov.

Pri výučbe cudzieho jazyka pre špecifické účely predstavujú zručnosti, teda „nadobudnuté pohotovosti správne čo najrýchlejšie a s čo najmenšou námahou vykonávať určitú činnosť na základe osvojených vedomostí (Petlák, 1997), kľúčový koncept (Woodrow, 2018). Na základe uvedeného možno konštatovať, že výučba anglického jazyka s prístupom ESP je základom pre rozvíjanie transverzálnych (prenositeľných) zručností učiacich sa.

Na určenie požiadaviek na zručnosti študentov v odbore Krízový manažment na Fakulte bezpečnostného inžinierstva (FBI) Žilinskej univerzity v Žiline (UNIZA) a na revíziu vzdelávacích programov bol zvolený nasledujúci dvoj-krokový proces:

1. Analýza transverzálnych zručností absolventov slovenských univerzít (Horný, Ďurina & 2016),
2. Profil absolventa odboru krízový manažment (FBI – Profil absolventa, 2025).

Analýza P. Horného a J. Ďurinu, ktorá predstavuje náš primárny zdroj, poskytuje rozsiahly prehľad tejto problematiky. Hoci autori (Horný & Ďurina, 2016) uvádzajú, že nie je možné identifikovať jednu hlavnú transverzálnu zručnosť, ktorá zaručí úspech na pracovnom trhu, vo všeobecnosti existuje pozitívna korelácia medzi transverzálnymi zručnosťami a profesionálnym úspechom jednotlivca. Odborná publikácia identifikovala najžiadanejšie kompetencie absolventov nasledovne:

- Schopnosť prevziať zodpovednosť,
- Schopnosť identifikovať a riešiť problémy,
- Schopnosť zvládať stresové situácie,
- Proaktívny prístup,
- Práca s informáciami,
- Schopnosť robiť nezávisle rozhodnutia,
- Schopnosť kreatívne a flexibilne myslieť a konať,
- Schopnosť pracovať v tíme,
- Znalosť cudzích jazykov,
- Schopnosť pracovať v interkultúrnom prostredí.

Krízový manažment sa vyznačuje interdisciplinaritou, pričom spája koncepty z oblasti riadenia rizík, vzťahu s verejnosťou, psychológie a komunikácie. Absolvent študijného programu Krízový manažment sa v rámci inžinierskeho štúdia špecializuje na krízové riadenie a ochranu obyvateľstva. Môže pôsobiť ako krízový manažér v štátnej správe, samospráve, v podnikovej bezpečnosti, riadení rizík a krízovom manažmente v podniku. Na všetkých pracovných pozíciách sú absolventi schopní zabezpečiť riadenie kontinuity činností, zlepšovanie kvality manažérskych systémov a prevádzky. Sú kvalifikovaní na vykonávanie manažérskych činností spojených s riadením procesov, vedením jednotlivcov a pracovných tímov, ako aj komunikáciu a konzultácie s rôznymi zainteresovanými stranami. Okrem toho vedú, motivujú a hodnotia podriadených zamestnancov, pričom zabezpečujú ich vzdelávanie a ďalší rozvoj.

Na základe porovnania údajov uvedených v oboch zdrojoch, možno identifikovať najžiadanejšie transverzálne zručnosti budúcich absolventov:

- Schopnosť vedenia ľudí,
- Schopnosť identifikovať a riešiť problémy,
- Schopnosť robiť nezávisle rozhodnutia,
- Schopnosť adaptácie a flexibility,
- Organizácia a plánovanie práce.

2. VÝSLEDKY

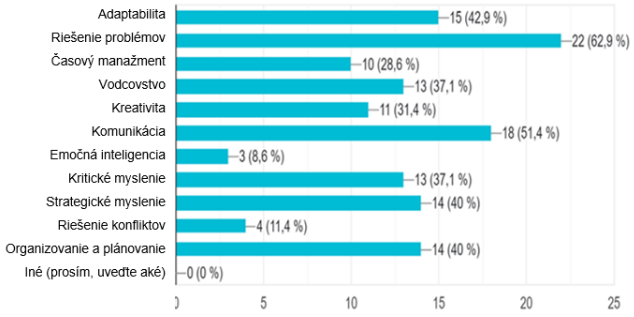
Výskumný dotazník bol koncipovaný s cieľom identifikovať mieru sebauvedomenia a sebahodnotenia študentov v súvislosti s významom transverzálnych zručností (tzv. prenosných kompetencií) v ich budúcom profesijnom pôsobení. Zber dát prebiehal v zimnom semestri akademického roka 2023/2024 medzi študentmi 4. a 5. ročníka dennej formy štúdia študijného programu Krízový manažment na Fakulte bezpečnostného inžinierstva Žilinskej univerzity v Žiline. Po aplikácii účelového výberu respondentov bol dotazník distribuovaný prostredníctvom oficiálnych univerzitných e-mailových adries. Výskumný súbor tvorilo 35 študentov, ktorých odpovede bolo možné považovať za validné.

Úvodná časť dotazníka sa zameriavala na zisťovanie profesijných záujmov študentov, konkrétne ich motivácie a očakávaní v súvislosti s budúcim zamestnaním. Východiskovým predpokladom bolo, že respondenti prejavia silný záujem v oblasti pracovného uplatnenia v odbore, ktorý zodpovedá ich vysokoškolskému vzdelávaniu. Tento predpoklad sa potvrdil – 69 % účastníkov výskumu uviedlo záujem o prácu v oblasti zodpovedajúcej ich štúdiu. Zvyšných 31 % respondentov zvolilo možnosť „neviem/ možno“, čo poukazuje na istú mieru neistoty alebo otvorenosť voči alternatívnym profesijným smerovaniam.

V druhej časti výskumu mali študenti na výber maximálne tri odpovede na štyri predložené otázky:

1. Ktoré zručnosti považujete za najdôležitejšie pre váš budúci kariérny úspech?

Výsledky sú zobrazené na nižšie uvedenom obrázku.



Obrázok 1 Zručnosti pre budúci úspech

Podľa výsledkov výskumu nadpolovičná väčšina respondentov (63 %, teda 22 z 35 odpovedí) považuje schopnosť riešiť problémy za kľúčovú vlastnosť pre úspešné uplatnenie na trhu práce. Ďalej sa za významné zručnosti považujú schopnosť prispôsobiť sa (43 %) a komunikačné zručnosti (51 %). Naopak, najnižšiu váhu respondenti prisudzujú emocionálnej inteligencii, ktorú považuje za dôležitú približne 9 % účastníkov.

2. Ktoré zručnosti považujete za tie, ktoré ste doposiaľ najviac rozvíjali?

Takmer polovica respondentov (49 %) označila možnosť schopnosti v oblasti organizovania a plánovania. Na druhom mieste sa umiestnili dve zručnosti – komunikácia a kritické myslenie, obe s hodnotou 43 %. Tretie miesto patrí opätovne dvom zručnostiam, teda prispôsobivosti a riešeniu problémov, pričom každá dosiahla hodnotu 37 %. Rovnako ako v prvej otázke, aj v tomto prípade bola za najmenej rozvinutú schopnosť označená emocionálna inteligencia.

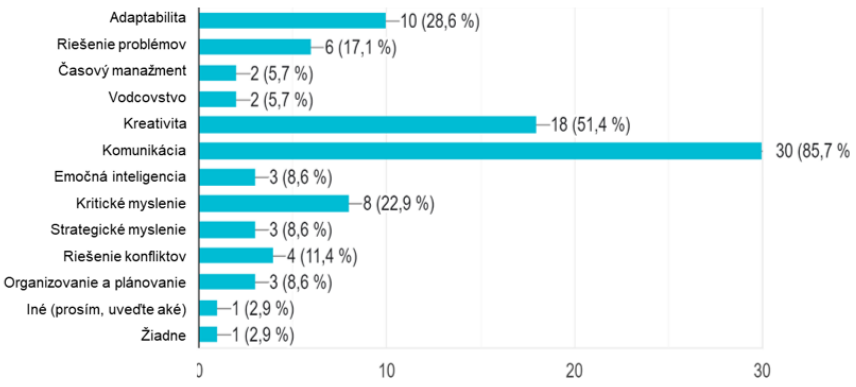
Tretia otázka sa zameriavala na identifikáciu zručností, ktoré je potrebné zdokonaliť:

3. Ktoré zručnosti považujete za tie, ktoré je potrebné najviac zdokonaliť?

V tejto oblasti boli najčastejšie vybrané odpovede pomerne podobné. Takmer polovica (46 %) považuje časový manažment za zručnosť, na ktorej zlepšení by sa mali najviac sústrediť, pričom túto možnosť zvolilo 16 zo 35 študentov. Na druhom mieste sa umiestnili vedenie ľudí a komunikácia, pričom každá z týchto zručností získala 40 % hlasov. Naopak, prispôsobivosť bola vyhodnotená ako zručnosť, na ktorú nie je potrebné zameriavať pozornosť.

Posledná otázka sa týkala zručností nadobúdaných počas hodín anglického jazyka:

4. Ktoré zručnosti považujete za tie, ktoré ste rozvíjali počas seminárov anglického jazyka?



Obrázok 2 Zručnosti nadobudnuté počas seminárov cudzieho jazyka

Ako je zobrazené na Obr. 2, najviac respondentov vyjadrilo preferenciu rozvoja komunikačných zručností. Až 86 % respondentov (30 z 35) identifikovalo túto zručnosť ako tú, ktorú majú príležitosť rozvíjať v rámci výučby cudzích jazykov. Viac než polovica účastníkov prieskumu (51 %, 18 z 35) uviedla, že sa zameriavajú na rozvíjaní svojej kreativity, zatiaľ čo 28 % respondentov (10 z 35) si vybralo prispôsobivosť. Na rozdiel od toho študenti vnímajú nedostatok príležitostí na rozvoj schopností časového manažmentu a vedenia ľudí v rámci hodín anglického jazyka.

3. UČEBNICA *ENGLISH FOR CRISIS MANAGEMENT*

Na základe nastavenia jazykovej výučby na UNIZA, ako aj podrobnej analýzy relevantných dokumentov a výsledkov dotazníka, bola vypracovaná vysokoškolská učebnica s názvom *English for Crisis Management* (Môcová & Smolková & Kovács, 2025).

Cieľom učebnice je pripraviť študentov inžinierskeho stupňa na požiadavky profesionálnej praxe a pracovného života. Publikácia spája konceptualizáciu výučby anglického jazyka pre špecifické účely (ESP) s problematikou krízového manažmentu, pričom sa zameriava na rozvoj mäkkých a prenositeľných zručností a osobnostný rozvoj učiacich sa (Kulla, 2025). Učebnica integruje aplikovanú lingvistiku, metodológiu výučby odborného jazyka a rozvoj transverzálnych zručností. Autori kladú mimoriadny dôraz na terminologickú presnosť, praktickú relevantnosť a aktuálnosť vybraných tematických oblastí. Učebnica je ako študijný materiál určená najmä pre študentov Krízového manažmentu a príbuzných odborov. Rozsah učebnice *English for Crisis Management* je zložený z 20 kapitol – pokrýva teda obsahovú náplň pre minimálne dva semestre vysokoškolskej výučby. Krízový manažment, ako interdisciplinárna vedná disciplína, pokrýva široké spektrum tém. Z toho dôvodu obsah učebnice charakterizuje rozmanitosť tém, od štátnej bezpečnosti (napr. Unit 19 – *Integrated Rescue System in Slovakia*), krízových situácií (napr. Unit 20 – *Mass Casualty Incidents*) podnikového riadenia (napr. Unit 8 – *Cutting Business Costs*), pracovného rozvoja (napr. Unit 9 – *A Happy Workplace*), ľudského zdravia (napr. Unit 15 – *First Aid*), rozvoja samotných transverzálnych zručností (napr. Unit 6 – *Leadership*) po osobnostný rozvoj (napr. Unit 2 – *Your Life Passion*). Pri samotnom koncipovaní učebnice *Eglish for Crisis Management* bol využitý model navrhovania výučbových materiálov podľa T. Hutchinsona a A. Watersa (1987). Obsah každej kapitoly bol štruktúrovaný v nasledujúcom poradí: lead-in (úvod), imput (vstup), practice (precvičovanie), production (produkcia), review (zhrnutie).

Pokiaľ ide o metódy, aktivity a techniky práce, učebnice *English for Crisis Management* reflektuje všetky stupne Bloomovej taxonómie kognície (Anderson a kol., 2001), pričom sa zameriava najmä na zručnosti vyššieho rádu, teda analýzu, tvorbu a hodnotenie, ktorých rozvoj je nevyhnutný pre získavanie samotných transverzálnych zručností. Rozvíjanie mäkkých zručností u študentov prebieha efektívne prostredníctvom interaktívnych a na študenta orientovaných vyučovacích metód, akými sú práca vo dvojiciach a skupinách, projektovo orientované vyučovanie či simulácie kritických situácií. Uvedené prístupy podporujú posilňovanie komunikačných a kooperatívnych schopností, schopnosti riešiť problémy, adaptability a i. Sebahodnotenie a vzájomné hodnotenie medzi študentmi napomáhajú formovaniu reflexie a zodpovednosti, zatiaľ čo personalizácia aktivít zvyšuje ich angažovanosť a motiváciu. Kolaboratívne formy učenia zároveň vytvárajú priestor pre rozvoj vyjednávacích zručností, empatie a vodcovských kompetencií. Tieto stratégie poskytujú autentické situácie, v ktorých si študenti osvojujú a upevňujú transverzálne zručnosti nevyhnutné pre ich osobný a profesionálny rozvoj.

ZÁVER

Analýza údajov v rámci výskumu potvrdzuje, že implementácia ESP v cudzojazyčnej výučbe predstavuje významný nástroj na rozvoj odbornej jazykovej spôsobilosti študentov v oblasti krízového manažmentu, ako aj transverzálnych kompetencií, ktoré sú nevyhnutné pre úspešné uplatnenie sa na trhu práce. Napriek obmedzenej veľkosti výskumného súboru a potreby ďalšej analýzy, výsledky dotazníkového výskumu realizovaného medzi študentmi druhého stupňa štúdia na Fakulte bezpečnostného inžinierstva na Žilinskej univerzity v Žiline potvrdzujú, že respondenti za kľúčové pre svoju budúcu kariéru považujú najmä schopnosť rieši problémy, schopnosť komunikovať a byť flexibilní. Zároveň identifikovali komunikáciu ako zručnosť, ktorú mali možnosť najintenzívnejšie rozvíjať počas seminárov cudzieho jazyka. Tieto zistenia boli premietnuté to vysokoškolskej učebnice *English for Crisis Management*, ktorá bola navrhnutá ako prostriedok na rozvíjanie mäkkých zručností v uvedenom študijnom odbore. Učebnica prostredníctvom simulácií, kooperatívnych aktivít, vzájomného hodnotenia sa personalizovaných aktivít napomáha rozvoju vyšších kognitívnych procesov a praktických kompetencií relevantných pre profesijné pôsobenie v oblasti krízového riadenia. Tento model výučby reflektuje aktuálne výzvy vo vzdelávacom a spoločenskom kontexte a zároveň poskytuje aplikovateľný rámec pre ďalšie odborné disciplíny, ktorých zámerom je systematicky prepojiť jazykové vzdelávanie so získavaním transverzálnych kompetencií.

POĎAKOVANIE

Tento článok vznikol s podporou Slovenskej národnej grantovej agentúry KEGA v rámci projektu: KEGA 007ŽU-4/2023 Job Labs – Výučba cudzích jazykov pre potreby trhu práce na UNIZA.

LITERATÚRA

Almonte, R. (2022). *A practical guide to soft skills: Communication, psychology, and ethics for your professional life*. Routledge. *https://doi.org/10.4324/9781003212942*

Anderson, L. W., & Krathwohl, D. R. (Eds.). (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives. Longman.

Horný, P., & Ďurina, J. (2016). Transferable competences of Slovak university graduates. CVTI. Retrieved from https://www.vysokoskolacidopraxe.sk/files/horny_durina_prenositelnekompetencie-absolventov-slovenskych-vs.pdf

Hutchinson, T., & Waters, A. (1987). English for specific purposes: A learning-centred approach. Cambridge University Press.

Hrmo, R. & Turek, I. 2003. Kľúčové kompetencie 1. Bratislava: STU.

Hymes, D. (1972). On communicative competence. In J. Pride & J. Holmes (Eds.), Sociolinguistics (pp. 269–285). Penguin Books.

Kulla, A. (2025). Book review – Lenka Môcová, Katarína Smolková, Éva Kovács: English for crisis management. Apps - Academic Journal of Applied Linguistics and Languages, 3(1), 48–49. Retrieved from https://ojs.tuzvo.sk/index.php/apps/article/view/143

Môcová, L., Smolková, K., & Kovács, É. (2025). English for crisis management. Vydavateľstvo EDIS. https://doi.org/ISBN 978-80-554-2183-4

Petlák, E. 1997. Všeobecná didaktika. Bratislava: Iris.

Woodrow, L. (2018). Course design in English for specific purposes. Routledge. https://doi.org/ISBN 798-1-138-10067-1

Národný systém povolaní (n.d.). Register povolaní. Retrieved from https://www.sustavapovolani.sk/register-zamestnani

Profil absolventa. (n.d.). Fakulta bezpečnostného inžinierstva, Žilinská univerzita v Žiline. Retrieved from https://fbi.uniza.sk/uploads/files/1676016750-ing-km-profilabsolventa

Ústav celoživotného vzdelávania, UNIZA. (n.d.). Zameranie. Retrieved from: https://ucv.uniza.sk/cudzie-jazyky/zameranie/

Katarína Smolková, Mgr.

Žilinská univerzita v Žiline, Ústav celoživotného vzdelávania – Sekcia cudzích jazykov, Univerzitná 8215/1, 010 26, Žilina, Slovensko

katarina.smolkova@uniza.sk

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.32-41
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

PROTECTION OF ENCLOSED UNIVERSITY FACILITIES IN THE EUROPEAN UNION AGAINST CBRN THREATS: LESSONS LEARNED FROM PAST INCIDENTS AND PREPAREDNESS STRATEGIES

JOSEF RAJDL, JOZEF SABOL

ABSTRACT: *The paper examines the protection of enclosed university facilities in the European Union against chemical, biological, radiological and nuclear (CBRN) threats. It analyses key incidents, such as the 2001 explosion at the AZF factory in Toulouse, the 2018 Novichok poisonings, and the 2018 ricin attack in Cologne. It explores current preparedness measures, including training initiatives and infrastructural improvements inspired by these events. The 2023 shooting at the Faculty of Arts of Charles University in Prague serves as a case study, highlighting the need for rapid response, effective communication and psychological support. The paper also proposes specific measures to enhance the security of universities and other higher education institutions. These measures include, among others, detection systems, entry control systems and cooperation with local authorities and agencies, aiming to minimise the risks posed by both CBRN and conventional threats.*

KEYWORDS: *CBRN threats, university security, emergency preparedness, decontamination, Charles University shooting.*

INTRODUCTION

Universities face increasing CBRN-related risks, yet documented university-specific incidents are very sparse. Therefore, this paper analyses analogous public-space CBRN incidents to extract lessons relevant to enclosed academic environments. Such incidents—though they occur in industrial, business, or political contexts—reveal vulnerabilities directly applicable to universities, where enclosed spaces, high population density, and laboratory activities elevate risk.

This paper explores how enclosed university environments across the European Union (EU) are increasingly vulnerable to unconventional threats—specifically chemical, biological, radiological, and nuclear (CBRN) hazards. Drawing on high-profile incidents such as the 2001 Toulouse, France Azote Fertilisant (AZF) factory explosion, the 2018 Novichok poisonings in the United Kingdom, and the attempted 2018 ricin attack in Cologne, Germany, the analysis highlights how such events, though not always university-centred, offer critical lessons for academic settings.

The 2023 mass shooting at Charles University in Prague is presented as a case study to illustrate the broader implications of emergency readiness in educational institutions. The paper assesses universities' existing preparedness, examines gaps in infrastructure and training, and evaluates national and EU-level coordination frameworks. In doing so, it sheds light on the developing concept of campus resilience, including both physical safeguards and psychological response strategies.

This paper is based primarily on results and analyses from the UNICOPS project. References to eNOVATION project, the EU Centres of Excellence (CoE), and national emergency plans such as the UK's National CBRN governance arrangements and France's Plan ORSEC serve only to illustrate complementary EU-level training resources.

1. CBRN INCIDENTS IN THE EUROPEAN UNION

Although major intentional CBRN attacks on European university campuses remain rare, documented events such as discoveries of legacy radioactive sources and chemical-reaction evacuations show that academic institutions nevertheless face tangible hazards. The four cases published on the following pages underline the need for systematic hazardous-materials inventories, regular audits of legacy equipment and stocks, rigorous lab ventilation and maintenance programmes, tailored incident response plans, and improved governance of technology parks and spin-off research facilities.

1.1 Discovery of radioactive sources at the University of Bordeaux, France, 2015

On 18 September 2015, staff at a joint INSERM (French National Institute of Health and Medical Research) / University of Bordeaux laboratory discovered two previously undocumented sealed radioactive sources in a research room. The event was reported to the French Nuclear Safety Authority (ASN) and declared a Level-2 incident; incident follow-up included radiological monitoring, characterisation of the sources, dose assessments for potentially exposed personnel and implementation of ASN-requested corrective measures. This case highlights the persistent risk of *legacy* or forgotten radioactive sources in older research facilities and underscores the need for systematic inventories, decommissioning protocols, and periodic radiological audits in university laboratories.

1.2 Discovery of legacy radioactive sources and residual contamination at University Hospitals of Strasbourg, France

Inspections in 2020–2021 at buildings operated by the University Hospitals of Strasbourg revealed legacy radioactive sources and localised residual contamination tied to historical medical radiotherapy and research activities dating back many decades. The case required radiological characterisation, mapping of contamination points, packaging and removal of legacy sources, and dosimetry evaluations for workers — demonstrating that legacy radiological hazards may persist at university-affiliated sites and require dedicated resources to identify and remediate them before reuse or refurbishment of older buildings.

1.3 Evacuation after chemical reaction at Radboud University, Netherlands, 2023

On 29 August 2023, a chemical reaction in a laboratory inside the Mercator III building on the Radboud University campus (Nijmegen) released fumes that prompted an immediate evacuation of the building and the attendance of the local fire service and hazardous-materials responders. No serious injuries were reported; the affected laboratory was sealed for cleaning and specialist remediation before re-use. The event emphasises that routine laboratory operations in university campuses can produce sudden airborne chemical hazards in multi-use buildings and underlines the importance of robust ventilation maintenance, spill-response plans and well-rehearsed evacuation procedures.

1.4 Explosion at the New University of Lisbon technology park, Portugal, 2024

On 4 July 2024, an explosion occurred in the technology-park area of the Faculty of Science and Technology at the New University of Lisbon, Caparica (Almada), with emergency services mobilised and at least one fatality reported. The event (investigated by national authorities) illustrates that larger-scale accidents — including those involving prototype systems, gas or pressurised containers or process equipment in university innovation parks — can produce consequences similar to industrial incidents and therefore require that campus risk governance covers technology parks, spin-off labs and incubators in addition to conventional teaching and research spaces.

Specific CBRN contamination incidents in EU university facilities, such as lecture halls or libraries, are not widely documented, likely because of their rarity or sensitivity. However, several notable CBRN-related incidents in the EU provide critical context for understanding the broader threat landscape and its implications for educational institutions. Starting on the next page are key examples, their circumstances, substances involved, decontamination procedures, and lessons learned.

1.5 TOULOUSE AZOTE FERTILISANT (AZF) FACTORY EXPLOSION IN 2001

The September 2001 explosion at the AZF factory in Toulouse, France**,** which killed 31 people and injured thousands, brought to the public's attention the critical need for stringent chemical storage regulations in urban areas. The Seveso III Industrial Safety Protocol (Directive 2012/18/EU) had to be revised to enhance risk management for facilities handling hazardous substances. Emergency services focused on evacuating affected areas, treating respiratory and ocular injuries, and monitoring air quality.

Contaminated areas were cleaned using water-based solutions to neutralise chemical residues. Long-term efforts included soil and water remediation to address environmental contamination. The incident emphasised the need for urban planning to separate industrial zones from educational institutions, reducing exposure risks. Regular audits of nearby industrial facilities and collaboration with local authorities are now seen as essential for campus safety. For universities, this highlighted the importance of preparing for external chemical threats, such as airborne contaminants, that could affect campus facilities. Universities must implement air quality monitoring systems and rapid evacuation protocols to protect students and staff. Training programs should include scenarios for chemical spills to ensure preparedness for such external threats.

1.6 NOVICHOK POISONINGS IN MARCH 2018

These poisonings took place in Salisbury, UK, of Sergei Skripal and his daughter, Yulia Skripal, demonstrating the challenges of identifying and containing chemical agents in public spaces. See Fig.1 below.

Figure 1 Individuals in protective suits and a tent covering the bench where Skripal collapsed (Authors, 2025)

Novichok is a highly toxic nerve agent developed for chemical warfare. The incidents, involving a nerve agent, led to severe health impacts and international diplomatic tensions. Universities can apply these lessons by installing chemical detection systems in high-traffic areas, such as lecture halls and laboratories. Staff training on recognising symptoms of chemical exposure, such as respiratory distress or neurological symptoms, is crucial for early intervention. Rapid response protocols, including coordination with local hazmat teams, should be established to contain contamination. The incidents also highlighted the need for secure storage of research chemicals to prevent misuse. Public awareness campaigns can educate campus communities about reporting suspicious substances, enhancing overall safety. These proactive measures reduce the risk of chemical threats on campuses.

Decontamination efforts involved sealing off affected areas, including public spaces and buildings, and using specialised chemical neutralisation agents. Responders wore Level A hazmat suits, and contaminated objects were removed or destroyed. Public health campaigns informed residents about the risks of secondary exposure.

1.7 POLONIUM-210 POISONING IN 2006

In November 2006, Alexander Litvinenko was poisoned with Polonium-210 in London. Po-210 is a highly radioactive isotope causing severe radiation poisoning. This incident exposed the insidious nature of radiological threats, which are difficult to detect without specialised equipment. Universities must invest in radiation detectors for laboratories and public spaces to mitigate similar risks. Training personnel in radiological safety protocols, including handling and disposal of radioactive materials, is essential. The incident also underscored the importance of international cooperation in tracking radiological

substances, as universities often collaborate globally on research. Emergency response plans should include procedures for isolating contaminated areas and providing medical support. Public health campaigns can raise awareness about radiological risks, ensuring a proactive approach to safety. Regular drills simulating radiological incidents can further enhance preparedness and protect campus communities from such threats.

Affected areas, including hotel rooms and public spaces, were sealed and decontaminated using specialised radiological cleaning techniques, including HEPA (high-efficiency particulate air) filtration, vacuuming, and chemical washing. Contaminated materials were disposed of as radioactive waste.

1.8 RICIN PLOT IN COLOGNE IN 2018

The ricin plot, uncovered on 12 June 2018 in Cologne, Germany, involved a Tunisian extremist, Sief Allah H. He produced ricin, a biological toxin derived from castor beans, capable of causing severe organ damage. This marked the first time a jihadi terrorist in the West successfully created this biological agent for a planned terrorist attack. See Fig. 2 below.

The plot was swiftly resolved when the suspect was arrested in his apartment, highlighting the effectiveness of electronic surveillance and intelligence sharing. As the plot was intercepted before execution, no actual contamination occurred. However, preparedness measures included plans for biological decontamination, such as using bleach-based solutions and isolating affected areas.

Figure 2 Police officers wear protective clothes and respiratory masks during the operation on June 12, 2018, in Cologne, Germany (Authors, 2025)

Universities must implement strict access controls for laboratories handling biological agents, with biometric security and regular audits. Monitoring online communications for radicalisation is critical, as the Islamic State inspired the suspect. Training programs should include protocols for identifying and reporting suspicious activities to ensure early intervention. These measures strengthen university defences against biological threats.

The incident underscored the need for vigilance in monitoring hazardous substances and securing research facilities. Universities with laboratories handling biological agents must implement strict access controls and monitoring systems. These incidents, while not directly involving universities, demonstrate the diverse nature of CBRN threats and their relevance to enclosed public spaces, including educational institutions. The lack of specific university incidents suggests that such events are either rare or not publicly reported, necessitating a focus on preparedness and lessons from broader CBRN events.

1.9 POLIO INCIDENT IN THE NETHERLANDS IN 2022

Utrecht Science Park/Bilthoven is a research hub in the Netherlands, hosting facilities that study infectious diseases. The 2022 poliovirus incident in the Netherlands revealed the importance of wastewater monitoring for early detection of biological contaminants. Regular wastewater testing can provide early warnings of biological threats, allowing for rapid containment and was intensified after the incident. Universities with research facilities that handle pathogens must ensure up-to-date vaccination status for laboratory personnel to prevent outbreaks. Collaboration with public health authorities is essential to align university protocols with national guidelines. Training should include biosafety measures, such as proper handling and disposal of biological agents. Public awareness campaigns can

educate students and staff about the importance of vaccination, reducing the risks of spreading disease. These strategies enhance university preparedness for biological incidents, ensuring campus safety.

2. PREPAREDNESS MEASURES IN EU UNIVERSITIES FOR CBRN THREATS

Past CBRN incidents, such as the Toulouse, France AZF factory explosion and the Cologne ricin plot, have significantly shaped up university preparedness strategies. These events highlighted the need for enhanced laboratory security, including biometric access controls and regular audits of hazardous materials. Regular training and drills for staff and students, simulating CBRN scenarios, have become standard to ensure rapid response capabilities. Collaboration with national and local emergency services, as seen in the response to the Charles University shooting, ensures coordinated action during crises. Investments in detection equipment, such as chemical and radiation sensors, and decontamination facilities reflect lessons from incidents like the Novichok poisonings, emphasising proactive safety measures.

The first EU CBRN CoE (Centre of Excellence) initiative was formally launched in 2010. The CoE supports partner countries in mitigating CBRN risks through capacity building and training. Universities benefit from access to advanced research on CBRN defence technologies, such as portable chemical detectors and decontamination systems. The initiative fosters interagency collaboration, enabling universities to align with national security frameworks. For example, universities in Germany have adopted the CoE guidelines to enhance laboratory safety post the Cologne ricin plot. Training programs developed through the CoE equip faculty with the skills to handle CBRN incidents, thereby improving campus resilience. Partnerships with regional centres ensure access to cutting-edge resources, reducing response times during emergencies. Universities should integrate the CoE best practices into their emergency plans, ensuring compliance with EU standards. Regular workshops with the CoE experts can further enhance preparedness, making universities proactive in addressing CBRN threats.

National emergency plans, such as the UK's national CBRN governance arrangements and France's Plan ORSEC, include protocols for CBRN incidents. Universities are required to integrate these plans into campus-specific procedures and coordinate with local authorities. For instance, the Netherlands universities adopted wastewater monitoring protocols following the 2022 polio incident. The EU civil protection mechanism facilitates cross-border cooperation and provides guidelines for managing CBRN threats. Universities can adapt these for campus use, establishing clear lines of command. Audits are conducted regularly to ensure compliance with national standards. Joint exercises with emergency services enhance preparedness. These measures reflect lessons from past incidents, ensuring robust response capabilities in future. Universities should also participate in national CBRN simulations to test their protocols and improve readiness for real-world scenarios.

Universities develop tailored emergency response plans that include evacuation, decontamination, and communication procedures. For example, the University of Copenhagen conducts annual CBRN drills, simulating chemical spills. These plans designate decontamination zones and secure storage for hazardous materials used in research. CBRN response teams, composed of trained faculty and staff, are established to manage crises. Regular audits ensure compliance with safety standards, while student orientation programs include safety briefings. Lessons from the explosion at the AZF factory in Toulouse emphasise the need for clear evacuation routes and communication systems. Universities should invest in mobile applications to deliver real-time alerts, improving response efficiency. Collaboration with local fire and hazmat teams can further streamline emergency responses, ensuring campus safety during CBRN incidents.

Regular training and drills are critical to prepare university communities for CBRN threats. The eNOVATION initiative, coordinated by the Belgian national crisis centre, develops advanced training methods for first responders, which universities can adopt. For example, German universities conduct biannual CBRN drills, involving police and hazmat teams. These exercises simulate scenarios as chemical leaks, thus ensuring staff and students are familiar with protocols. Training includes recognising symptoms of chemical or biological exposure and improving early detection. Post-incident reviews, as seen after the Cologne ricin plot, refine training programs. Universities should increase drill frequency and include students to enhance community resilience. Partnerships with national training programs can provide access to advanced simulation tools, improving preparedness.

Infrastructure upgrades have been implemented in several universities, including the installation of advanced air filtration systems, secure storage facilities, and decontamination zones. Loughborough University installed radiation detectors in laboratories soon after the Polonium-210 incident. Air sampling

devices, inspired by the explosion at the AZF factory in Toulouse, mitigate chemical risks. Biometric access controls prevent unauthorised laboratory access, a lesson from the Cologne ricin plot. Regular maintenance ensures equipment reliability, while partnerships with technology providers enhance capabilities. Universities should prioritise funding for these upgrades to ensure compliance with EU safety standards and reduce vulnerabilities. Regular infrastructure audits can identify gaps, ensuring campuses are equipped to handle CBRN threats effectively.

3. Case Study - Shooting Incident at Charles University

On December 21, 2023, a tragic shooting occurred at the Faculty of Arts of Charles University in Prague, resulting in 14 deaths and 25 injuries. The gunman, a 24-year-old postgraduate student named David Kozák, was found dead at the scene, having committed suicide after being confronted by police. This incident, while not a CBRN event, provides critical insights into emergency response in university settings and offers a basis for comparison with potential CBRN incidents. Some students, who escaped from the shooting, are trying to find a safe place and are shown in Figure 3 below.

The shooting began at approximately 15:00 local time in the Faculty of Arts building, located in Jan Palach Square, a popular tourist area in Prague's historic Old Town. Student David Kozák, armed with a rifle and other weapons, targeted students and staff in classrooms and corridors. The attack was described as a premeditated violent act, possibly inspired by mass shootings abroad, though not linked to international terrorism. Earlier that day, Kozák's father was found dead, and he was later connected to a double murder in Klánovice.

Figure 3 Students crouched on a ledge at Charles University building to hide from gunfire (Authors, 2025)

Police and emergency services responded within minutes, securing the area and providing the first medical aid to the injured. Prior alerts about Kozák's intentions facilitated the rapid response, as he was suspected of planning to take his own life. Emergency medical teams treated 11 seriously injured, eight moderately injured, and five lightly wounded individuals, demonstrating effective triage.

The university's emergency plan was also promptly activated, with clear communication channels established to guide individuals to evacuation routes or shelter-in-place procedures. See Fig. 3 above. Some of the students escaped through windows and onto ledges, highlighting the need for flexible response strategies in extreme situations. Social media footage showed students barricading themselves in classrooms, indicating they were aware of lockdown protocols.

The incident had a profound psychological impact on the university community, particularly affecting the deaf studies program, where eight students and a professor were among the victims. The Czech Government declared a National Day of Mourning on 23 December 2023, and Charles University organised a memorial service to honour the victims. The event underscored the need for comprehensive mental health support post-incident, as reported by Charles University.

The shooting at Charles University's Faculty of Arts confirmed the great value of several lessons learned from previous incidents elsewhere. A rapid police response minimised casualties, underscoring the need for immediate action. Clear communication via digital platforms and public address systems guided students and staff, a model for CBRN incidents. Pre-existing lockdown protocols enabled effective responses, underscoring the value of regular drills. The significant psychological trauma experienced

by survivors necessitated robust mental health resources. Therefore, universities should establish counselling services and peer support groups to address trauma. Collaboration with local authorities, as seen in the swift response, is critical for managing crises. Regular reviews of security protocols can help prevent future incidents and ensure campus safety. These lessons should be applied to enhance CBRN preparedness, particularly in crisis management.

4. COMPARISON AND LESSONS LEARNED

A thorough comparison between the Charles University shooting and potential CBRN incidents reveals several reinforced strengths and persisting vulnerabilities. Drawing on the incidents discussed in previous chapters, we can better evaluate current readiness and propose further enhancements.

The Charles University shooting demonstrated commendable strengths in emergency response. The rapid deployment of armed police, immediate area lockdown, and swift triage by emergency medical teams prevented further casualties. This type of decisive action should serve as a blueprint for CBRN scenarios. Quick mobilisation, particularly if hazardous materials are involved, can be the difference between containment and catastrophe. Interagency cooperation functioned efficiently. Police, fire departments, medical services, and the university administration worked in tandem to control the situation. Such coordination is paramount for CBRN emergencies, where hazmat response teams must integrate with university safety officers. Events like the 2018 ricin plot in Cologne further emphasise the importance of early intelligence and law enforcement coordination in preventing incidents.

Communication systems functioned but proved not to be entirely fail-safe. The incident showed that communication tools—public address systems, mobile alerts, and social media—were well-utilised and effective. However, their over-reliance on electricity and mobile connectivity could be problematic in CBRN attacks involving infrastructure sabotage. Universities should invest in redundant communication systems, including battery-powered or battery-backed-up public address systems and offline alert applications. Moreover, multilingual messaging should be standard, given the diverse nature of university populations. The 2018 Novichok incident showed that effective public health communication can reduce panic and help direct public behaviour.

While basic lockdown procedures were followed well during the Prague shooting, many students lacked clarity on whether to evacuate or shelter in place. This exposes a weak point that could have severe consequences in a CBRN situation. CBRN scenarios require tailored drills that include chemical spill simulations, radiological decontamination practices, and biological exposure protocols.

Some university infrastructure items have been modernised, but many still need upgrading. Audits conducted at Charles University shortly after the incident revealed ageing ventilation systems and limited biometric access in research labs. In contrast, Loughborough University's proactive installation of radiation detectors following the Litvinenko incident illustrates a high standard of modernising infrastructure. Most EU universities still lack advanced chemical detection systems in non-laboratory environments like libraries or cafeterias. Similarly, not all facilities are equipped with secure, negative-pressure rooms or decontamination chambers.

Psychological preparedness is still a critical weak spot**.** Charles University provided immediate counselling after the shooting, a model response for emotional recovery. However, the trauma associated with invisible threats like radiation or pathogens can be even more psychologically destabilising. Long-term psychological care, not just post-incident but also preventive education about CBRN risks, should be incorporated into campus wellness programs. Lessons from the aftermath of the Novichok poisonings show that communities exposed to CBRN threats endure lingering fear and uncertainty. Universities should offer multilingual mental health support and proactive resilience-building programs.

5. STRATEGIC RECOMMENDATIONS TO STRENGTHEN EU UNIVERSITY RESILIENCE

Based on the case analysis, the following key recommendations are proposed to strengthen CBRN preparedness in EU universities:

The development of redundant, battery-operated, or at least battery-backed-up communication systems must be prioritised. Beyond public address systems and mobile phone applications, universities must prepare for CBRN-specific disruption scenarios. These include manual signalling tools, printed

emergency instructions in multiple languages, and clear signage to direct movement during low-visibility events (e.g., smoke or chemical mist).

Universities' participation in EU and national CBRN programs should be expanded to include active involvement in training initiatives such as the EU Centres of Excellence and eNOVATION. These programs offer simulations, virtual reality training, and collaborative exercises that can significantly enhance university staff preparedness.

All enclosed university buildings should be evaluated for CBRN-readiness, and infrastructure upgrades prioritised. Investment in ventilation systems with HEPA and chemical filters, radiation and gas detectors, and secure access controls must become standardised. EU or national grants can be pursued to support such upgrades. CBRN preparedness must extend beyond laboratories, and a campus-wide emergency culture must be established. Libraries, cafeterias, and administrative areas should also have marked shelter zones, stocked decontamination kits, and accessible emergency instructions. Awareness campaigns during orientation weeks can embed a culture of safety. Standing support teams composed of counsellors, psychologists, and trained peer supporters should be created. Offer post-incident trauma care and pre-incident awareness about coping with uncertainty. Universities can collaborate with public health agencies to streamline services and ensure readiness for mass-scale psychological interventions. Universities must review existing statutes and policies to ensure swift activation of emergency powers. Legal clarity on campus lockdowns, staff duties, and communication responsibilities will reduce hesitation during CBRN crises. Case studies from the UK's Defra's CBRN emergency arrangements and France's plan ORSEC provide guidance. By implementing these strategies, EU universities can significantly raise their preparedness for future CBRN or hybrid threats, thereby enhancing the safety and resilience of academic communities across the continent.

CONCLUSION

The protection of enclosed university facilities against CBRN threats is no longer a hypothetical challenge. Recent incidents such as the Charles University shooting, past poisonings involving Novichok and ricin, and evolving geopolitical tensions highlight the fact that academic institutions in Europe are increasingly vulnerable to both conventional and unconventional attacks. These events underline the urgent need for comprehensive risk assessments, cross-sectoral coordination, and a proactive approach to resilience.

Throughout this paper, we have examined critical areas where EU universities have demonstrated strength—such as rapid emergency response and inter-agency coordination—as well as areas still requiring serious improvement. The lack of consistent CBRN-specific drills, outdated infrastructure in many facilities, and limited psychological preparedness stand out as persistent vulnerabilities that could severely undermine the response in case of a real CBRN crisis. What emerges is the necessity of mainstreaming CBRN preparedness across all layers of university operations. This includes not only laboratory and research spaces, but also lecture halls, libraries, cafeterias, and student residences. Just as critical is the need to embed a safety culture that is not reactive but anticipatory, supported by legal clarity, regular training, robust infrastructure, and well-funded emergency protocols.

The recommendations provided in this paper are not merely aspirational—they are actionable, and in many cases, already implemented in pockets across the EU. The goal now must be to scale these best practices, supported by EU-wide frameworks such as the EU Centres of Excellence and national programs such as the UK's CBRN Governance Arrangements and France's Plan ORSEC. In closing, safeguarding university campuses against CBRN threats is a shared responsibility among government, university leadership, emergency services, and the academic community. Only by working in unison can we ensure that places of learning remain bastions of safety, science, and civil resilience in an increasingly unpredictable and turbulent world.

ACKNOWLEDGMENT

This paper has been supported by the research project UNICOPS 101 190 929 carried out under the European Union HORIZON Programme.

REFERENCES

A.M. van Roon, S.J. Lanooij, H.E. de Melker, Bilthoven (January 30 2025). The National immunisation programme in the Netherlands. Available from: https://www.rivm.nl/publicaties/national-immunisation-programme-in-netherlands-surveillance-and-developments-in-2023

An official website of the European Union. Inception of the CBRN risk mitigation CoE (Centres of Excellence) in 2010. Available from: https://cbrn-risk-mitigation.network.europa.eu/eu-cbrn-centres-excellence_en

BBC News. Ricin threat in Cologne. On June 12 2018 German anti-terror police searched flats where the ricin was produced. Available from: https://www.bbc.com/news/world-europe-44494010

Belgian National Crisis Centre (NCCN) in Leuven. Project eNOVATION - CBRN Training & Exercises, September 23-24 2024. Available from: https://www.enovation-project.eu

Charles University Forum Magazine. Statements of Charles University on the shooting at the Faculty of Arts cover the period from December 21 2023 until January 19 2024. Available from: https://cuni.cz/UKEN-1913.html

Česká televize (Czech TV24 – 24 hours News channel). December 22 2023. Available from: https://ct24.ceskatelevize.cz/clanek/domaci/minutu-po-minute-strelbu-na-prazske-filozoficke-fakulte-neprezilo-ctrnact-lidi-policie-pokracuje-344393

French Nuclear Safety Authority (Autorité de sûreté nucléaire — ASN). Bordeaux University: discovery of radioactive sources and incidental exposure of persons (Level-2 incident). 23 Oct 2015 (news archive). Available from: https://www.french-nuclear-safety.fr/information/news-archives/bordeaux-university-discovery-of-radioactive-sources-and-incidental-exposure-of-persons

IAEA / ERF & Laka (reports collated). Discovery of legacy radioactive sources and residual contamination — University Hospitals of Strasbourg (HUS). Reported to ASN 12 Oct 2020; further activity documented 2021. Available from: https://www-news.iaea.org/ErfView.aspx?mid=7ac96508-cd63-4e2c-b711-12fe6c93ed7e and https://www.laka.org/docu/ines/event/1190 . IAEA News+1

INSERM. Radioactive sources discovered at the University of Bordeaux. 22 Oct 2015. Available from:

https://presse.inserm.fr/en/radioactive- sources-discovered-at-the-university-of-bordeaux/56303/

Loughborough University, UK. Radiation detectors installed soon after polonium incident in 2006. Available from: https://www.lboro.ac.uk/services/health-safety/

Lusa / New University of Lisbon (news agencies). One dead in Lisbon technology park explosion (New University of Lisbon, Caparica). 4 July 2024. Available from news agency Lusa coverage and from: https://english.news.cn/20240704/0113d1239bc243ef9373892e4cb44bd2/c.html.

PHE (Public Health England) national agency. The March 2018 Novichok poisonings in Salisbury, UK, of Sergei and daughter Yulia Skripal. Available from: https://navigator.health.org.uk/theme/wiltshire-novichok-poisonings

Radboud University. Mercator III evacuated after chemical reaction. 29 Aug 2023. Available from: https://www.ru.nl/en/staff/news/mercator-iii-evacuated-after-chemical-reaction . Radboud University

The BBC. Gunman dead after killing 14 people at Prague's Charles University on 21 December 2023. Available from: https://www.bbc.com/news/world-europe-67793962

The CNN. Prague shooting on December 21 2023. Prague, the Czech capital in shock. Available from: https://www.cnn.com/2023/12/22/europe/prague-shooting-attack-friday-intl/index.html

The Guardian. Student shoots 14 people dead and injures 25 others at Charles University in Prague, Czech Republic on December 21 2023. Available from: https://www.theguardian.com/world/2023/dec/21/prague-shooting-charles-university-deaths-injuries

UK National CBRN Governance on April 2018 became Defra (Department for Environment, Food & Rural Affairs) dealing with CBRN emergencies. Available from: https://www.gov.uk/government/groups/government-decontamination-service

University of Copenhagen, Denmark. Annual university CBRN drills since 2005. Available from: https://akut.ku.dk/english/organization

Wikipedia. AZote Fertilisant (AZF) factory explosion of three hundred tons of ammonium nitrate in Toulouse, France on September 21 2001. Available from: https://en.wikipedia.org/wiki/AZF_(factory)#Explosion

Wikipedia. ORSEC plan. September 13 2005. A clear overview of the French emergency response plan, organizational structure, and relevance to CBRN preparedness. Available from: https://en.wikipedia.org/wiki/ORSEC_plan

Wikipedia. Poisoning of A. Litvinenko by Polonium-210 on Nov 1 2006 in London. Available from: https://en.wikipedia.org/wiki/Poisoning_of_Alexander_Litvinenko

Wikipedia. The Seveso-III Directive 2012/18/EU is a key EU regulation aimed at controlling major industrial accident hazards involving dangerous substances. Updated in 2012. Available from: WikipediaEnvironment.

Josef Rajdl
External researcher participating in the EU project under the EU Horizon Programme conducted by the Police Academy of the Czech Republic in Prague (PACR), Lhotecká 559/7, 143 00 Prague 4, Czech Republic
pepikrajdl@email.cz

Jozef Sabol
Head of the research team at the PACR, Head of the Department of Crises Management, the Police Academy of the Czech Republic in Prague, Lhotecká 559/9, 143 00 Prague 4, Czech Republic
sabol@polac.cz

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.42-51
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

COMPARISON OF MATHEMATICAL MODELS OF REGRESSION ANALYSIS ON YOUTH CRIME AND DELINQUENCY

SAMUEL HUBOČAN, VIKTOR ŠOLTÉS

ABSTRACT: This paper presents a comparative analysis of regression models applied to juvenile crime and minors' delinquency in the Slovak Republic. The aim of the research is to identify the most appropriate mathematical model for predicting the future development of juvenile crime and minors' delinquency, based on official statistical data from the Ministry of the Interior of the Slovak Republic for the period 2010–2024. The research analyses linear, exponential, logarithmic, polynomial, and power regression models, and evaluates their reliability using the coefficient of determination (R^2). The results show that the logarithmic model is the most suitable for the state and rate of minors' delinquency ($R^2 = 0.8526$; $R^2 = 0.8819$), while the polynomial model ($R^2 = 0.981$; $R^2 = 0.968$) proved to be the most reliable for the state and rate of juvenile crime. An analysis of demographic trends and the crime index reveal a downward trend in both groups, with the prediction models indicating a continuation of this trend. The research provides important information for the development of preventive strategies and policies aimed at reducing youth crime. The research also highlights the fact that, although crime and delinquency show a declining tendency, schools are increasingly facing the emergence of violent socio-pathological phenomena. The findings of this study can serve as a starting dataset for future research on direct criminogenic factors.

KEYWORDS: *Criminology. Crime analysis. Statistical Research. Minors. Juveniles.*

INTRODUCTION

Youth crime and delinquency represent one of the most significant socio-pathological phenomena of contemporary society, which requires systematic scientific research and effective preventive measures. In the context of the Slovak Republic, similarly to other European countries, it is possible to observe changing trends in youth crime, which require precise analysis and prediction of future development (Lantz, 2024), (Vaško, 2023). Regression analysis can be used as a basic tool for such research tasks. The use of statistical methods in criminology allows not only to analyse the current state, but also to create reliable prediction models that can serve as a basis for the creation of preventive strategies (Lacey, 2016), (Malik, 2015).

The specificity of youth crime lies in its different characteristics compared to adult crime. According to multiple research the most fundamental difference lies in the neurobiological development of the brain – significant endogenous criminogenic factor. Juvenile offenders aged 14-18 have an underdeveloped prefrontal cortex that matures approximately at the age of 25. This area of the brain is responsible for planning, self-control, impulse regulation, and assessing the consequences of actions. The immaturity of the prefrontal cortex explains why youth is significantly more impulsive, less able to control their emotions, and weaker at anticipating the long-term consequences of their actions (Steinberg, 2009; Icenogle, 2019). When it comes to exogenic criminogenic factors, youth can be more susceptible to peer pressure, fear of missing out and parent-child's relationships, when compared to adults (Gašpierik, 2010). Minors (persons under 14 years of age) and juveniles (persons aged 14-18 years) represent special categories that require a differentiated approach to crime analysis (Criminal code of the Slovak Republic, 2025). Research on crime in these age groups is particularly important in terms of early identification of risk factors and implementation of effective preventive measures (Olaoye, 2024), (Gašpierik, 2010).

The research uses official statistical data from the Ministry of the Interior of the Slovak Republic (2025) and the Statistical Office of the Slovak Republic (2025) for the period 2010-2024, which allows for a comprehensive longitudinal analysis. Demographic trends in the population of minors and juveniles in the monitored period show different characteristics - while the population of minors recorded an increase until 2022 with a subsequent decrease, the population of juveniles shows a gradual decrease throughout the monitored period.

The aim of this study is to compare the effectiveness (i.e., the ability to accurately describe historical data and provide reliable predictions) of different mathematical regression analysis models in predicting the development of crime and delinquency, evaluated through the coefficient of determination R^2. Specifically, the analysis of linear, exponential, logarithmic, polynomial, and power models can be used to identify the most reliable approach based on the coefficient of determination R^2 (Hendl, 2004). The results of this comparative analysis can contribute to improving the methodology of youth crime and delinquency prediction and provide valuable information for law enforcement agencies and public policy makers. This research offers the review and comparison of different regression models which can be utilized. The contribution of this study is to provide professional and scientific public with demonstration of this method that can be also utilized for specific types of crime with combination of factors directly impacting the occurrence of socio-pathological phenomena.

1. CRIME ANALYSIS

Crime is a phenomenon that changes and develops over time. Crime statistics processed by the Ministry of the Interior of the Slovak Republic can be used as data sets for crime analysis. Crime analysis allows to create overviews of the development of registered crime over the monitored period. This information can be used for creation of crime prevention strategies. Criminology is a discipline that studies crime based on statistics, known perpetrators, victims. Criminology also studies possible prevention options, suitable response when crime emerges and consequences that can be the result of crime. The crime analysis is the study of quantitative and qualitative variables that can be clearly identified. Crime analysis studies:

- crime state,
- crime rate,
- structure,
- dynamics,
- clearance rate of crime (Gašpierik, 2010), (Dzurčanin, 2003).

For the purposes of this work, the state, rate and dynamics of crime will be further examined. The crime state is a quantitative indicator expressing the number of registered crimes in a certain territory at a certain time. It is expressed in absolute numbers. The crime state does not take into account the size of the population, which makes it an indicator with low informative value. The crime rate can be considered a more accurate quantitative indicator. This indicator takes into account the size of the population. As a generally accepted rule, it indicates the number of crimes per 100,000 inhabitants. It is calculated as the ratio of the number of registered crimes to the number of inhabitants and then multiplied by 100,000. The level of crime is expressed by the crime index I_k, and is calculated as (Dianiška, 2022), (Gašpierik, 2010):

$$I_k = \frac{State\ of\ crime}{Population} . 100\ 000$$

Where: I_k – Index of Crime.

The dynamics of the crime expresses changes in the state, rate or crime structure in a certain period. It is possible to distinguish the tendency of crime development as (Dianiška, 2022), (Gašpierik, 2010):
• growing development tendency (ascending),
• declining development tendency (descending),
• stagnant development tendency (steady).

Based on the above information, it can be stated that through statistical data processed by the Ministry of the Interior of the Slovak Republic, it is possible to study selected quantitative crime indicators. Using the regression analysis, it is possible to predict the future development of the number of crimes (crime state and crime rate) committed in the territory of the Slovak Republic. For the purposes of this paper, the possible future development according to the regression function of crime rate of juveniles and minors born in the Slovak Republic will be examined.

Minor is a person (child) who is younger than 14 years of age. A person (also a child) aged 14 to 18 years is a juvenile. This description is based on the Criminal Code of the Slovak Republic. There is also a term youth, which is often used in the context of crime and delinquency. Youth can be described as "young adults", people who are under the age of 26 years. It is a specific group of people who are preparing to become a productive asset to the whole society and contribute to its development (Národný inštitút vzdelávania a mládeže, 2005).

According to the Statistical Office of the Slovak Republic it is possible to observe an increase in population of minors from year 2010 to 2022 (from 770732 to 817966 minors). The increase of population stopped in 2022, and since the 2022 a decrease of population can be observed up to the year 2024 with 803662 minors. Development of population of juveniles is a bit different. The development is steady – over the observed period from 2010 to 2022 it is possible to observe a slow decrease of population from 266014 to 219761 juveniles. This data is later used to calculate the crime rate. The development of population of minors and juveniles is shown in figure 1 and figure 2.

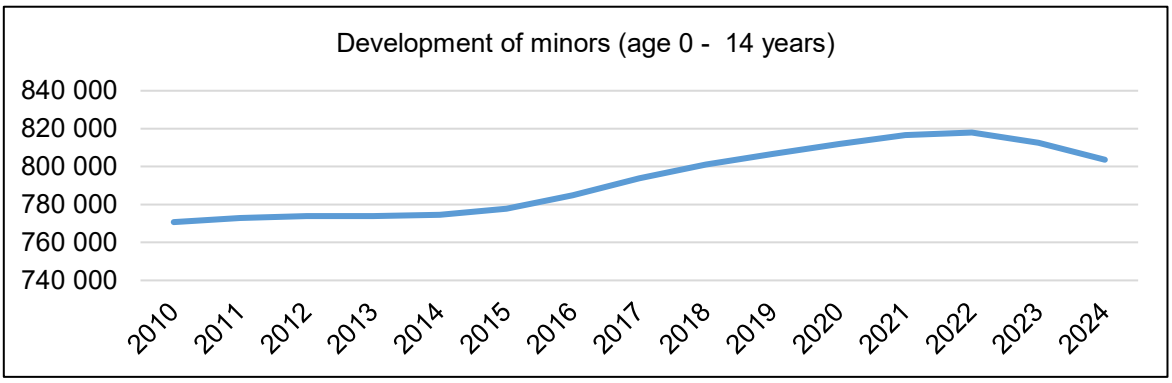


Figure 1 Development of minors (Statistical Office of the Slovak Republic)

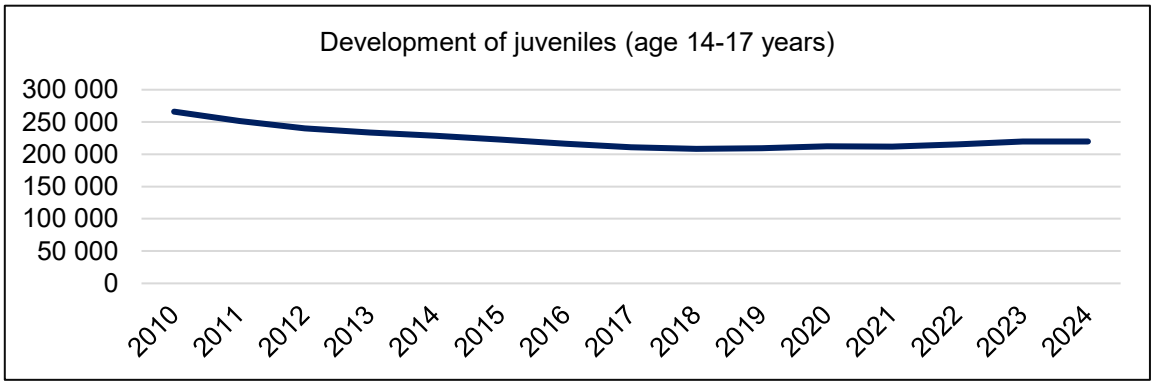


Figure 2 Development of juveniles (Statistical Office of the Slovak Republic)

According to this information it is possible to investigate possible future development of crime state and crime rate which can be used to determine possible need of new preventive measures.

2. METHODS

Within the framework of the analysis, data published by the Ministry of the Interior of the Slovak Republic and the Statistical Office of the Slovak Republic are processed. Based on the data, overviews of the crime state and rate from 2010 to 2024 are processed in the MS Excel program. Data on the number of

minors and juveniles in the territory of the Slovak Republic for the monitored time period are also processed.

The crime rate is calculated according to the formula given in Introduction (the population is considered only as population of minors or juveniles). A graph of the crime situation and crime rate for the monitored period is then created using MS Excel. Trend lines reflecting various mathematical models are gradually inserted in the above graphs. Trend lines for linear, exponential, logarithmic, polynomial and power models are processed. Mathematical models of equations are also generated by MS Excel for individual trend lines, to which the determination coefficient R^2 is subsequently assigned, defining the reliability of the model. A prediction of the future development of the status and level of juvenile and minor crime is then created for the most reliable model.

3. RESULTS

Official statistical data provided by Ministry of Interior of the Slovak Republic and Statistical Office of the Slovak Republic have been processed. In the table 1 it is possible to observe development of crime of juveniles and delinquency of minors and calculated crime rate for selected year.

Table 1 Development of minors and their crimes

Year	Minors			Juveniles			
	Number of Crimes	Number of Minors	Index of Crime Rate	Year	Number of Crimes	Number of Juveniles	Index of Crime Rate
2010	1105	770 732	143,37	2010	4282	266 014	1609,69
2011	1112	772 971	143,86	2011	4216	251 669	1675,22
2012	845	773 912	109,19	2012	3669	240 322	1526,70
2013	783	773 992	101,16	2013	3615	233 648	1547,20
2014	726	774 550	93,73	2014	3264	228 722	1427,06
2015	694	777 828	89,22	2015	2764	222 798	1240,59
2016	678	784 965	86,37	2016	2448	216 225	1132,15
2017	687	793 756	86,55	2017	2404	211 047	1139,08
2018	694	801 103	86,63	2018	2349	208 368	1127,33
2019	656	806 711	81,32	2019	2232	209 257	1066,63
2020	576	811 855	70,95	2020	1968	212 220	927,34
2021	696	816 652	85,23	2021	1735	212 079	818,09
2022	592	817 966	72,37	2022	1826	215 265	848,26
2023	393	812 652	48,36	2023	1741	219 748	792,27
2024	378	803 662	47,035	2024	1443	219 761	656,62

Presented data of crime state and crime rate can be graphically shown in figure 3 (for minors) and figure 4 (for juveniles).

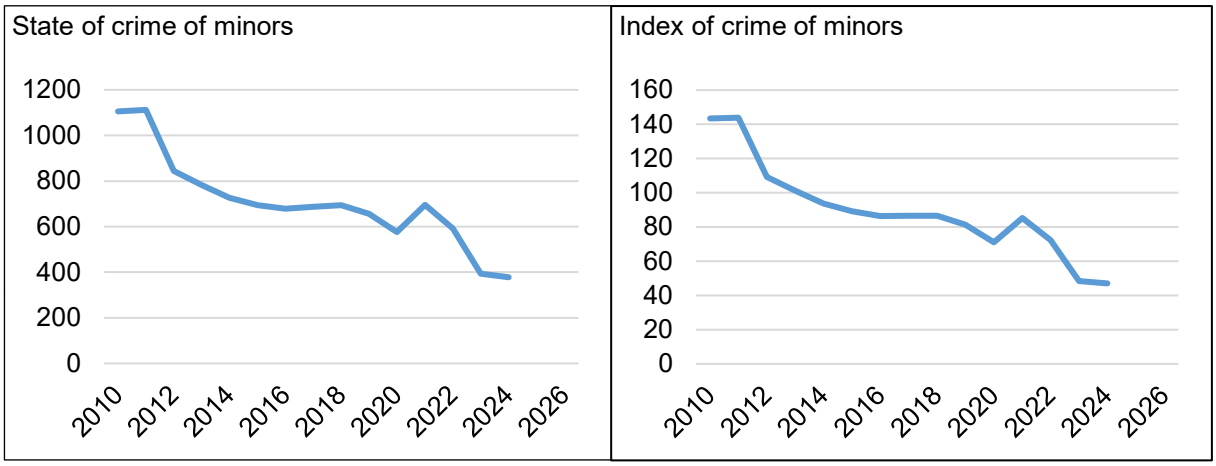


Figure 3 State and index of crime of minors

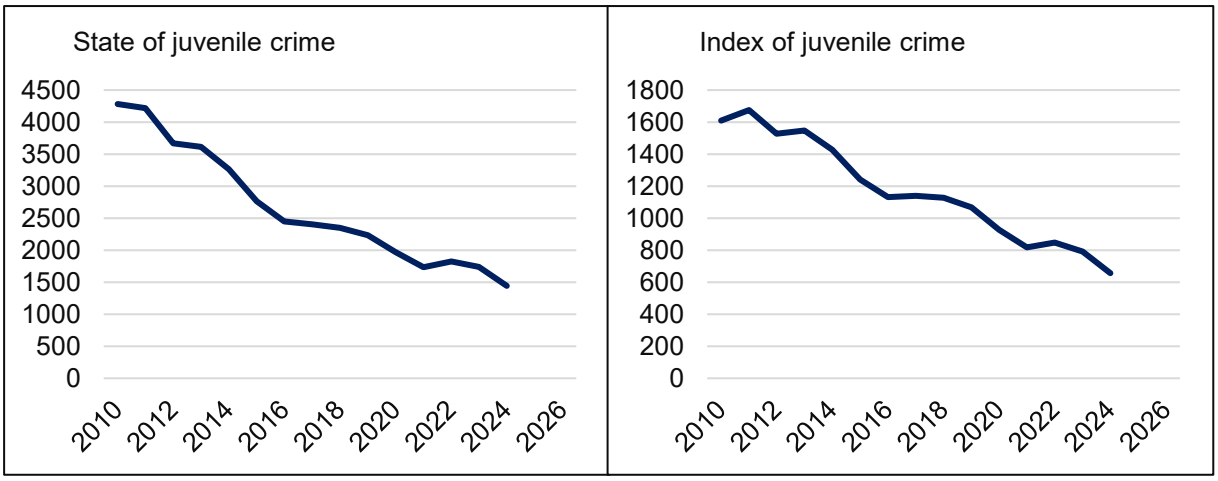


Figure 4 State and index of juvenile crime

For the presented graphical representation of analysed data, it is possible to analyse possible regression functions. The regression functions are presented in figure 5 (for minors) and figure 6 (for juveniles).

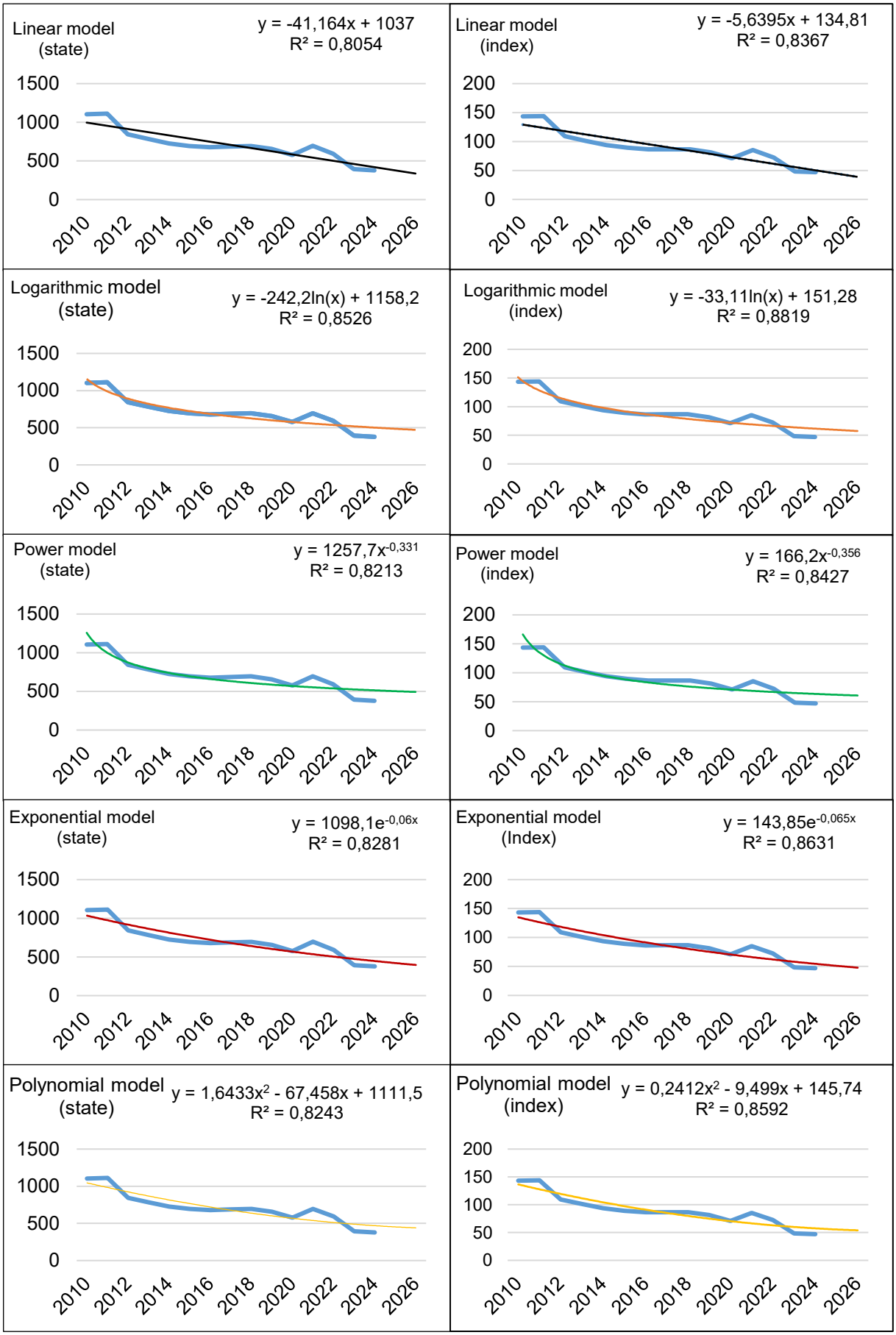


Figure 5 Examined regression models of crime state and rate of minors

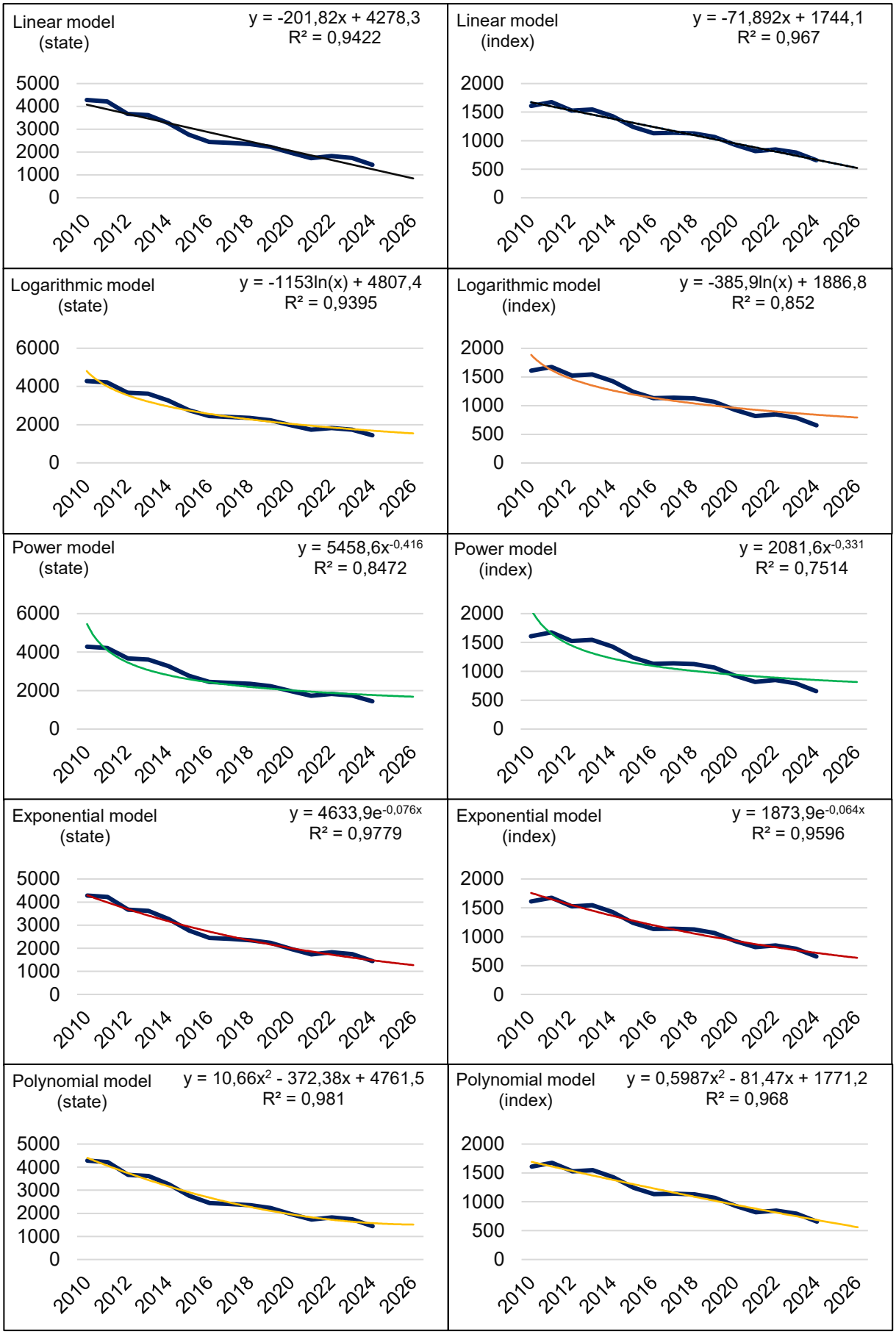


Figure 6 Examined regression models of crime state and rate of juveniles

4. CONCLUSION AND DISCUSION

The real state and level cannot be clearly predicted, as several factors can directly influence the development of crime and delinquency. These factors can include external factors - those that objectively affect minors and juveniles and can influence their criminality (leisure activity options, financial situation of the environment, employment in the region, quality of education, etc.). The second group is internal factors (child upbringing, parental behaviour, peer behaviour, peer pressure, individual psychology and development, genetic predispositions, etc.) (Gašpierik, 2010), (Dianiška, 2022).

In general, it can be stated, that the total crime state and the crime rate of juveniles are significantly higher than those of minors. Based on the analysis performed, it can be stated that in all cases the tendency of the future development of minor delinquency and juvenile crime appears to have a declining trend.

Interestingly, the linear regression model demonstrates strong coefficients of determination both for state and index of crime, particularly for juveniles (R^2 = 0.81-0.84 for minors and 0.94-0.97 for juveniles as shown in Figure 6). This raises a critical methodological question regarding model selection criteria. While R^2 values are exceptionally high, the linear model possesses a fundamental logical limitation: it mathematically allows for negative crime values at future time points, which is conceptually impossible (a negative number of crimes or negative crime rate has no meaningful interpretation). From a practical standpoint, the logarithmic model for minors and polynomial model for juveniles better respect the logical constraints of the problem domain. However, it is acknowledged that for short-term predictions (1-3 years) the linear model could serve as a pragmatic tool for practitioners seeking simplicity over mathematical rigor, particularly for juveniles where the linear model maintains superior R^2 values.

The one reason, why the linear model is particularly high is not clear from the performed analysis. There might be multiple reasons, such as growing standard of living, low unemployment rate of adults/parents, changes in legislation or it can be an indication, that a continuous investment in prevention programs is effective crime prevention measure.

Based on the highest determination coefficient R^2, it is possible to select and consider the models presented in Table 3 as the most accurate for the state and level of criminality (delinquency).

Table 2 Mathematical models of regression functions according to the highest coefficient of determination

Delinquency of Minors	
Crime state	**Crime rate**
Logarithmic model	Logarithmic model
$y = -242{,}2\ln(x) + 1158{,}2$	$y = -33{,}11\ln(x) + 151{,}28$
R^2=0,8526	R^2=0,8819
Crime of Juvenile	
Crime state	**Crime rate**
Polynomial model	Polynomial model
$y = 10{,}66x^2 - 372{,}38x + 4761{,}5$	$y = 0{,}5987x^2 - 81{,}47x + 1771{,}2$
R^2 = 0,981	R^2 =0,968

Based on the above findings, it is possible to assume a stable decrease in the development of the state and level of crime and delinquency. From the selected mathematical functions, it is possible to predict the development of the state and level of crime and delinquency for the coming years. The values calculated based on the mathematical functions (from table 3) can be seen in Table 4.

Table 3 Prediction according to the mathematical model

Delinquency of Minors			
Crime state prediction		**Crime rate prediction**	
Year	State	Year	Crime Index
2025	502	2025	61,62
2026	486	2026	59,48
2027	471	2027	57,47
Crime of Juvenile			
Crime state prediction		**Crime rate prediction**	
Year	State	Year	Crime Index
2025	1574	2025	683,86
2026	1532	2026	620,95
2027	1511	2027	559,23

It can be stated that the mathematical functions describing the models represent a gradual downward trend in the state and level of juvenile crime and minor's delinquency. However, these models cannot be taken as binding. They represent only an informative prediction that can serve as a basis for crime prevention subjects in creating prevention programs. These findings also represent a possible basis for future research when specific factors influencing socio-pathological behaviour will be examined.

It is also important to point out, that even though the crime and delinquency have declining tendency, the schools are having issues with emergence of violent socio-pathological phenomena, such as radicalization or violent extremism. This fact can be the result of high latency of crime, or lack of coherent situational awareness of school management that does not report antisocial behaviour (possible law violations) to the police authorities possibly leading to tragical violent incidents in the future. Based on the above information, it is necessary to examine those factors that have an impact on the criminality and delinquency, identify them as criminogenic factors and act on them with appropriate preventive measures.

The practical significance of this research extends to law enforcement agencies, educational institutions and school administration, policy makers and academic research. Law enforcement agencies can utilize these prediction models to allocate resources efficiently and design preventive measures and intervention strategies. Specifically, the identified declining trends in both minors and juveniles' delinquency provide evidence-based justification for continued investment in prevention programs, while the distinction between age groups allows for age-tailored prevention strategies. School administrators and educators can use these forecasts to anticipate resource needs for socio-pathological prevention. Policy makers require reliable data for evidence-based decision-making regarding legislative changes and preventive policies. The research also serves as a foundational dataset for future interdisciplinary studies examining the direct criminogenic factors (socioeconomic, neurobiological, or environmental) that drive crime dynamics.

The comparative analysis of regression models contributes methodologically to criminology by demonstrating that logarithmic models (for minors) and polynomial models (for juveniles) provide superior logical validity compared to linear approaches for this problem domain, which has implications for crime prediction methodology in other research contexts.

5. LIMITATIONS OF THIS RESEARCH

Table 4 represents the practical output of this research. The predictions indicate a continuous decline in both juvenile crime and minors' delinquency through 2027. However, the accuracy of these forecasts can only be validated through subsequent empirical observation. These predictions should be interpreted as baseline scenarios representing the continuation of current trends under stable socioeconomic and legislative conditions. Table 4 projections can serve as a reference point for

detecting anomalies. If actual values significantly diverge from predictions, this will indicate a significant change in criminogenic factors.

A critical limitation of the current models pertains to their assumption of stable legislative and institutional contexts. The regression models presented are based on historical crime statistics from 2010-2024, a period with specific legal definitions. Recent and anticipated legislative changes in the Slovak Republic may significantly alter the predictive accuracy of these models. Changes in the legislation might reflect in next 1-2 years – especially changes in the misdemeanour amendment (small thefts). These changes in legislation will be studied separately in next research.

The crime statistics that were used to process the regression analysis. These open-source data may represent imperfections and depend on the accuracy of reporting by state administration entities. Information on the possible recidivism of offenders or information on the age and gender of minors and juveniles was also not considered.

ACKNOWLEDMENT

This contribution was processed within the framework of project KEGA “Gamifikácia a inovácia učebných pomôcok v oblasti kriminológie a verejnej spravy” (058ŽU-4/2025).

REFERENCES

Criminal Code of the Slovak Republic 300/2005 Z. z.

Dianiška, G., Strémy, T., Vráblová, M., (2022). Kriminológia. 4. Edition. Plzeň, Aleš Čeněk.

Dzurčanin, Š. (2003) Kriminológia pre bezpečnostný manažment. Žilina, EDIS.

Gašpierik, L. (2010). Prevencia criminality a inej protispoločenskej činnosti. Multiprint Košice.

Hendl, J., (2004). Přehled statistických metod spracovaní dat. Praha: Portál, ISBN 80-7178-820-1

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

Lantz, B., & Knapp, K. G. (2024). T*rends in juvenile offending: What you need to know.* Council on Criminal Justice. Retrieved from https://counciloncj.org/trends-in-juvenile-offending-what-you-need-to-know/

Lacey, A. A. (2016). A mathematical model of serious and minor criminal activity. *Applied Mathematics Research*, 12(3), 123-145.

Malik, T., Ali, S. A., Rasheed, A., & Siddiqui, A. A. (2015). Assessment of statistical approaches to model low count data: An empirical application to youth delinquency. *International Journal of Statistics in Medical Research*, 4(3), 282-286.

Ministry of the Interior of the Slovak Republic (2025). Crime statistics. Retrieved from: https://www.minv.sk/?statistika-kriminality-v-slovenskej-republike-xml

Národný inštitút vzdelávania a mládeže (2005). Review of Youth Policy – Slovak National Report. Retrieved from: https://www.minedu.sk/data/att/d61/2289.869f85.pdf

Olaoye, F., Egon, A. (2024) Predictive policing and crime prevention. *Crime & Delinquency*. Retrieved from https://www.researchgate.net/publication/383565286_Predictive_Policing_and_Crime_Prevention

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

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

Vaško, A., Klátik, J., (2023) Criminal Law Protection of a Child by means of Slovak Criminal Law and European Union Law, *Access to Justice in Eastern Europe,* 3(20), 120-131. https://doi.org/10.33327/AJEE-18-6.3-a000301

Samuel Hubočan - Ing.

Faculty of Security Engineering, Department of Security Management

e-mail: samuel.hubocan@uniza.sk

Viktor Šoltés - Doc., Ing., PhD.

Ministry of Interior of the Slovak Republic

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.52-59
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

VIETNAMESE ORGANISED CRIME IN THE CZECH REPUBLIC: IDENTIFICATION OF CURRENT THREATS AND RISK ASSESSMENT

LUBOŠ MARTINEK

ABSTRACT: *The issue of Vietnamese organised crime represents a current, adaptive, and challenging security threat in the Czech context. Based on a review of scholarly literature and employing analytical–synthetic and descriptive methods, this paper briefly examines the Vietnamese ethnic group within the structures of organised crime in the Czech Republic. It offers a working definition of Vietnamese organised crime and, in its core section, presents the results of an expert investigation. This investigation focused on identifying current security threats posed by Vietnamese organised crime in the Czech Republic and assessing their associated risks. The findings indicate that Vietnamese organised crime is primarily oriented towards economic crime and drug-related offences, with the highest-risk security threats falling within these areas. The paper also emphasises the need for continuous analysis, systematic identification of security threats, and ongoing risk assessment to support the development and implementation of appropriate preventive and repressive measures.*

KEYWORDS: *Security threat. Vietnamese. Gangs. Organised crime. Criminal activities.*

INTRODUCTION

Ensuring the security of citizens and society is one of the fundamental duties of a democratic state governed by the rule of law. The Czech Republic, like other nations, must be adequately prepared to confront current and constantly evolving security threats. One such threat is the notoriously pervasive organised crime. In its contemporary form, organised crime, through its complex network of personal and business connections, often transcends national borders. Coupled with its engagement in illegal activities, it poses a risk to specific values that are inherently meant to be safeguarded against such threats. These values include, for instance, democratic foundations, economic interests, and the rights and legitimate claims of both individuals and legal entities. This issue is also highlighted in the Security Strategy of the Czech Republic (Ministry of Foreign Affairs of the Czech Republic, 2023), which has long identified organised crime as a priority security threat necessitating continuous preventive measures and effective counteraction. Consequently, organised crime represents not only a societal challenge but also a systemic issue.

The threat posed by serious and organised crime to the European Union (EU) and its member states is also highlighted in Europol's 2025 analytical report (Europol, 2025), which states that this threat is ubiquitous, dangerous, and undergoing significant transformation. Key changes are identified in the fundamental tools, modes of operation, and structures of criminal networks, which are noted for their destructive and destabilising impact on internal security, the economy, and the rule of law. Furthermore, the report emphasises the crucial importance of threat-oriented analysis concerning the impact of serious and organised crime on the EU's internal security. This analysis serves as a foundation for setting EU priorities in combating such crime and for directing law enforcement agencies towards the most serious challenges within the extensive criminal landscape.

The author's contribution is specifically focused on Vietnamese organised crime, considering the long-standing and significant presence of individuals of Vietnamese nationality within organised criminal groups in the Czech Republic. Despite a certain foundational level of research, Vietnamese organised crime in the Czech Republic remains under-explored, and the results published so far suggest an inadequate reflection of current trends (such as developments in modes of operation). This situation is significantly influenced by objective factors such as community closedness, language barriers, and high latency, which make acquiring relevant and comprehensive information about such groups considerably challenging (Martinek & Kratina, 2025).

The aim of this contribution is to briefly and fundamentally introduce the Vietnamese ethnic group's involvement in organised crime structures in the Czech Republic using a literature review,

analytical-synthetic methods, and descriptive methods. It seeks to define Vietnamese organised crime for practical purposes and, using the research technique of expert inquiry conducted through the "*round-table*" method, to conduct an exploratory pilot study aimed at identifying current security threats posed by Vietnamese organised crime in the Czech Republic and to assess their risks.

1. VIETNAMESE ETHNICITY AND ORGANISED CRIME IN THE CZECH REPUBLIC

Within the international criminal landscape, the EU, or Europe from a geographical perspective, occupies a pivotal position. Its close connections with other continents render it a source, transit, and destination area for various forms of illegal trade and the provision of illicit services. Criminal networks operating within the EU have demonstrable reach into more than 150 countries across continents, including regions in Asia, Africa, the Americas, and the southern Pacific. The transnational nature of their operations is significantly reflected in the ethnic and national heterogeneity of organised criminal groups. Typically, such groups are composed either of individuals from neighbouring states or foreign nationals with significant diasporic representation in the affected countries, where regional specifics influence not only the functioning of criminal groups but also efforts to combat them (Europol, 2025).

Significant Vietnamese diasporas have established themselves in various countries worldwide, with estimates suggesting that the Vietnamese community abroad numbers approximately four million individuals (Nožina & Kraus, 2020). Prominent and often socially isolated communities exist, for example, in the United States, Canada, Australia, and several European countries, including the Netherlands, France, Germany, Poland, and the Czech Republic. The largest and longest-established Vietnamese diaspora in Europe is in France, estimated to number over 350,000 people as of 2017 (Le Petit Journal, 2017). A substantial representation of Vietnamese nationals is also found in Germany, where, according to official statistics from 2022 (Statistisches Bundesamt, n.d.), there are 120,535 residents. In the Czech Republic, Vietnamese consistently form the third-largest group of foreigners, with an upward trend. For instance, in 2021, there were 64,808 individuals living in the Czech Republic with proper residence permits, and by 2023, this number had increased to 67,783 (Czech Statistical Office, n.d.).

Due to extensive emigration from Vietnam, Vietnamese organised crime groups represent the most influential actors among criminal organisations from Southeast Asia. These groups are inherently diverse and exhibit a variable nature with significant differences in their activity preferences and scope, size and geographic reach, as well as in their internal organisation. Based on current knowledge, it can be stated that their structure and operational mechanisms at least partially reflect elements of all three general models of organised crime—hierarchical, local-cultural, and business (United Nations Office on Drugs and Crime, n.d.) — and that they have gradually evolved into flexible, highly adaptable criminal networks (Le, 2012). Through these networks, they are capable of effectively operating and expanding their criminal activities on a transnational level.

In the context of the Czech Republic, the Vietnamese ethnic group is identified as one of the key actors in the realm of organised crime. Regular expert surveys conducted by the Institute for Criminology and Social Prevention (IKSP) reveal that Vietnamese individuals have consistently ranked prominently within the structures of organised crime in the Czech Republic. This fact is illustrated by Figure 1, compiled based on published results of such expert surveys (Marešová et al., 2000; Marešová et al., 2002; Marešová et al., 2003; Marešová et al., 2005; Marešová et al., 2006; Marešová et al., 2008; Marešová et al., 2009; Marešová et al., 2010; Marešová et al., 2012; Marešová et al., 2013; Marešová et al., 2014; Diblíková et al., 2018; Scheinost et al., 2018; Scheinost et al., 2021; Scheinost et al., 2022; Scheinost et al., 2023). It shows development trends over selected years. The data presented clearly indicate that individuals of Vietnamese ethnicity have consistently ranked among the top ten since 1999, occupying the first position predominantly from 2009 to 2022, with the exception of 2019 and 2022, when they dropped to second place in the overall ranking.

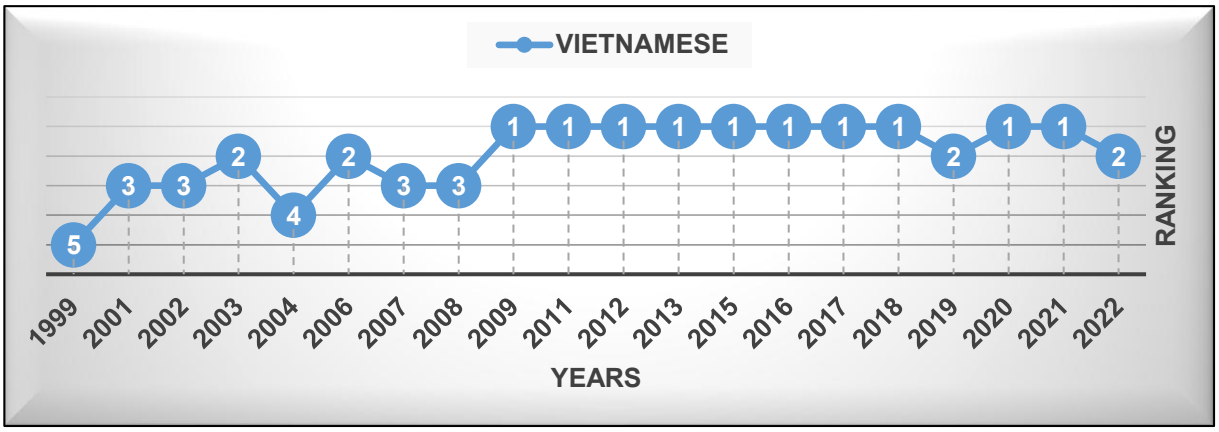


Figure 1 Development of the Representation Rate of Vietnamese in Organised Crime Structures within the Czech Republic Based on Expert Estimates for Selected Years

The significant position of Vietnamese organised crime groups in the Czech Republic began to form in connection with migration waves prior to 1989, which in some cases also brought manifestations of criminal activity. Currently, these groups are characterised by a high degree of adaptability, allowing them to prefer various forms of illegal activities or expand them, depending on current demand in the illegal market, presence of competition, societal changes, or the economic profitability of specific criminal activities (Martinek, 2024).

The criminal activities of these groups are characterised by a high degree of latency, sophistication, and systematic organisation. According to the 2022 annual report by the National Organised Crime Agency (National Organised Crime Agency, 2023), Vietnamese criminal groups, like in previous years, primarily focus on economic crime (such as tax fraud, money laundering), drug-related crime, corruption, and illegal migration-related crime.

Many forms of crime committed by Vietnamese organised crime groups are characterised by being provided as "*services*" aimed at satisfying the needs not only of members of the Vietnamese community but also other entities, including criminal organisations. In these cases, such actors appear as clients, while Vietnamese organised crime groups act as intermediaries or providers. These "*services*" referred to in the Vietnamese community as DỊCH VỤ, can be understood as certain parallel and independent systems of legal entities. Their operation, or use, is typically associated with the collection of predetermined fees. The existence and nature of these practices are also evidenced by specific cases adjudicated by Czech courts, as illustrated by the decision of the Prague City Court on January 22, 2016, file no. 43 T 2/2010, or the decision of the Prague City Court on December 5, 2018, file no. 56 T 6/2017-14166.

2. WORKING DEFINITION OF VIETNAMESE ORGANISED CRIME

The central term in this contribution is organised crime. Despite being an established and widely used term that is the subject of ongoing scholarly discourse, a unified and generally accepted definition of this phenomenon has not yet been achieved within theory (Diviák, Coutinho, & Stivala, 2020). As a result, the literature and legal documents, both nationally and internationally, offer a range of definitions that can differ significantly in certain aspects. For example, criminological definitions often focus on the descriptive characteristics of organised crime, emphasising the identification of its typical features. In contrast, legal definitions primarily focus on the subject. It is also crucial to distinguish organised crime clearly from the term organised criminality, which is committed by organised groups representing a lower type of group criminal activity (Němec, 2003). In practice and some theoretical approaches, these terms are sometimes undesirably conflated.

Given these circumstances, it was necessary to define the subject of inquiry—Vietnamese organised crime—as a theoretical basis for the study, ensuring respondents have a unified and comprehensible

understanding. The working definition of Vietnamese organised crime was guided by the author's chosen legal definition of the subject of organised crime (organised criminal group), the interpretation of organised groups as subjects of organised criminality, the Vietnamese nationality of the perpetrators while considering the possible mixed composition of groups, the primary intent of organised crime groups to consistently and systematically gain financial profit (Martinek, 2019), and their potential activity not only on a national but also an international level.

An organised criminal group is defined as: "*a community of at least three criminally responsible persons with an internal organisational structure, division of roles, and allocation of activities, aimed at systematically committing intentional criminal activities*" (Criminal Code of the Czech Republic, 2009, § 129). According to the law, such a group does not require a hierarchical arrangement (Šámal, 2023), and thus groups with a looser organisation or lower degree of organisation can also be legally assessed as subjects of organised crime, provided they meet the mandatory features listed (cf. Supreme Court of the Czech Republic, 2024).

An organised group is understood as: "*an association of more than (at least three) persons, within which a certain division of tasks among individual members is carried out, and whose activity is therefore characterised by planning and coordination, increasing the likelihood of successfully committing a crime, and thus its harmfulness and severity... An internal organisational and hierarchical structure with superior-subordinate relationships is not necessary, nor is a focus on systematically committing intentional criminal activities, which characterises the qualitatively more serious organised criminal group in the sense of § 129 of the Criminal Code, which must be distinguished from an organised group not directly defined by the Criminal Code*" (Supreme Court of the Czech Republic, 2023, p. 1).

Based on the above summary, Vietnamese organised crime was conceptualised for working purposes as a higher type of group criminal activity, the subject of which is at least one organised criminal group—a community composed of at least three criminally responsible persons predominantly of Vietnamese ethnicity, with an internal organisational structure of a vertical and/or horizontal nature, a division of roles, and an allocation of activities among members, oriented towards the intentional and systematic commission of criminal activities to achieve systematic financial gain, operating on a national or international level either independently or in cooperation with other entities, particularly within criminal networks, and not to be equated with an organised group.

3. METHODOLOGY FOR IDENTIFYING THREATS AND ASSESSING THEIR RISKS

To identify current security threats posed by Vietnamese organised crime in the Czech Republic and to evaluate the risks arising from them, the research technique of expert inquiry was utilised, conducted through the "round-table" method (Martinek, 2024).

Given the specificity of the phenomenon being studied, the respondents consisted of four police specialists in the detection and documentation of Asian organised crime, who are part of the National Organised Crime Agency of the Criminal Police and Investigation Service of the Police of the Czech Republic. The selection of respondents was based on their expert competence, verified by their total length of service in the operational components of the police and the duration of their current assignment in the aforementioned field. The participating specialists were predominantly experienced, as all reported having eight or more years of practice in the operational components of the police, and two of them had nine or more years in the monitoring of Vietnamese or Asian organised crime. The remaining experts had been involved in the respective field for up to two years.

The reliability and validity of the expert responses were ensured through independent evaluation prior to the discussion and a certain level of anonymisation. Each expert first recorded their opinions individually, without influence from others and without knowing the identities of other participants in the subsequent group discussion. Timed intervals during the moderated discussion guaranteed that all participants had equal opportunities to contribute. Experts were also assured that their responses would remain publicly non-identifiable.

During the guided discussion held on January 16, 2024, the group of participants was first provided with an explanation of the understanding of the research subject, namely Vietnamese organised crime (see Chapter 2). Subsequently, the respondents were asked to state the illegal activities of Vietnamese organised crime groups that they personally perceive as security threats. Following this identification of security threats, they were to comprehensively assess the level of risk potential each threat posed to the internal security and legitimate interests of the Czech Republic, and based on this assessment, determine the specific risk level (high, medium, or low) they believe arises from each threat. They were also required to justify the assignment of the highest risk to a specific security threat.

4. RESULTS OF THE EXPERT INQUIRY

The results of the expert inquiry are illustrated in Figure 2 below. It is evident from the graph that the experts identified a total of twelve illegal activities currently posing security threats, perpetrated by Vietnamese organised crime groups within the Czech Republic. The list primarily highlights forms of activities of Vietnamese criminal groups in the Czech Republic considered the most prevalent according to the latest expert estimates (Scheinost et al., 2022; Scheinost et al., 2023). These include activities such as illegal production and smuggling of cigarettes and alcohol, which were predominant in the 1990s, and the less widely known yet unlawfully and extensively conducted activities of gambling and betting. Conversely, the graph does not feature activities that have significantly diminished over time, such as the previously typical distribution of pirated media or violent criminal activities, which were strongly associated with the operations of Vietnamese organised crime groups. For instance, in 1996, violence among Vietnamese gangs escalated in Germany, particularly in Berlin, Brandenburg, Saxony, and Thuringia, with 26 known murders and 15 attempted murders, resulting in 35 Vietnamese victims. This violence was largely attributed to the rivalry between different groups (Bundeskriminalamt, 1997).

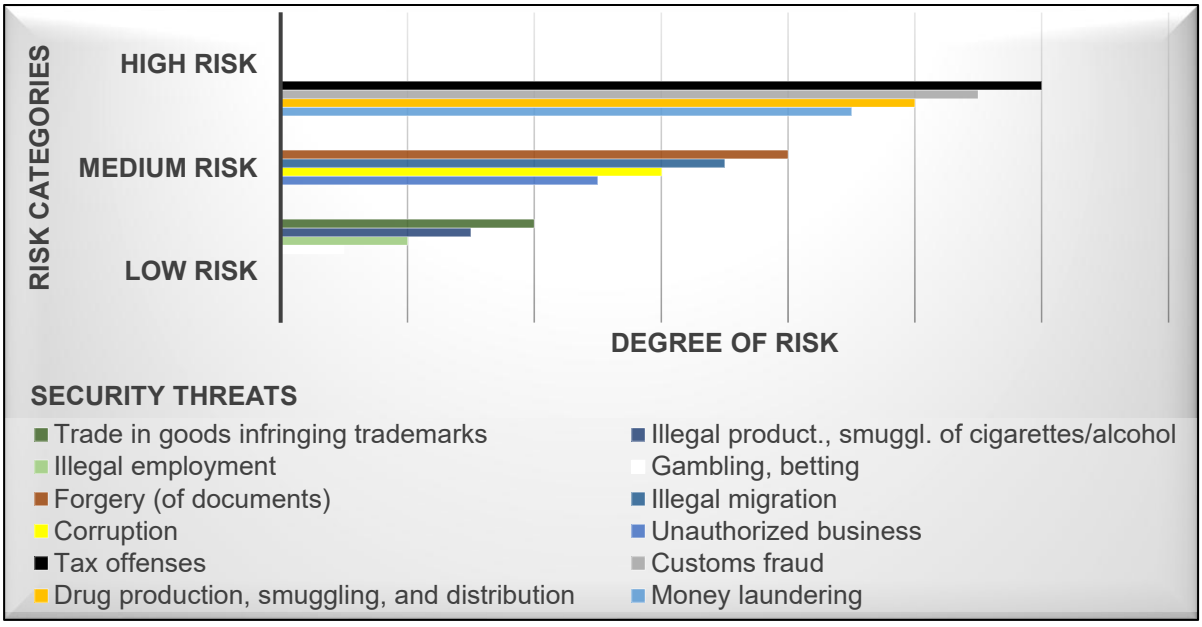


Figure 2 Identified Security Threats of Vietnamese Organised Crime and Evaluation of the Risks Arising from Them

Experts provided detailed commentary on certain activities. They unanimously agreed that violence is not currently perceived as a security threat, as Vietnamese criminal groups are now more focused on economic crime, with violent criminal acts occurring only rarely and in exceptional situations. Moreover, violence does not usually manifest in its most extreme forms, such as murder or torture, and is primarily directed within the community. Additionally, all experts mentioned that unauthorised business activities pose a security threat, particularly in connection with enterprises known as KARAOKE and intermediary services called DỊCH VỤ, emphasising the role of "*money transfer*

services". One expert noted that activities like counterfeiting and illegal migration often involve collaboration with staff from the Embassy of the Socialist Republic of Vietnam in Prague, who "*assist*" in document legalisation. Furthermore, two respondents expressed their views on potential future developments, predicting that Vietnamese organised crime groups in the Czech Republic might increasingly shift their activities to cyberspace (e.g., internet fraud).

The content of Figure 2 also illustrates how respondents assessed the level of risk arising from specific, previously identified illegal activities, or security threats. The specific risk level was determined based on the experts' subjective assessment, primarily grounded in their personal experiences and knowledge not only of Vietnamese organised crime but also of the legal environment and relevant court cases in the Czech Republic.

High risk was attributed by experts to tax-related crimes, customs fraud, drug production, smuggling and distribution, and money laundering. The perception of tax-related crimes as a high-risk security threat was unanimously justified by the respondents due to the Vietnamese community's basic orientation towards consumer goods sales and the related need to import goods from Asia (China, Vietnam, etc.). They added that Vietnamese criminal groups, offering "*customs services*" known as DỊCH VỤ HẢI QUAN (cf. Nožina & Kraus, 2020), play a key role in this, resulting, among other things, in tax evasion amounting to tens of billions of crowns annually. Conversely, gambling and betting pose the least risk, according to the experts, primarily occurring as illegal casino operations and betting activities.

CONCLUSION

Vietnamese organised crime represents a significant and current security threat, challenging not only law enforcement agencies in the Czech Republic but also in other countries with substantial Vietnamese diasporas.

Findings from the exploratory pilot study indicate that Vietnamese organised crime in the Czech context is primarily focused on economic crime and drug-related offenses, with identified high-risk security threats mainly falling within these areas. However, other relevant threats with significant risk potential, such as corruption, counterfeiting, and unauthorised business activities, should not be overlooked. The primary impact of these illegal activities by Vietnamese criminal groups concerns economic interests, yet their nature can negatively affect other protected societal values. Notably, drug production, smuggling, and distribution have undeniable and severe impacts on public health (particularly for users of narcotic and psychotropic substances), the environment (inadequate disposal of toxic waste from drug production), and are sources of other drug-related crimes (e.g., crimes committed under the influence of drugs, aimed at acquiring drugs or funds for their use, or crimes against drug addicts).

Effectively managing the security threats associated with Vietnamese organised crime requires a comprehensive and coordinated approach, accounting for its dynamic development and international nature. Key elements of this approach undoubtedly include continuous analysis, timely identification of current threats, and systematic risk assessment. Equally important is the identification and monitoring of crime indicators—signals suggesting the occurrence of specific illegal activities. Examples include the sudden arrival of groups of Vietnamese migrants accommodated at the same addresses with limited freedom of movement, or small businesses with a high proportion of cash transactions, irregular accounting, rapid turnover, and frequent cash withdrawals. These activities have practical implications as they form the essential foundation for developing and implementing appropriate preventive and repressive measures aimed at reducing security risks, protecting state-protected values, and ensuring the capability of security forces to respond swiftly and effectively to new forms of criminal activity.

REFERENCES

Bundeskriminalamt. (1997). Mitglieder vietnamesischer Straftätergruppierungen in Deutschland (Ausschreibung des BKA Wiesbaden). Bundeskriminalblatt, 47(100), 1–2.

Czech Statistical Office. (n.d.). Cizinci podle kategorie pobytu a státního občanství (stav k 31. 12. 2023) [Foreigners by residence category and citizenship (as of 31 December 2023)] [Database]. https://vdb.czso.cz/vdbvo2/faces/cs/index.jsf?page=vystup-objekt-vyhledavani&bkvt=Y2l6aW5jaQ..&vyhltext=cizinci&katalog=31032&pvo=CIZ04 (Accessed 13 September 2025)

Diblíková, S., Cejp, M., Hulmáková, J., Pešková, M., Scheinost, M., & Večerka, K. (2018). Analýza trendů kriminality v České republice v roce 2017 [Analysis of crime trends in the Czech Republic in 2017] (p. 77). Institut pro kriminologii a sociální prevenci. https://iksp.gov.cz/storage/169/447-Analyza-trendu-kriminality-v-CR-v-roce-2017.pdf

Diviák, T., Coutinho, J. A., & Stivala, A. D. (2020). A man's world? Comparing the structural positions of men and women in an organized criminal network. Crime, Law and Social Change, 74(5), 547–569. https://doi.org/10.1007/s10611-020-09910-5

Europol. (2025). European Union serious and organized crime threat assessment – The changing DNA of serious and organized crime [PDF]. Publications Office of the European Union. https://doi.org/10.2813/0758057

Le, V. (2012). Organized crime typologies: Structure, activities and conditions. International Journal of Criminology and Sociology, 1, 121–131. https://doi.org/10.6000/1929-4409.2012.01.12

Le Petit Journal. (2017). TÊT SPECIAL 2017 – Celebrations of Têt in France by the Vietnamese community. https://lepetitjournal.com/ho-chi-minh/actualites/special-tet-2017-les-celebrations-du-tet-en-france-par-la-communaute-vietnamienne-79888

Marešová, A., Baloun, V., Cejp, M., & Kadeřábková, D. (2002). Kriminalita v roce 2001 [Crime in 2001] (p. 37). Institut pro kriminologii a sociální prevenci. https://iksp.gov.cz/storage/169/284.pdf

Marešová, A., Baloun, V., Cejp, M., Kadeřábková, D., & Martinková, M. (2005). Kriminalita v roce 2003 [Crime in 2003] (p. 39). Institut pro kriminologii a sociální prevenci. https://iksp.gov.cz/storage/169/314.pdf

Marešová, A., Baloun, V., Cejp, M., & Martinková, M. (2006). Kriminalita v roce 2004 [Crime in 2004] (p. 49). Institut pro kriminologii a sociální prevenci. https://iksp.gov.cz/kriminalita-v-roce-2004

Marešová, A., Baloun, V., Cejp, M., & Martinková, M. (2008). Kriminalita v roce 2006 [Crime in 2006] (p. 49). Institut pro kriminologii a sociální prevenci. https://iksp.gov.cz/storage/169/342.pdf

Marešová, A., Baloun, V., Cejp, M., Martinková, M., & Kadeřábková, D. (2003). Kriminalita v roce 2002 [Crime in 2002] (p. 47). Institut pro kriminologii a sociální prevenci. https://iksp.gov.cz/storage/169/297.pdf

Marešová, A., Biedermanová, E., Cejp, M., Holas, J., Martinková, M., & Tomášek, J. (2012). Analýza trendů kriminality v roce 2011 [Analysis of crime trends in 2011] (p. 55). Institut pro kriminologii a sociální prevenci. https://iksp.gov.cz/storage/169/402.pdf

Marešová, A., Cejp, M., Holas, J., Kuchařík, K., Martinková, M., & Scheinost, M. (2013). Analýza trendů kriminality v roce 2012 [Analysis of crime trends in 2012] (p. 31). Institut pro kriminologii a sociální prevenci. https://iksp.gov.cz/storage/169/411.pdf

Marešová, A., Cejp, M., Holas, J., & Martinková, M. (2009). Kriminalita v roce 2007 [Crime in 2007] (p. 30). Institut pro kriminologii a sociální prevenci. https://iksp.gov.cz/storage/169/358.pdf

Marešová, A., Cejp, M., Holas, J., Martinková, M., & Rozum, J. (2014). Analýza trendů kriminality v roce 2013 [Analysis of crime trends in 2013] (p. 34). Institut pro kriminologii a sociální prevenci. https://iksp.gov.cz/storage/169/417-Analyza-trendu-kriminality-v-roce-2013.pdf

Marešová, A., Cejp, M., Kadeřábková, D., & Martinková, M. (2000). Kriminalita v roce 1999 [Crime in 1999] (p. 27). Institut pro kriminologii a sociální prevenci. https://iksp.gov.cz/storage/169/260.pdf

Marešová, A., Cejp, M., Karban, M., Martinková, M., & Vlach, J. (2009). Analýza trendů kriminality v roce 2008 [Analysis of crime trends in 2008] (p. 36). Institut pro kriminologii a sociální prevenci. https://iksp.gov.cz/storage/169/367.pdf

Marešová, A., Cejp, M., Martinková, M., & Tomášek, J. (2010). Analýza kriminality v roce 2009 a v předchozím dvacetiletém období [Analysis of crime in 2009 and in the previous twenty-year period] (p. 31). Institut pro kriminologii a sociální prevenci. https://iksp.gov.cz/storage/169/382.pdf

Martinek, L. (2019). Vývoj vietnamského organizovaného zločinu v České republice [Development of Vietnamese organized crime in the Czech Republic]. Drugs Forensics Bulletin, 25(4), 23–29.

Martinek, L. (2024). Organizovaný zločin z jihovýchodní Asie v České republice: vietnamské kriminální skupiny [Organized crime from Southeast Asia in the Czech Republic: Vietnamese criminal groups] (Rigorosum thesis). Policejní akademie České republiky v Praze.

Martinek, L., & Kratina, T. (2025). Fenomén čínského organizovaného zločinu a jeho potenciální zapojení do dovozu prekurzorů a pre-prekurzorů k výrobě drog z Čínské lidové republiky do Evropy [The phenomenon of Chinese organized crime and its potential involvement in the import of precursors and pre-precursors for drug production from the People's Republic of China to Europe]. Drugs Forensics Bulletin, 31(2), 11–24.

Municipal Court in Prague. (2016, January 22). Rozsudek sp. zn. 43 T 2/2010 [Judgment file no. 43 T 2/2010].

Municipal Court in Prague. (2018, December 5). Rozsudek sp. zn. 56 T 6/2017–14166 [Judgment file no. 56 T 6/2017–14166].

Ministry of Foreign Affairs of the Czech Republic. (2023). Bezpečnostní strategie České republiky 2023 [Security Strategy of the Czech Republic 2023] [PDF]. https://mocr.mo.gov.cz/images/id_40001_50000/46088/Bezpecnostni_strategie_Ceske_republiky_2023.pdf

National Organized Crime Agency. (2023). Výroční zpráva za rok 2022 [Annual report for 2022]. Czech Police. https://policie.gov.cz/clanek/vyrocni-zprava-ncoz-2022.aspx

Nejvyšší soud České republiky. (2023, July 26). Usnesení sp. zn. 5 Tdo 655/2023 [Decision file no. 5 Tdo 655/2023]. https://sbirka.nsoud.cz/sbirka/22216/

Nejvyšší soud České republiky. (2024, May 28). Usnesení velkého senátu trestního kolegia sp. zn. 15 Tdo 50/2024 [Decision of the Grand Chamber of the Criminal Division file no. 15 Tdo 50/2024]. https://sbirka.nsoud.cz/sbirka/23145/

Němec, M. (2003). Mafie a zločinecké gangy: Aktuální problémy vzniku, výskytu a působení zločineckých gangů a mafií a boj proti nim [Mafia and criminal gangs: Current problems of the emergence, occurrence and operation of criminal gangs and mafias and the fight against them]. Eurounion.

Nožina, M., & Kraus, F. (2020). Vietnamese organized crime in the Czech Republic. https://doi.org/10.1007/978-3-030-43613-1

Scheinost, M., Biedermanová, E., Blatníková, Š., Diblíková, S., Hulmáková, J., Večerka, K., & Zeman, P. (2022). Analýza trendů kriminality v České republice v roce 2021 [Analysis of crime trends in the Czech Republic in 2021] (p. 169). Institut pro kriminologii a sociální prevenci. http://www.ok.cz/iksp/docs/470_Analyza_trendu_kriminality_v_CR_v_roce_2021.pdf

Scheinost, M., Cejp, M., Pojman, P., & Diviák, T. (2018). Trendy vývoje organizovaného zločinu a jeho vybraných forem [Trends in the development of organized crime and its selected forms] (pp. 34-35). Institut pro kriminologii a sociální prevenci. https://iksp.gov.cz/storage/169/446-Trendy-vyvoje-organizovaneho-zlocinu.pdf

Scheinost, M., Diblíková, S., Frydrych, J., Háková, L., Holas, J., Hulmáková, J., Kasal, Z., Kudrlová, K., Kutil, L., Šereda, P., Štěpánek, Z., Večerka, K., & Vlach, J. (2021). Analýza trendů kriminality v České republice v roce 2020 [Analysis of crime trends in the Czech Republic in 2020] (p. 204). Institut pro kriminologii a sociální prevenci. https://iksp.gov.cz/storage/169/470_Analyza-trendu-kriminality-vCeske-republice-v-roce-2020.pdf

Scheinost, M., Diblíková, S., Grohmannová, K., Hulmáková, J., Paloušová, V., Přesličková, H., Roubalová, M., & Večerka, K. (2023). Analýza trendů kriminality v České republice v roce 2022 [Analysis of crime trends in the Czech Republic in 2022] (p. 138). Institut pro kriminologii a sociální prevenci. https://www.iksp.cz/analyza-trendu-kriminality-v-ceske-republice-v-roce-2022

Šámal, P. (Ed.). (2023). Trestní zákoník: Komentář [Criminal Code: Commentary] (3rd ed.). C. H. Beck.

Statistisches Bundesamt. (n.d.). Ausländische Bevölkerung nach Familienstand und Staatsangehörigkeit [Foreign population by family status and nationality] (Data for 2022) [Dataset]. https://www-genesis.destatis.de/genesis/online?operation=ergebnistabelleUmfang&levelindex=3&levelid=1694887988614&downloadname=12521-0002#abreadcrumb (Accessed 13 September 2025)

United Nations Office on Drugs and Crime. (n.d.). Teaching module series: Organized crime [Online educational material]. https://sherloc.unodc.org/cld/en/education/tertiary/organized-crime.html (Accessed 14 September 2025)

Zákon č. 40/2009 Sb., trestní zákoník [Act No. 40/2009 Coll., Criminal Code].

Luboš Martinek, Lt. Col. PhDr. MBA

Police of the Czech Republic, National Organized Crime Agency of the Criminal Police and Investigation Service, Criminal Structures Command, Foreign Criminal Structures Division, p.o. BOX 41/NCOZ, 156 80 Prague 5, The Czech Republic

Police Academy of the Czech Republic in Prague, Studies of Security and Law doctoral programme, Lhotecká 559/7, 143 00 Prague, p.o. BOX 54, The Czech Republic

e-mail: lubos.martinek2@pcr.cz

ORCID: 0009-0006-1458-1012

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.60-66
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

FIRE PROTECTION OF WOOD BASED ON MULTICOMPONENT MIXTURES OF SUBSTANCES

OLEH HRYHOR, IHOR MALADYKA, IVAN NESEN, SERHII ROTTE

ABSTRACT: The article presents the results of scientific research aimed at determining and improving the fire-protective properties of powdered substances and their impregnating solutions for the fire protection of wooden products, building materials and structures. A research methodology is proposed for the development of effective fire-extinguishing and fire-retardant agents for wood, based on three-component mixtures in which one of the components is a nitrogen-containing compound. Experimental findings show that a three-component mixture consisting of monoammonium phosphate, ammonium sulphate and carbamide, in appropriate proportions, provides highly effective fire protection for wood. In addition, a composition in the form of an epoxy polymer was developed, containing a mixture of ammonium phosphate and urea-formaldehyde resin, intended for use as a surface fire-retardant coating for wood.

Keywords: *firefighting powder, fire efficiency, gas chromatography, epoxy polymer, non-additivity.*

INTRODUCTION

Recent decades have seen a rise in fire hazards due to the widespread use of wood, synthetic, and polymeric materials in industry and daily life. This has increased the likelihood of fires and, consequently, led to a greater number of deaths and injuries from dangerous fire factors like high temperatures and toxic decomposition products released during combustion.

It is difficult to encounter a fire involving a single class; most incidents typically involve class A, B, and C fires. Among the fire loads represented by solid combustibles (Class A fires), wood is the most commonly encountered material.

An analysis of scientific, technical, and patent literature (Shkarabura et. al. 2002, Shkarabura et. al. 2003) indicates that most developments of fire-extinguishing powder compositions are based on improving formulations using already known and well-tested components. Intensive research is currently underway to determine the optimal composition of these powders to achieve maximum fire-extinguishing efficiency and versatility, which is reflected in the large number of existing formulations.

New formulations of fire-retardant agents are being developed based on two-component flame retardants. Research is underway to create new formulations aimed at both enhancing efficacy and reducing the cost of fire-extinguishing and fire-protective agents—objectives that cannot be fully achieved with the existing single- or two-component mixtures. This highlights the relevance of further scientific research aimed at developing new, more effective, and economically viable multicomponent mixtures of substances as fire-extinguishing and fire-retardant agents for wood.

1. MAIN RESULTS

To facilitate the development of efficient fire-extinguishing and fire-retardant agents, it is essential to investigate the theoretical framework underlying the preparation of three-component compound mixtures. To represent the composition (active basis) of three-component systems, it is appropriate to use an equilateral triangle (Figure 1). The vertices of the triangle ABC correspond to the pure components A, B, and C. The sides of the triangle represent the binary mixtures AB, BC, and AC. The points on the sides of the triangle ABC indicate the percentage content of components in the binary systems AB, BC, and AC. Any point inside the triangle corresponds to a defined composition of a three-component mixture. For example, point G represents a ternary composition abc (where a is the concentration of component A, b is the concentration of component B, and c is the concentration of component C). This method of constructing the composition of three-component systems is known as the Gibbs–Rosenbaum method.

Using the above-described method, we constructed an equilateral triangle whose sides are divided into percentages at 20% intervals (Figure 2).

Three-component systems are studied by first obtaining a composition diagram. The corresponding efficiency values are then plotted on perpendiculars drawn to the plane of the diagram. By connecting these points, an efficiency surface is generated.

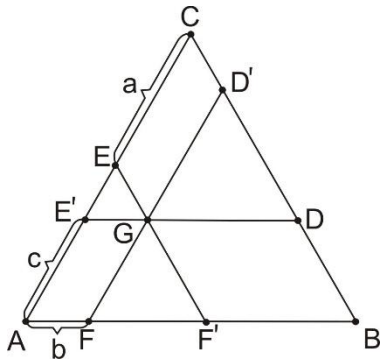


Figure 1 Three-component system

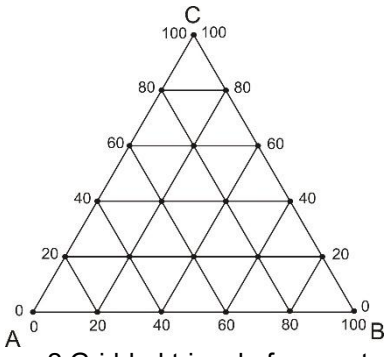


Figure 2 Gridded triangle for constructing three-component compositions

After determining the efficiency for each point, the data were entered into the Statsoft Statistica software matrix. This program was then used to construct the additive surface (Figure 3), the efficiency surface of the three-component mixture (Figure 4), a zone map (Figure 5), and a contour plot (Figure 6). Furthermore, the equation describing the dependence of efficiency on the mixture's composition was derived.

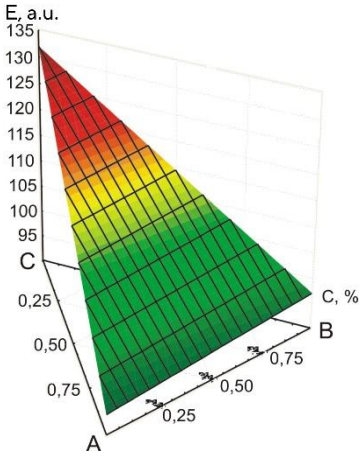


Figure 3 Additive efficiency surface of the three-component mixture

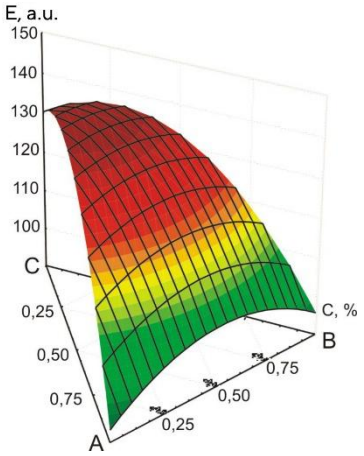


Figure 4 Efficiency surface of the three-component mixture

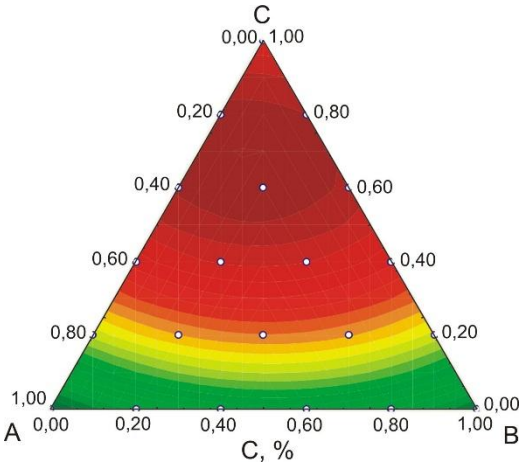


Figure 5 Zonal map of the efficiency surface of the three-component mixture

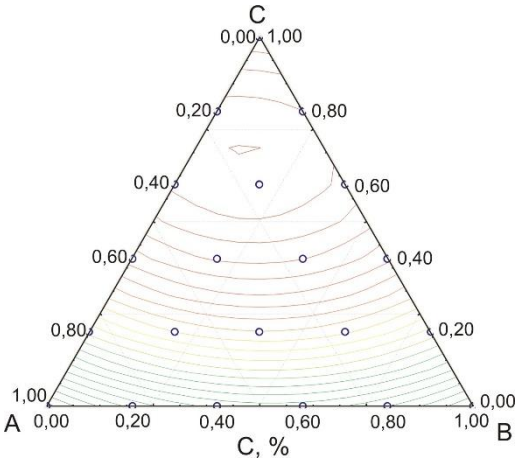


Figure 6 Contour plot of the efficiency surface of the three-component mixture

The darkest color on the zonal map indicates the maximum efficiency of the given mixture. By selecting the mixture concentrations within this zone, further studies can be conducted to determine the most optimal concentrations of the components in the mixture.

Experimental studies of the fire-extinguishing powders were carried out using a laboratory setup based on a Bunsen burner.
A mathematical calculation was performed to determine the dependence of the fire-extinguishing efficiency of powders on the initial temperature. The results showed a linear relationship:

$$E(t) = a_0 + a_1 \cdot t, \quad (1)$$

where t is the temperature in °C, E is the fire-extinguishing efficiency, a_0 is the free term, a_1 is the angular coefficient.

During the analysis of the experimental graphs, as described in the work (Maladyka, 2005), to determine the nature of the dependence of the slope coefficients on the melting temperature of the powders and to approximate this dependence using the corresponding function $f(t_m)$ the MathCAD program was applied. This program allowed the determination of the unknown coefficients of the function. As a result, the following function was obtained:

$$f(t_m) = 22 \cdot {t_m}^{-0,75} + 0.45, \quad (2)$$

where t_m is melting temperature of the powder in °C.

This function allows determining the slope coefficient a_1 for a fire-extinguishing powder if its melting temperature is known. Using the function $f(t_m)$, it is possible to determine the predicted increase in fire-extinguishing efficiency E_2 of a powder when preheated to a certain temperature t_2, if its fire-extinguishing efficiency E_1 at a lower temperature t_1 (ambient temperature) is known.

$$E_2 = E_1 + (22 \cdot {t_m}^{-0,75} + 0.45) \cdot (t_2 - t_1) \quad (3)$$

Calculations using this formula allow drawing conclusions regarding the feasibility of preheating the fire-extinguishing mixture.

Research was conducted on the effect of nitrogen-containing compounds (carbamide, urotropine, and diphenylamine) on the effectiveness of fire-extinguishing powders. The results showed a maximum increase in efficiency at a nitrogen compound content of about 1%. Similar results were obtained by adding 1% carbamide to two-component salt mixtures of monoammonium phosphate and ammonium sulfate in a 1:1 ratio, and diammonium phosphate and ammonium sulfate in a 1:1 ratio. These mixtures are used for wood impregnation. The obtained results indicate the possibility of increasing the

effectiveness of existing fire-extinguishing powders and creating advanced fire-extinguishing and fire-protective compositions for wood.

A study was conducted to investigate three-component mixtures of inorganic salts that had previously shown a synergistic effect as two-component mixtures. The experiments demonstrated (Figure 7) that the effectiveness of the three-component mixtures was enhanced compared to their two-component counterparts.

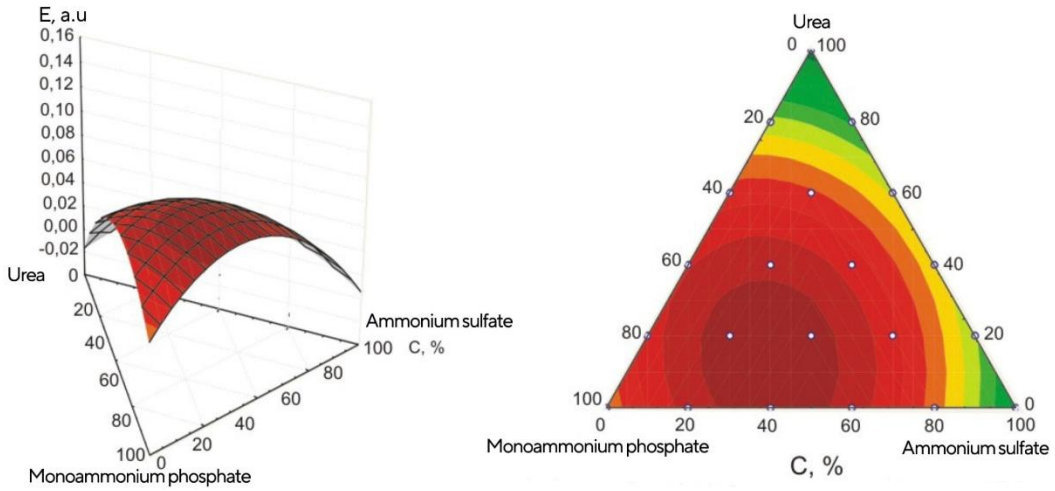


Figure 7 Results of determining the zone of maximum efficiency for a three-component mixture (monoammonium phosphate, ammonium sulfate, carbamide)

As can be seen from Figure 7, the zone of maximum efficiency is observed between points (80; 20; 0), (40; 60; 0), and (40; 20; 40), which form an equilateral triangle, and further research was continued inside it.

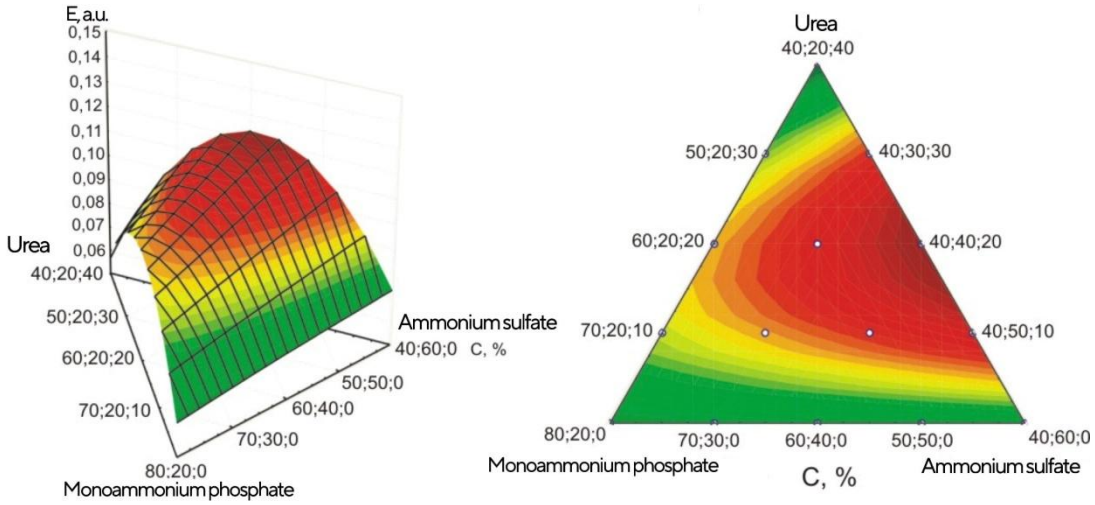


Figure 8 Results of determining the zone of maximum efficiency for a three-component mixture (monoammonium phosphate, ammonium sulfate, carbamide)

As the studies have shown, a mixture of the aforementioned salts in a ratio of monoammonium phosphate (40%), ammonium sulfate (40%), and carbamide (20%) yielded the best results for fire extinguishment.

To assess the feasibility of preparing impregnation solutions, a study was conducted using optical spectroscopy to investigate the inhibitory effect of aqueous solutions of ammonium sulfates, phosphates, and carbamide on an n-heptane flame. It was established that these solutions have a significant inhibitory effect on combustion processes and can be effectively used for the fire protection

of cellulose-containing materials. Furthermore, it was found that at a carbamide mass concentration in the range of 15–25%, a synergistic effect is enhanced, which reduces the relative intensity of OH• radical emission by 24%. These properties are also preserved in a composition based on monoammonium phosphate, ammonium sulfate, and carbamide.

For the purpose of determining the temperature ranges at which the thermal decomposition of salts occurs most intensively, thermogravimetric studies of the thermal decomposition processes were carried out in a dynamic mode using a Q-1500 D derivatograph. The following mixtures were tested: mixture of diammonium phosphate (50%), ammonium sulfate (49%), and carbamide (1%); mixture of monoammonium phosphate (50%), ammonium sulfate (49%), and carbamide (1%); mixture of carbamide (50%) and monoammonium phosphate (50%); mixture of monoammonium phosphate (40%), ammonium sulfate (40%), and carbamide (20%). The results demonstrated that incorporating urea into the mixture increases the wood's heat absorption capacity. The most significant effect was observed in mixture 4, corresponding to the endothermic events at 164 °C (Figure 9).

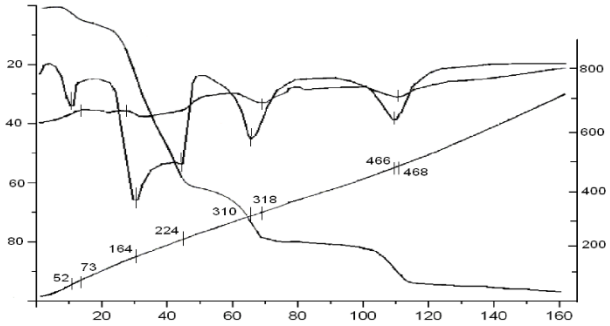


Figure 9 Thermogravimetric analysis curves of a mixture of monoammonium phosphate (40%), ammonium sulfate (40%), and urea (20%)

Thermogravimetric studies of the thermal degradation processes of pine sawdust samples were carried out, as well as of wood treated with fire-retardant agents based on ammonium phosphates and sulfates with the addition of carbamide, in an atmosphere of normal air composition (oxygen content – 21%)

The results of gas chromatographic studies on the pyrolysis of untreated and treated wood, using fire retardants based on monoammonium phosphate, ammonium sulfate, and carbamide (Table 1), show that the degradation products differ significantly in their nitrogen content and the amount of combustible gases.

Table 1 Qualitative and quantitative composition of gaseous products of wood thermal decomposition.

Component	Content of components in volatile decomposition products, %			
	Pine wood, untreated	Pine wood treated with diammonium phosphate (20 %) + ammonium sulfate (10 %)	Pine wood treated with monoammonium phosphate (15 %) + carbamide (15 %)	Pine wood treated with monoammonium phosphate (15 %) + ammonium sulfate (10 %) + carbamide (10 %)
CO	39.08	15.9	11.91	11.04
CO_2	51.93	Not detected	40.51	38.76
CH_4	6.05	0.58	0.19	0.16
$C_2H_6 + C_2H_4$	0.45	Not detected	Not detected	Not detected
C_3H_8	0.19	Not detected	0.07	Not detected
C_3H_6	0.32	Not detected	Not detected	Not detected
H_2	0.73	0.44	0.14	0.12
O_2	0.26	Not detected	0.44	Not detected
N_2	0.99	83.27	46.99	49.92

The average mass loss of samples treated with a mixture of monoammonium phosphate and carbamide was 8.9%, with a fire-retardant salt absorption rate of 54.0 kg/m³ (on a dry basis). The maximum temperature of the flue gases was 237 °C.

In order to evaluate the fire-retardant properties of wood treated with mixtures based on monoammonium phosphate and urea, as well as mixtures of monoammonium phosphate, ammonium sulfate, and urea, experimental investigations were carried out to determine the fire-protective effectiveness of the impregnation agents, following the methodology prescribed by GOST 16363.
The average mass loss for samples treated with a mixture of monoammonium phosphate, ammonium sulfate, and carbamide was 7.4%, with a fire-retardant salt absorption rate of 54.0 kg/m³ (on a dry basis). The maximum temperature of the flue gases was 213 °C.

Based on the mass loss values of the samples after fire tests, wood treated with the impregnating mixtures of monoammonium phosphate and carbamide, as well as monoammonium phosphate, ammonium sulfate, and carbamide, demonstrated high fire-retardant effectiveness.

To develop fire-retardant polymer coatings for wooden structures, it is necessary to investigate the flammability of filled epoxy polymers with the addition of flame retardants. The influence of a two-component fire retardant and intumescent additive system (monoammonium phosphate: carbamide and monoammonium phosphate: urea-formaldehyde resin) on the flammability of epoxy polymers was investigated using the "fire tube" method. The results showed that with the combined use of these fire retardants and additives, the materials transitioned into the group of non-combustible materials. The flammability of the filled epoxy polymers was assessed based on the oxygen index (OI) and resistance to a heated rod (heat resistance), which was used to calculate the mass loss of the polymer coating samples.

The results showed that the highest Oxygen Index (OI) value is achieved in compositions with a higher content of monoammonium phosphate. Regarding heat resistance, compositions containing a mixture of monoammonium phosphate with urea-formaldehyde resin are more resistant to a heated rod than those with a mixture of monoammonium phosphate and carbamide. Based on these findings, optimal compositions of epoxy composites were identified. These materials belong to the group of non-combustible materials and have an OI of 33-35%.

To determine the effect of selected fire retardants and additives on the thermo-oxidative degradation of an epoxy coating, thermogravimetric analysis was conducted on epoxy polymer samples containing monoammonium phosphate, urea, and urea-formaldehyde resin. The results indicate the optimal conditions for forming a fire-retardant coating for wood based on epoxy-polymeric binders (as reported in the work (Maladyka, 2006)).

To test the fire-retardant coating for wood based on epoxy-polymeric binders (Maladyka, 2006), experimental studies were conducted to determine its fire-retardant effectiveness in accordance with GOST 16363. The results of these studies are presented in Table 2.

Table 2 Results of the studies on determining the fire-retardant effectiveness of coatings

Composition of the fire-retardant coating	Protective layer thickness					
	0.5 mm		1 mm		1.5 mm	
	Average sample mass loss, g	Average sample mass loss, %	Average sample mass loss, g	Average sample mass loss, %	Average sample mass loss, g	Average sample mass loss, %
Carbamide	9.36	6.84	8.89	5.93	11.61	6.38
Urea-formaldehyde resin	19.51	13.82	17.05	11.96	19	11
Monoammonium phosphate, urea-formaldehyde resin	4.05	2.4	3.99	2.65	4.73	2.63
Monoammonium phosphate, carbamide	4.15	2.86	3.88	2.51	5.05	3.09

As shown by the research results, the coatings with mixtures of monoammonium phosphate and carbamide, and monoammonium phosphate and urea-formaldehyde resin, demonstrated the highest fire-retardant effectiveness.

CONCLUSIONS

The study confirms that two-component powder mixtures of inorganic salts can produce a synergistic or antagonistic effect, depending on their proportions. A synergistic effect was also found in two- and three-component fire-extinguishing powder mixtures when one of the components is an amine. Thermal analysis of multicomponent mixtures showed that a two-component mixture of monoammonium phosphate and ammonium sulfate is thermally stable up to 200 °C. In contrast, a three-component mixture of monoammonium phosphate, ammonium sulfate, and carbamide exhibits significant endothermic effects in the 120–165 °C temperature range. Furthermore, thermogravimetric analysis demonstrated that adding a mixture of monoammonium phosphate and urea-formaldehyde resin to epoxy polymers reduces the oxidation rate of the carbonized residue at 500–600 °C. Consequently, this blend is recommended as a more effective fire-protective coating for wood.

REFERENCES:

Shkarabura M.H., Tyshchenko O.M., Maladyka I.H., Diadchenko O.I. Vohnehasi poroshky – mozhlyvi napriamy pidvyshchennia efektyvnosti. // Visnyk ChDTU. – Cherkasy: ChDTU, 2002. – Vyp. 4. – S. 98-101.

Shkarabura, M.H., Maladyka, I.H., Diadchenko, O.I. Vzaiemnyi vplyv vohnehasnykh poroshkiv na inhibuvannia protsesu horinnia. // Problemy pozharnoi bezopasnosti. – Kharkiv: Folio, 2003. – Vyp. 14. – S. 230-234.

Maladyka I.H. Vplyv khimichnoi budovy skladovykh vohnehasnykh kompozytsii na neadytyvni yavyshcha pid chas prypynennia protsesu horinnia. // Problemy pozharnoy bezopasnosti. – Kharkiv: Folio, 2005. – Vyp. 17. – S. 110-113.

Maladyka I.H. Eksperymentalni doslidzhennia pokryttiv dlia derevyny na osnovi epoksiaminnykh kompozytsii, modyfikovanykh neorhanichnymy soliami. // Nauk. Visnyk budivnytstva. – Kharkiv: KhDTUBA, 2006. – №37. – S. 180-188.

Vohnezakhyst derevyny ta vyrobiv z nei: Navchalnyi posibnyk:/ Zhartovskyi, V. M., But, V. P., Tsapko, Yu. V., Maladyka, I. H., Zhartovskyi, S. V., – Cherkasy: APB im. Heroiv Chornobylia MNS Ukrainy, 2009. – 252 c.

Oleh Hryhor, Doctor of Political Sciences, Professor.

Rector of Cherkasy State Technological University, 460 Shevchenko Boulevard, Cherkasy, 18006, Ukraine, chdtu@chdtu.edu.ua, +380472513672

Ihor Maladyka, PhD in Technical Sciences, Associate Professor.

Department of Geodesy, Land Management, Building Structures, and Life Safety, Cherkasy State Technological University, 460 Shevchenko Boulevard, Cherkasy, 18006, Ukraine, i.maladyka@chdtu.edu.ua.

Ivan Nesen, PhD.

Department of Information Systems and Civil Protection Organization, National University of Civil Protection of Ukraine, 8 Onopriienko Street, Cherkasy, 18034, Ukraine, nesen_ivan@nuczu.edu.ua.

Serhii Rotte, PhD in Technical Sciences, Associate Professor.

Department of Geodesy, Land Management, Building Structures, and Life Safety, Cherkasy State Technological University, 460 Shevchenko Boulevard, Cherkasy, 18006, Ukraine, s.rotte@chdtu.edu.ua.

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.67-76
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

METÓDY ZÁCHRANY OSÔB POMOCOU LEZECKEJ TECHNIKY V OPUSTENÝCH BANIACH PRÍSLUŠNÍKMI HAZZ

ROPE-BASED RESCUE METHODS FOR PEOPLE IN ABANDONED MINES USED BY THE FIRE AND RESCUE SERVICE

MAREK PLAVČKO, IVANNA BETUŠOVÁ, MIROSLAV BETUŠ

ABSTRACT: *This paper addresses the rescue of persons from abandoned underground mines using rope techniques employed by members of the Fire and Rescue Corps of the Slovak Republic. Abandoned mine workings pose a significant safety risk, particularly due to their deteriorated technical condition, unstable geological environment, and the frequent presence of unauthorized individuals. The aim of the research was to test and evaluate selected rescue methods directly in the environment of the former Bankov magnesite mine near Košice. Several experimental rescue exercises were conducted, during which various rope techniques were applied under real conditions. The evaluation criteria included evacuation time, the amount of equipment required, the level of technical difficulty, and overall safety for both rescuers and rescued persons. The results showed that some techniques are better suited for inclined or vertical mine passages, while others are more effective in horizontal workings. Based on these findings, recommendations were formulated for the practical application of the most effective methods by Fire and Rescue Corps units. The study contributes to increasing preparedness and operational efficiency in underground rescue situations, where time is a critical factor in saving human lives.*

KEYWORDS: *Rescue. Rope Techniques. Abandoned Mines. Fire and Rescue Corps*.

ÚVOD

Bezpečnosť v podzemných priestoroch je jednou zo základných podmienok ochrany života a zdravia obyvateľstva. Opustené banské diela, ktoré vznikli v minulosti ako súčasť ťažobnej činnosti, sa postupne menia na rizikové prostredie. Ich technický stav sa v dôsledku prirodzených geologických procesov a chýbajúcej údržby neustále zhoršuje (Sanmiquel et al., 2018; Stojadinović et al., 2012; Singo et al., 2022).

Tieto priestory sú zároveň čoraz častejšie navštevované neodbornou verejnosťou, najmä v rámci tzv. urbex aktivít. Takéto konanie so sebou prináša značné nebezpečenstvá – riziko pádu, zasypania, straty orientácie, podchladenia alebo udusenia v dôsledku nedostatku kyslíka či prítomnosti nebezpečných plynov (Brodny & Tutak, 2018; Kowalska et al., 2021; Li et al., 2023).

V prípade ohrozenia života alebo zdravia je nevyhnutné, aby zasahujúce zložky disponovali účinnými metódami záchrany. V podzemných priestoroch nemožno využiť štandardné spôsoby evakuácie, preto je nutné testovať a aplikovať špecifické lezecké techniky. Ich cieľom je umožniť bezpečný a rýchly presun ohrozených osôb do bezpečia pri zachovaní maximálnej ochrany zasahujúcich príslušníkov (Hildebrandt et al., 2019; Su & Hu, 2024; Naeini & Badri, 2023; Qiang et al., 2025).

Cieľom tejto práce je analyzovať a porovnať vybrané metódy záchrany osôb z opustených baní pomocou lezeckej techniky. V rámci experimentov sa hodnotil najmä čas potrebný na evakuáciu, náročnosť jednotlivých postupov a ich vhodnosť pre podmienky banského prostredia.

1. MATERIÁLY A METÓDY

Samotný výskum bol realizovaný v podzemných banských priestoroch bývalej magnezitovej bane Bankov, ktorá sa nachádza v blízkosti mesta Košice. Lokalita bola zvolená z dôvodu vhodných podmienok na simuláciu záchranných zásahov – šachty a horizontálne chodby umožnili overiť použiteľnosť rôznych postupov.

V rámci výskumu boli definované tieto hodnotiace kritériá:

- čas potrebný na záchranu – od začiatku zásahu po úspešnú záchranu,
- technická náročnosť – zložitosť jednotlivých krokov a potreba špecializovaných zručností,
- materiálno-technické zabezpečenie – množstvo a typ potrebného lezeckého vybavenia,
- bezpečnosť – riziká pre zasahujúcich hasičov a aj zachraňované osoby.

Testované boli tri základné lezecké techniky:

- Jednoduchá lanovka – základná metóda, pri ktorej je osoba spustená po nosnom lane z vyššie položenej časti bane do nižšej úrovne. Výhodou je rýchla príprava a krátky čas zásahu, nevýhodou obmedzená použiteľnosť len pri menších vzdialenostiach.
- Tirolský traverz – metóda využívajúca nosné lano natiahnuté medzi dvomi pevnými bodmi, po ktorom je osoba transportovaná horizontálne alebo šikmo. Výhodou je univerzálne použitie aj vo väčších priestoroch, nevýhodou vyšší čas potrebný na osadenie systému.
- Tirolský traverz motorovým navijakom – rozšírená verzia Tirolského traverzu, kde pohyb osoby zabezpečuje motorový navijak. Tento systém umožňuje plynulejší presun na väčšie vzdialenosti a znižuje fyzickú záťaž záchranárov. Nevýhodou je potreba dodatočného technického vybavenia a dlhší čas na prípravu.

Každá z metód bola odskúšaná niekoľkokrát pri rôznych priestorových podmienkach. Pri experimentoch sa simulovala reálna situácia, keď je potrebné dostať osobu z ohrozeného úseku podzemného diela na bezpečné miesto. Výsledky meraní boli spracované do tabuliek a použité na porovnanie efektívnosti jednotlivých postupov.

2. VÝSLEDKY

V rámci experimentov uskutočnených v magnezitovej bani Bankov sa testovali tri vybrané metódy záchrany osôb: jednoduchá lanovka, tirolský traverz a tirolský traverz s motorovým navijakom. Pre každú metódu sa sledovali nasledovné parametre:

- čas príchodu a prieskumu,
- čas potrebný na vybudovanie lanového systému,
- čas samotnej záchrannej činnosti,
- celkový čas zásahu.

Výsledky meraní sú zhrnuté v tabuľkách 1 až 4.

Tabuľka 1 Časový priebeh udalosti (vlastné spracovanie)

Parameter	Čas (min)
Čas od vzniku udalosti po spozorovanie (t_obs)	2
Čas ohlásenia udalosti (t_report)	4
Čas spracovania hovoru (t_call)	3
Čas príjazdu hasičov na miesto (t_d1)	7
Spolu (t_event)	**16**

Tabuľka 2 Časový prieskumnej skupiny (vlastné spracovanie)

Parameter	Čas (min)
Čas obliekania výstroja (t_gear)	3
Čas kotvenia lana (t_anchor)	5
Čas zostupu k zranenej osobe (t_reach1)	3
Čas vyšetrenia a určenia spôsobu záchrany (t_eval)	4
Spolu (t_survey)	**15**

Tabuľka 3 Časy lezeckej činnosti podľa jednotlivých metód (vlastné spracovanie)

Parameter	Metóda 1 (jednoduchá lanovka) (min)	Metóda 2 (tirolský traverz) (min)	Metóda 3 (tirolský traverz s navijakom) (min)
Čas druhého zostupu k osobe (t_reach2)	5	3	3
Čas imobilizácie (t_immob)	4	4	4
Čas nakladania do nosidiel (t_load)	7	6	6
Čas samotnej evakuácie (t_extract)	29	8	4
Spolu (t_climb)	**45**	**21**	**17**

Tabuľka 4 Celkový čas lezeckej záchrany podľa metód (vlastné spracovanie)

Parameter	Metóda 1 (min)	Metóda 2 (min)	Metóda 3 (min)
Čas prieskumu (t_survey)	15	15	15
Čas budovania systému (t_setup)	5	17	17
Čas lezeckej činnosti (t_climb)	45	21	17
Celkový čas záchrany (t_rescue_total)	**65**	**53**	**49**

Okrem meraní časových parametrov sa zohľadňovali aj ďalšie faktory, ktoré významne ovplyvňujú efektívnosť zásahu. Vybrané kritériá zahŕňali počet zasahujúcich hasičov, množstvo použitého vybavenia, subjektívne hodnotenie náročnosti zásahu a budovania systému, ako aj komfort zachraňovanej osoby počas evakuácie.

Výsledky tohto hodnotenia sú uvedené v tabuľke 5. Z tabuľky vyplýva, že metóda jednoduchá lanovka bola síce technicky najmenej náročná na vybudovanie, avšak z pohľadu času, komfortu a fyzickej záťaže hasičov vyšla ako najmenej vhodná. Naopak, tirolský traverz (s motorovým navijakom aj bez neho) vykazoval výrazne lepšie hodnoty v parametroch komfortu a bezpečnosti.

Na určenie váhy jednotlivých kritérií bola aplikovaná metóda Fullerovho trojuholníka. Tento prístup umožnil stanoviť, ktoré kritériá sú rozhodujúce pri výbere najefektívnejšej metódy záchrany. Výsledky párového porovnania kritérií sú uvedené v tabuľke 6. Ako najdôležitejší faktor bol identifikovaný celkový čas záchrany, nasledovaný počtom zasahujúcich hasičov a množstvom použitého vybavenia.

Na základe váhového hodnotenia sa ako najefektívnejšia ukázala metóda 3 – Tirolský traverz s motorovým navijakom, ktorá dosiahla najlepšie skóre vo väčšine kritérií.

Tabuľka 5 Hodnotenie záchranných metód podľa kritérií (vlastné spracovanie)

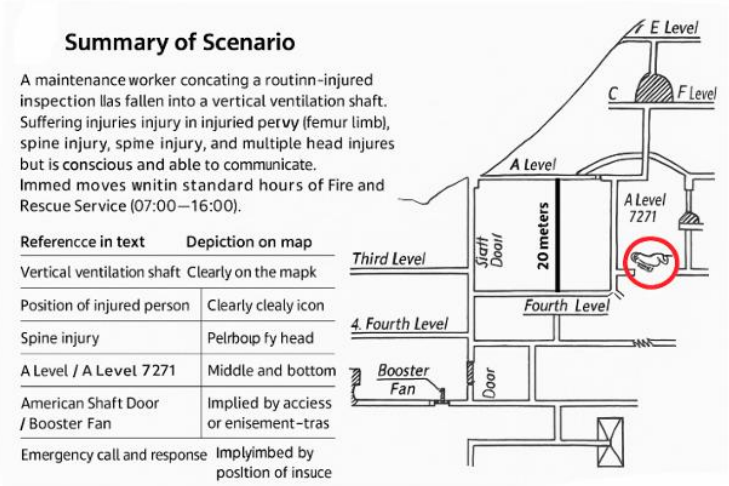
Kritérium	Metóda 1 (jednoduchá lanovka) (min)	Metóda 2 (tirolský traverz) (min)	Metóda 3 (tirolský traverz s navijakom) (min)
Celkový čas záchrany (t_rescue_total) [min]	65	53	49
Počet zasahujúcich hasičov	11	10	9
Množstvo lezeckého vybavenia	3	1	1
Náročnosť zásahu (1–10)	8	6	4
Náročnosť budovania systému (1–10)	2	6	6
Komfort pre zachraňovanú osobu (1–10)	2	9	9

Tabuľka 6 Fullerov trojuholník – váhy kritérií (vlastné spracovanie)

Kritérium	Počet „víťazstiev“ v párovom porovnaní	Váha kritéria (Wi)
Celkový čas záchrany (K1)	5	najvyššia
Počet hasičov (K2)	3	vysoká
Množstvo vybavenia (K3)	2	stredná
Náročnosť zásahu (K4)	1	nízka
Náročnosť budovania systému (K5)	2	stredná
Komfort pre zachraňovaného (K6)	1	nízka

Po vyhodnotení časových parametrov (tab. 1 – 4) a viac-kritériálneho hodnotenia (tab. 5 – 6) boli výsledky doplnené aj o obrazovú dokumentáciu priebehu experimentov. Obrázky ilustrujú jednak podmienky v bani Bankov, jednak samotné metódy záchrany.

Schéma na obrázku 1 zobrazuje polohu zranenej osoby vo vetracej šachte a priľahlých priestoroch. Jasne sú vyznačené horizontálne chodby, portál a naklonená plošina, na ktorej sa zranený nachádzal.



Obrázok 1 Náčrt miesta nehody (vlastné spracovanie)

Na obrázku 2 je znázornený pohľad na zabezpečený portál s oceľovým zábradlím, ktoré bolo v havarijnom stave a znemožňovalo jeho využitie pri záchranných prácach.

Obrázok 2 Vstup do vetracej šachty (vlastné spracovanie)

Obrázok 3 zobrazuje vstupnú časť do vetracej šachty so železným zábradlím. Tento priestor slúžil ako nástupný bod pre lezecké skupiny.

Obrázok 3 Nástupný priestor pre lezecké skupiny (vlastné spracovanie)

Na obrázku 4 sú znázornené hodnoty (rýchlosť vetra, teplota, vlhkosť, rosný bod). Počas cvičenia bola teplota 3,9 °C, vlhkosť 70,6 % a maximálna rýchlosť vetra 13,2 km/h.

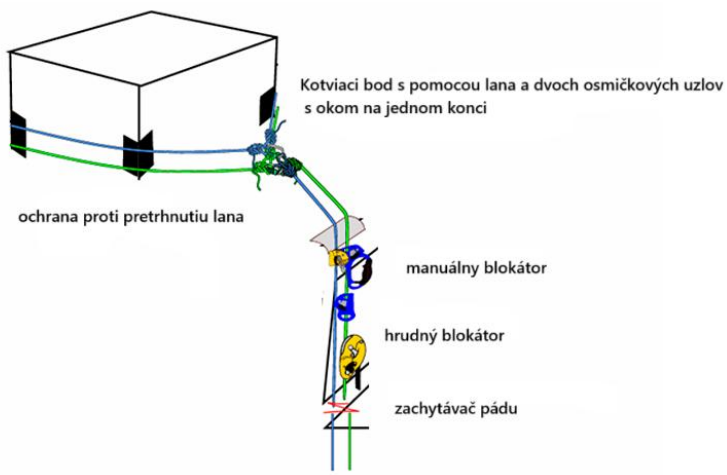
Obrázok 4 Meteorologické podmienky počas zásahu (vlastné spracovanie)

Na obrázku 6 sú znázornené hodnoty nameraných plynov vo vetracej šachte. Merania koncentrácie CO, CO_2 a H_2S ukázali, že hodnoty boli v norme a nebolo potrebné použitie autonómnych dýchacích prístrojov.

Obrázok 5 Hodnoty nameraných plynov vo vetracej šachte (vlastné spracovanie)

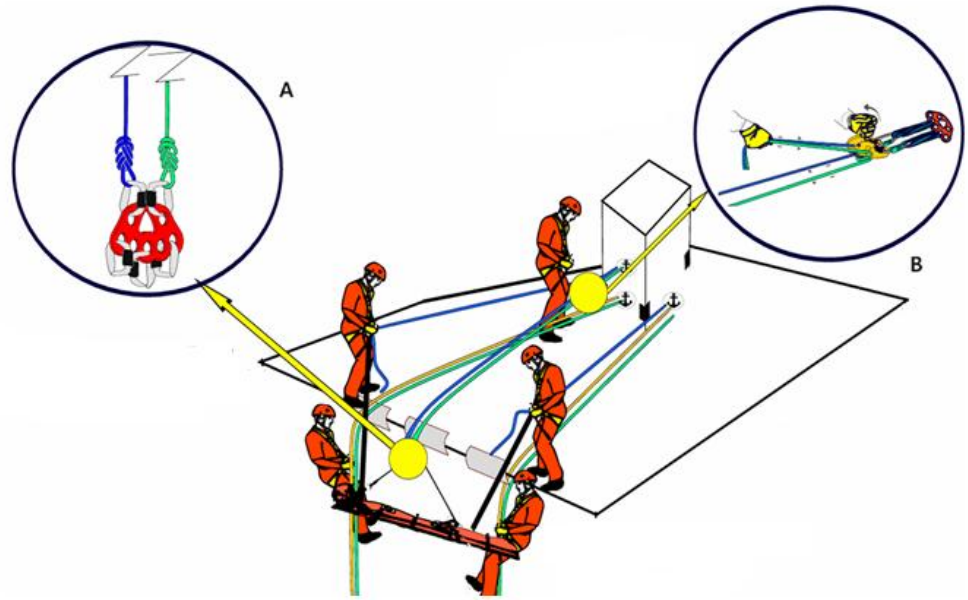
Okrem všeobecných údajov o prostredí a časových parametroch zásahu sa osobitná pozornosť venovala samotným lezeckým technikám, ktoré boli predmetom skúmania. V rámci experimentov sa testovali tri vybrané metódy – jednoduchá lanovka, tirolský traverz a tirolský traverz s motorovým navijakom. Každá z nich bola prakticky nasadená v reálnych podmienkach a následne vyhodnotená z pohľadu času, technickej náročnosti, komfortu zachraňovanej osoby a bezpečnosti zasahujúcich. Nasledujúce obrázky dokumentujú priebeh a charakteristické znaky jednotlivých metód.

Na obrázku 6 je znázornený systém záchrany – jednoduchá lanovka, kde zasahujúci hasič sa spúšťa na nosnom lane k zranenej osobe. Výhodou metódy je rýchla príprava a nízka technická náročnosť, avšak limitovaná použiteľnosť na väčšie vzdialenosti.



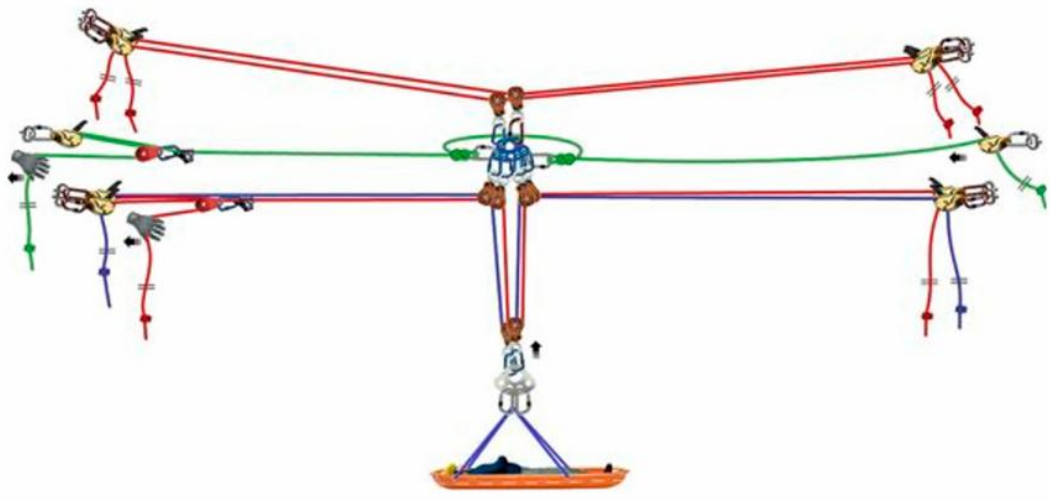
Obrázok 6 Jednoduchá lanovka – zostup k zranenej osobe (vlastné spracovanie)

Na obrázku 7 je znázornenie transportu zranenej osoby smerom nadol po nosnom lane pomocou nosidiel. Komfort zachranňovaného je nízky a pohyb je menej plynulý.



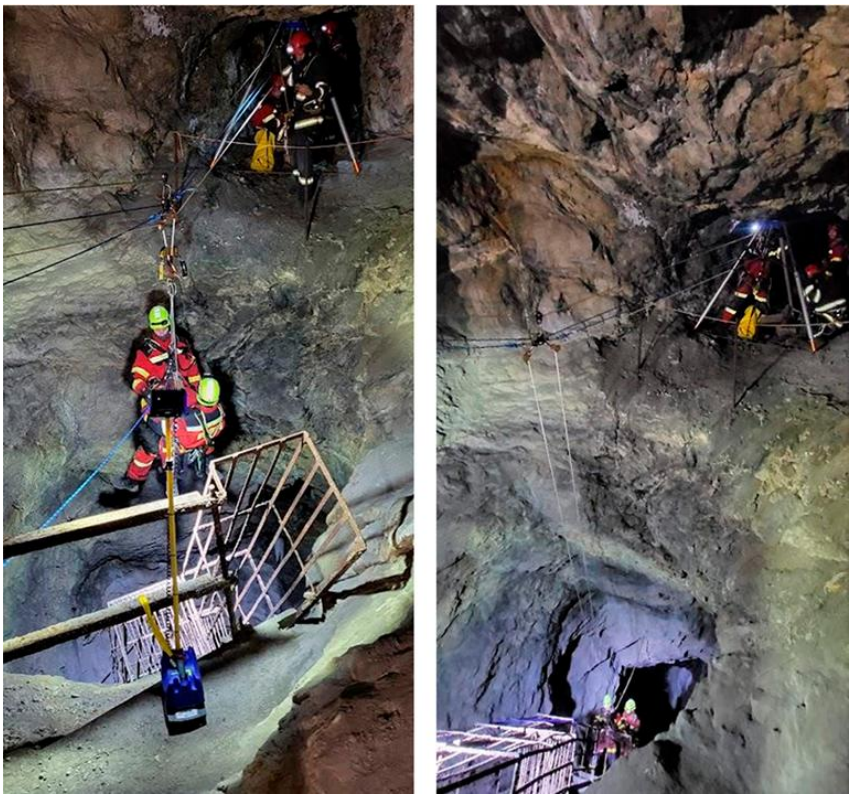
Obrázok 7 grafické znázornenie prechodu cez hranu s evakuačnými nosidlami z priestoru vetracej šachty (A – znázornenie kotviacej dosky na ktorej sú napojené evakuačné nosidlá, B – znázornenie kladkostroja na vyťahovanie nosidiel) (vlastné spracovanie)

Na obrázku 8 je znázornená metóda Tirloského traverzu, kde metóda je založená na manipulácii s bremenom (v tomto prípade s evakuačnými nosidlami) vo vertikálnom aj horizontálnom smere. Tento spôsob záchrany je však náročnejší na čas, vybudovania kotviacich stanovísk, traverzu, počet použitých pomôcok ale aj počet lezcov, ktorí zostavujú tento lanový systém. Po vykonaní prieskumu pomocou jednoduchej lanovej dráhy dvomi lezcami a po určení spôsobu záchrany použitím tyrolského traverzu môže byť osoba vyslobodená rýchlejšie a bezpečnejšie.



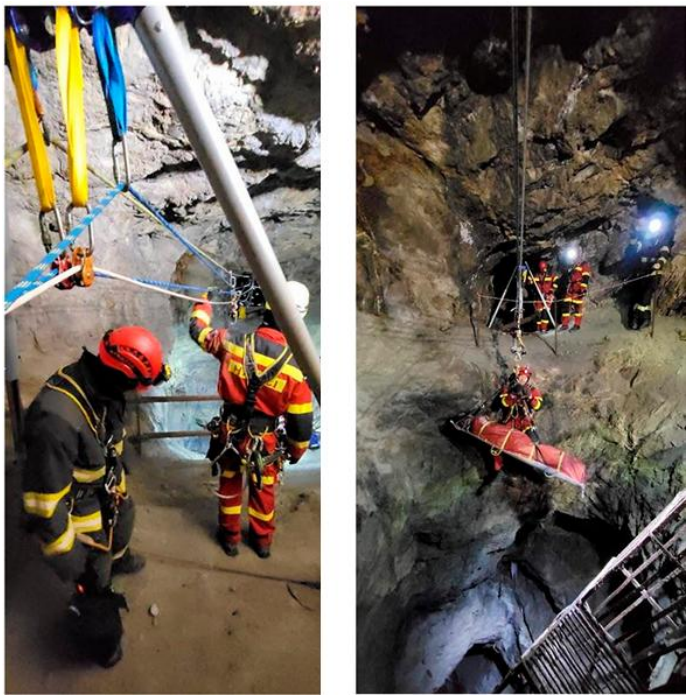
Obrázok 8 Tirolský traverz (vlastné spracovanie)

Na obrázku 9 je znázornená samotná záchrana pomocou Tirolského traverhu.



Obrázok 9 Záchrana pomocou Tirolského traverzu (vlastné spracovanie)

Na obrázku 10 je znázornený systém rozšírenej verzie Tirolského traverzu, kde pohyb nosidiel zabezpečuje elektrický navyjak. Tento prvok znižuje fyzickú záťaž zasahujúcich hasičov a urýchľuje evakuáciu.



Obrázok 10 Záchrana pomocou Tirolského traverzu a motorového navyjaku (vlastné spracovanie)

3. DISKUSIA

Výsledky experimentov preukázali výrazné rozdiely medzi jednotlivými metódami záchrany osôb z podzemných priestorov. Najväčší vplyv na efektivitu zásahu mal celkový čas potrebný na evakuáciu, ktorý priamo rozhoduje o šanci na prežitie zachraňovanej osoby.

Metóda jednoduchej lanovky sa ukázala ako najrýchlejšia z hľadiska prípravy systému, no zároveň najdlhšia pri samotnej evakuácii. Tento postup je vhodný najmä pri kratších vzdialenostiach alebo keď nie je k dispozícii zložitejšie vybavenie. Nevýhodou je obmedzený komfort pre zachraňovanú osobu, ktorý môže pri dlhšom transporte viesť k sekundárnym zraneniam či zhoršeniu zdravotného stavu.

Naopak, tirolský traverz poskytol vyššiu mieru bezpečnosti a komfortu, pričom celkový čas zásahu bol kratší ako pri jednoduchej lanovke. Hlavnou nevýhodou však zostáva dlhší čas potrebný na budovanie systému a vyššia technická náročnosť, čo môže byť v prostredí s nestabilnými podmienkami rizikové. Najlepšie hodnotenia dosiahla metóda tirolského traverzu s motorovým navijakom. Táto technika skrátila čas evakuácie na minimum a zároveň znížila fyzickú záťaž hasičov. Motorový navijak zabezpečil plynulý a kontrolovaný presun, čo významne prispelo k vyššiemu komfortu aj bezpečnosti. Nevýhodou je potreba špeciálneho technického vybavenia a dostatočného priestoru na jeho nasadenie.

Z hľadiska počtu zasahujúcich hasičov boli rozdiely medzi metódami relatívne malé, no aj tu metóda s navijakom preukázala miernu výhodu. Hodnotenie pomocou Fullerovho trojuholníka potvrdilo, že rozhodujúcim kritériom je celkový čas zásahu, čo zodpovedá zásade, že pri záchrane v podzemí je kľúčovým faktorom rýchlosť.

Tieto výsledky sú v súlade s doterajšími poznatkami z medzinárodnej praxe, kde sa pri podobných zásahoch uprednostňujú technické systémy umožňujúce rýchlu a bezpečnú evakuáciu, aj za cenu vyššej náročnosti na materiálne zabezpečenie (Sanmiquel et al., 2018; Stojadinović et al., 2012; Singo et al., 2022; Brodny & Tutak, 2018; Kowalska et al., 2021).

ZÁVER

Výskum realizovaný v podzemných priestoroch bývalej magnezitovej bane Bankov potvrdil, že výber vhodnej lezeckej techniky má zásadný vplyv na úspešnosť a bezpečnosť záchranných zásahov.

Jednoduchá lanovka je síce rýchlo nasaditeľná, no pri dlhšej evakuácii predstavuje vysoké riziko a obmedzený komfort pre zachraňovanú osobu.

Tirolský traverz je univerzálnejší a bezpečnejší, avšak časovo náročnejší na prípravu. Tirolský traverz s motorovým navijakom sa ukázal ako najefektívnejšia metóda, pretože výrazne skrátil celkový čas zásahu, znížil fyzickú záťaž zasahujúcich a zvýšil bezpečnosť aj komfort evakuovanej osoby.

Na základe zistení možno odporučiť, aby jednotky HaZZ v podmienkach podzemných banských diel uprednostňovali práve techniky s využitím mechanizovaných prvkov, ktoré dokážu výrazne urýchliť priebeh zásahu. Zároveň je potrebné zabezpečiť dostatočný výcvik príslušníkov v používaní týchto systémov a pravidelne preverovať ich pripravenosť v reálnych podmienkach.

Výsledky prispievajú k zvýšeniu úrovne pripravenosti a efektívnosti zásahov HaZZ v prostredí opustených baní, kde je čas rozhodujúcim faktorom pri záchrane ľudských životov.

LITERATÚRA

Brodny, J., & Tutak, M. (2018). Analyzing similarities between the European Union countries in terms of the structure and volume of energy production from renewable energy sources. Energies, 11, 2407. https://doi.org/10.3390/en11092407.

Hildebrandt, R., Marszowski, R., Lubosik, Z., & Jarosławska-Sobór, S. (2023). Transforming underground coal mine workings into critical cyber security facilities in the perspective of the European Green Deal plan. Scientific Papers of Silesian University of Technology. Organization and Management Series, 182, 79–97. https://doi.org/10.1111/j.0361-3666.2003.00237.x

Kowalska, D., Jarosławska-Sobór, S., & Brodny, J. (2021). Occupational health and safety management in the mining sector—A multiple case study. Resources, 10, 65. https://doi.org/10.3390/resources10060065.

Li, X., Zhou, Z., Li, X., Zhang, L., & Zhou, J. (2023). Investigation on coal miners' unsafe behavior and management system optimization based on grounded theory and SEM. Sustainability, 15, 11803. https://doi.org/10.3390/su151511803

Su, G., & Hu, E. (2024). Research on coal mine safety risk evolution and key hidden dangers under the perspective of complex network. Scientific Reports, 14, 20624. https://doi.org/10.1038/s41598-024-71004-2

Naeini, S. A. B., & Badri, A. (2023). Identification and categorization of hazards in the mining industry: A systematic review of the literature. International Review of Applied Sciences and Engineering, 15, 1–19. https://doi.org/10.1556/1848.2023.00621

Sanmiquel, L., Bascompta, M., Rossell, J. M., Anticoi, H. F., & Guash, E. (2018). Analysis of occupational accidents in underground and surface mining in Spain using data-mining techniques. International Journal of Environmental Research and Public Health, 15, 462. https://doi.org/10.3390/ijerph15030462

Stojadinović, S., Svrkota, I., Petrović, D., Denić, M., Pantović, R., & Milić, V. (2012). Mining injuries in Serbian underground coal mines—A 10-year study. Injury, 43, 2001–2005. https://doi.org/10.1016/j.injury.2011.08.018

Singo, J., Isunju, J. B., Moyo, D., Bose-O'Reilly, S., Steckling-Muschack, N., & Mamuse, A. (2022). Accidents, injuries, and safety among artisanal and small-scale gold miners in Zimbabwe. International Journal of Environmental Research and Public Health, 19, 8663. https://doi.org/10.3390/ijerph19148663

Qiang, X., Li, G., Fan, C., Zhao, W., & Wang, Q. (2025). The full lifecycle evolution model of accidents: A case study of underground metal mines in China. Applied Sciences, 15, 4004. https://doi.org/10.3390/app15074004

Marek Plavčko, pplk., Ing., Bc.

Krajské riaditeľstvo Hasičského a záchranného zboru v Košiciach, Požiarnická č. 4, 040 01, Košice

e-mail:marek.plavcko@minv.sk

Ivanna Betušová, Ing.

Fakulta banictva, ekológie, riadenia a geotechnológií, Technická univerzita v Košiciach, Letná č. 1/9, blok A, 2. posch., 042 00, Košice

e-mail:ivanna.betusova@tuke.sk

Miroslav Betuš, pplk., Ing., PhD.

Fakulta banictva, ekológie, riadenia a geotechnológií, Technická univerzita v Košiciach, Letná č. 1/9, blok A, 2. posch., 042 00, Košice

e-mail: miroslav.betus@tuke.sk

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.77-87
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

THE MAJOR CHALLENGES FACING SLOVAK ROAD AND RAILWAYS INFRASTRUCTURE: CURRENT CONDITIONS, ADMINISTRATION AND PRIORITIES

MICHAL MIŠKE, LUCIA FIGULI

ABSTRACT: The aim of the paper is to assess the current condition of bridges in Slovakia with an emphasis on two key determinants: the ownership and administration of structures and their structural health condition. The study combines official data from the Road Database of the Slovak Road Administration (SSC), available information from the Slovak Railways (ŽSR), findings of the Supreme Audit Office of the Slovak Republic (NKÚ SR), and analytical outputs of the Value for Money Division (UHP). The paper presents an analysis of data related to ownership, administration, categories of current health condition, and accompanying documentation, providing a transparent overview of where the highest risks are concentrated. These infrastructures were identified for the purposes of the REMAKE 3D project. As part of this project, several activities were undertaken to collect information and data; however, such information is often inaccessible or does not exist. The paper includes details about bridge ownership based on a comparison of owner databases, a BIM model of bridge M7441, and an example of image processing for defect detection. The conclusion and discussion section outlines proposals for future research.

KEYWORDS: *Bridges, Road Infrastructure, Railway Infrastructure, Model.*

INTRODUCTION

The health condition of Slovakia bridges in the first quarter of the twenty-first century is alarming. In recent years, Slovakia has joined the group of European countries that have recorded bridge collapses. As illustrated in Figure 1, this group also includes neighbouring Czechia, as well as Germany and Italy. In Slovakia various type of prestressed girders are used for many years and after the years in services the numbers of defects on precast prestressed girder are presented as removed concrete cover, corroded tendons with some ruptured wires, corroded anchors, water leakage through the carriageway and insulation, overloading of construction, hollow space or voids within concrete caused during casting of the girder, absence of shear reinforcement in prestressed girders, minimal reinforcement ratio was not fulfilled, absence of bonded post-tensioned prestressing, inadequate grouting of tendons and incorrect position of girders on the bearings as reported in Bujnakova (2017) and Bujnakova (2020). In other cases, collapses were triggered by hydraulic and geotechnical hazards such as scouring at foundations followed by slope instability, or by acute external actions attributable to the human factor, exemplified by the road bridge in Baltimore (USA) where a large, uncontrolled vessel impacted the structure. Slovakia's challenges are further compounded by ageing infrastructure, exposure to increasingly volatile hydrological events, and fragmented ownership and management responsibilities. These systemic factors shape inspection regimes, maintenance planning, and the timeliness of interventions, and they strongly influence the distribution of bridges across the poorest condition categories. The result is a widening gap between identified needs and executed work, with mounting operational restrictions and growing lifecycle costs.

In Germany, a bridge collapsed in September 2024 in the city of Dresden. The investigation found that the bridge, completed in 1971, had suffered corrosion damage during its construction through a combination of manufacturing methods employed 50 years ago and the influence of the weather on the steel during construction. This corrosion, combined with material fatigue caused by traffic stress, led to the bridge's failure. Over 68% of the tendons in the carriageway on the collapsed section were found to be severely damaged to the point of failure (Gerrard, 2024).

Figure 1 Map of countries that have experienced recent bridge collapses (Moravcik 2025)

In Italy, the Morandi Bridge in Genoa collapsed on 14 August 2018 primarily due to long-term corrosion damage to the prestressing tendons within the reinforced-concrete stays at Pier 9, which precipitated a sudden failure of the load-bearing system and a subsequent progressive collapse of the span; 43 people were killed. Corrosion was accelerated by increased moisture and chloride exposure in the marine and industrial environment, while the low-redundancy design (few load-carrying elements per pylon) and inadequate maintenance or monitoring progressively eroded the structure's reliability margins (Ponte Morandi 2025). Unfortunately, this is not an isolated case in Italy (Figuli 2021).

In Slovakia, the number of collapsed bridges has been steadily increasing. A pedestrian bridge collapsed in Spišská Nová Ves in 2020, followed by further incidents in Trstená over the Oravica River in 2021. In the past, a pedestrian bridge over the Turiec River collapsed in 2006, despite an inspection performed just one year earlier. Other reported cases include failures in Brodské and Chorvátsky Grob. The primary causes of these failures in Slovakia include ageing infrastructure, delayed allocation of financial resources, and untimely preventive measures. All these factors highlight the resilience—or lack thereof—of bridge structures and their structural health condition, which is the focus of this paper. The condition assessment is presented in Figure 2, accompanied by Table 1, which lists the exact numbers of bridges in each condition category according to the Slovak Road Administration Annual Report from 2023 (published in 2024).

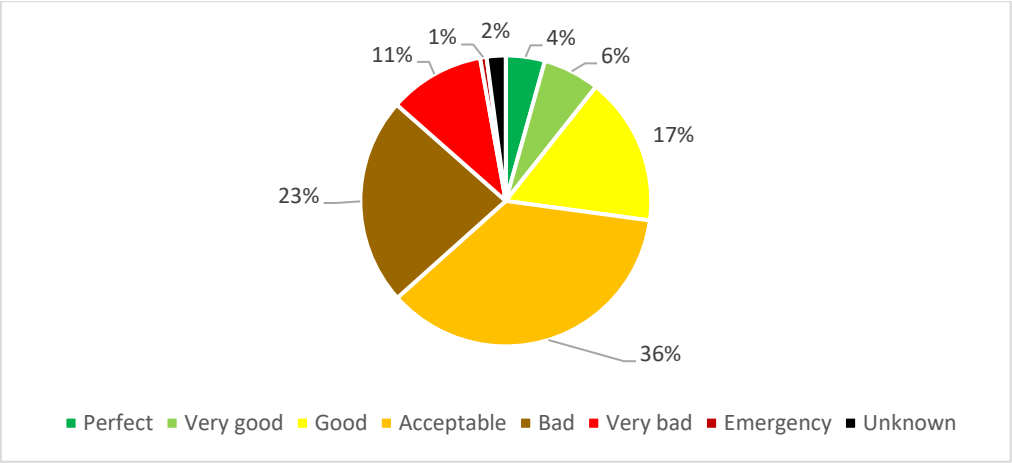


Figure 2 Classification of bridges according to structural condition

An initial examination of Table 1 does not reveal any fundamental problems; nevertheless, in terms of the evolution of the structural condition of bridges in Slovakia, it is important to reiterate the negative trend.

Table 1 Number of Bridges in each structural condition (Slovak Road Administration, 2024)

Structural conditions	Number of Bridges
Perfect	361
Very good	522
Good	1370
Acceptable	3008
Bad	1918
Very bad	885
Emergency	59
Unknown	176

Looking retrospectively, Slovakia's bridges were in better condition ten years ago, in 2015. For comparison, there were 522 bridges in perfect condition, 707 in very good condition, and 3,012 in good structural condition. In 2015, only 25 bridges in Slovakia were classified as being in emergency condition. Ten years later, this number has more than doubled. This trend is driven by several factors, which are analysed in detail in the second chapter of this article.

1. INFRASTRUCTURE PROJECT APVV REMAKE 3D

For the purposes of this paper, the challenges and proposed solutions focus on bridges identified within the APVV REMAKE 3D project (Figuli, 2025). These structures were selected following an initial screening of the area in the vicinity of the district town of Púchov. Table 2 lists 20 items of transport infrastructure; in addition to bridges, the project scope also includes the dam of the Nosice Reservoir, the Diel Tunnel carrying the new high-speed railway corridor between Bratislava and Žilina (ŽSR, 2024), as well as a pedestrian underpass and a pedestrian footbridge (Doprastav, 2025).

Table 2 Type of infrastructure of Púchov district (Figuli, 2025)

No.	Type of infrastructure	Title	Owner	Structural Conditions	Documentation
1	Dam wall	Nosice Dam	Slovak Water Management Company	???	Confidential
2	Footbridge	Footbridge for passengers and general public	Púchov City	Perfect (1)	Bridge record, overview drawing, technical inspection
3	Road bridge	???	???	???	???
4	Road bridge	???	???	???	???
5	Road bridge	???	Agricultural Cooperative Mestečko	???	???
6	Railway bridge	Viaduct	Slovak Railways	Perfect (1)	Scan
7	Railway bridge	Viaduct	Slovak Railways	Perfect (1)	Scan
8	Railway bridge	Viaduct	Slovak Railways	Perfect (1)	Scan
9	Railway bridge	Viaduct	Slovak Railways	Perfect (1)	Scan
10	Railway bridge	New railway bridge over Nosický canal	Slovak Railways	Perfect (1)	FEM model, drawings
11	Underpass	Underpass for passengers of Railway Station Nosice	Slovak Railways	Perfect (1)	???
12	Railway bridge	New railway bridge over Váh	Slovak Railways	Perfect (1)	???
13	Road bridge	New road bridge in 159,506	SC of Trenčín district	Perfect (1)	Technical inspection, drawing, FEM model
14	Road bridge	Road bridge over railway in 158.120	Slovak Road Administration	Good (3)	Bridge notebook, drawings, technical report
15	Road bridge	Road bridge Prístovec in Púchov	Slovak Road Administration	Good (3)	Bridge notebook
16	Road bridge	49_061 Road bridge over Váh in Púchov	Slovak Road Administration – IVaSC Žilina	Bad (5)	Complet project documentation, scan
17	Road bridge	Road bridge near Nimnica on the road 507	SC of Trenčín district	Bad (5)	BIM model, Concrete hardness test
18	Bicycle bridge	Cycling bridge near road 507	Out of Púchov territory	???	???
19	Road bridge	Road bridge over the Nimnický Brook	???	???	???
20	Railway tunel	Tunnel Diel	Slovak Railways	Perfect (1)	???

In Table 2, several information gaps are evident and clearly visible, along with an excessive number of different owners and administrators within the relatively small area of the town of Púchov. The table also

identifies bridges in poor condition, for which preventive measures to enhance their resilience should be adopted.

2. THE CHALLENGES IN ACHIEVING BETTER STRUCTURAL HEALTH OF TRANSPORT INFRASTRUCTURE

The first and most obvious factor is structural conditions and negative trend of bridges in Slovakia observed over recent years. For example, Figuli (2021) reports poor bridge conditions not only in Slovakia but also in Italy. Bujňáková (2020) describes this phenomenon as a growing risk for prefabricated bridges, of which there is an extremely large number in Slovakia. In another publication, Miške (2025) presents results on how strongly the structural condition depends on the year of construction. But the dependence is found to be very weak, suggesting that older bridges do not necessarily tend to be in worse condition in comparison to new bridges (Figuli 2023). Which determinants can be considered most influential in explaining the adverse progression of the bridge conditions? From the perspective of road and deck quality, the most problematic seasons are summer and winter. Overloaded heavy goods vehicles constitute the most immediate risk. Field enforcement is challenging static weigh stations have limited capacity, mobile weighing is costly and coordination intensive. A practical response combines several measures (Slomka-Slupik 2021):

- Weigh-In-Motion (WIM) gates on major corridors and ahead of sensitive bridges, with automated screening and notification for targeted pullovers,
- Geofencing and permitting regimes for oversize or overweight transports (mandated routes, time windows, escorts),
- Control of axle loads and load distribution,
- Dynamic restrictions (temporary speed reductions, one-way operation over the bridge) where diagnostics indicate reduced residual capacity.

At the sub-national level, it is advisable to install local WIM lines on approach roads to industrial zones and link them to a maintenance prioritisation model: bridges exposed to a high share of heavy goods traffic should have shorter inspection cycles, earlier prescribed diagnostic tests, and timely strengthening of critical details like waterproofing, drainage, deck surfacing, reinforcement protection. This approach minimises the risk of sudden operational restrictions and extends the bridge's lifecycle at acceptable cost.

Secondly, another fundamental problem is the fragmentation of the bridges in terms of ownership and management. In practice, this results in non-standardised assessment procedures, differing levels of maintenance, divergent priorities in the allocation of financial resources, and variable decision quality often determined by the internal rules of a given owner. Within the set of 20 transport objects included in the REMAKE 3D project, as many as eight different owners were identified, illustrating the degree of fragmentation. In addition to municipalities and self-governing regions, other administrators include the National Highway Company (NDS), the remaining regional road authorities, and private owners. This diversity translates into disparities in capacities (staffing, technical, and process), in the periodicity and quality of inspections, in the methodologies used (e.g., the scope of diagnostics and the use of non-destructive testing). The consequence is that the same types of defects may be evaluated differently, and identical risks may receive different intervention priorities across administrators (Alonso 2023).

Figure 3 Defects on bridge M7441 (Figuli 2025)

NDS typically exhibits a more favourable condition profile, largely due to a higher share of newly built sections (e.g., the Višňové tunnel and bypass links around Bratislava) and relatively more stable financing from the state budget and European funds. By contrast, sub-national administrators of class II/III roads often operate with constrained budgets and less accessible project preparation, which leads to deferred rehabilitation and faster degradation of bridges with higher age and traffic loading.
The key system-level response is to unify the rules across owners by:

- Harmonising inspection methodologies and condition classification,
- implementing risk-based prioritisation (combining condition, network criticality, and detourability),
- introducing multi-year rehabilitation programmes with transparent funding allocation,
- setting minimum standards for diagnostics and record-keeping (including open data),
- and strengthening the capacities of smaller administrators through methodological and technical support.

According to Table 2, another major issue concerns technical documentation. Each bridge owner is responsible for maintaining a complete record set; in practice, however, files are frequently incomplete, outdated, or missing altogether. In the REMAKE 3D sample, for nearly half of the twenty identified objects it was impossible to retrieve the documents needed to streamline the project workflow. For some bridges, e. g. bridge M7441 in Nimnica, the entire dossier had to be reconstructed: the concrete strength class was unknown, technical drawings were obsolete, and the bridge record card contained insufficient data. One of the few available documents was an inspection report, which confirms that the bridge is in poor structural condition and recommends preventive measures to improve resilience and extend service life. Without such measures, temporary replacement and full rehabilitation are likely.

By comparing the individual information systems of the owners referenced in the APVV REMAKE 3D project, we can also illustrate their ability to maintain bridges, keep information up to date, and, consequently, manage documentation. In terms of clarity and the ability to retrieve data, the best information system is operated by the Slovak Road Administration (SSC), where it is possible to view the necessary bridge information under the sections “Road Structures” and “Other Road Structures.” An example from the Slovak Road Administration database is shown in Figure 4. In the illustration, bridge M7441 is selected; the filter provides key details such as the bridge ID, year of construction, structural/technical condition, owner, and the estimated load-carrying capacity.

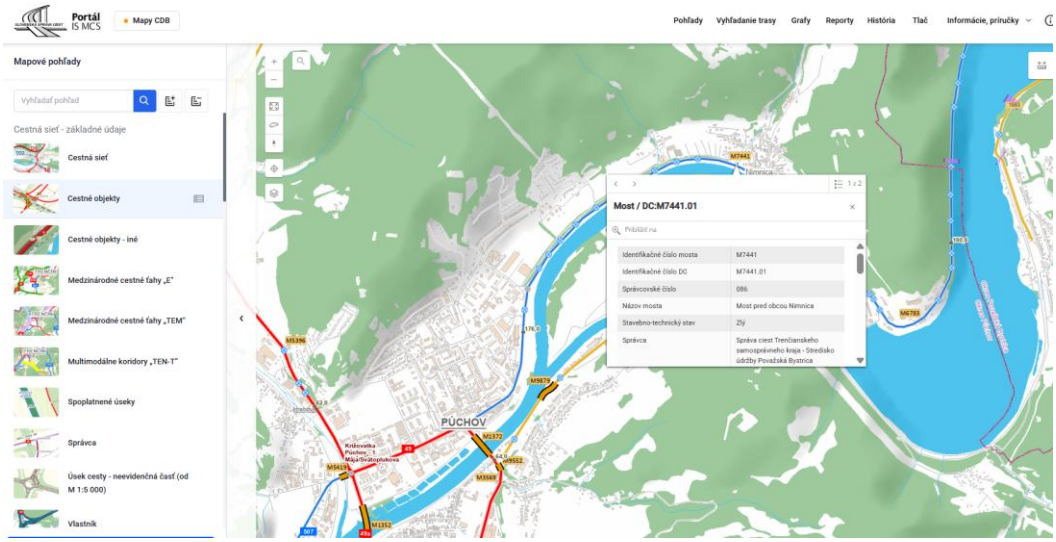


Figure 4 Road databank of the Slovak Road Administration

Another owner of bridges within the Púchov area is the Trenčín Self-Governing Region. However, its information system for road structures, in Figure 5, provides only a map of the so-called Road Maintenance Districts and the classification of the respective roads. It is not possible to retrieve more detailed information or inspection results for specific road bridges. Most information can ultimately be found in the national Road Database. This may explain why the Trenčín Region does not offer the same information-system capabilities as the Slovak Road Administration.

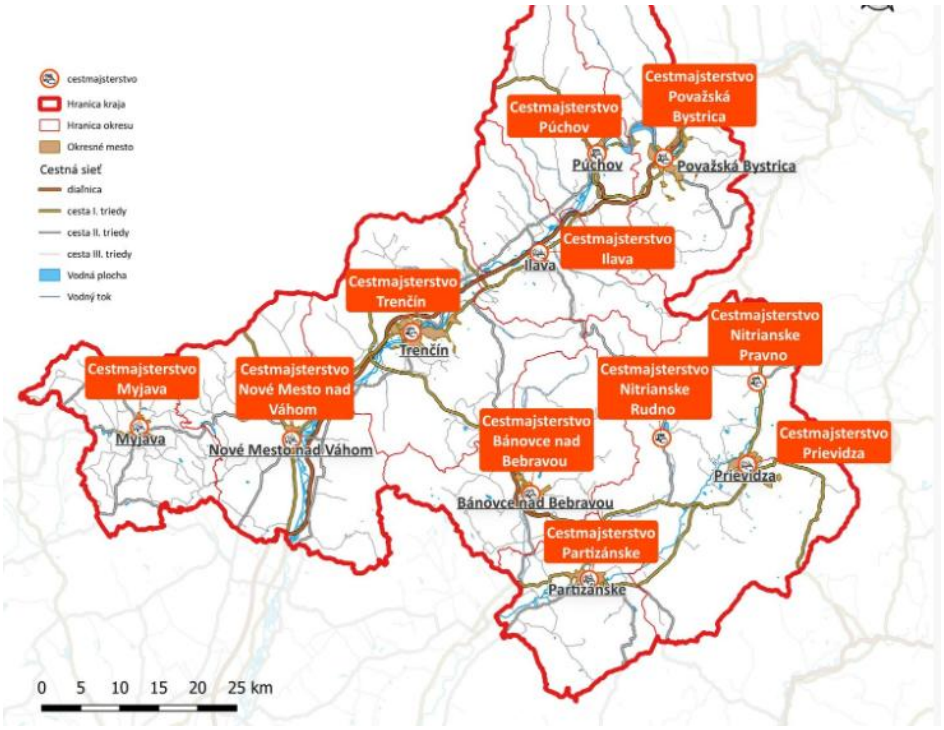


Figure 5 Road administration of the Trenčín Region

The last information system is the Information System of the Railways of the Slovak Republic (Figure 6). However, this system is highly non-intuitive. It does not provide options to display different layers; only the routes i.e., railway corridors that are highlighted on a plain white map background. As with the Trenčín Region's information system, it does not offer details on railway infrastructure such as bridges or tunnels. Information on railways is tightly guarded and generally inaccessible to the public, primarily for security reasons.

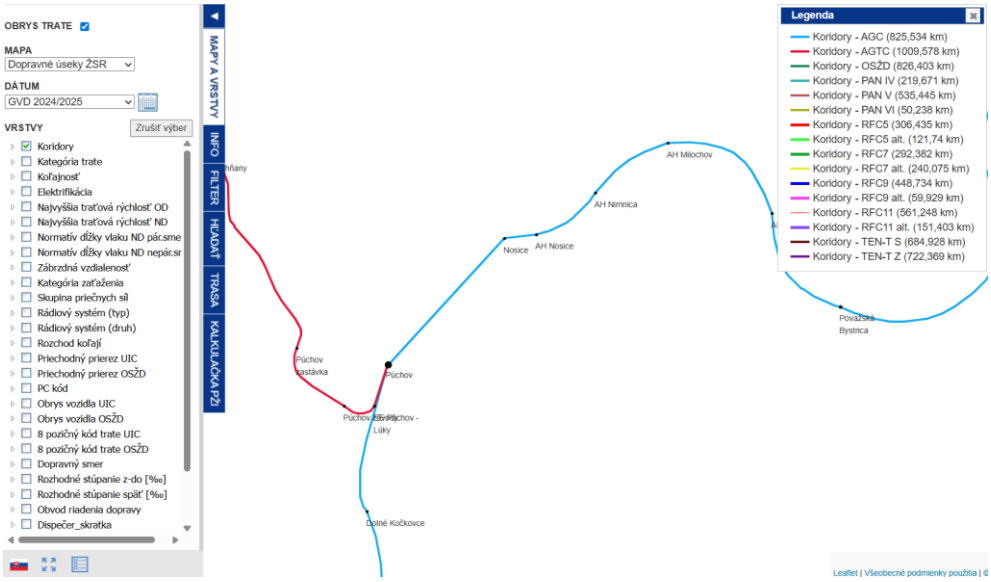


Figure 6 Information system of Slovak Railways

Unfortunately, none of the other owners of bridges in the APVV REMAKE 3D project have any information system or database. The unavailability of key information can lead to incorrect managerial decisions, which in turn may negatively affect the structural condition of the road or railway infrastructure.

The value of documentation is not merely archival, it directly affects diagnostic accuracy, load-rating reliability, the choice of intervention, and cost. Absent or inconsistent records demand conservative assumptions, additional testing, and redesign effort delaying decisions and inflating budgets. Conversely, a current, standardised dossier enables risk-based prioritisation and reduces the probability of over or under design.
To address these gaps, we propose a minimum “Bridge Documentation Set” and a process for its upkeep:

- Core records: as-built drawings, material specifications (including concrete strength class and reinforcement details), design load model, expansion joints/bearings data, and waterproofing details,
- condition history: full inspection lineage, defect logs with geolocation, photographs, and repair records,
- capacity evidence: calculations or load ratings, results of non-destructive tests (rebound hammer, UPV, GPR), cores where applicable, and any finite-element models.
- administrative data: ownership and manager of record, traffic class, detour availability, and criticality ranking,
- digital management: a common data environment (CDE) with version control, mandatory metadata, and open exchange formats, e. g. IFC/BIM, PDF/A, scheduled reviews tied to inspection periodicity.

For bridge M7441 specifically, priority actions include targeted material identification (cores with chloride profiling and carbonation depth), verification of reinforcement from GPR, bearing and joint assessment, and an updated load rating. Preventive measures should favour incremental, cost-effective interventions localized concrete repair and re-alkalisation where feasible, cathodic protection or corrosion inhibitors on high-risk zones, waterproofing and drainage upgrades, and deck surfacing improvements before committing to major capital works. This staged approach preserves safety, extends service life, and optimises limited budgets (Alonso 2023). A BIM model was also created for bridge M7441, as the available documentation was outdated and lacked sufficient technical detail. BIM is widely used today and offers numerous applications throughout the project lifecycle.

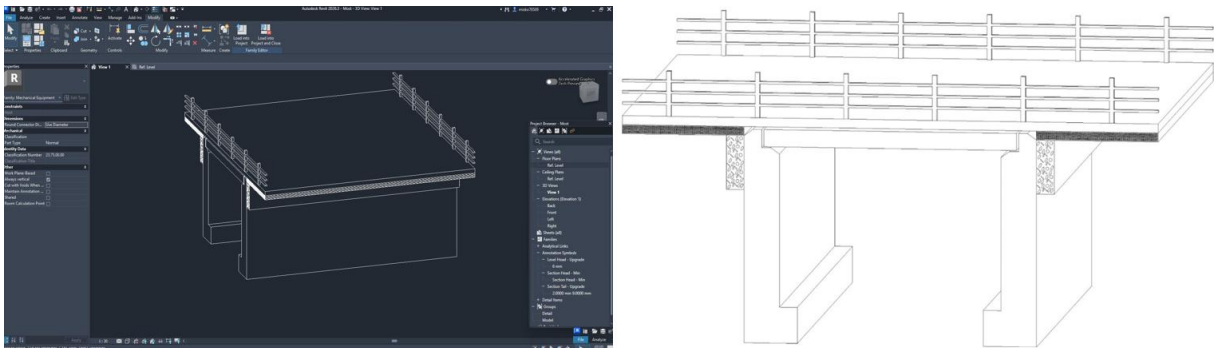


Figure 7 BIM model of M7441 bridge

DISCUSSION AND CONCLUSION

The analysis shows that the condition of bridges in Slovakia results from a confluence of technical, organizational, and process factors. The negative trend in structural condition is not driven by age alone, but primarily by environmental exposure (chlorides, hydrological extremes, thermal cycles), heavy-traffic loading, and uneven quality of asset management. Ownership fragmentation and divergent inspection methodologies lead to inconsistent diagnostics, differing priorities, and delayed implementation of interventions. A critical risk accelerator is incomplete or missing documentation, which increases uncertainty in load-rating, inflates preparation costs, and slows decision-making.

In general, the risk landscape is broader than discussed here. Nevertheless, from a practical bridge-management perspective, these three risks are foundational and tightly interlinked with others that are

either seasonal such as floods, scour, freeze–thaw damage, or landslides, or as extraordinary, including accidental impacts (ships, vehicles), fires, or rare geotechnical failures. Climate variability amplifies several of these hazards by increasing hydrological extremes and thermal gradients, which in turn accelerate deterioration mechanisms already highlighted. Crucially, the three core risks act as multipliers: poor condition and fragmented ownership reduce preparedness and slow interventions, while documentation gaps hinder rapid diagnostics during emergencies. Addressing the core set through harmonized inspections, risk-based prioritisation, and robust documentation, therefore delivers co-benefits: it improves resilience to seasonal stresses, shortens recovery after extraordinary events, and reduces the likelihood that a local defect cascades into a network-level disruption.

Practice points to core recommendations are:

- harmonise inspection methodologies and condition classification across owners and link them to shorter inspection cycles for bridges with high heavy-goods traffic shares,
- implement risk-based prioritisation and multi-year rehabilitation programmes tied to risk, network criticality, and detour ability, with transparent funding allocation,
- establish a minimum Bridge Documentation Set and manage it within a common data environment, including systematic collection of diagnostic data and updated load-capacity calculations.

The deployment of WIM systems, geofencing for oversize or overweight transport, and operational restrictions where residual capacity is reduced lowers fatigue effects and the risk of sudden operational limitations. Overall, shifting from reactive to proactive, data-driven bridge management is key to improving safety, resilience, and the efficiency of public expenditures. Of course, there are also some strategies such as implementation of advanced technologies (UAV for defect detection, image processing, vibration sensors, humidity sensors, digital twins) to have relevant information in real time. Nevertheless, the implementation of these technologies is costly, and the high number of bridges in Slovakia makes widespread deployment unrealistic at present.

ACKNOWLEDGEMENT

This article was supported by IGP I-24-028-05 GS_Miške Michal and by The Ministry of Education, Science, Research and Sport of the Slovak Republic and Slovak research and development agency, grant number APVV-22-0562 Strengthening the REsilience MAnagement of Key infrastructue Elements using advances in 3D modeling

REFERENCES

Alonso, R. L. T., et al. (2023). The Use of De-Icing Salts in Post-Tensioned Concrete Slabs and Their Effects on the Life of the Structure. Retrieved September 23, 2025, from https://www.mdpi.com/2076-3417/13/12/6961

Bujňáková, P., Strieška, M. (2017). Development of Precast Concrete Bridges during the last 50 Years in Slovakia. Procedia Engineering, Retreived September 22, 2025, from doi:10.1016/j.proeng.2017.06.013

Bujňáková, P. (2020): Anchorage system in old post-tensioned precast bridges. Civil and Environmental Engineering, 16, vol. 2, 2020, p. 379 – 3871, ISSN 13365835. available at: doi 10.2478/cee-2020-0038

Gerrard, N. (2024). Cause of German bridge collapse revealed as entire structure has to be demolished. Retrieved September 24, 2025, from https://www.constructionbriefing.com/news/cause-of-german-bridge-collapse-revealed-as-entire-structure-has-to-be-demolished/8049290.article?zephr_sso_ott=PY3BXP

Figuli, L. et al. (2023). Long life structural health monitoring of selected bridges. Retrieved September 17, 2025, from https://www.sciencedirect.com/science/article/pii/S2352146523004295

Figuli, L. et al. (2025). Project of APVV: REMAKE 3D. Retrieved September 22, 2025, from https://remake3d.uniza.sk/

Figuli, L et al. (2021). Recent developments on inspection procedures for infrastructure using UAVs. Modern Technologies Enabling Safe and Secure UAV Operation in Urban Airspace. Amsterdam: IOS Press. 2021. p. 21-31 ISBN 978-164368189-4

Miške, M. (2025). Aplikácia korelačnej analýzy na stavebnotechnický stav mostov na Slovensku. Retrieved September 17, 2025, from https://drive.google.com/file/d/1gebpMciT8ig9dm6eEisLuGwbAHk78igs/view

Moravčík, M., et al. (2025). Determination of the load-carrying capacity of existing post-tensioned continuous segmental bridge using step-by-step analysis supported by static proof-load testing. Retrieved September 22, 2025, from https://www.sciencedirect.com/science/article/abs/pii/S2352012425016753

Ponte Morandi: online la relazione della Commissione Ispettiva Mit. Ministero delle infrastutture e dei trasporti. Retrieved September 21, 2025, from https://www.mit.gov.it/comunicazione/news/ponte-morandi-online-la-relazione-della-commissione-ispettiva-mit

Slomka-Slupik, B., et al. (2021). Concrete Examination of 100-Year-Old Bride Structue above the Klodnica River Flowing through the Agglomeration of Upper Silesia in Gliwice: A Case Study. Retrieved September 20, 2025 from https://pmc.ncbi.nlm.nih.gov/articles/PMC7922151/

Slovak Road Administration. (2024). Výročná správa za rok 2023. Retrieved September 20, 2025, from https://www.ssc.sk/files/documents/vyrocne_spravy/vyrspr_2023.pdf

Doprastav a. s. (2023). ŽSR, Modernizácia trate Púchov – Žilina, pre rýchlosť do 160 km/h, I. etapa. Doprastav a. s. Retrieved September 21, 2025, from https://www.asb.sk/stavebnictvo/inzinierske-stavby/zsr-modernizacia-trate-puchov-zilina-pre-rychlost-do-160-km-h-i-etapa

ŽSR. (2024). 2023 Výročná správa. Retrieved September 20, 2025, from https://www.zsr.sk/files/o-nas/vyrocne-spravy/vyrocnasprava2023.pdf

Michal Miške - Ing.

ŽILINSKÁ UNIVERZITA V ŽILINE, Faculty of Security Engineering, Department of Security Engineering

e-mail: michal.miske@uniza.sk

Lucia Figuli – doc. Ing. ,PhD.

ŽILINSKÁ UNIVERZITA V ŽILINE, Faculty of Security Engineering, Department of Security Engineering

e-mail: lucia.figuli@uniza.sk

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.88-98
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

FYZICKÉ ÚTOKY NA PEŇAŽNÉ AUTOMATY: TYPOLÓGIA A TRENDY

PHYSICAL ATTACKS ON ATMS: TYPOLOGY AND TRENDS

LUKÁŠ LENCSÉS, LUCIA FIGULI

ABSTRACT:
This article examines the growing problem of physical attacks on cash ATMs, defining the security features of these devices, classifying attack typologies, and evaluating statistical trends for the European Union and Slovakia using publicly available reports. Findings indicate a marked increase in physical ATM attacks between 2020 and 2024 (from 3,722 to 5,953 incidents) and the predominance of explosive methods, with most events occurring at night or in the early morning. The analysis shows that material losses peaked early in the period and subsequently declined, with only modest fluctuations thereafter. The article concludes with a recommendation to reassess and expand the testing standards of EN 1143-1 due to the vulnerability of ATMs to bomb attacks.

KEYWORDS: *ATM, Bomb attacks. EN 1143-1.*

ÚVOD

Peňažné automaty, nazývané aj bankomaty, sú dnes neoddeliteľnou súčasťou našich každodenných životov. Umožňujú nám rýchly a jednoduchý prístup k peniazom takmer kedykoľvek a kdekoľvek, bez potreby návštevy pobočky banky. No práve ich dostupnosť a vysoký obsah hotovosti z nich robí časté ciele kriminálnych útokov.

Aj napriek čoraz väčšej snahe digitalizovania platieb v Európskej únii, je hotovosť stále dominantným spôsobom platenia. Na Slovensku je až 60% všetkých predajných transakcií vykonávaných v hotovosti, čo predstavuje len o 2% menej ako v Nemecku. Napriek tomu je situácia v Nemecku ďaleko zložitejšia, a vysoký počet peňažných automatov, ktorými disponuje, je jednou z hlavných príčin zvýšenej frekvencie útokov. Len v roku 2022 bolo v Nemecku vykradnutých takmer 500 peňažných automatov (Ižip, 2024).

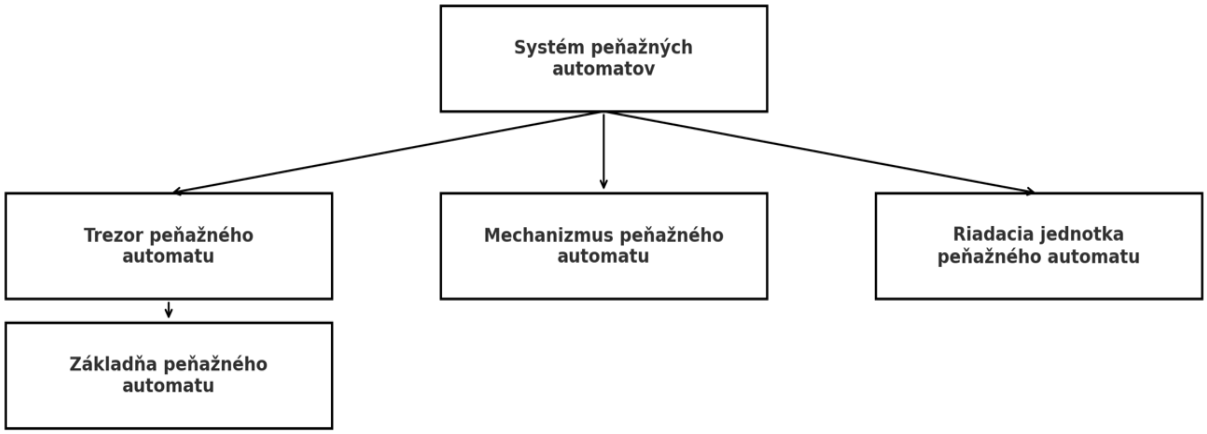
Kým v minulosti boli typické najmä podvody s kartami alebo zneužívanie softvéru bankomatov, v posledných rokoch sú čoraz častejšie práve fyzické útoky. Tie majú za cieľ násilným spôsobom otvoriť alebo poškodiť trezorovú časť bankomatu tak, aby sa páchatelia dostali k hotovosti.

Zvýšenú mieru fyzických útokov na peňažné automaty možno pripísať viacerým faktorom. V prvom rade ide o jednoduchý prístup k hotovosti, ktorý je pre páchateľov priamou motiváciou. Peňažné automaty sú často umiestnené na verejne prístupných miestach, mimo priameho dohľadu bankových zamestnancov alebo bezpečnostných služieb. Obrovský vplyv majú aj sociogénne činitele, ako chudoba, ekonomická stagnácia, nezamestnanosť a migrácia.

Obmedzený počet relevantných vedeckých článkov a publikácii iba zdôrazňuje daný problém. Väčšina publikácií sa témou zaoberá len okrajovo: analýza hodnoty daktyloskopických stôp po výbuchu bankomatu (Smet, 2021), hodnotenie odolnosti na základe plynovej explózie v trezoroch (Radeanu, 2019), Analýza použitých výbušnín pri útokoch na bankomaty v Brazílii (Lograd, 2022), proces hodnotenia odolnosti proti vlámaniu pri použití výbušnín (Zvaková, 2021).

1. KONŠTRUKCIA A BEZPEČNOSTNÉ PRVKY PEŇAŽNÝCH AUTOMATOV

Požiadavky na konštrukciu a skúšky odolnosti proti vlámaniu pre trezory rieši európska technická norma EN 1143-1, ktorá v úvode definuje predmetnú terminológiu. Pod pojmom peňažný automat sa rozumie automatizované zariadenie, ktoré zákazníkom umožňuje rýchly prístup k hotovosti a základným bankovým službám bez nutnosti návštevy pobočky. Obrázok 1 zobrazuje štandartnú bankomatovú schému podľa normy EN 1143-1. (EN 1143-1, 2019)



Obrázok 1 Schéma peňažného automatu podľa EN 1143-1 (EN 1143-1, 2019)

Systém peňažného automatu - predstavuje celý peňažný automat ako komplexné zariadenie. Zabezpečuje funkciu od uloženia a ochrany hotovosti, cez technické operácie, až po komunikáciu s bankovou sieťou. Najviac chránenou časťou peňažného automatu je trezor peňažného automatu. Podlieha certifikácii podľa normy EN 1143-1. Norma rozlišuje viacero bezpečnostných tried podľa toho, koľko času a aké nástroje sú potrebné na prekonanie trezoru. V praxi sa pri bankomatoch najčastejšie používajú trezory v triedach II až IV, pričom v exponovanejších lokalitách sa môžu uplatniť vyššie triedy. Konštrukčne ide o viacvrstvové oceľové schránky so zosilnenými dvierkami, certifikovanými zámkami, detekčnými senzormi a často aj s integrovanými systémami na znehodnotenie bankoviek (ISZB). (EN 1143-1, 2019)

Základňa peňažného automatu - slúži ako kotviaci prvok, upevňuje trezor k podlahe alebo stene (EN 1143-1,2019).

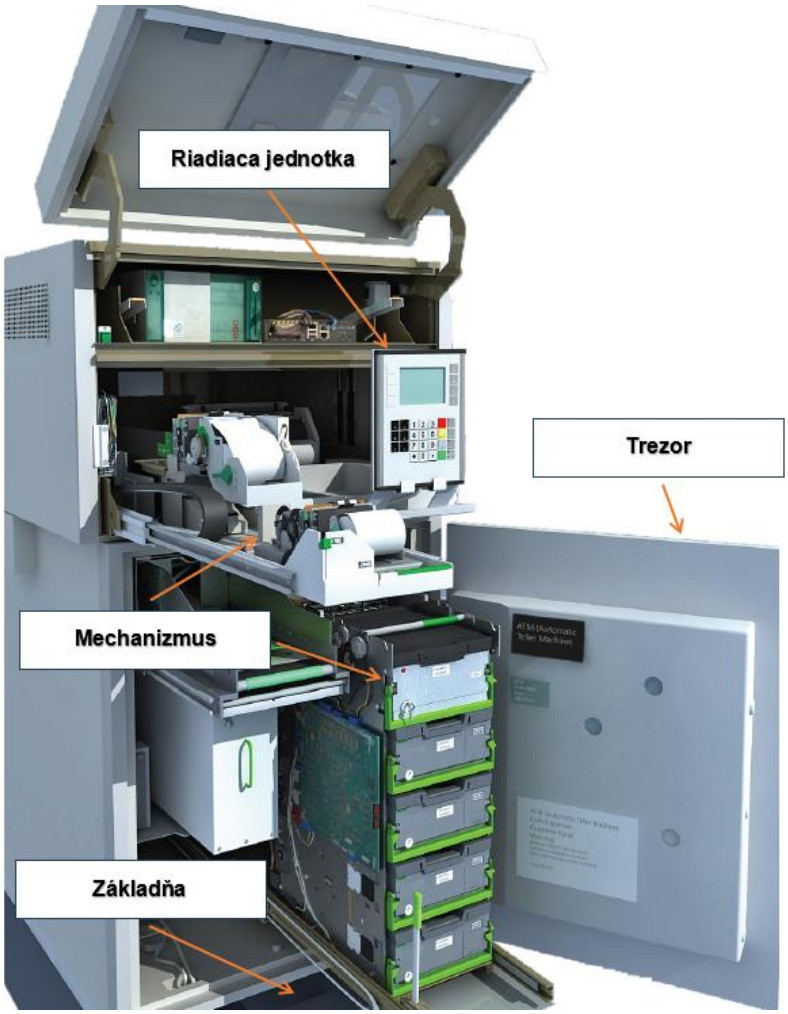
Mechanizmus peňažného automatu - zahŕňa technické a pohyblivé časti bankomatu. Obsahuje (Roddam, 2024):

- kazetový systém - kazety s bankovkami,
- výdajnú jednotku - vyberá bankovky z kaziet a podáva ich zákazníkovi,
- snímače - kontrolujú, či bola vydaná správna bankovka a či nie je poškodená.

Riadiaca jednotka peňažného automatu - počítačový modul s pripojeným softvérom, ktorý funguje ako centrálny systém bankomatu. Zabezpečuje: komunikáciu s bankovým systémom, spracovanie transakcií, ovládanie periférií(Roddam, 2024).

Bezpečnostné prvky peňažného automatu - bankomaty sú konštruované tak, aby dokázali odolať rôznym formám fyzického útoku. Ich konštrukcia zahŕňa pevné oceľové krytie a zosilnené uzamykacie systémy, ktoré výrazne komplikujú akýkoľvek pokus o neoprávnené vniknutie. Tieto bezpečnostné prvky pravdepodobnosť poškodenia zariadenia. Medzi ďalšie bezpečnostné prvky bankomatov zaradujeme (Europol, 2019):

- ISZB - inteligentné systémy na znehodnocovanie bankoviek,
- systémy bezpečnostnej hmly,
- kamery CCTV.



Obrázok 2 Grafická schéma peňažného automatu (Uplogix, 2013)

2. TYPOLÓGIA FYZICKÝCH ÚTOKOV NA PEŇAŽNÉ AUTOMATY

Organizácia EAST (European Association for Secure Transactions), cieľom ktorej je dosiahnuť jednotné používanie definícií medzi organizáciami a orgánmi činnými v trestnom konaní pri popise fyzických útokov na peňažné bankomaty, rozoznáva útoky na peňažné bankomaty (EAST,2023):

Útoky s použitím výbušných látok

Pri prekonávaní peňažných automatov sa pre svoju časovú efektívnosť využívajú útoky s použitím výbušných látok. Umožňujú za krátky čas prekonať objektovú ochranu a dostať sa k vnútorným priestorom trezoru (EAST,2023).

Explozívne útoky sú páchané pomocou (EAST,2023):

- plynu - do vnútra trezorovej časti alebo priestoru bankomatu sa zavedie horľavá plynno-vzdušná zmes a následne dôjde k jej zapáleniu/odpáleniu tak, že vzniknutý tlak alebo plameň naruší konštrukciu trezoru a umožní páchateľom dostať sa k hotovosti,
- výbušniny - páchatelia vkladajú do trezoru pevné trhaviny a ich odpálením otvoria dvierka trezoru. Tieto útoky môžu prebiehať v niekoľkých fázach. Prvý výbuch slúži na získanie prístupu – vytvorenie otvoru v trezore, ktorým sa následne vkladajú pevné trhaviny, ktoré sú potom odpálené s cieľom otvoriť trezor.

Obrázok 3 Pozostatok peňažného automatu po útoku výbušninou (Briška, 2025)

Vytrhnutie bankomatu – „Rip-out“

„Rip-out“ označuje fyzickú krádež bankomatu ako celku, páchateľ alebo skupina násilím odstráni bankomat zo svojej inštalácie a následne ho odvezie na miesto, kde ho otvorí mimo dohľadu. Ide o rýchlu, vysoko deštruktívnu metódu, ktorej cieľom je získať prístup k hotovosti bez zdĺhavého mechanického prelamovania trezora na mieste (EAST,2023).

Pre metódu „Rip-out“ sú typické tieto nástroje (EAST,2023):

- vozidlá,
- laná,
- háky.

„Rip-out“ útoky spôsobujú značné materiálne škody a majú široké dôsledky. V mnohých krajinách sa tejto metóde venujú špecializované policajné operácie a banky zintenzívnili technické i organizačné protokoly (EAST,2023).

Obrázok 4 Pozostatok peňažného automatu po „Rip-out“ útoku (Figuli, 2025)

Násilné otvorenie trezoru – „In-situ“

Útoky „In-situ“ predstavujú skupinu fyzických zásahov, pri ktorých páchatelia používajú rôzne nástroje s cieľom násilne prekonať konštrukciu bankomatu a dostať sa k hotovosti. Patria sem rôzne formy priameho mechanického prelamovania, od vŕtania a rezania až po násilné páčenie. Kombinácia týchto metód býva veľmi častá v závislosti od cieľa, dostupnosti techniky a pripravenosti páchateľov. V závislosti od použitých nástrojov rozdeľujeme „in-situ“ útoky na (EAST,2023):

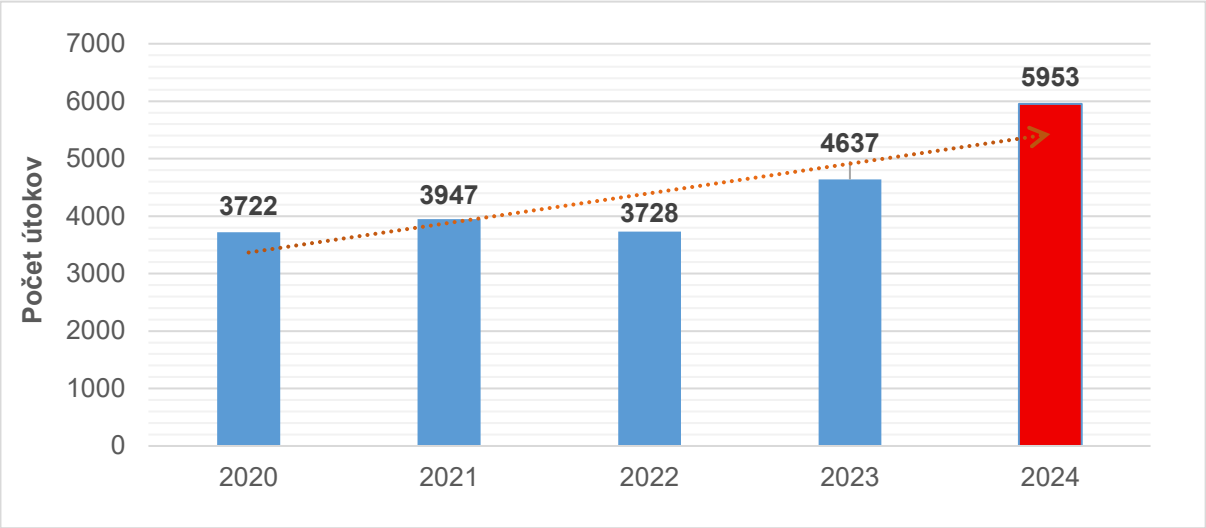
- termické rezanie - útok, pri ktorom útočník používa termický rezací spôsob aby získal otvor do vnútra,
- vŕtanie - pokus o prekonanie trezorových častí vytvorením otvorov v pevnej konštrukcii pomocou vŕtania, ktorými sa snažia vyradiť mechanizmy zámku alebo dosiahnuť na vnútorné priestory,
- rezanie - použitie rezacích elektrických nástrojov (brúska, píla) na rezanie plášťa a dvierok trezoru s cieľom získať prístup,
- násilné otvorenie - pokus o násilné otvorenie trezoru použitím mechanických síl.

Obrázok 5 Pozostatok peňažného automatu po „Rip-out“ útoku (Doherty, 2017)

3. Analýza fyzických útokov

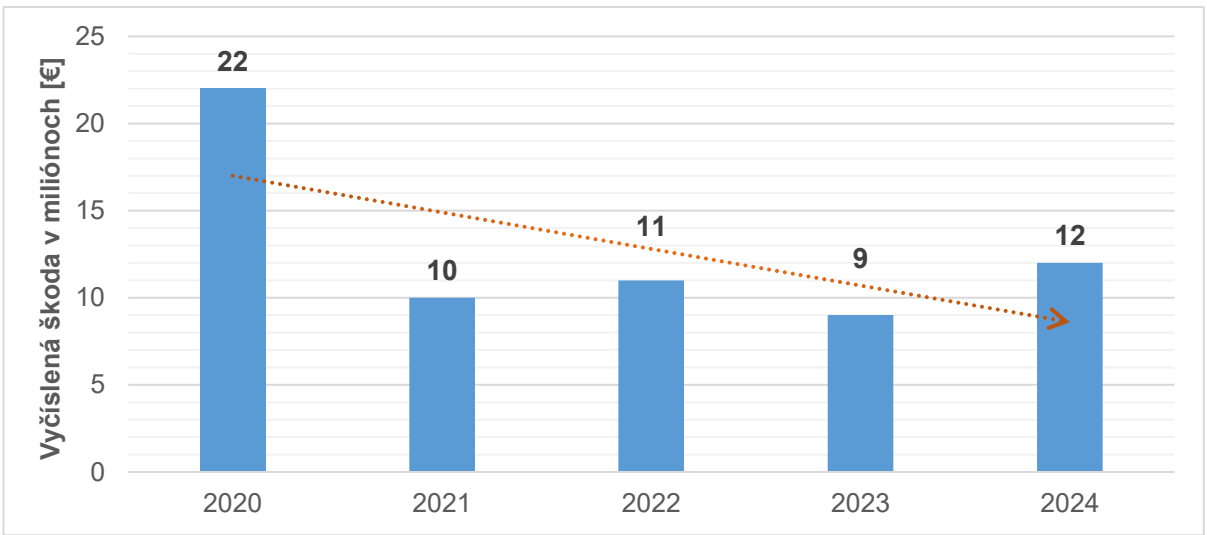
Vo svete a Európskej únii

Medzi rokmi 2020 a 2024 počet fyzických útokov na bankomaty v EU vzrástol z 3 722 prípadov na 5 953 prípadov, teda približne o 60 % za päť rokov. Zaznamenáme mierny nárast v roku 2021 oproti roku 2020 (3 722 → 3 947), mierny pokles v roku 2022 (3 947 → 3 728), potom výraznejší nárast v roku 2023 (3 728 → 4 637) a silný skok v roku 2024, kedy počet útokov dosiahol 5 953 (EAST, 2025).



Obrázok 6 Vývoj fyzických útokov na bankomaty v EU 2020-2024

Medzi rokmi 2020 a 2024 klesli celkové hlásené škody z €22 mil. na €12 mil., predstavuje to teda pokles približne o 45,5 % za päť rokov. Napriek tomu sa hodnoty každoročne menia: po prudkom poklese v roku 2021 (−54,5 % oproti 2020) nasledoval mierny nárast v 2022 (+10 %), ďalší pokles v 2023 (−18 %) a opäť výraznejší nárast v 2024 (+33,3 % oproti 2023) (EAST, 2025).



Obrázok 7 Výška škody spôsobená fyzickými útokmi v EU 2020-2024

Lúcio Lograd vo svojej štúdii chemickej analýzy výbušnín použitých pri lúpežiach bankomatov a trezorov v Brazílii v období 2014–2020 analyzoval reálne prípady s cieľom charakterizovať typy výbušnín, ktoré boli použité pri útokoch, a kvantifikovať ich relatívne zastúpenie (viď. Tabuľka 1) (Lograd, 2022).

Tabuľka 1 Identifikované zloženie výbušnín z analýzy prípadov v Brazílii

Typ výbušniny	**Počet prípadov**
Zmesi na báze chlorátov alebo perchlorátov	49
Výbušná emulzia	20
Čierny prach (black gunpowder)	12
Negatívne / nejednoznačné výsledky	11
Organická (PETN)	1

Najčastejšie identifikovanou skupinou výbušných látok boli **zmesi na báze chlorátov alebo perchlorátov**, ktoré sa vyskytli až v 49 prípadoch. Tento výsledok potvrdzuje, že ide o najrozšírenejší typ využívaný pri skúmaných útokoch. **Výbušné emulzie** sa objavili v 20 prípadoch a predstavujú druhú najpočetnejšiu kategóriu, čo poukazuje na ich relatívne časté presunutie z legálneho priemyselného prostredia do trestnej činnosti. **Čierny prach** bol zistený v 12 prípadoch, čo korešponduje s jeho dostupnosťou v pyrotechnických výrobkoch. **Organický PETN** bol zachytený len v jednom prípade, čo naznačuje jeho veľmi zriedkavý výskyt v skúmanej oblasti a období (Lograd, 2022).

Tabuľka 2 Kategorizácia výbušných látok použitých pri útokoch

Kategória	**Popis**	**Bežné zdroje**
Zmesi na báze chlorátov alebo perchlorátov	Anorganické soľné zmesi používané ako oxidačné zložky.	Pyrotechnika a ohňostroje, niektoré priemyselné chemikálie a špecializované dodávky pre priemyselné aplikácie.
Výbušná emulzia	Priemyselne vyrábané emulzie využívané v ťažbe a stavebníctve.	Dodávky a výrobky pre ťažobný a stavebný sektor.
Čierny prach	Tradičný pyrotechnický prach používaný v pyrotechnike.	Pyrotechnické produkty, petrochemikálie pre historické alebo rekreačné použitie, obchodné predajne pyrotechniky.
Organické – PETN	Organický vysoko výbušný materiál, v civilnom prostredí menej bežný.	Priemyselné/vojenské aplikácie a špecializovaní výrobcovia;

Situácia v Slovenskej republike

Vzhľadom na absenciu relevantných štatistických údajov týkajúcich sa útokov na bankomaty je pre Slovensko zhodnotenie situácie značne komplexnejšie. Štatistický úrad Slovenskej republiky síce ponúka štatistiku trestných činov, avšak samostatný trestný čin „útok na bankomat“ neexistuje a preto podľa trestnoprávnej klasifikácie je možných niekoľko zaradení:

- krádež (§ 212 TZ),
- poškodzovanie cudzej veci (§ 245 TZ),
- úmyselné všeobecné ohrozenie (§ 284 TZ).

Úplne prvé útoky na peňažné automaty na Slovenku boli realizované spôsobom „rip-out“, čiže násilným vytrhnutím za pomoci automobilov. V poslednej dobe sa situácia začala zhoršovať. Len za mesiac September evidujeme útoky na peňažné automaty v Maduniciach, Piešťanoch a Košiciach, všetko za použitia výbušnín. Za posledných 10 rokov je použitie výbušnín najčastejším spôsobom útokov na peňažné automaty v SR. Vypátrať páchateľov je pre orgány činné v trestnom konaní zložité, nakoľko na mieste činu nezanechávajú relevantné stopy, sú maskovaní a často krát používajú odcudzené evidenčné čísla motorových vozidiel. Nie je vylúčené, že sa môže jednať aj o organizované skupiny zo zahraničia. Posledný útok bol zaznamenaný v **Bratislave 30.9.2025,** kde došlo k výbuchu bankomatu, ktorý bol umiestnený pri mestskom úrade (Murajdová, 2025).

Analýzu najznámejších útokov na bankomaty v Slovenskej republike môžeme vidieť v tabuľke 3.

Tabuľka 3 Medializované prípady fyzických útokov na bankomaty za posledných 5 rokov v Slovenskej republike

Dátum	Lokalita	Čas	Škoda	Metóda útoku
22. 8. 2020	Tomášov	2:30	NEZISTENÉ	výbušnina
26. 9. 2020	Košice	3:00	90 000 €	výbušnina
19. 12. 2020	Topoľníky	v noci	15 500 €	výbušnina
13. 8. 2021	Pruské	v noci	0 €	nezistená metóda
18. 8. 2021	Drietoma	v noci	NEZISTENÉ	výbušnina
16. 6. 2021	Šoporňa	4:00	NEZISTENÉ	nezistená látka (výbuch)
16. 6. 2021	Výčapy-Opatovce	v noci	NEZISTENÉ	fyzické poškodenie
16. 6. 2021	Turňa nad Bodvou	v noci	77 000 €	výbušnina
22. 10. 2021	Rišňovce	v noci	NEZISTENÉ	výbušnina
2. 11. 2021	Nitra (Klokočina)	4:20	NEZISTENÉ	výbušnina
23. 11. 2021	Ladce	2:56	80 000 €	výbušnina
24. 10. 2022	Ivanka pri Nitre	3:00	NEZISTENÉ	výbušnina
25. 10. 2022	Ivanka pri Dunaji	4:15	150 000 €	výbušnina
4. 5. 2023	Oslany	5:00	NEZISTENÉ	výbušnina
10. 7. 2023	Ladce	v noci	18 940 €	vyrezanie otvoru
21. 6. 2024	Novoť (Orava)	4:30	0 €	výbušnina
10. 7. 2024	Dunajská Lužná	4:15	200 000 €	výbušnina
7. 11. 2024	Tvrdošovce	v noci	0 €	výbušnina
11. 12. 2024	Zlaté Klasy	4:00	0 €	výbušnina
25. 12. 2024	Bešeňová	ráno	0 €	plynová výbušnina
16.09.2025	Madunice	v noci	NEZISTENÉ	výbušnina
19.09.2025	Piešťany	v noci	NEZISTENÉ	výbušnina
19.09.2025	Košice	ráno	NEZISTENÉ	výbušnina
29.09.2025	Novoť	v noci	NEZISTENÉ	výbušnina
30.09.2025	Bratislava	ráno	NEZISTENÉ	výbušnina

Údaje v tabuľke 3 vychádzajú zo sekvenčného zberu medializovaných prípadov, teda nejde o úplný oficiálny register Polície SR alebo Ministerstva vnútra SR. Uvádzané sumy a metódy sú také, ako boli medializované, v niekoľkých prípadoch chýbajú presné údaje („NEZISTENÉ“). Sumy v stĺpci „škoda“ sa skladajú zo spôsobenej škody vplyvom útoku, ako aj celkovej odcudzenej sumy páchateľmi. Výsledky je potrebné interpretovať ako trendový obraz na základe verejne dostupných správ, nie ako definitívnu štatistiku.

Obrázok 8 Mapa fyzických útokov na bankomaty 2020-2025 (Google maps,2025)

ZÁVER

Z uvedenej analýzy fyzických útokov na peňažné automaty vyplýva, že výskyt týchto útokov v posledných rokoch narastá nie len v EU, ale aj na Slovensku. Prevládajú fyzické metódy s použitím explozívnych látok a „rip-out“ techník. Útoky sa väčšinou odohrávajú v nočných až skorých ranných hodinách, spôsobujú značné materiálne škody a sú ťažko vyšetrované vzhľadom na profesionálnu prípravu páchateľov, ich maskovanie a organizovanosť.

Neustále sa zvyšujúce množstvo prípadov indikuje neefektívnosť v posudzovaní odolnosti trezorov podľa európskej normy EN 1143-1, nakoľko samotné testovanie odolnosti voči výbuchom prebieha podľa normy odlišným spôsobom, ako postupujú páchatelia. Dodatočná certifikácia T2, vznikla ako reakcia na ďalšie nedostatky v bezpečnostných požiadavkách normy, vzhľadom na uvedenie nových a výkonnejších nástrojov na trh, schopných efektívnejšie prekonávať obranu trezorov.

Použitie výbušných látok na preniknutie do trezora peňažného automatu začína byť preferovaným spôsobom útoku páchateľov. Páchatelia používajú plyn alebo výbušniny, ktorých účelom je vyvolať silný tlakový impulz alebo poškodenie mechaniky úschovného zariadenia tak, aby získali prístup k hotovosti. Takéto explózie zároveň často poškodzujú aj okolitú infraštruktúru a zvyšujú riziko pre osoby v blízkosti miesta činu. Z týchto dôvodov uvedená analýza zdôrazňuje potrebu výskumu v predmetnej oblasti, zameraním sa na kombináciu technických riešení na zvýšenie odolnosti peňažných automatov od účinkov výbuchu.

POĎAKOVANIE

Príspevok bol podporený SPS NATO G6001 Multi Cable-Driven Robot for Detecting/Detonating Unexploded Mines and Ordnance.

LITERATÚRA

IŽIP, R. (2024, 10. AUGUSTA). *Hotovosť je kráľovnou, až kým neprídu gangy. TREND*. retrieved 30 september 2025 https://www.trend.sk/spravy/hotovost-je-kral-kym-nepridu-gangy-nemecko-ukazuje-problem-zavislosti-kesi

De Smet, M., Ramaekers, K., Verhoeven, E., Vermeulen, S., & Bekaert, B. (2021). *Influence of ink and smoke ATM security systems on dactyloscopy and subsequent DNA analysis after detonation.* Forensic Science International: Genetics, 54, 102540. https://doi.org/10.1016/j.fsigen.2021.102540

Radeanu, C., Vasilescu, G., Kovacs, A., Laszlo, R., & Miron, C. (2019). *Evaluation of the safety level to the high-quality vault with a V resistance level, based on the gas explosion test.* In *19th International Multidisciplinary Scientific GeoConference (SGEM 2019)* (pp. 845–850). STEF92 Technology. DOI: 10.5593/sgem2019/1.2/S06.107. Retrieved 30 September 2025, from https://www.researchgate.net/publication/334734721_EVALUATION_OF_THE_SAFETY_LEVEL_TO_THE_HIGH-QUALITY_VAULT_WITH_A_V_RESISTANCE_LEVEL_BASED_ON_THE_GAS_EXPLOSION_TEST

Lograd, L., Silva, M. N., Laboissiere, J. C. A., & Braga, J. W. B. (2022). *Profile of explosives's use in ATMs/cash safes robberies in Brazil.* Journal of Forensic Sciences, 67(1). https://doi.org/10.1111/1556-4029.15056. Retrieved 30 September 2025, from https://www.researchgate.net/publication/360413726_Profile_of_explosives%27s_use_in_ATMscash_safes_robberies_in_Brazil

Zvakova, Z., Boros, M., Figuli, L., & Velas, A. (2021). *Evaluation Process of the Burglary Resistance When Explosives Are Used to Create an Opening in the Barriers.* Symmetry, 13(9), 1740. https://doi.org/10.3390/sym13091740. Retrieved 30 September 2025, from https://www.mdpi.com/2073-8994/13/9/1740

STN EN 1143-1 – Bezpečnostné úschovné objekty – požiadavky, klasifikácia a metódy skúšania odolnosti proti vlámaniu

Roddam, J. (2024, October 8). *System design: Design an ATM Machine.* DEV Community. Retrieved 30 September 2025, from https://dev.to/jayaprasanna_roddam/system-design-design-an-atm-machine-3l9p

European Union Agency for Law Enforcement Cooperation (Europol) & European Crime Prevention Network (EUCPN). (2019). *Preventing physical ATM attacks: Developing an effective approach.* Europol. Retrieved 30 September 2025, from https://www.europol.europa.eu/sites/default/files/documents/preventing_physical_atm_attacks.pdf

Uplogix. (2013, December 13). *M2M Management Case Study: ATMs.* Uplogix. Retrieved 30 September 2025, from https://uplogix.com/2013/12/m2m-management-case-study-atms/

European Association for Secure Transactions (EAST). (n.d.). *Terminal physical attack definitions & terminology: ATM / ATS.* EAST. Retrieved 30 September 2025, from https://www.association-secure-transactions.eu/wp-content/uploads/EAST-Terminal-Physical-Attack-Definitions-Terminology-ATM-ATS.pdf

Briška, P. (2025, 20. mája). *Billa je po výbuchu bankomatu zatvorená, banka potvrdila, že išlo o útok plynovou metódou.* MY Trnava (SME). Retrieved 30 September 2025, from https://mytrnava.sme.sk/c/23493341/pred-billou-v-piestanoch-explodoval-v-noci-bankomat.html

Figuli, L. (2023). *Mechanické zábranné prostriedky predmetovej ochrany.* [PowerPoint]. Retrieved 30 September 2025

Doherty, S. (2017, 26. December). *ATM thieves destroyed a cash machine outside Rainham railway station.* KentLive. Retrieved 30 September 2025, from https://www.kentlive.news/news/kent-news/atm-thieves-destroyed-cash-machine-975971

European Association for Secure Transactions (EAST). (2025, April 14). *European terminal fraud attacks double — For release to the media on 14 April 2025.* EAST. Retrieved 30 September 2025, from https://www.association-secure-transactions.eu/wp-content/uploads/European-Terminal-Fraud-attacks-double-for-release-to-the-media-on-14-April-2025.pdf

Murajdová, A. (2025, 29. septembra). *Výbuch v obci na severe Slovenska. Zlodeji odpálili ďalší bankomat.* TVNOVINY.sk. Retrieved 30 September 2025, from https://tvnoviny.sk/domace/clanok/990402-vybuch-v-obci-na-severe-slovenska-zlodeji-odpalili-dalsi-bankomat

Lukáš Lencsés - 1, Ing.
Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva
e-mail: lencses@uniza.sk

Lucia Figuli - 2, Doc. Ing. Phd.
Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva
e-mail: figuli@uniza.sk

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.99-108
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

BEZPEČNOSTNÍ OPATŘENÍ VE ZDRAVOTNICKÝCH ZAŘÍZENÍCH: ANALÝZA A DOPORUČENÍ

SECURITY MEASURES IN HEALTHCARE FACILITIES: ANALYSIS AND RECOMMENDATIONS

JITKA KOSÁČKOVÁ, RENATA HAVRÁNKOVÁ

ABSTRACT: This article addresses security measures in healthcare facilities, focusing on hospitals as soft targets exposed to increasing threats. The aim is to analyse current protection systems and propose measures to enhance resilience. Using both qualitative and quantitative methods, the research included analysis of legislation, technical standards, internal guidelines, and a comparison of security practices in selected Czech hospitals. The outcome is the MOBIZ methodology, which emphasises clear responsibilities, continuous staff training, and the involvement of all organizational levels. Pilot testing confirmed its applicability and demonstrated that an integrated approach combining technical, organisational, and human factors effectively reduces risks and strengthens resilience in healthcare facilities.

KEYWORDS: *Healthcare Facilities. Patient Safety. Security. Soft Targets.*

ÚVOD

Bezpečnost zdravotnických zařízení je nezbytným předpokladem pro poskytování kvalitní péče a ochranu pacientů, zaměstnanců i návštěvníků. Zdravotnická zařízení jsou vzhledem ke své povaze a koncentraci osob zařazovány mezi měkké cíle, což zvyšuje jejich zranitelnost vůči bezpečnostním incidentům.

Zkušenosti z posledních let potvrzují, že zdravotnická zařízení se musí systematicky připravovat na celé spektrum bezpečnostních hrozeb. Účinná bezpečnostní politika nesmí být omezena pouze na technická opatření, ale musí být založena na komplexním souboru organizačních a procesních mechanismů. Tyto mechanismy zahrnují zejména pravidelné vyhodnocování hrozeb a rizik, cyklickou odbornou přípravu zaměstnanců, průběžnou aktualizaci krizové dokumentace a realizaci taktických cvičení, jejichž výsledky slouží jako podklad pro optimalizaci preventivních a reakčních opatření. Jeho cílem je kriticky zhodnotit dosavadní opatření a formulovat doporučení, jež mohou přispět k posílení odolnosti zdravotnických zařízení vůči širokému spektru bezpečnostních hrozeb.

Cílem tohoto výzkumu bylo vytvořit jednotnou metodiku **MOBIZ – Metodika opatření pro bezpečnostní incidenty ve zdravotnictví** a stanovit komplexní rámec pro ochranu zdravotnických zařízení jako měkkých cílů před bezpečnostními hrozbami, které mohou ohrozit život, zdraví a bezpečnost pacientů, zaměstnanců i návštěvníků.

1. METODIKA VÝZKUMU

Metodologický rámec výzkumu vychází z kombinace kvalitativních a kvantitativních přístupů. Základními výzkumnými nástroji byla obsahová analýza právních předpisů, interních směrnic zdravotnických zařízení a technických norem. Tento postup umožnil systematicky zmapovat legislativní i provozní požadavky v oblasti bezpečnosti a vytvořit východisko pro návrh metodiky.

Metodika byla zpracována na základě upravených postupů uvedených v dokumentu *Základy ochrany měkkých cílů* (MV ČR, 2017) a v publikaci *Systém hodnocení bezpečnosti vybraných objektů měkkých cílů* (Mrázková & Hromada, 2019). Oba přístupy byly adaptovány na specifické podmínky zdravotnických zařízení, zejména na jejich otevřenost, provozní charakter a zranitelnost vůči cíleným bezpečnostním incidentům.

Komparativní analýza bezpečnostních opatření byla provedena v devíti nemocnicích s urgentním příjmem různé velikosti a zřizovatelské struktury. Soubor zahrnoval státní nemocnice zřizované Ministerstvem zdravotnictví ČR, velká nestátní zařízení s kapacitou nad 1 000 lůžek i menší nestátní nemocnice s kapacitou do 500 lůžek. Analýzu doplnily polostrukturované rozhovory s odborníky na krizové řízení a bezpečnostní management, které přinesly expertní perspektivu a zpřesnily interpretaci získaných dat.

Hodnocení proběhlo prostřednictvím Hospital Security Indexu (H-SI), který posuzuje fyzickou, elektronickou, mechanickou a organizačně-provozní bezpečnost. Každé dílčí kritérium bylo hodnoceno na čtyřbodové škále 0–3 (0 = nezajištěno, 1 = zajištěno nedostatečně, 2 = zajištěno uspokojivě, 3 = zajištěno plně a efektivně). Součty bodů v jednotlivých oblastech byly následně přepočteny pomocí váhových koeficientů a normalizovány na škálu 0–100, kde 0 představuje kriticky nízkou a 100 maximální dosažitelnou úroveň bezpečnosti. Výsledné hodnoty H-SI jsou dále interpretovány podle čtyř úrovní: 0–25 velmi nízká, 26–50 nízká, 51–75 střední a 76–100 vysoká úroveň bezpečnosti

2. VÝSLEDKY KOMPARATIVNÍ ANALÝZY A ROZHOVORŮ

Komparativní analýza byla provedena v devíti nemocnicích s urgentním příjmem různé velikosti (1–3 státní nemocnice, 4–6 velké nestátní nemocnice nad 1 000 lůžek, 7–9 menší nestátní nemocnice do 500 lůžek).

2.1 Souhrnné výsledky H-SI

Hodnoty H-SI se v hodnoceném souboru nemocnic pohybovaly v rozmezí od 20,9 bodu (nejnižší úroveň bezpečnosti) do 80,7 bodu (nejvyšší úroveň). Nejlépe byly hodnoceny nemocnice zřizované Ministerstvem zdravotnictví ČR, které vykazovaly vysokou míru standardizace postupů a stabilní systém řízení bezpečnosti. Naopak nejnižší hodnoty byly zaznamenány u menších nestátních nemocnic.

Tabulka 1 Souhrnné výsledky hodnocení H-SI (vlastní výzkum)

Nemocnice	Fyzická	Elektronická	Mechanická	Organizační	Celkový H-SI
1	30,0	14,1	14,6	15,6	**74,2**
2	30,0	16,7	16,7	17,3	**80,7**
3	30,0	13,0	11,5	9,3	**63,8**
4	30,0	14,1	11,5	16,0	**71,6**
5	13,3	7,8	7,3	4,4	**32,8**
6	16,7	7,8	7,3	9,8	**41,6**
7	13,3	9,9	9,4	4,4	**37,0**
8	6,7	5,7	6,3	2,2	**20,9**
9	16,7	9,4	10,4	5,3	**41,8**

2.2 Interpretace výsledků

Z výsledků vyplývá, že státní nemocnice (1–3) dosahují systematicky vyšší úrovně bezpečnosti ve všech hodnocených oblastech, zejména díky standardizovaným postupům, funkčnímu řízení bezpečnosti a pravidelnému školení personálu. Velké nestátní nemocnice (4–6) vykazují výraznou variabilitu – nemocnice 4 se blíží úrovni státních zařízení, zatímco nemocnice 5 a 6 spadají do pásma nízké bezpečnosti. Nejnižší úroveň byla zaznamenána u menších nestátních nemocnic (7–9), zejména v elektronické a organizačně-provozní oblasti.

Tato zjištění odpovídají poznatkům z polostrukturovaných rozhovorů, v nichž odborníci upozorňovali na nedostatečné pokrytí kamerovými systémy, absenci přístupových technologií, nepravidelná školení zaměstnanců, rozdílnou úroveň připravenosti na spolupráci s integrovaným záchranným systémem

(IZS), neaktuální bezpečnostní dokumentaci a zásadní roli bezpečnostního manažera v organizacích s vyšší bezpečnostní kulturou
Interpretace dat byla strukturována podle čtyř pilířů Hospital Security Indexu (H-SI). Fyzická oblast ukázala nedostatky v režimu vstupů a nastavení role ostrahy. Elektronická oblast potvrdila výrazné rozdíly v rozsahu a funkčnosti kamerových systémů a tísňových prvků. Mechanická oblast poukázala na variabilní úroveň bariér proti neoprávněnému vstupu. Organizačně-provozní oblast identifikovala největší slabiny, zejména v řízení bezpečnosti, dokumentaci a systematickém vzdělávání personálu.

Souhrnná interpretace poskytla komplexní obraz o bezpečnostní odolnosti hodnocených nemocnic a zároveň identifikovala klíčová slabá místa, která mají největší dopad na jejich schopnost reagovat na bezpečnostní incidenty. Tato zjištění byla následně zapracována do návrhu metodiky MOBIZ, kde tvoří základ struktury doporučených opatření ve fyzické, elektronické, mechanické a organizačně-provozní oblasti. Metodika tak přímo reflektuje empirické poznatky získané z komparativní analýzy a odborných rozhovorů.

Konkrétní výsledky komparativní analýzy i rozhovorů tvoří empirický základ navrhované metodiky **MOBIZ – Metodiky opatření pro bezpečnostní incidenty ve zdravotnictví** a jsou podrobně prezentovány v následující části.

3. MOBIZ – METODIKA OPATŘENÍ PRO BEZPEČNOSTNÍ INCIDENTY VE ZDRAVOTNICTVÍ

Metodika MOBIZ vymezuje metodický rámec prevence a zvládání bezpečnostních incidentů ve zdravotnických zařízeních. Zaměřuje se na právní a strategické dokumenty, bezpečnostní plán, analýzu bezpečnostních prvků a doporučení pro praxi. Metodika vychází z legislativy a technických norem a je přizpůsobena specifickým podmínkám prostředí zdravotnických zařízení.

3.1 Dokumentace ochrany měkkých cílů

Právní rámec ochrany zdravotnických zařízení jako měkkých cílů vychází z platných zákonů, prováděcích vyhlášek, strategických a koncepčních dokumentů České republiky, interní dokumentace jednotlivých zdravotnických zařízení a závazných technických norem. Jeho účelem je vymezit povinnosti subjektů v oblasti prevence, připravenosti a reakce na bezpečnostní incidenty, které mohou ohrozit život, zdraví či osobní bezpečnost pacientů, zaměstnanců a dalších osob přítomných v prostředí zdravotnických zařízení.

Ukotvení problematiky měkkých cílů v bezpečnostním prostředí České republiky ukazuje, že stát si je vědom rizik spojených s ochranou těchto objektů a usiluje o jejich systematickou ochranu a prevenci možných útoků. V této souvislosti jsou vyvíjeny snahy o posílení prevence, zvýšení úrovně ochrany a zlepšení schopnosti reakce na teroristické hrozby (Jakubcová a kol., 2018).

Zásadním dokumentem bezpečnostní politiky státu je Bezpečnostní strategie České republiky 2023, která navazuje na předchozí strategické a koncepční materiály. Jejím cílem je prosazovat bezpečnostní zájmy ČR prostřednictvím systémového a koordinovaného přístupu a účinně využívat multilaterální, bilaterální i národní nástroje k řízení bezpečnostního prostředí a k efektivní alokaci zdrojů (Česká republika, 2023).

Na tuto strategii navazuje Koncepce ochrany měkkých cílů pro roky 2017–2020, jejímž cílem bylo vytvořit fungující národní systém ochrany měkkých cílů umožňující pružně a komplexně reagovat na vznikající hrozby (MV ČR, 2017). V rámci její implementace vydává ministerstvo vnitra řadu metodických materiálů, jako např. Metodiku koordinace měkkého cíle pro fáze po závažném incidentu, Vyhodnocení ohroženosti měkkého cíle či Bezpečnostní plán měkkého cíle, které jsou veřejně dostupné (MV ČR, 2025).

Dalším významným dokumentem je Strategie pro boj proti terorismu od roku 2013, vydaná Ministerstvem vnitra ČR, která zdůrazňuje prevenci a ochranu měkkých cílů, analyzuje teroristické

hrozby a identifikuje ohrožené objekty v ČR. Jejím hlavním cílem je posílit schopnost státu reagovat na teroristické útoky a minimalizovat jejich dopady na společnost (MV ČR, 2013).

Česká republika zároveň podporuje a implementuje evropské strategické dokumenty, zejména Evropskou bezpečnostní strategii: Bezpečná Evropa v lepším světě (Rada EU, 2003) a Evropskou strategii vnitřní bezpečnosti – ProtectEU (Evropská komise, 2025), které akcentují význam prevence terorismu a systematické ochrany měkkých cílů.

Klíčovým technickým dokumentem v oblasti zdravotnictví je ČSN P CEN/TS 16850 – Ochrana společnosti: pokyny pro řízení bezpečnosti ve zdravotnických zařízeních. Tato norma poskytuje komplexní rámec pro řízení bezpečnosti zdravotnických zařízení. Definuje postupy pro ochranu osob, identifikaci a zabezpečení kritických procesů, stanovuje požadavky na bezpečnostní vybavení, školení personálu i úpravu prostor pro rizikové pacienty. Je přizpůsobena specifikům různých typů zařízení, včetně zdravotnických zařízen, zařízení sociální péče a léčeben, a její pokyny vytvářejí základní systém řízení bezpečnosti v celém resortu (ČSN P CEN/TS 16850, 2020).

Při posouzení ohrožení je však klíčové vědět, co je třeba chránit, proti komu jsou tyto hodnoty chráněny a jakým způsobem mohou hrozby na zdroje působit (Kalvach, 2016). Skutečné zvýšení bezpečnosti měkkých cílů proto nelze zajistit pouze právními předpisy, ale především faktickými preventivními a reaktivními opatřeními organizačního, technického i komunikačního charakteru.

3.2 Bezpečnostní plán a resilience zdravotnických zařízení

Resilience zdravotnických zařízení je podmíněna komplexním souborem bezpečnostních opatření, jejichž cílem je chránit pacienty, zaměstnance i návštěvníky a zajistit kontinuitu poskytované péče. Podle Ministerstva vnitra ČR (2025) je klíčovým nástrojem této ochrany **bezpečnostní plán**, který umožňuje řídit preventivní, přípravná i reakční opatření a tím minimalizovat dopady násilných útoků či mimořádných událostí.

Tento plán se opírá o čtyři základní dimenze bezpečnostních prvků – **fyzickou, elektronickou, mechanickou a organizačně-provozní**. Jejich vzájemná provázanost určuje schopnost zdravotnického zařízení účinně čelit incidentům a minimalizovat jejich dopady. Aby však mohl plán plnit svou roli, je nezbytné, aby organizace dokázala systematicky identifikovat a vyhodnocovat rizikové situace a přijímat na jejich základě odpovídající opatření. Klíčovou roli v tomto procesu hraje **bezpečnostní manažer** či jiný pověřený pracovník, který odpovídá za oblast bezpečnosti, koordinuje implementaci plánu a zajišťuje komunikaci s Policií ČR a dalšími složkami IZS (Kalvach a kol., 2016).

3.2.1 Bezpečnostní plán zdravotnického zařízení

Bezpečnostní plán je klíčovým nástrojem posilování resilience zdravotnických zařízení, protože zajišťuje kontinuitu péče i při mimořádných událostech. Kalvach a kol. (2016) ve své metodice zdůrazňuje nutnost zaměřit se při ochraně měkkých cílů na organizační strukturu, která zajišťuje formulaci a realizaci bezpečnostní politiky, zpracování bezpečnostního plánu a řízení konkrétních opatření.

Užitečný metodický rámec pro tvorbu a pravidelnou revizi bezpečnostního plánu nabízí metoda **PDCA** (Plan–Do–Check–Act – naplánuj, proveď, zkontroluj, jednej). Ve svém článku ji Zelenák & Kyselák (2024) představují jako praktický nástroj, který zdravotnickým zařízením umožňuje systematicky plánovat opatření, uvádět je do praxe, vyhodnocovat jejich účinnost a následně provádět úpravy na základě získaných zkušeností. Tímto způsobem lze zajistit, aby plán zůstal dlouhodobě funkční a odrážel aktuální hrozby i provozní podmínky.

S ohledem na charakter zdravotnického zařízení jako měkkého cíle se doporučuje, aby měl plán podobu strukturovaného dokumentu reflektujícího legislativní rámec, specifika provozu i aktuální bezpečnostní hrozby. Standardně se člení do čtyř částí: základní, operativní, pomocné a přílohové. Základní část vymezuje účel, cíle, právní rámec, odpovědnosti i způsoby zajištění akceschopnosti zdravotnického zařízení. Operativní část obsahuje konkrétní postupy řešení mimořádných událostí, svolání krizového štábu, aktivace zaměstnanců a typové scénáře. Její aktuálnost je třeba ověřovat pravidelnými cvičeními.

Pomocná část poskytuje podpůrné nástroje, přehled kontaktů, grafické podklady a související dokumentaci. Přílohová část pak nabízí přehled rizik a vzorové postupy pro řešení vybraných scénářů, například útoku aktivního střelce, výhružného telefonátu, nálezu podezřelého předmětu, jednání s agresivní osobou či použití nebezpečných chemických, biologických, radiačních, jaderných a výbušných látek (CBRNE) (MV ČR, 2025).

Bezpečnostní plán je nutné chápat jako živý dokument, který se pravidelně reviduje, testuje a přizpůsobuje aktuálním podmínkám. Jeho efektivní implementace posiluje bezpečnostní kulturu organizace a zvyšuje její schopnost reagovat na mimořádné situace. Součástí plánu by měl být také přehled dostupných sil a prostředků, jak organizačních a personálních, tak technických (mechanických i elektronických), a jasné vymezení jejich role v prevenci i při řešení incidentu (MV ČR, 2025).

Právě fyzická bezpečnost tvoří první z těchto pilířů a zároveň praktické naplnění bezpečnostního plánu v každodenním provozu zdravotnického zařízení.

3.2.2 Fyzická bezpečnost

Fyzická bezpečnost je základním pilířem ochrany prostředí zdravotnických zařízení a významně přispívá k jejich celkové resilienci. Jejím jádrem je činnost **bezpečnostní služby (ostrahy)**, která jako jediná složka systému dokáže bezprostředně zasáhnout při hrozícím nebo probíhajícím incidentu. Primárním cílem ostrahy je ochrana osob, majetku a kontinuity zdravotní péče (ČSN P CEN/TS 16850, 2020). Opatření zahrnují fyzickou kontrolu osob vstupujících do areálu, sledování nezvyklého chování, inspekci zavazadel a prevenci vnášení nebezpečných předmětů (Nevrkla & Lapková, 2017). Pracovníci ostrahy provádějí kontrolu vstupu, pochůzkovou činnost nebo obsluhují velín a bezpečnostní technologie. Výkon služby musí být zajištěn nepřetržitě (24/7) – buď prostřednictvím vlastních zaměstnanců zdravotnického zařízení, externí bezpečnostní agentury nebo kombinací obou variant (MV ČR, 2025).

Nedílnou součástí fyzické bezpečnosti jsou pravidelná školení a cvičení. Musí zahrnovat simulace násilných incidentů, nácvik evakuace a koordinační cvičení se složkami IZS. Doporučuje se je realizovat alespoň jednou ročně a jejich výsledky využívat k aktualizaci vnitřních postupů. Obsah školení je třeba průběžně přizpůsobovat aktuálním hrozbám a zapojit do něj všechny pracovníky ostrahy. Činnost ostrahy má být přesně vymezena standardizovanými postupy, které tvoří součást bezpečnostní dokumentace zařízení. Ta zahrnuje plán ostrahy, směrnice pro výkon služby, provozní režimy objektů a závazné postupy pro řešení incidentů. Pouze jejich důsledná aplikace zajistí připravenost zařízení a posílí jeho bezpečnostní kulturu (Kalvach a kol., 2016).

Dalším prvkem bezpečnostního plánu jsou **režimová opatření** – interní pravidla upravující chování zaměstnanců v rámci objektu. Definují postupy pro vstup do budovy, pravidla pro vjezd vozidel, obsluhu elektronických bezpečnostních systémů a další každodenní činnosti (ČSN P 73 4450-1, 2013).

Jak již bylo zmíněno, mezi prostředky k ochraně měkkých cílů patří **technická bezpečnostní opatření** (Tabulka 1). Pouhá existence technických bezpečnostních opatření není postačující. Je nezbytné mít vytvořené standardizované procedury a postupy, které stanoví, jak tato opatření budou používána a jak budou vyhodnocována (Kalvach a kol., 2016; ČSN P CEN/TS 16850, 2020).

Tabulka 2 Technická bezpečnostní opatření (Kalvach a kol., 2016)

Technická bezpečnostní opatření	
Elektronické prvky	**Mechanické prvky**
Kamerový systém	Double door
Poplachové zabezpečovací a tísňové systémy	Ploty, zdi
Vnitřní rozhlas	Bezpečnostní okna
Rentgen	Zátarasy
Přístupové a docházkové systémy	Mříže a okenice
Další	Další

3.2.3 Elektronické prvky bezpečnosti ve zdravotnických zařízeních

Elektronické bezpečnostní prvky představují klíčovou součást komplexního systému ochrany zdravotnických zařízení. Základním opatřením je **kamerový dohled**, který musí zajišťovat nepřetržité monitorování obvodu budovy bez slepých míst. Záznamy je vhodné uchovávat minimálně 24 hodin, ideálně 72 hodin, přičemž kamery by měly být vybaveny nočním viděním a detekcí pohybu pro efektivní provoz i za zhoršených světelných podmínek (ČSN EN 62676-1-1, 2014; Kalvach a kol., 2016).

Účinnost kamerového systému je podmíněna řízeným vstupem do objektu. Během provozní doby by měl být vstup kontrolován fyzickou ostrahou, mimo provoz pak zajištěn elektronickými systémy. Vstupní body je žádoucí doplnit o rentgenová zařízení a detektory kovů či výbušnin, které zabraňují vnášení nebezpečných předmětů. Pozornost je třeba věnovat také okolí zdravotnického zařízení – parkoviště má být monitorováno kamerovým systémem, záznam by měl být uchováván alespoň 12 hodin, což umožňuje zpětnou kontrolu pohybu osob i vozidel. Nedílnou součástí ochrany jsou **poplachové zabezpečovací a tísňové systémy** (PZTS), které je vhodné instalovat ve všech budovách a napojit na dohledové a poplachové přijímací centrum (DPPC). To musí zajišťovat nepřetržitý monitoring a být schopno detekovat podezřelé chování, neoprávněný pohyb či výskyt odložených předmětů. Na rizikových pracovištích je účelné doplnit systém o tísňová tlačítka pro rychlé a skryté přivolání pomoci, přičemž provoz DPPC má být svěřen kvalifikovanému personálu (ČSN EN 50131-1, 2007; Kalvach a kol., 2016)

Neméně důležitou součástí elektronické ochrany je vnitřní rozhlas, který slouží jako klíčový nástroj krizové komunikace. Instalace ve všech prostorách zdravotnického zařízení umožňuje efektivní informování osob při mimořádných událostech. Pro dosažení maximální účinnosti má být systém propojen s **elektrickou požární signalizací** (EPS) podle normy ČSN EN 54-16 (2009). Tím lze okamžitě přenést varovné hlášení nebo příkaz k evakuaci do celého objektu, což významně zkracuje reakční dobu a posiluje ochranu pacientů i zaměstnanců. Tento systém je vhodné doplnit o detekční zařízení, například rentgeny či detektory kovů a výbušnin, instalovaná u hlavních vstupů za účelem prevence vnášení nebezpečných předmětů (Kalvach a kol., 2016).

Významnou roli hrají také systémy kontroly vstupu. **Elektronický systém kontroly osob** (EASC) je vhodné implementovat v celém objektu a integrovat s ostatními bezpečnostními prvky. Tento systém umožňuje blokaci či uvolnění přístupových bodů podle aktuální situace a jeho funkčnost je nutné pravidelně testovat (ČSN EN 60839-11-1, 2014). Přístupové mechanismy mezi jednotlivými místnostmi je pak žádoucí doplnit o elektronické uzamykací prvky dle normy ČSN EN 1627 a nastavovat oprávnění v závislosti na rizikovosti konkrétních prostor (Vyhláška č. 528/2005 Sb., 2005; ČSN EN 1627, 2022).

Doplňujícím prvkem mohou být čtečky dokladů, které je účelné instalovat na vybraných místech a integrovat do přístupového systému za účelem ověřování totožnosti osob. Současně je vhodné zajistit funkční **systém šíření varování** prostřednictvím specializovaných krizových a notifikačních platforem, například O_2 KISS, Everbridge či BlackBerry AtHoc, doplněných o informační panely, SOS tlačítka a geolokační cílení zpráv. Osvětlení s pohybovými čidly je účelné umístit do exponovaných prostor a propojit s kamerovým dohledem a poplachovými systémy (Kalvach a kol., 2016). Individuální bezpečnostní ochranu pak představují prostředky určené přímo pro personál – zejména na rizikových pracovištích je vhodné zaměstnance vybavit **elektronickými bezpečnostními náramky** nebo SOS tlačítky pro okamžité přivolání pomoci. Signál má být směrován přímo na bezpečnostní službu nebo dispečink zdravotnického zařízení, a to v souladu s ČSN CEN/TS 16850 (2020) jako součást systému řízení bezpečnosti.

3.2.4 Mechanické prvky zabezpečení zdravotnických zařízení

Druhou skupinu technických bezpečnostních systémů, kterou je nutno zmínit, jsou **mechanické prvky,** které tvoří základní vrstvu bezpečnosti zdravotnického zařízení. Jejich správné navržení a implementace významně přispívají k ochraně před neoprávněným vstupem, násilným vniknutím a jinými bezpečnostními incidenty.

Exteriérové dveře je vhodné vybavit uzamykatelným bezpečnostním zámkem a konstruovat je tak, aby odpovídaly požadavkům na zvýšenou mechanickou odolnost dle normy ČSN EN 1627 (2022). Pro vyšší účinnost se doporučuje jejich propojení s elektronickými prvky – kamerovým dohledem, čipovým přístupem či biometrickým ověřováním. V případě mimořádné události musí být zajištěna možnost nouzového uzamčení objektu. Kvalitní bezpečnostní dveře dokážou odolat výbuchu, střelbě či násilným pokusům o vniknutí a spolu s přístupovými systémy tvoří účinný nástroj pro kontrolu vstupu (Kalvach a kol., 2016). Neméně významná jsou **bezpečnostní okna**, která se vyrábějí v různých třídách odolnosti – proti střelbě, výbuchu či prohození předmětů. Jejich funkčnost však závisí na správném ukotvení do nosných stěn. Alternativní ochranu mohou poskytnout těžké závěsy zvyšující odolnost proti tlakové vlně (ČSN P CEN/TS 16850, 2020; ČSN EN 1627, 2022)

Důležitou roli hrají také **režimová opatření** při vjezdu do areálu. Vstup vozidel je vhodné regulovat závorami, automatickým rozpoznáváním registračních značek a kamerovým systémem. Přístup lze omezit fyzickými překážkami – zábradlím, pevnými sloupky či zelení – které zamezují nájezdu vozidel mimo vyhrazené trasy. Celý areál by měl být ohraničen oplocením vysokým minimálně dva metry, přičemž vstupní brány mají být uzamykatelné a napojené na kontrolní systémy (Kalvach a kol., 2016).

Další specifickou kategorii tvoří **fyzické bariéry** – například turnikety, vstupní zábrany nebo pevné bloky. Tyto prvky umožňují regulaci pohybu osob a vozidel, přičemž jejich konstrukce musí respektovat požadavky na bezbariérovost a bezpečný provoz. Současně mají být integrovány do přístupového systému zdravotnického zařízení. Dle Kalvacha a kol. (2016) se za důležitý doplňkový prvek ochrany považují pevné sloupky, betonové bloky či výsuvné patníky, které mají být instalovány zejména v kritických zónách – u hlavních vstupů, zásobovacích tras či urgentního příjmu. Jejich funkcí je zabránit vjezdu nepovolaných vozidel a omezit přístup neoprávněných osob, aniž by narušovaly provoz zdravotnického zařízení (ČSN CEN/TS 16850, 2020).

Mechanické prvky tedy tvoří pevný základ fyzické ochrany. Jejich účinnost je však podmíněna správným nastavením organizačně-provozních opatření, která propojují technické prostředky s každodenním chodem zdravotnického zařízení.

3.2.5 Organizačně-provozní opatření

Součástí bezpečnostního řízení zdravotnického zařízení je soubor **organizačně-provozních opatření**, jejichž cílem je posílení odolnosti vůči bezpečnostním hrozbám a zajištění provozní kontinuity v krizových situacích.

Zdravotnické zařízení by mělo disponovat **dokumentací zaměřenou na ochranu měkkých cílů**, která se pravidelně aktualizuje v návaznosti na identifikované rizikové faktory. Tato dokumentace má být začleněna do strategického plánování a bezpečnostní politiky organizace. Pro zajištění krizové připravenosti se doporučuje zpracování souboru dokumentů, zahrnujícího plán krizové připravenosti, požární poplachové plány, evakuační plán, pandemický plán, havarijní plán, traumatologický plán a další provozní směrnice. Obsah těchto dokumentů má odpovídat platné legislativě a provozním specifikům daného zařízení (MV ČR, 2025).

Klíčovou roli hraje zapojení zaměstnanců. Ti se mají pravidelně účastnit **školení** zaměřených na krizovou dokumentaci a praktické zvládání mimořádných událostí. Vedoucí pracovníci se soustředí na řízení incidentů a koordinaci zásahů, zatímco ostatní zaměstnanci absolvují výuku přizpůsobenou charakteru pracoviště a míře rizika. Doporučená jsou rovněž **taktická cvičení**, která je vhodné realizovat minimálně jednou ročně ve spolupráci se složkami IZS. Tím se posiluje připravenost personálu i celková bezpečnostní kultura organizace (Kalvach a kol., 2016).

Součástí prevence je také pravidelná **analýza hrozeb a rizik**. Výstupy těchto analýz slouží jako podklad pro aktualizaci bezpečnostních postupů, plánování školení a provádění cvičení. Jejich systematické využívání podporuje dlouhodobé zvyšování resilience organizace (Kalvach, 2025).

Organizačně-provozní opatření se tak stávají mostem mezi technickými prvky a každodenním fungováním zdravotnického zařízení. Na jejich základě vzniká bezpečnostní politika, která sjednocuje pravidla, vymezuje odpovědnosti a určuje rámec spolupráce s externími složkami.

3.2.6 Bezpečnostní politika zdravotnického zařízení

Efektivní řízení bezpečnosti vyžaduje jasně definovanou bezpečnostní politiku, která stanovuje odpovědnosti, pravidla a rámec koordinace. Klíčovým prvkem je ustanovení bezpečnostního manažera, jenž zajišťuje vyhodnocování rizik, aktualizaci plánů, organizaci školení a komunikaci se složkami IZS. Součástí jeho role je také vyhodnocování bezpečnostních incidentů a dohled nad implementací metodiky ochrany měkkých cílů (Kalvach a kol., 2025).

Bezpečnostní politika však musí zahrnovat i zapojení všech zaměstnanců. Neodborný personál má být školen v rozpoznávání podezřelých osob, předmětů či situací a v základních postupech v případě mimořádných událostí. Školení se přizpůsobuje specifikům jednotlivých pracovišť a klade důraz na prevenci, rychlou reakci a spolupráci s IZS (Kalvach a kol., 2016).

Pro sjednocení postupů je třeba zavést standardizované procedury, písemně zpracované a pravidelně aktualizované. Mezi klíčové oblasti patří:

- režim vstupu osob do objektu (identifikace, autorizace a kontrola zaměstnanců, pacientů, návštěvníků i externích osob);
- režim vjezdu vozidel do areálu (podmínky pro služební, dodavatelská i návštěvnická vozidla) (Kalvach a kol., 2016).

Další součástí politiky je tematický plán školení a koordinační plán managementu, který jasně určuje úkoly vedení zdravotnického zařízení při mimořádné události a vymezuje odpovědnosti členů krizového štábu. Jeho funkčnost je nutné ověřovat modelovými situacemi (Ben David, 2025).

Bezpečnostní politika má rovněž zahrnovat aktivní spolupráci s Policií ČR, Hasičským záchranným sborem ČR, zdravotnickou záchrannou službou a obecní policií. Těmto složkám se doporučuje nabídnout možnost prohlídky objektu, zapojit je do plánování veřejných akcí, konzultovat analýzu ohroženosti a informovat je o mimořádných událostech. Pravidelná komunikace a koordinace postupů přispívají k efektivnímu zvládání mimořádných situací (Kalvach a kol., 2025).

V neposlední řadě se doporučuje navázat partnerskou spolupráci s dalšími měkkými cíli v regionu, jako jsou školy, kulturní instituce, úřady či obchodní centra. Společná opatření, výměna informací, vzájemné varování při výskytu hrozeb a pořádání cvičení zaměřených na krizové scénáře mohou významně přispět k posílení bezpečnostní připravenosti nejen zdravotnického zařízení , ale i širšího okolí (Kalvach a kol., 2016).

Závažným útokům je těžké čelit, když již nastanou, proto je důležité mít připravená opatření pro prevenci a zmírnění dopadů. Znalost místního prostředí je klíčovým faktorem, který dává personálu výhodu při plnění bezpečnostních úkolů. Místní personál má lepší povědomí o běžném chování a rutinách v daném prostředí. Personál musí být obeznámen s místními sociokulturními normami a může snáze rozpoznat neobvyklé chování nebo situace, které by jinak mohly uniknout pozornosti (Kalvach a kol., 2018).

Je nutné zmínit, že důkladné vyšetření každého incidentu má za cíl vyvodit odpovídající důsledky a zlepšit preventivní opatření. Poučení z každé události by mělo sloužit jako podklad pro lepší prevenci v budoucnosti (Háva, 2004).

3.3 Doporučení pro zdravotnická zařízení

Na základě provedené analýzy lze formulovat tato klíčová doporučení pro posílení bezpečnostní resilience zdravotnických zařízení:

- **Pravidelná revize bezpečnostního plánu** – udržovat plán jakožto živý dokument, pravidelně jej testovat a přizpůsobovat aktuálním hrozbám a provozním podmínkám.
- **Aktualizace krizové dokumentace** – průběžně doplňovat evakuační, havarijní, pandemické, traumatologické a další plány, aby odpovídaly legislativním požadavkům a provozním specifikům zařízení.
- **Posilování fyzické bezpečnosti** – zajišťovat nepřetržitou činnost ostrahy, jasně definovat její postupy a pravidelně realizovat školení a cvičení zaměřená na řešení mimořádných událostí.
- **Rozvoj technických opatření** – efektivně kombinovat elektronické (kamerové systémy, PZTS, přístupové systémy) a mechanické prvky (dveře, okna, bariéry), přičemž jejich využívání má být zakotveno ve standardizovaných postupech.
- **Systematické vzdělávání a cvičení personálu** – zajišťovat pravidelná školení všech zaměstnanců, včetně taktických cvičení se složkami IZS, s důrazem na praktické dovednosti a krizovou komunikaci.
- **Organizačně-provozní opatření** – nastavit jasná pravidla pro vstup osob, vjezd vozidel a každodenní provozní režim, která podporují prevenci incidentů a kontinuitu péče.
- **Rozvoj spolupráce a standardizace postupů** – posilovat partnerství s IZS a dalšími institucemi v regionu, sdílet zkušenosti, využívat dotační programy a zavádět jednotné bezpečnostní postupy vymezující kompetence a odpovědnosti.

ZÁVĚR

Analýza potvrzuje, že zdravotnická zařízení představují vysoce exponované měkké cíle, jejichž ochrana vyžaduje komplexní a integrovaný přístup. Účinná bezpečnostní strategie musí propojit fyzická a technická opatření s organizačními mechanismy, systematickou krizovou připraveností, pravidelným vzděláváním zaměstnanců a úzkou spoluprací se složkami IZS. Bezpečnostní plán je nutné chápat jako dynamický dokument, který se průběžně reviduje, testuje a přizpůsobuje aktuálním hrozbám i provozním podmínkám. Výsledky komparativní analýzy ukazují, že zásadním předpokladem bezpečnostní resilience je rovnováha mezi prevencí, včasnou reakcí a schopností organizace adaptovat se na měnící se rizika.

Navržená metodika MOBIZ představuje praktický nástroj pro jednotné řízení bezpečnosti v nemocnicích. Její pilotní ověření v Nemocnici České Budějovice a.s. prokázalo využitelnost v podmínkách velké krajské nemocnice, zejména při tvorbě bezpečnostního plánu a typových karet činností. Metodika má potenciál stát se sjednocujícím rámcem i pro další zdravotnická zařízení.

Studie je limitována velikostí výzkumného souboru (devět nemocnic v ČR) a částečnou subjektivitou hodnocení vyplývající z použití indexu a rozhovorů. Do budoucna by bylo vhodné rozšířit výzkum na širší vzorek nemocnic, případně mezinárodně, a dále rozvíjet softwarovou aplikaci podporující automatizované vyhodnocování H-SI a řízení bezpečnostních opatření.

LITERATURA

Ben David, G. (2025). *Metodika koordinace měkkého cíle pro fáze po závažném incidentu: aneb jak se vyrovnat s nastalou závažnou situací*. Ministerstvo vnitra České republiky, Odbor bezpečnostní politiky.

Česká republika. (2023). *Bezpečnostní strategie České republiky 2023*. Ministerstvo zahraničních věcí ČR. https://mzv.gov.cz/file/5161086/Bezpecnostni_strategie_2023.pdf (cit. 29. 9. 2025)

ČSN EN 1627. (2022). *Dveře, okna, lehké obvodové pláště, mříže a okenice – Odolnost proti vloupání – Požadavky a klasifikace*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN 50131-1. (2007). *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN 54-16. (2009). *Elektrická požární signalizace – Část 16: Ústředny pro hlasová výstražná zařízení*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN 60839-11-1. (2014). *Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN 62676-1-1. (2014). *Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN P 73 4450-1. (2013). *Fyzická ochrana prvku kritické infrastruktury – Část 1: Obecné požadavky*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN P CEN/TS 16850. (2020). *Ochrana společnosti – Pokyny pro řízení bezpečnosti ve zdravotnických zařízeních*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Evropská komise. (2025). *Evropská strategie vnitřní bezpečnosti – ProtectEU*. Evropská komise.

Háva, P. (2004). *Násilí na pracovišti v oblasti zdravotnických a sociálních služeb v ČR: Vstupní teoretická studie*. Institut zdravotní politiky a ekonomiky.

Jakubcová, L., a kol. (2018). Měkké cíle v pojetí Hasičského záchranného sboru České republiky. In *Měkké cíle a jejich ochrana*. Policejní akademie České republiky v Praze.

Kalvach, Z. (2016). *Metodika pro zvýšení ochrany měkkých cílů*. Ministerstvo vnitra České republiky.

Kalvach, Z. (2025). *Vyhodnocení ohroženosti měkkého cíle: aneb co, kdy, kde a od koho vám hrozí* (2. vyd.). Ministerstvo vnitra České republiky, Odbor bezpečnostní politiky. https://mv.gov.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx (cit. 28. 9. 2025)

Kalvach, Z., a kol. (2016). *Základy ochrany měkkých cílů: Metodika*. Ministerstvo vnitra České republiky.

Ministerstvo vnitra České republiky. (2013). *Strategie České republiky pro boj proti terorismu od roku 2013*. https://mv.gov.cz/soubor/strategie-ceske-republiky-pro-boj-proti-terorismu-pdf.aspx (cit. 28. 9. 2025)

Ministerstvo vnitra České republiky. (2016). *Ochrana měkkých cílů*. https://www.mvcr.cz/clanek/ochrana-mekkych-cilu.aspx (cit. 29. 9. 2025)

Ministerstvo vnitra České republiky. (2017). *Koncepce ochrany měkkých cílů pro roky 2017–2020*. https://www.mvcr.cz/soubor/koncepce-ochrany-mekkych-cilu-2017-2020.aspx (cit. 29. 9. 2025)

Ministerstvo vnitra České republiky. (2025). *Metodické materiály k ochraně měkkých cílů*. https://www.mvcr.cz (cit. 29. 9. 2025)

Ministerstvo vnitra České republiky, Odbor bezpečnostní politiky. (2025). *Bezpečnostní plán měkkého cíle* (2. upravené vyd.). Ministerstvo vnitra ČR.

Mrázková, L., & Hromada, M. (2019). *Ochrana měkkých cílů: Systém hodnocení bezpečnosti vybraných objektů měkkých cílů*. Leges.

Nevrkla, J., & Lapková, D. (2017). *Metodika ochrany měkkých cílů*. Soft Targets Protection Institute, z. ú., Univerzita Tomáše Bati ve Zlíně.

Rada Evropské unie. (2003). *Evropská bezpečnostní strategie: Bezpečná Evropa v lepším světě*. Rada EU.

Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. (2005). *Sbírka zákonů České republiky*.

Zelenák, M., & Kyselák, J. (2024). Bezpečnost zdravotnických zařízení. *Krizový manažment, 23*(2), 28–37. https://doi.org/10.26552/krm.C.2024.2.28-37

Jitka Kosáčková, Mgr.

Nemocnice České Budějovice a.s., B. Němcové 585/54, České Budějovice, Česká republika

ČVUT v Praze, Fakulta biomedicínského inženýrství, Katedra zdravotnických oborů a ochrany obyvatelstva, Sportovců 2311, Kladno, Česká republika

e-mail: kosackova.jitka@nemcb.cz

Renata Havránková, Mgr., Ph.D.

ČVUT v Praze, Fakulta biomedicínského inženýrství, Katedra zdravotnických oborů a ochrany obyvatelstva, Sportovců 2311, 272 01 Kladno, Česká republika

Jihočeská univerzita v Českých Budějovicích, Zdravotně sociální fakulta, Ústav radiologie, toxikologie a ochrany obyvatelstva, J. Boreckého 1167/27, 370 11 České Budějovice, Česká republika

e-mail: renata.havrankova@fbmi.cvut.cz

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.109-116
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

VLASTNÁ OCHRANA AKO CESTA K ZVYŠOVANIU BEZPEČNOSTI NA UNIVERZITÁCH

SELF-PROTECTION AS A PATH TO ENHANCING SECURITY AT UNIVERSITIES

ANDREJ VEĽAS

ABSTRACT: The article focuses on the protection of university campuses as soft targets, with an emphasis on the possibilities of applying self-protection under Act No. 473/2005 Coll. on the Provision of Private Security Services. The first part analyses the Slovak legal framework that allows universities to establish their own security department with the powers of a private security service, including the use of physical security equipment and, with the employer's consent, weapons. The second part provides an international comparison of university security models, with special attention given to campus police in the USA as fully fledged police forces, the British model of internal security services, and campus protection systems in other countries. The result is an analytical table summarising the legal regulations, powers, and requirements of the individual models. Based on this comparison, the article recommends a hybrid self-protection model for Slovak universities that would combine the advantages of an internal security service with close cooperation with state and municipal police. The aim of the article is to support discussion on enhancing security in the university environment and to contribute to the development of methodological procedures for the protection of soft targets in the education sector.

KEYWORDS: *Self-Protection. University Security. Campus Police. Soft Targets, Private Security.*

ÚVOD

Univerzitné kampusy patria medzi tzv. mäkké ciele (soft targets) – priestory ľahko prístupné širokej verejnosti, s vysokou koncentráciou osôb a so spravidla nízkymi, alebo žiadnymi ochrannými opatreniami, čo zvyšuje ich zraniteľnosť voči kriminalite a násilným útokom (vrátane útokov ozbrojeného útočníka) (MV SR, 2025). V odbornej literatúre a v bezpečnostnej praxi sa mäkké ciele a „preplnené miesta" (crowded places) definujú ako miesta ľahko dostupné, s predvídateľnou koncentráciou ľudí a limitovanými ochrannými mechanizmami; príkladmi sú školy, športové arény, nákupné centrá či stanice verejnej dopravy (CISA, 2019). V posledných troch rokoch sa práve ochrana takýchto lokalít v Slovenskej republike stala prioritou bezpečnostných zložiek a bezpečnostného výskumu (predovšetkým na UNIZA), ktorý identifikuje opatrenia v prevencii, pripravenosti a reakcii (notifikácie, plánovanie, tréningy, integrované technológie a pod.) a navrhuje nové riešenia na národnej úrovni. Naďalej existuje a realizuje pravidelné pracovné stretnutia Pracovná skupina pre ochranu mäkkých cieľov pod vedením 1. štátnej tajomníčky Ministerstva vnútra Slovenskej republiky (ďalej len MV SR) Dr.h.c. Prof. JUDr. Lucie Kurilovskej, PhD. V Českej republike sa ochrane mäkkých cieľov začal venovať Zdeněk Kalvach, ktorý definoval mäkké ciele ešte pred vznikom normy ISO 22341 Security and resilience – Protective security – Guidelines for Crime Prevention Through Environmental Design (Kalvach, 2016). V Českej republike existuje taktiež pracovná skupina pod vedením Národní centrály proti organizovanému zločinu určená k metodickej podpore prevádzkovateľov a vlastníkov mäkkých cieľov (MV ČR, 2025). Obe pracovné skupiny sa zaoberajú problematikou fyzickej ochrany (v ČR fyzického dohledu) ako nevyhnutnej súčasti - prvku systému ochrany objektov, ktorý dopĺňa technickú ochranu a organizačné, či režimové opatrenia (Loveček, 2015). V Slovenskej republike na rozdiel od Českej republiky existuje právny rámec tvorený zákonom NR SR č. 473/2005 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti, ktorý umožňuje organizácii a teda aj univerzite zriadiť vlastnú ochranu, ako formu bezpečnostnej služby prevádzkovanej pre vlastnú potrebu. Uvedený zákon umožňuje použitie vecných bezpečnostných prostriedkov a za stanovených podmienok aj strelných zbraní na zaistenie bezpečnosti organizácie a teda aj univerzity.

.

1. BEZPEČNOSŤ UNIVERZITÝCH KAMPUSOV V SR A ZAHRANIČÍ

Bezpečnosť na slovenských univerzitách bola riešená vydaním niekoľkých odporúčaní, minimálnych bezpečnostných štandardov, letákov a inštruktážnych videí na web stránkach Ministerstva vnútra Slovenskej republiky a pridelením prostriedkov na bezpečnostné audity vysokých škôl. Celkovo šlo o 1 milión Eur pre verejné vysoké školy a 70 tisíc Eur pre súkromné vysoké školy pridelených na bezpečnostné audity a iné aktivity, či opatrenia v téme bezpečnosti. Univerzity realizovali školenia vybraných, alebo aj všetkých zamestnancov v problematike ochrany mäkkých cieľov. Mnohé školy zaviedli pravidelné vzdelávanie v problematike ochrany pred ozbrojeným útočníkom do pravidelných školení zamestnancov k témam Bezpečnosť a ochrana života a zdravia pri práci, Ochrana pred požiarmi, či k problematike Ochrany osobných údajov. Vybrané školy investovali do bezpečnostných technológií formou systémov kontroly vstupov a kamerových monitorovacích systémov a zvýšenia fyzickej ochrany formou SBS. Boli realizované cvičné evakuácie na vybraných objektoch univerzít a nácviky reakcie na scenáre typu Ozbrojený útočník (na Trnavskej univerzite a na Žilinskej univerzite). Systematické riešenie formou metodiky je v štádiu príprav a malo by byť výsledkom projektu APPV-23-0437 Stratégia a metodika ochrany mäkkých cieľov so zameraním na základné, stredné a vysoké školy riešeného na Fakulte bezpečnostného inžinierstva Žilinskej univerzity v Žiline.

Popri dostupných právnych predpisoch, odporúčania a štandardoch je pre navrhovanie primeraných opatrení prínosná komparácia zahraničných modelov: americké „campus police“ (plnohodnotné policajné zbory na univerzitách), britský a nemecký model interných „security“ služieb bez plných policajných právomocí, či kanadský „special constable“ rámec s čiastočnými policajnými oprávneniami na kampuse.

V USA má väčšina univerzít vlastné policajné zložky (campus police departments), ktoré sú často ozbrojenými policajnými zbormi. Disponujú právomocami rovnocennými s mestskou alebo štátnou políciou, vrátane obmedzenia osobnej slobody, detektívnej služby a použitia donucovacích prostriedkov. Americké univerzitné policajné oddelenia podliehajú zákonu zvanému Clery Act (pozn. autora: Clery zákon – podľa zavraždenej študentky Jeanne Clery), ktorý ukladá povinnosť zverejňovať štatistiky kriminality, vydávať varovania v čase ohrozenia a zverejňovať bezpečnostné politiky. Nedodržiavanie je sankcionované (napr. rekordná pokuta 14 mil. USD pre Liberty University v roku 2024), čo zdôrazňuje dôležitosť systémovej transparentnosti a súladu s nariadeniami (tzv. compliance) (Clery, 2025). Štandardizácia je v Spojených štátoch zabezpečená akreditáciou Medzinárodnej asociácie administrátorov bezpečnostných zložiek kampusov IACLEA pre kampus safety (IACLEA, 2025). IACLEA ponúka akreditovaný program, ktorý stanovuje normy pre operatívu, školenia, krízové riadenie a vzťah s komunitou.

Veľká Británia má na univerzitách bezpečnostné služby, ktoré nemajú policajné právomoci, ale ich hlavnou úlohou je vykonávať dohľad. Policajné zásahy rieši štátna alebo mestská polícia. Historickou výnimkou je Cambridge University Constabulary, ktorá si zachovala obmedzené právomoci, no v praxi funguje len symbolicky (Sabaté, 2025). Veľká Británia má zákon, ktorým reguluje súkromné bezpečnostné služby (ďalej len SBS) a autoritu, ktorá vydáva licencie na ich prevádzkovanie. Pre bezpečnostné služby pre vlastnú potrebu (in-house) nie je licencia potrebná. Použitie zbraní je zakázané (Finkeldey, 2024).

V Kanade fungujú na univerzitách špeciálni policajti s určenými policajnými právomocami, ktorí vykonávajú predovšetkým dohľad. Nemajú schválený jednotný zákon, ktorý by riešil súkromné bezpečnostné služby, ale provincie upravujú právne predpisy zamerané na súkromnú bezpečnosť. Zákon o Policajnom zbore (Community Safety and Policing Act z roku 2019) rieši bezpečnosť univerzít prostredníctvom „Special Constables“. Ide o zložku určenú prevažne na monitorovanie bezpečnosti podľa britského modelu a zásah vykonáva štátna polícia. Použitie zbraní je zakázané, rozsah právomocí sa určuje v memorandách s mestskou políciou (Cook, 2021).

V Nemecku riešia univerzity bezpečnosť cez externé súkromné bezpečnostné služby, alebo vlastných zamestnancov, ktoré reguluje pomerne jednoduchý predpis Gewerbeordnung v paragrafe 34 Pfandleihgewerbe, ako podnikanie v oblasti súkromnej bezpečnosti. Použitie zbraní súkromnými

bezpečnostnými službami je zakázané. Oprávnenia sa vzťahujú predovšetkým na kontrolu vstupov. Všetky vážne incidenty rieši policajný zbor.

Tabuľka 1 Komparácia modelov bezpečnosti na univerzitách

Kritérium	Slovensko	USA	Veľká Británia	Kanada	Nemecko
Spôsob výkonu	Prevažne informátori, alternatívne SBS alebo Vlastná ochrana	Univerzitná polícia (campus police)	bezpečnostná služba	Špeciálna polícia (constables)	univerzitná bezpečnostná služba
Právny základ	Zákon NR SR č. 473/2005 Z. z.	Štátne zákony + Clery Act	Univerzitné predpisy, spolupráca s políciou	Zákon o bezpečnosti a policajnej činnosti v komunite	Domové právo + zmluvy
Právomoci	Obmedzenie osobnej slobody, zásah, vecné bezpečnostné prostriedky, zbraň	Plné policajné	Obmedzené (obmedzenie osobnej slobody)	Čiastočné policajné právomoci	Bez policajných práv
Transparentnosť	Smernice pre prevádzkovanie vlastnej ochrany/povinné správy	Povinné reporty (Clery)	Dobrovoľná	Dohľad policajnej rady	Interné predpisy
Ozbrojenie	Väčšinou neozbrojení, zbraň je možná	Rôzne, zbraň je možná	Neozbrojení	Rôzne, podľa dohody	Väčšinou neozbrojení

Na základe poznaní a porovnania v Tabuľke 1 je možné konštatovať, že vo svete existujú rôzne modely bezpečnosti na univerzitách. Prioritou bezpečnostných zložiek je predovšetkým monitorovanie bezpečnostného prostredia a samotný zásah je v rovine bežných bezpečnostných incidentov týkajúcich sa výtržností, či narušeniu režimu. V Spojených štátoch si množstvo útokov na školách a naďalej narastajúci počet, žiadali radikálnejšie oprávnenia pre zvýšenie bezpečnosti kampusov.

2. VLASTNÁ OCHRANA A JEJ ASPEKTY

Napriek existencii technických systémov podporujúcich organizačné a režimové opatrenia, existujú rezervy v organizácii fyzickej ochrany univerzít a celkovo aj škôl na Slovensku. V súčasnej dobe má väčšina univerzít informátorov (vrátnikov) bez špecifických právomocí. Títo zamestnanci majú právomoci, ako ktorákoľvek iná osoba v objekte. Nemôžu zasahovať, pretože na to nie sú vyškolení, nemôžu viesť evidencie, zakázať vstup, ani prevádzkovať zabezpečovací systém, či monitorovať pohyb osoby v chránenom priestore. Často sú to osoby s nejakým zdravotným znevýhodnením.

Zákon NR SR č. 473/2025 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov (zákon o súkromnej bezpečnosti) definuje v paragrafe 6 vlastnú ochranu ako prevádzkovanie bezpečnostnej služby pre vlastnú potrebu, ak je zabezpečovaná aspoň jednou osobou v pracovnoprávnom vzťahu. Bezpečnostná služba je definovaná ako:

- strážna služba,
- profesionálna cezhraničná preprava eurovej hotovosti cestnou dopravou,
- detektívna služba,
- odborná príprava a poradenstvo.

Pre použitie v univerzitnom prostredí na zvýšenie bezpečnosti je vhodná strážna služba podľa paragrafu 3, ktorou sa rozumie:

- ochrana majetku na verejne prístupnom mieste,

- ochrana majetku na inom než verejne prístupnom mieste,
- ochrana osoby,
- ochrana majetku a osoby pri preprave,
- ochrana prepravy majetku a osoby,
- zabezpečovanie poriadku na mieste zhromažďovania osôb,
- prevádzkovanie zabezpečovacieho systému alebo poplachového systému, prevádzkovanie ich častí, vyhodnocovanie narušenia chráneného objektu alebo chráneného miesta (ďalej len „prevádzkovanie zabezpečovacieho systému alebo poplachového systému“),
- vypracúvanie plánu ochrany alebo
- monitorovanie pohybu a konania osoby v chránenom objekte, na chránenom mieste alebo v ich okolí.

Vybrané body uvedené v zákone sú využiteľné v bežnom živote univerzity a to od ochrany majetku, cez ochranu osôb, cez zabezpečenie poriadku na mieste zhromažďovanie osôb, prevádzkovanie zabezpečovacích systémov a monitorovanie pohybu a konania osoby v univerzitných kampusoch.

Ďalšou možnosťou je využitie detektívnej služby, ktorú reguluje paragraf 4 a obsahuje:

- hľadanie osoby,
- hľadanie majetku,
- získavanie údajov, ktoré môžu slúžiť ako dôkazný prostriedok v konaní pred súdom alebo správnym orgánom,
- získavanie údajov o osobnom stave fyzickej osoby a získavanie informácií o konaní fyzickej osoby alebo právnickej osoby alebo o ich majetkových pomeroch,
- získavanie informácií v súvislosti s vymáhaním pohľadávky alebo
- získavanie údajov o protiprávnom konaní ohrozujúcom obchodné tajomstvo.

Z týchto bodov sa javia ako využiteľné prvé tri a posledné dva body. Posledné dva sa týkajú vymáhaní pohľadávok, s ktorými majú univerzity problémy pri výkone podnikateľskej činnosti a posledný bod týkajúci sa ochrany obchodných tajomstiev je využiteľný pri ochrane duševného vlastníctva univerzít.

Bezpečnostnú službu možno prevádzkovať na základe licencie na prevádzkovanie bezpečnostnej služby. Pre získanie licencie je potrebné splniť náležitosti v zákone. Taktiež všetci zamestnanci vlastnej ochrany by museli absolvovať odbornú prípravu, pravidelné skúšky odbornej spôsobilosti, absolvovať psychotesty a preverenie zdravotnej spôsobilosti. Zároveň by sa náklady zvýšili o príspevok na nákup ošatenia, obuvi a zakúpenie vecných bezpečnostných prostriedkov.

Výhodou, ktorú majú zamestnanci vlastnej ochrany oproti informátorom je možnosť presvedčiť sa, či ten, kto vstupuje do chráneného objektu alebo na chránené miesto alebo z neho vystupuje, nemá pri sebe alebo na sebe predmety pochádzajúce z protiprávnej činnosti súvisiacej s chráneným objektom. Týka sa to samozrejme aj zbraní a iných nebezpečných predmetov. Zároveň majú možnosť zakázať vstup nepovolaným osobám, viesť evidencie vstupu, alebo výstupu osôb, evidenciu vjazdu, alebo výjazdu dopravných prostriedkov, vyžadovať preukázanie totožnosti, používať technické prostriedky pre záznam vstupu a výstupu osôb, predviesť na strážne pracovisko osobu pristihnutú pri páchaní protiprávnej činnosti a dokonca vyviesť nepovolanú osobu z objektu. Osoba vykonávajúca vlastnú ochranu môže viditeľne nosiť a použiť vecné bezpečnostné prostriedky (tomfa, obušok, obranný sprej, putá, atď.). So súhlasom zamestnávateľa môže pri výkone služobnej činnosti používať zbraň.

3. METODOLÓGIA

Článok je postavený na teoreticko-analytickom a komparatívnom prístupe. Základnou použitou metódou bola analýza dokumentov, pričom pozornosť bola venovaná slovenskému legislatívnemu rámcu, predovšetkým zákonu NR SR č. 473/2005 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a súvisiacim právnym predpisom. Ďalej bola realizovaná analýza literatúry, ktorá vychádzala zo zahraničných vedeckých štúdií, oficiálnych správ a politických dokumentov zameraných na univerzitnú bezpečnosť a fungovanie campus police.

Na rozšírenie perspektívy bola využitá komparatívna analýza, ktorá porovnala slovenský model vlastnej ochrany s bezpečnostnými modelmi v iných krajinách (USA, Veľká Británia, Kanada a Nemecko). Tento prístup umožnil identifikovať kľúčové podobnosti a rozdiely v právnom základe, právomociach, organizačných štruktúrach a požiadavkách na transparentnosť.

Súčasťou metodického postupu je aj prípadová štúdia Univerzity Žilina (UNIZA), v rámci ktorej boli realizované kvantitatívne prepočty. Tie zahŕňajú kalkuláciu nákladov na vlastnú ochranu a odhad potrebného počtu pracovníkov (vrátnikov/strážnikov) na zabezpečenie jednotlivých objektov univerzitného kampusu. Výsledky týchto výpočtov umožňujú porovnať ekonomickú a organizačnú náročnosť vlastnej ochrany s outsourcingom súkromnej bezpečnostnej služby.

4. PRÍPADOVÁ ŠTÚDIA – VLASTNÁ OCHRANA V PODMIENKACH UNIZA

Ustanovenie vlastnej ochrany v prostredí univerzity je možné požiadaním o vydanie licencie na vlastnú ochranu na Krajskom riaditeľstve Policajného zboru Slovenskej republiky.

S prevádzkovaním vlastnej ochrany je spojené vedenie evidencií osôb poverených výkonom fyzickej ochrany, evidenciu služieb, zásahov a inšpekčnú knihu dozoru. Osoby vo výkone vlastnej ochrany musia mať odbornú spôsobilosť podľa zákona, zákonom predpísané označenie a identifikačný preukaz.

Vzhľadom na uvedené aspekty prevádzkovania vlastnej ochrany, je na prvý pohľad možné konštatovať, že náklady na vlastnú ochranu sú vyššie ako na bežných informátorov. Týka sa to nákladov na ošatenie, obuv, vecné bezpečnostné prostriedky, náklady na školenia odbornej spôsobilosti, príplatky za zvýšenú náročnosť práce a pod. Vhodným riešením sa javí komerčne dodávaná súkromná bezpečnostná služba. Pozitívom je, že pri zaistení fyzickej ochrany objektu outsourcovanou súkromnou bezpečnostnou službou nevznikajú objednávateľovi žiadne dodatočné náklady. Nie je zaťažený založením a prevádzkovaním vlastnej ochrany a zamestnaním pracovníkov fyzickej ochrany objektu. Je však potrebné brať na vedomie, že náklady za outsourcovanú súkromnú bezpečnostnú službu v sebe zahŕňajú aj zisk prevádzkovateľa, ktorý sa pri zaistení fyzickej ochrany objektu internými zamestnancami nevytvára. Negatívom je že, zamestnanci vykonávajúci fyzickú ochranu objektu sú v plnom rozsahu pod vedením konateľa strážnej služby. Nie sú zamestnancami univerzity. Súkromné bezpečnostné služby robia výber zamestnancov len sporadicky. Vzhľadom na nízku mzdu v odvetví vyberajú osoby, ktoré spĺňajú predpoklady na základe zákona o súkromnej bezpečnosti (odborná spôsobilosť, bezúhonnosť, spoľahlivosť, zdravotná spôsobilosť). Nezohľadňujú ďalšiu kvalifikáciu, prax, nepreverujú uchádzačov a nezaujímajú sa o referencie. Zároveň neinvestujú do rozvoja zamestnancov a znalosť cudzieho jazyka je na minimálnej úrovni.

Pozitíva a negatíva realizácie fyzickej ochrany objektu internými zamestnancami je možné zhrnúť nasledovne. Zamestnanci vykonávajúci vlastnú ochranu sú v plnom rozsahu pod vedením univerzity. Rektor, alebo ním poverená osoba má priamy dosah na obsah plánu fyzickej ochrany objektu, rozdelenie úloh a zodpovedností, kontrolu plnenia pracovných úloh, plánovanie služieb a iné. Režim fyzickej ochrany objektu je možné prispôsobiť aktuálnej bezpečnostnej situácii. Nie je potrebné rokovať s treťou stranou, vytvárať dodatky k zmluve o poskytnutí SBS, nevzniká tu riziko škôd z omeškania ani riziko zmluvných pokút. Výhodou je teda i určitá forma optimalizácie. Zamestnanci vlastnej ochrany poznajú chránený priestor, dobre sa v ňom orientujú a poznajú nadriadených zamestnancov a ich kompetencie, ako aj postupy pre riešenie mimoriadnych situácií, na rozdiel od outsourcovanej spoločnosti, kde vzhľadom na vyššiu fluktuácia, resp. migráciu zamestnancov toto nie je možné zabezpečiť. Vlastní zamestnanci majú záujem o kontinuálne fungovanie spoločnosti, ktorej sú zamestnancami. Univerzita si ich môže vybrať, vyškoliť, investovať do ich rozvoja. Môže ich motivovať finančne. Pri výkone ochrany je zásadným aspektom zabezpečenie citlivých informácií o chránených objektoch a priestoroch. Evidencie incidentov a databázy pre potreby zaistenia bezpečnosti sú vedené systematicky a zmysluplne. Zamestnanci vlastnej ochrany môžu participovať na evakuácii objektu, môžu plánovať nácviky. Realizujú zásahy podľa potreby. Nevýhodou sú vyššie náklady ako na komerčne dodávanú SBS a náklady súvisiace s plánovaním, administratívou, účtovníctvom a vedením evidencií.

Pre pokrytie jedného vstupného bodu 24/7 do objektu (vrátnica) je potrebné 5 pracovníkov v trvalom pracovnom pomere. Pre obchôdzku areálu jednou osobou je potrebných ďalších 5 pracovníkov. Univerzita má niekoľko objektov odčlenených ich lokalizáciou. Fakulta bezpečnostného inžinierstva v meste, Fakulta riadenia a informatiky na Vlčincoch, Internáty Veľký Diel, v blízkom okolí je lokalizovaná Nová Menza a knižnica. Hlavné jadro tvorí univerzitný kampus na Veľkom Diele. Internáty a Stará Menza sú situované aj na sídlisku Hliny. Podľa dostupných informácií na stránkach Slovenskej komory súkromnej bezpečnosti pre rok 2025 je hodinová cena práce za výkon SBS v rozpätí 11,318 €/hod až 15,563 €/hod.

Prevádzka na jednom stanovišti 24/7 ročne je 8 418 hodín (podľa modelu SKSB). Počet zamestnancov pre plné pokrytie stanovišťa: cca 5 osôb plný úväzok (na pokrytie smien, dovoleniek, PN, náhradný personál). Ak použijeme stred hodnoty hodinovej ceny: (11,318 + 15,563)/2 = 13,4405 €/hod, čo je priemerná cena výkonu za hodinu práce. Ročné náklady na jedno stanovište budú: 8 418 hod × 13,4405 €/hod = 113 140,7 €/rok a náklady na jedného pracovníka 22 628,14 €/rok.

Náklady na rovnošatu (tričko, mikina, bunda, nohavice, obuv letná + zimná, čiapka, reflexná vesta, rukavice, opasok, nášivky, košeľa, tričká) je možné vyčísliť vo výške približne 400 Eur/osoba. Obmena by mala byť každé 3-4 roky. Vecné bezpečnostné prostriedky (obušok, baterka, putá + puzdrá) sa kupujú zväčša jednorazovo a ich cena je do 200 Eur/osoba. Pri výpočte presných nákladov je potrebné pripočítať náklady na mimoriadne akcie (Dni otvorených dverí, kultúrne a spoločenské podujatia, športové podujatia a iné). Výhodou vlastnej ochrany je, že je okamžite k dispozícii a umožňuje aj aktívny monitoring kamerových systémov.

Žilinská univerzita má 13 vrátnic (stanovíšť), pre ktoré vychádzajú ročné náklady na vlastnú ochranu pri priemernej hodinovej cene 13,4405 €/h približne na 1,47 mil. €. Po pridaní obchôdzkovej služby (1 ďalšia pracovná pozícia, čo znamená navýšenie o 5 pracovníkov) celkové ročné náklady stúpnu približne na 1,58 mil. €. Vstupné náklady na uniformy a vecné bezpečnostné prostriedky predstavujú pri 65 pracovníkoch približne 39 tis. € (pri 70 os. približne 42 tis. €). S ohľadom na modelové výpočty SKSB (min. nákladová sadzba okolo 14,739 €/h) je vhodné počítať s prevádzkovou rezervou, resp. citlivosťou 10–15 % v závislosti od mzdových a režijných podmienok a kalendára mimoriadnych akcií.

Ak by sa zvýšil počet pracovníkov na obchôdzky na dvoch (čo je nevyhnutné pre zásah) a pridali ďalšie dve pracovné pozície v plánovanom Monitorovacom centre, ktoré by vyhodnocovalo poplachové signály a správy, ako aj obrazové informácie z kamerových systémov, budú odhadované priame ročné náklady pri priemernej sadzbe pri 1,92 mil. € (s intervalom 1,62–2,23 mil. € podľa použitej hodinovej ceny). Vstupné náklady na uniformy a vecné bezpečnostné prostriedky pre približne 85 pracovníkov sú okolo 51 tis. €, s amortizáciou rovnošiat v cykle 3–4 roky.

5. DISKUSIA

Výsledky analýzy ukazujú, že slovenský model vlastnej ochrany predstavuje prakticky realizovateľnú a využiteľnú alternatívu k outsourcingu komerčných bezpečnostných služieb. V porovnaní so zahraničnými prístupmi je však jeho postavenie podobné modelom používaným vo Veľkej Británii alebo Nemecku, kde univerzitná bezpečnosť zostáva prevažne v rukách civilných bezpečnostných pracovníkov bez plných policajných právomocí. Na rozdiel od Spojených štátov amerických, kde kampusová polícia pôsobí ako plnohodnotná ozbrojená zložka s právomocou vyšetrovania a zatýkania, slovenský rámec limituje zásahy vlastnej ochrany na úroveň SBS. To znamená, že v prípade trestných činov je nevyhnutná okamžitá súčinnosť s Policajným zborom SR.

Diskutovať možno aj o výhodách a nevýhodách tohto usporiadania. Medzi hlavné výhody patrí znalosť špecifického prostredia, lojalita pracovníkov k univerzite a vyššia flexibilita pri prispôsobovaní bezpečnostných opatrení aktuálnym potrebám akademickej komunity. Limity súvisia najmä s finančnou náročnosťou, potrebou pravidelnej odbornej prípravy (aj keď v skrátenej forme) a s obmedzenými právomocami oproti štátnej polícii. V porovnaní s outsourcingom môže byť vlastná ochrana dlhodobo efektívnejšia, avšak iba vtedy, ak univerzita dokáže zabezpečiť stabilné financovanie a profesionálny manažment.

Zahraničné skúsenosti, najmä z USA a Kanady, poukazujú na význam transparentnosti a dôvery. Povinnosti podľa Clery Act, ako napríklad včasné varovania a pravidelné zverejňovanie štatistík kriminality, prispievajú k posilňovaniu dôvery študentov a zamestnancov v kampusovú bezpečnosť. Podobné postupy by mohli byť inšpiráciou pre slovenské univerzity – aj keď by šlo iba o dobrovoľné opatrenia nad rámec zákona. Zároveň sa ukazuje potreba zavádzania hybridného modelu, ktorý by spájal výhody internej vlastnej ochrany s externými kapacitami SBS a formálnou spoluprácou so štátnou a mestskou políciou prostredníctvom memoránd o spolupráci.

Diskutabilnou otázkou zostáva aj legitimita a spoločenské vnímanie univerzitnej bezpečnosti. Výskumy zo zahraničia ukazujú, že dôvera študentov v kampusovú políciu či bezpečnostné služby závisí nielen od ich efektívnosti, ale aj od toho, do akej miery konajú spravodlivo, transparentne a rešpektujú akademické slobody. V slovenskom prostredí je preto potrebné hľadať rovnováhu medzi potrebou ochrany univerzitného prostredia a zachovaním jeho otvorenosti a autonómie.

ZÁVER

Bezpečnosť univerzitných kampusov predstavuje komplexnú problematiku, ktorá si vyžaduje systémový a dlhodobý prístup. Slovenská legislatíva v podobe zákona NR SR č. 473/2005 Z. z. vytvára univerzitám unikátnu možnosť zriadiť vlastnú ochranu ako formu bezpečnostnej služby prevádzkovanej pre vlastnú potrebu. Táto forma má oproti bežným informátorom výrazné výhody – od vyššej úrovne oprávnení, možnosti prevádzkovať technické systémy, vykonávať evidencie a zásahy, až po možnosť využívať vecné bezpečnostné prostriedky a so súhlasom zamestnávateľa aj zbraň.

Komparácia so zahraničnými modelmi ukazuje, že Slovensko stojí v tomto ohľade medzi britsko-nemeckým modelom (interná ochrana alebo súkromné služby bez policajných právomocí) a kanadsko-americkým prístupom (špeciálni constables či plnohodnotné campus police). Zatiaľ čo USA kladú dôraz na policajné právomoci kampusovej polície a transparentnosť, Kanada zavádza hybridný model „special constables“ pod dohľadom policajnej rady. Nemecko a Veľká Británia sa spoliehajú najmä na Hausrecht a outsourcing bezpečnostných služieb.

V prípade Univerzity v Žiline možno konštatovať, že zriadenie vlastnej ochrany by znamenalo vyššie priame náklady v porovnaní s informátormi, avšak univerzita by získala vyššiu mieru kontroly, flexibility a pripravenosti na mimoriadne situácie. Orientačný výpočet ukazuje, že jedno stanovište 24/7 si vyžaduje približne 5 pracovníkov a ročné náklady na úrovni 113 000 € (pri strednej sadzbe podľa SKSB, 2025). Dodatočné náklady spojené s rovnošatou, výstrojom a školeniami sú však jednorazové alebo periodické a v horizonte niekoľkých rokov sa rozpočítajú. Univerzita by tak mohla získať profesionálny bezpečnostný útvar so znalosťou prostredia, lojálnym k inštitúcii a schopným reagovať nielen na každodenné incidenty, ale aj na krízové situácie. Pri zohľadnení výhod a nevýhod sa javí ako optimálne riešenie hybridný model – kombinácia vlastnej ochrany pre kľúčové objekty (hlavný vstup, internáty, knižnica) a externej SBS pre doplnkové a krátkodobé služby (podujatia, jednorazové akcie).

Zriadenie vlastnej ochrany na UNIZA by mohlo byť zároveň pilotným projektom v slovenskom vysokoškolskom prostredí a slúžiť ako metodický príklad pre ostatné univerzity, ktoré uvažujú o posilnení svojej bezpečnosti v kontexte mäkkých cieľov.

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.

LITERATÚRA

CISA (2019). Cybersecurity and Infrastructure Security Agency. Security of Soft Targets andCrowded Places–Resource Guide. April 2019, U.S. Department of Homeland Security

MV SR (2025). Akčný plán pre ochranu mäkkých cieľov na rok 2025. Ministerstvo vnútra Slovenskej republiky https://rokovania.gov.sk/RVL/Material/30565/1

Finkeldey, J. G., Dennison, C. R., Reyes, N. T., DiRusso, A., & Brown, M. (2024). Contact with and Perceptions of Campus Police Among College Students at a Small-Town University. *Criminal Justice Review*, *50*(3), 289-310. https://doi.org/10.1177/07340168241240450

Kalvach Z. (2016) Basic of soft target protection – guidelines. Soft Targets Protection Institute Prague.

Loveček Tomáš, Veľas Andrej, Ďurovec Martin (2015). Poplachové systémy Žilina: Žilinská univerzita v Žiline, 2015. ISBN 978-80-554-1144-6.

MV ČR (2025). Ochrana měkkých cílů. Retrieved September 19, 2025, from https://mv.gov.cz/clanek/ochrana-mekkych-cilu-archiv.aspx

RTVS (2024) Vysoké školy dostanú peniaze na zvýšenie bezpečnosti. Retrieved September 19, 2025, from https://spravy.stvr.sk/2024/04/vysoke-skoly-dostanu-od-rezortu-skolstva-peniaze-na-realizaciu-bezpecnostnych-auditov/

SKSB (2025) Slovenská komora súkromnej bezpečnosti. Minimálne mzdové náklady na výkon práce (cena práce) zamestnanca SBS v strážnej službe pri dodržaní zákonom stanovených podmienok. Retrieved September 26, 2025, from https://www.sksb.sk/

SME (2025) Ozbrojený útočník s rukojemníkom: Policajti nacvičovali na univerzite. Retrieved September 19, 2025, from https://mytrnava.sme.sk/c/23465773/ozbrojeny-utocnik-na-unverzite-s-rukojemnikom-policajti-nacvicovali-na-univerzite.html

IACLEA (2025). The Designation of Excellence in Campus Public Safety. Retrieved September 26, 2025, from https://iaclea.org/accreditation/

CLERY (2025). Clery Center. Retrieved September 26, 2025, from https://www.clerycenter.org/the-clery-act

Sabaté O, Goenaga A. (2025). The Rise of Modern Police Forces in the United Kingdom: Tracking Legislative Debates Around Police Reform (1803–1945). *Social Science History*. 2025;49(2):395-421. doi:10.1017/ssh.2025.30

Cook, K. (2021) “Are you the real police?” “No. We’re the campus police.” An examination of the way Ontario Special Constables govern risk on post-secondary campuses. University of Waterloo. Dissertation theses.

Zákon NR SR č. 473/2025 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov (zákon o súkromnej bezpečnosti)

Andrej Veľas, prof. Ing. PhD.

Katedra bezpečnostného manažmentu, Fakulta bezpečnostného inžinierstva, Žilinská univerzita v Žiline, 1.mája 32, 01026 Žilina, +421 41 513 6650, andrej.velas@uniza.sk

e-mail: andrej.velas@uniza.sk

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.117-127
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

POUŽITÍ ARMÁDY ČESKÉ REPUBLIKY PŘI ŘEŠENÍ KRIZOVÝCH SITUACÍ NEVOJENSKÉHO CHARAKTERU NA ÚZEMÍ STÁTU

USE OF THE ARMY OF THE CZECH REPUBLIC IN RESOLVING CRISIS SITUATIONS OF A NON-MILITARY NATURE ON THE TERRITORY OF THE STATE

JIŘÍ KALENDA, JIŘÍ BARTA

ABSTRACT: *The article clarifies the place and role of the armed forces within the security system of the Czech Republic. It is based on the current legal framework and outlines the legislation governing the deployment of the Army of the Czech Republic. It provides examples of the army's use within the state territory, both in ensuring internal security and in assisting the population during natural disasters and industrial accidents. It also addresses the issue of how the forces and resources of the Army of the Czech Republic are requested and employed within the Integrated Rescue System. The article further raises questions concerning the state's possibilities and capabilities in today's rapidly evolving security environment.*

KEYWORDS: *Security system, emergency, crisis situation, Army of the Czech Republic*

ÚVOD

Od počátku své existence musí lidstvo zápasit nejen o záchranu hmotných a kulturních hodnot, ale především o uchování samotného života. Vědeckotechnický pokrok přinesl lidské společnosti vedle řady příznivých stránek i zvýšení rizika vzniku krizových situací. Lidské poznání dokáže již poměrně dokonale objasnit zdroje a zákonitosti průběhu působení přírodních a společenských jevů, vyvolávajících tyto situace, ale nedokáže vzniku dané situace plně zabránit. S vývojem společnosti dochází i k proměnám bezpečnostního prostředí a jsou nalézány nové formy a metody k zajištění základních hodnot, nejen pro člověka.

Bezpečnost státu je stále více vymezena schopností čelit hrozbám společenského i přírodního charakteru, přičemž jejich hranice není jednoznačně vymezena. Hrozby se vzájemně prolínají a přerůstají jedna v druhou. Rozličný charakter hrozeb a míra jejich rizika klade další nové nároky nejen na integrovaný záchranný systém, ale i na ozbrojené síly, které již nadále nejsou jen nástrojem obrany státu a porážky protivníka, ale i jedním z řady nástrojů bezpečnosti v širším slova smyslu (Bezpečnostní strategie ČR, 2023), (Ministerstvo vnitra, 2016).

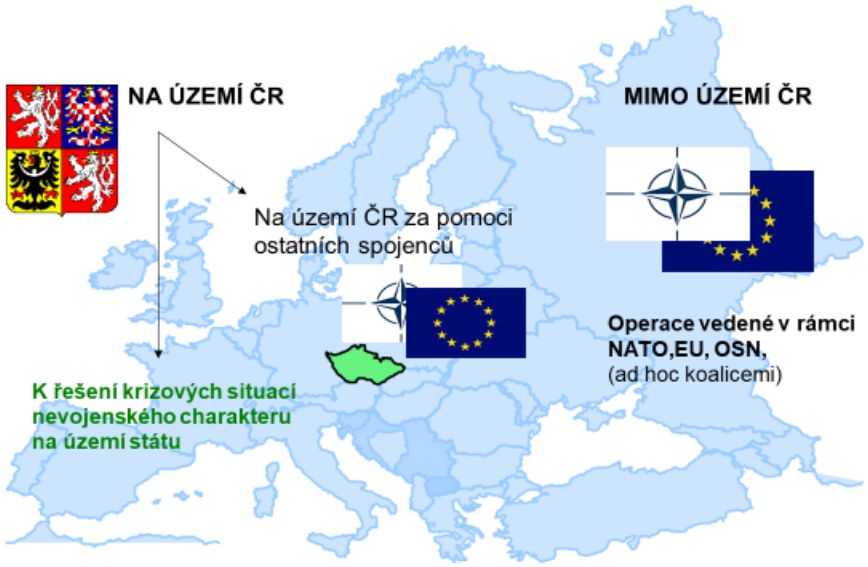
Cílem tohoto článku je poukázat široké veřejnosti na možnosti nasazení Ozbrojených sil České republiky v jiných, než vojenských operacích za účelem obrany státu, a to nejen na pomoc při záchranných a likvidačních pracích u řešení přírodních katastrof, ale i při dalších mimořádných událostech a krizových situacích.

1. MÍSTO A ÚLOHA OZBROJENÝCH SIL ČESKÉ REPUBLIKY V BEZPEČNOSTNÍM SYSTÉMU STÁTU

Zajištění bezpečnosti státu má komplexní a globální charakter. Možnosti České republiky (déle jen ČR) významně spoluurčují výkonnost českého hospodářství a míru mezinárodní spolupráce. Základním přístupem a nezpochybnitelnou hodnotou je princip kolektivní obrany a bezpečnosti v rámci mezinárodních organizací a mnohonárodních uskupení. Východiskem kolektivní obrany je pro ČR členství v Severoatlantické alianci (Bezpečnostní strategie ČR, 2023).

Bezpečnostní systém je institucionálním nástrojem pro tvorbu a realizaci bezpečnostní politiky ČR. Tvoří nedílnou součást bezpečnostní architektury Evropy a dalších mezinárodních institucí. Bezpečnostní systém je tvořen prvky zákonodárné, výkonné a soudní moci, územní samosprávy, ale i právnickými

a fyzickými osobami, které mají odpovědnost za zajištění bezpečnosti státu. Struktura bezpečnostního systému zahrnuje zejména prezidenta republiky, Parlament ČR, vládu ČR, Bezpečnostní radu státu a její pracovní orgány, ústřední správní úřady, krajské a obecní úřady a jejich výkonné orgány krizového řízení a dále ozbrojené síly, ozbrojené bezpečnostní sbory, zpravodajské služby, záchranné sbory, záchranné služby a havarijní služby (Zákon č. 110/1998 Sb.), (Zákon č. 239/2000 Sb.).



Obrázek 1 Použití ozbrojených sil České republiky (Jurenka, 2023)

Poslání a úkoly ozbrojených sil vychází z Ústavy České republiky (Ústavní zákon č. 1/1993 Sb.) a dalších zákonů. Principy obranné politiky definované v Bezpečnostní strategii ČR (2023) pak dále rozpracovává a konkretizuje Vojenská strategie ČR, která je výchozím dokumentem pro výstavbu a použití ozbrojených sil ČR. Ozbrojené síly ČR, zejména jejich hlavní součást Armáda ČR, představují rozhodující prvek bezpečnostního systému státu (Ministerstvo vnitra, 2016).

2. LEGISLATIVNÍ RÁMEC POUŽITÍ OZBROJENÝCH SIL ČESKÉ REPUBLIKY

Úkoly ozbrojených sil vychází z Ústavy České republiky a dalších zákonů (Ústavní zákon č. 1/1993 Sb.):

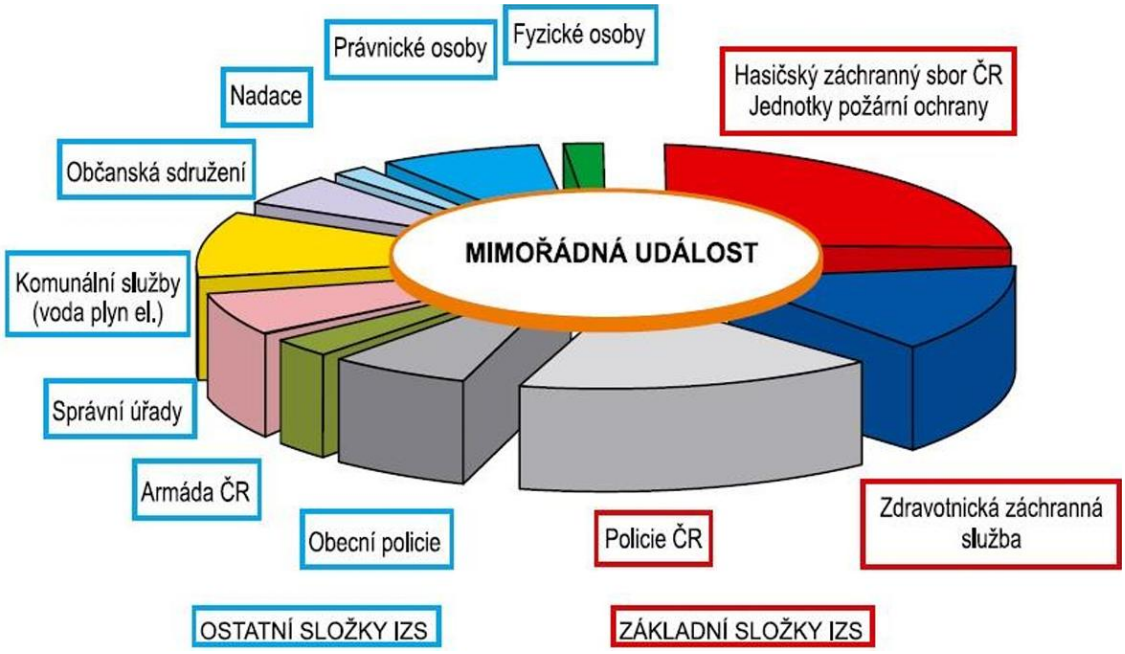
- Ústavní zákon č. 110/1998 Sb., o bezpečnosti ČR, který uvádí, že ozbrojené síly jsou jednou ze složek podílejících se na bezpečnosti ČR.
- Zákon č. 219/1999 Sb., o ozbrojených silách ČR upravuje postavení, úkoly a také členění ozbrojených sil ČR na Armádu ČR, Vojenskou kancelář prezidenta republiky a Hradní stráž. Zaměřuje se na definici úkolů jednotlivých částí ozbrojených sil, řízení ozbrojených sil a limity jejich použití. Upravuje i možnosti mezinárodní spolupráce s cizími ozbrojenými silami k plnění úkolů na základě mezinárodních smluv.
- Zákon č. 222/1999 Sb., o zajišťování obrany ČR se mimo jiné zabývá provedením opatření k obraně státu a výcvikem ozbrojených sil na území státu mimo vojenské újezdy (vojenské výcvikové prostory).
- Zákon č. 239/2000 Sb., o integrovaném záchranném systému definuje místo a úkoly vyčleněných sil a prostředků ozbrojených sil, jako ostatní složky integrovaného záchranného systému v ČR. Na obrázku 2 je zobrazena Armáda ČR jako jedna z ostatních složek integrovaného záchranného systému. V tomto pojetí se ozbrojené síly, jako ostatní složka integrovaného záchranného systému často zužují jen na Armádu ČR, protože Vojenská kancelář prezidenta republiky a Hradní stráž nemají dostatek personálu pro efektivní nasazení při řešení krizových situací nevojenského charakteru.
- Zákon č. 240/2000 Sb., o krizovém řízení řeší prioritně přednostní zásobování ozbrojených sil v době trvání krizových stavů ze stany vlády a hejtnanů.

- Zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy řeší systém hospodářské mobilizace a mobilizační dodávky, které jsou určeny pro přednostní zásobování ozbrojených sil v době trvání krizových stavů ze stany Správy státních hmotných rezerv.

Stěžejním zákonem pro použití Armády ČR při řešení krizových situací nevojenského charakteru na území ČR je zákon o ozbrojených silách ČR (Zákon č. 219/1999 Sb.), který sice uvádí, že základním úkolem ozbrojených sil je připravovat se k obraně státu a bránit ho proti vnějšímu napadení, ale plní též úkoly, které vyplývají z mezinárodních smluvních závazků ČR o společné obraně proti napadení. Současně však uvádí podmínky, za kterých mohou být ozbrojené síly ČR nasazeny při řešení mimořádných událostí a krizových situací nevojenského charakteru.

Podle § 14 zákona o ozbrojených silách ČR (Zákon č. 219/1999 Sb.) lze Armádu ČR použít k plnění těchto úkolů:

a) ke střežení objektů důležitých pro obranu státu,
b) k plnění úkolů Policie ČR, pokud síly a prostředky Policie ČR nebudou dostatečné k zajištění vnitřního pořádku a bezpečnosti, a to na dobu nezbytně nutnou,
c) k záchranným pracím při pohromách nebo při jiných závažných situacích ohrožujících životy, zdraví, značné majetkové hodnoty nebo životní prostředí nebo k likvidaci následků pohromy,
d) k odstranění jiného hrozícího nebezpečí za použití vojenské techniky,
e) k letecké dopravě ústavních činitelů,
f) k zabezpečení letecké zdravotnické dopravy,
g) k zabezpečení dopravy pro vlastní potřeby,
h) k poskytování leteckých služeb,
i) k zabezpečování dopravy na základě rozhodnutí vlády,
j) k zabezpečení kulturních, vzdělávacích, sportovních a společenských akcí,
k) k plnění humanitárních úkolů civilní obrany (Zákon č. 219/1999 Sb.).



Obrázek 2 Schematicky znázorněný podíl složek integrovaného záchranného systému při řešení mimořádných událostí nevojenského charakteru (Modul – G, 2020)

Převážnou část úkolů nevojenského charakteru plní Armáda ČR v rámci integrovaného záchranného systému jako vyčleněné síly a prostředky ozbrojených sil. Povolání vojáků v činné službě k plnění úkolů Policie ČR se řeší podle § 22 odst. 1 a 2 zákona o Policii ČR (Zákon č. 273/2008 Sb.), a podle zákona o ozbrojených silách ČR (Zákon č. 219/1999 Sb.). Pro nasazení vojáků je třeba vydání nařízení vlády o povolání vojáků v činné službě k plnění úkolů Policie ČR v souvislosti s konkrétními bezpečnostními opatřeními. Vojáci Armády ČR při plnění úkolů podle odstavce písm. b) § 14 (Zákon č. 219/1999 Sb.)

mají práva a povinnosti jako příslušníci Policie ČR. Úkoly plní ve vojenském stejnokroji s reflexní vestou nebo rukávovou páskou s označením „POLICIE“ dle vyhlášky o policejním označení (Vyhláška č. 122/2015 Sb.), ve smíšených hlídkách pod velením policisty.

Armáda ČR může být použita i v případě vzniku mimořádné události na jaderných elektrárnách. To je rozpracováno v nařízení vlády o povolání vojáků Armády ČR k plnění úkolů Policie ČR při radiačních haváriích na jaderných elektrárnách (Nařízení vlády č. 465/2008 Sb.). Základním úkolem nasazení sil a prostředků Armády ČR k plnění úkolů Policie ČR je, ve smíšených hlídkách, zabezpečit splnění úkolů pořádkové policie souvisejících s regulací pohybu osob, se zabezpečením veřejného pořádku a bezpečnosti při vzniku mimořádné události na jaderné elektrárně. K plnění těchto úkolů jsou mimo jiné útvary Armády ČR využiti i vojáci, vojenští studenti a technika Univerzity obrany (Nařízení vlády č. 465/2008 Sb.).

K plnění úkolů vyčleněných sil a prostředků ozbrojených sil v rámci integrovaného záchranného systému může být nasazena Aktivní záloha, která je součásti ozbrojených sil ČR. V době míru mohou být vojáci aktivní zálohy nasazeni k zabezpečení záchranných a likvidačních prací nebo při jiných závažných pohromách ohrožujících životy, zdraví, životní prostředí anebo značné majetkové hodnoty, ke střežení objektů důležitých pro obranu státu nebo k plnění úkolů spojených s podporou spojeneckých vojsk na území ČR. Aktivní záloha byla již nasazena v rámci Národního očkovacího centra v O_2 areně, ke střežení místa přespání (Rest Over Night – RON) Rančířov při přesunu alinčních vojsk na cvičení a naposledy v rámci operace „Migrace“ k posílení Police ČR při dočasném znovuzavedení ochrany státní hranice ČR se Slovenskem.

Použití Armády ČR k záchranným pracím a k likvidaci následků pohromy je dočasně organizované nasazením vojenských útvarů a vojenských zařízení s potřebným vojenským materiálem pod velením příslušného velitele nebo náčelníka. Koordinaci záchranných a likvidačních prací v místě nasazení složek integrovaného záchranného systému a v prostoru nasazení provádí velitel zásahu. Vnitřní řízení vyčleněných sil a prostředků ozbrojených sil je plně v kompetenci armádního velení. K nasazení Armády ČR při krizových situacích nevojenského charakteru dochází, pokud příslušné správní úřady, orgány územní samosprávy nebo požární ochrana nemohou zajistit záchranné práce nebo likvidaci následků pohromy vlastními silami (Zákon č. 239/2000 Sb.).

3. VYŽADOVÁNÍ NASAZENÍ VYČLENĚNÝCH SIL A PROSTŘEDKŮ OZBROJENÝCH SIL

Použití armády k záchranným pracím mohou cestou krajských operačních a informačních středisek hasičského záchranného sboru jednotlivých krajů vyžadovat hejtmani krajů a starostové obcí, v jejichž obvodu došlo k pohromě (obrázek 3), u náčelníka Generálního štábu, který rozhoduje o jejím nasazení (Zákon č. 219/1999 Sb.).

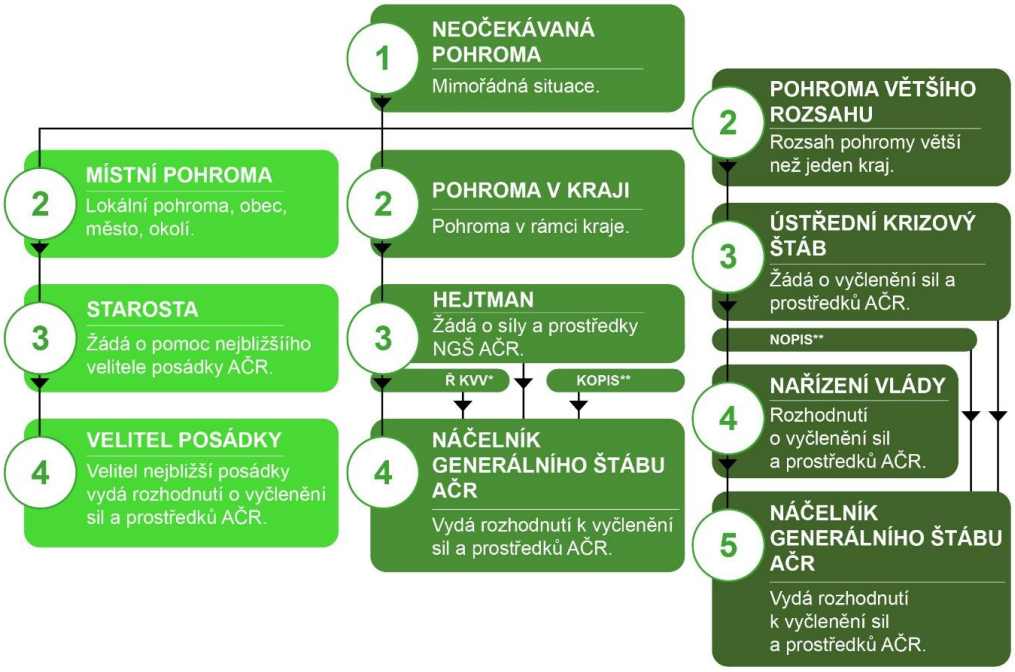
O nasazení vyčleněných síl a prostředků ozbrojených sil ČR k likvidaci následků pohromy – likvidační práce (Zákon č. 239/2000 Sb.) rozhoduje vláda ČR na návrh ministra vnitra, vydáním nařízení vlády na konkrétní řešení mimořádné události či krizové situace. Vláda ČR rozhoduje o nasazení vyčleněných sil a prostředků ozbrojených sil ČR při pohromách většího rozsahu, které zasáhly více krajů, cestou Národního operačního a informačního střediska Hasičského záchranného sboru ČR. Zejména pokud je situace rozsáhlá a vyžaduje koordinovanou celostátní reakci. Například loňské povodně způsobily značné škody na území dvou krajů, a proto vláda ČR rozhodla v pondělí 16. září 2024 o nasazení 2000 vojáků k likvidaci následků povodní (Armáda ČR, 2024). V rámci prevence při rozsahu těchto povodní nepomohly ani varovné zprávy Českého hydrometeorologického ústavu a jednotného systému varování a vyrozumění, které někteří lidé v později zasažených oblastech, nebrali na vědomí. O komparaci a účinnosti vyrovných systémů okolních států, včetně ČR a jejich možnostech byl již v roce 2020 publikován odborný článek (Lukáš, Mrázková, Šaur, 2020), ze kterého vyplynulo, že systém je na velmi dobré úrovni, ale vyžaduje modernizaci a přizpůsobení aktuálním hrozbám.

Aby při vyžadování nasazení Armády ČR nedocházelo ke ztrátě drahocenného času pro záchranu lidí a majetku různými schvalovacími procesy, může se na jednotlivé útvary Armády ČR obrátit přímo ten,

kdo je nejblíže ohrožení a potřebuje urgentně pomoc při řešení mimořádné události. Postup vyžadování vyčleněných sil a prostředků ozbrojených sil ČR je na obrázkuj 3. Například v případě povodní to jsou:

- Starosta obce – který může v případě bezprostředního ohrožení požádat o pomoc Armádu ČR, zejména pokud je situace lokální a vyžaduje rychlou reakci. Například se tak stalo v pátek 13. září 2024, kdy starosta města Strakonice požádal velitele místní posádky, 25. protiletadlového pluku, o pomoc 20 vojáků se stavbou protipovodňových hrází z pytlů plněných pískem.
- Hejtman kraje – může požádat o pomoc armády v rámci svého kraje, pokud je situace kritická a vyžaduje okamžitou reakci. Například hejtman Olomouckého kraje požádal 15. září 2024 o 12 vojáků se šesti nákladními vozidly T-815 k odstraňování stromů, které bránily průtoku vody. Následně podal spolu s hejtmanem Moravskoslezského kraje celkem 30 požadavků cestou krajského operačního informačního střediska Generálního ředitelství Hasičského záchranného sboru ČR (Armáda ČR, 2024).

Nasazení vyčleněných sil a prostředků ozbrojených sil je vždy koordinováno s integrovaným záchranným systémem, kde hlavní roli hrají příslušníci Hasičského záchranného sboru, kteří jsou zpravidla v roli velitele zásahu, nejen při povodních (Zákon č. 239/2000 Sb.).



Obrázek 3 Schéma postupu k vyčlenění jednotek Armády ČR pro pomoc při řešení mimořádných událostí nevojenského charakteru (Armáda ČR, 2024 – upraveno autorem)

4. HISTORICKÉ ZKUŠENOSTI S POUŽITÍM OZBROJENÝCH SIL NA ÚZEMÍ STÁTU

V historii naší republiky sehrála armáda při řešení mimořádných událostí a krizových situací významnou úlohu. Úkolům plněným v těchto oblastech byla vždy věnována vedením státu a velením armády patřičná pozornost. Zde je připomínka alespoň těch nejvýznamnějších.

- Po vzniku Československé republiky v říjnu 1918, bylo hlavním úkolem útvarů obsazení a uzavření státní hranice, nastolení státní správy a pořádku v příhraničním území.
- V únoru 1919 byla armáda podle rozhodnutí vlády Československé republiky použita znovu na uzavření státní hranice a k zabezpečení kolkování peněz. Armáda plnila úkoly hlídkování, pozorování a eskortování transportů peněz a kolků.
- V roce 1920, v období vládní krize, armáda asistovala četnictvu po vyhlášení stanného práva k obnově pořádku na Rosicku, Kladensku a v Praze.
- V květnu 1938 plnila armáda úkoly při zajištění státní hranice a vnitřního pořádku v příhraničním prostoru podle požadavku ministerstva vnitra.

- Po skončení II. světové války se československá armáda podílela na obnově veřejného pořádku. Nepřítelem byly zbytky německé armády a ozbrojené záškodnické skupiny a kriminální živly.
- V poválečném období (1948–1989) byla armáda významnou měrou orientována politickým vedením státu. Přesto lze konstatovat, že úkoly splnila podle platných zákonů.
- Účast Československé lidové armády na eliminaci povodní na Dunaji v roce 1966 přispěla k záchraně mnoha životů občanů a hospodářských statků.
- Asistence při leteckých haváriích, zdravotnického personálu při silničních a železničních nehodách, při odstraňování epidemií zvířat i epidemie cholery na Slovensku v roce 1973 ukázala na schopnost armády urychleně poskytovat účinnou pomoc.

V novodobé historii, která je datována vznikem ČR:

- Armáda ČR úspěšně zasahovala při povodních na Moravě v roce 1997, kde v rámci záchranných, zabezpečovacích a následných pracích bylo nasazeno celkem 19000 hasičů a 5700 vojáků s technikou. K posílení Policie ČR v oblasti plnění pořádkové a ochranné služby na zaplaveném území bylo nasazeno 2200 vojáků (Szaszo, 2010).
- V době rozsáhlých záplav v Čechách v roce 2002, v rámci asistenční operace na podporu Policie ČR v zaplaveném území bylo nasazeno 1200 vojáků a v operaci v rámci integrovaného záchranného systému bylo nasazováno denně kolem 4000 až 6000 vojáků a kolem 800 kusů vojenské techniky k odstraňování následků povodní (obrázek 4) (Armáda ČR, 2007).

Obrázek 4 Vojáci při výstavbě protipovodňové hráze v Praze v roce 2002 (Armáda ČR, 2024)

- Blesková povodeň zasáhla Liberecký kraj 7. srpna 2010 v ranních hodinách. Nejvíc povodeň postihla obce na Frýdlantsku, Liberecku a Českolipsku. Protrhly se hráze rybníků (např. Markvartický, Mlýnský) i hráz přehrady Kristýna. Přišlo o život 5 lidí. Zcela odtržené od okolí byly obce Višňová a Heřmanice. Do záchranných a likvidačních prací se na území Libereckého kraje zapojilo mimo hasičů, policistů, záchranářů zdravotnické služby a dobrovolníků také přibližně 1800 vojáků (Liberecký deník, 2012).
- V roce 2013 zasáhla většinu území Čech povodňová vlna způsobená vytrvalými dešti. V noci z 1. na 2. června 2013 překročily řeky na téměř padesáti místech ČR na úroveň hladiny 3 povodňového stupeně a 3 povodňový stupeň – stav ohrožení, byl vyhlášen. Vláda ještě ve stejný den vyhlásila nouzový stav pro celé území Čech kromě Pardubického a Karlovarského kraje. O den později začala platit povodňová bdělost – 1 povodňový stupeň i pro Jihlavsko, Znojemsko a okresy na severu Olomouckého a Moravskoslezského kraje. V Čechách se nouzový stav rozšířil i na Karlovarský kraj. Červnové záplavy zasáhly 700 obcí a vyžádaly si celkem 15 lidských životů. Armáda ČR poskytla přes 10500 vojáků a 2100 kusů techniky. Vojáci pracovali především na výstavbě protipovodňových zábran, zajišťovali přepravu humanitární pomoci, výstavbu provizorního ubytování pro zasahující složky a evakuované osoby, ale také

speciální ženijní práce, jako byly úpravy poničených komunikací, demolice objektů, asanační práce a také prováděli monitoring a evakuaci vrtulníky (Natoaktual.cz, 2013).

- Další nasazení Armády ČR bylo po říjnové a prosincové explozi v roce 2014, v muničním skladu v areálu Vojenského technického ústavu v katastru obce Vlachovice, část Vrbětice, ve Zlínském kraji. Vojáci Armády ČR se v rámci výpomoci Policii ČR zapojili do ostrahy objektu a do monitorování situace po sérii explozí a do střežení vnějšího perimetru, následně i do budování oplocení pro zajištění této bezpečné hranice. Ve Vrběticích se vystřídalo téměř 7000 příslušníků armády, prakticky všech jejích složek. Kromě střežení areálu se vojáci významnou měrou zapojili též do přepravy munice, pyrotechnické asanace a také řady další ženijních úkolů, z nichž nejvýznamnější byla právě součinnost při výstavbě nového dočasného oplocení areálu. Klíčové bylo logistické zabezpečení ze strany Armády ČR, které využívaly i další složky integrovaného záchranného systému. Armáda ČR ukončila činnost po 15 měsících, 5. února 2016 (Kramář, 2020) a dá se říci, že po celou dobu nasazení byla téměř zcela soběstačná.
- V březnu roku 2016, po teroristických útocích v Bruselu přešla ČR na návrh ministra vnitra a potvrzení vlády do prvního stupně ohrožení terorismem. Pro zajištění bezpečnosti bylo mimo jiné přistoupeno na požadavek ministra vnitra o posílení Policie ČR k ustanovení smíšených ozbrojených hlídek Armády ČR a Policie ČR. Smíšené ozbrojené hlídky se zapojily do hlídkové činnosti Policie ČR jak na letištích, tak v pražském metru, ale také u strategických budov či pietních a památných míst citlivých pro českou historii. Zvýšená opatření se rovněž týkala míst se zvýšenou kumulací lidí ve velkých městech, sportovních i kulturních akcí a v neposlední řadě i zastupitelských úřadů a konzulátů vybraných zemí v ČR. Smíšené ozbrojené hlídky byly složeny z velícího příslušníka Policie ČR a jednoho až dvou vojáků Armády ČR. Denně bylo nasazeno 550 vojáků a v hlídkách se střídali téměř dva měsíce (Právo a Novinky, 2016).
- V souvislosti s epidemií koronaviru Covid-19 v ČR byli vojáci Armády ČR nasazováni na pomoc integrovanému záchrannému systému jak podle zákona o zajišťování obrany (Zákon č. 219/1999 Sb.), tak podle zákona o integrovaném záchranném systému (Zákon č. 239/2000 Sb.) a to již od 10. března 2020, kdy bylo třeba kontrolovat na státních hranicích zdravotní stav osob, projíždějících přes ČR (obrázek 5). Vojáci i poté plnili služební úkoly v souvislosti s realizací opatření přijatých vládou ČR v rámci nouzového stavu i mimo něj k omezení šíření tohoto onemocnění. K těmto úkolům bylo vyčleněno a plnilo je celkem 11853 vojáků prakticky ze všech vojenských útvarů a zařízení (Fajnor, 2021), včetně studentů Univerzity obrany a příslušníků aktivní zálohy (obrázek 5), někteří se podíleli na více úkolech nebo se do jejich plnění zapojili opakovaně (Dvořáková, 2020), (Generální štáb, 2022).

Obrázek 5 Nasazení Armády ČR při pandemii Covid-19 v ČR (Dvořáková, 2020), (Fajnor, 2021)

- 24. června 2021 řádilo ničivé tornádo v obcích na Břeclavsku a Hodonínsku, poničilo 1200 domů, zranilo stovky lidí a 6 lidí při něm zahynulo (Natoaktual.cz, 2021). Vojáci Armády ČR byli nasazeni jak při záchranných, tak i likvidačních pracích, poskytovali i psychologickou pomoc a lékařský tým. Při likvidačních a úklidových pracích (obrázek 6) se na jižní Moravě vystřídalo téměř 1194 vojáků a nasazeno bylo 104 kusů techniky, většinou těžké ženijní techniky, včetně bagrů a nakladačů ze 7. mechanizované brigády. (Generální štáb, 2022).

Obrázek 6 Nasazení vojáků při likvidačních pracích po ničivém tornádu. (Natoaktual.cz, 2021)

- V pátek 13. září 2024 extrémní deštivé počasí mělo za následek ničivé povodně zejména v oblastech severní Moravy a Slezska, kde přes víkend napršelo i 500 mm vody na jeden čtvereční metr. Situaci už nešlo zvládat běžnými silami a prostředky a bylo tedy rozhodnuto o nasazení jednotek Armády ČR. Vojáci byli nasazováni na pomoc od 16. září až do 30. listopadu 2024 a celkem se na nasazení vystřídalo 5400 vojáků. Vypomáhali nejen s odstraňováním naplavenin, zásobováním pitnou vodou a humanitární pomocí, ale také při evakuaci obyvatel z nepřístupných míst vrtulníky a ženisté vybudovali mnoho mostních provizorií, jak je vidět na obrázku 7 (Dvořáková, 2024).

Obrázek 7 Nasazení Armády ČR při povodních na severu Moravy a Slezska (Dvořáková, 2024)

5. POROVNÁNÍ VYČLENĚNÝCH SIL A PROSTŘEDKŮ OZBROJENÝCH SIL PŘI ŘEŠENÍ NEVOJENSKÝCH MIMOŘÁDNÝCH UDÁLOSTÍ A KRIZOVÝCH SITUACÍ

I když hlavním úkolem ozbrojených sil ČR je připravovat se k obraně státu a bránit ho proti vnějšímu napadení, podílí se velkou měrou i na zajištění vnitřní bezpečnosti ČR, jak je vidět z dat tabulky 1. Jejich pomoc při řešení mimořádných událostí a krizových situací nevojenského charakteru v době, kdy příslušné správní úřady, orgány územní samosprávy nebo jednotky integrovaného záchranného systému nemohou zajistit záchranné nebo likvidační práce vlastními silami, je významná a nenahraditelná.

Tabulka 1 Odhadované počty nasazených vojáků Armády ČR při jednotlivých krizových stavech (Natoaktual.cz, 2013), (Kramář, 2020), (Generální štáb, 2022), (Dvořáková, 2024)

Krizový stav	Rok	Důvod	Územní rozsah	Odhadovaný počet vojáků
Stav nebezpečí	1997	Povodně	Moravskoslezský, Olomoucký kraj	5700
Nouzový stav	2002	Povodně	Praha, Středočeský, Jihočeský, Plzeňský, Karlovarský, Ústecký	5000
Nouzový stav	2006	Povodně	Jihočeský, Středočeský, Ústecký, Pardubický, Jihomoravský, Olomoucký, Zlínský	234
Stav nebezpečí	2010	Povodně	Liberecký kraj (Frýdlantsko), Ústecký kraj	1800
Nouzový stav	2013	Povodně	Praha, Středočeský, Jihočeský, Plzeňský, Ústecký, Liberecký, Královéhradecký	10500
Stav nebezpečí	2014	Povodně	Jihočeský kraj	7000
Nouzový stav	2020 – 2022	Pandemie COVID-19	Celá ČR	15000
Stav nebezpečí	2021	Tornádo	Jihomoravský kraj (Hodonínsko, Břeclavsko)	1194
Nouzový stav	2022	Migrační vlna	Celá ČR	74
Nouzový stav	2024	Povodně	Moravskoslezský, Olomoucký kraj	5400

Armáda ČR se ve větší či menší míře podílela při všech krizových stavech, které byly v posledních letech v ČR vyhlášeny. Jak je z tabulky 1 patrné, zpravidla čím větší území je zasaženo katastrofou, tím větší pomoc ze strany Armády ČR je potřeba nasadit. To závisí na konkrétní situaci v terénu a na rozsahu katastrofy.

Vyčleněné síly a prostředky ozbrojených sil ČR se na své možné budoucí úkoly při řešení mimořádných událostí a krizových situací nevojenského charakteru připravují i na mezinárodních cvičeních v rámci Severoatlantické aliance (CMX) a Evropské unie (CME), a na národních součinnostních cvičeních se složkami integrovaného záchranného systému.

ZÁVĚR

Jednotlivé státy i koalice hledají stále nové přístupy, metody a formy k zajištění bezpečnosti obyvatelstva a otázky bezpečnosti se stávají ústředním tématem všech mezinárodních jednání. S analýzou bezpečnostních rizik je přímo spojena problematika prevence a reakce vedoucí k jejich minimalizaci, popřípadě i k jejich eliminaci. K tomuto cíli musí směřovat bezpečnostní strategie ČR, NATO a EU.

S dynamickým vývojem bezpečnostního prostředí, které je charakterizováno rostoucí komplexností, proměnlivostí a obtížnou předvídatelností, je naše společnost konfrontována množstvím nových ohrožení společenského i přírodního charakteru. Tato situace vyžaduje neustálé vyhodnocování potencionálních hrozeb a z nich plynoucích rizik pro ČR, nepřetržitý monitoring zajištění bezpečnosti klíčových oblastí pro chod státu, jeho kritické infrstruktury a ochrany obyvatelstva, na čemž mají ozbrojené síly a zpravodajské služby České republiky podstatný podíl.

Institucionální nástroj k realizaci bezpečnosti tvoří bezpečnostní systém ČR, v němž právě ozbrojené síly představují jeden ze základních pilířů. Výstavba ozbrojených sil musí vytvářet primárně takové schopnosti, které budou efektivně využitelné a přínosné v podmínkách působení v mnohonárodních uskupení a rovněž zajistí plnění úkolů nevojenského charakteru na území ČR při řešení mimořádných událostí a krizových situací. Vyčleněné síly a prostředky ozbrojených sil mají v současnosti svou nezastupitelnou roli v rámci integrovaného záchranného systému v ČR.

Je možno konstatovat, že kdyby bylo k dispozici více nasaditelných vojáků s efektivní technikou, krizová situace by se mohla řešit snadněji i rychleji. V současnosti je takových sil a prostředků celkem nedostatek tím spíše, když je třeba zintenzivnit výcvik vojáků vzhledem ke dlouhodobě nedobré situaci na Ukrajině a k hlavnímu úkolu ozbrojených sil České republiky.

PODĚKOVANÍ

Tento článek byl financován z projektu Vedení pozemních operací (DZRO-FVL22-LANDOPS, financovatelem projektu je Ministerstvo obrany České republiky) na Univerzitě obrany, Fakultě vojenského leadershipu, v souladu se zákonem č. 130/2002 Sb., o podpoře výzkumu a vývoje.

LITERATURA

Armáda ČR. (2007). *POVODEŇ 2002 - vzpomínka na události před pěti lety*. [online] Dostupné z: https://www.mo.gov.cz/scripts/detail.php?id=9637

Armáda ČR. (2024). *Otázky a odpovědi: Pomoc vojáků při povodních.* [online] Dostupné z: https://acr.mo.gov.cz/informacni-servis/zpravodajstvi/otazky-a-odpovedi:-pomoc-vojaku-pri-povodnich-253856/

Bezpečnostní strategie České republiky. (2023). Praha: Ministerstvo zahraničních věcí ČR. [online] Dostupné z: https://mzv.gov.cz/file/5118610/Bezpecnostni_strategie_Ceske_republiky_2023.pdf

Dvořáková, M. (2020). *Posílení Policie ČR příslušníky Armády České republiky na státních hranících.* [online] Dostupné z: https://mocr.mo.gov.cz/informacni-servis/tiskove-zpravy/16-03-20:-posileni-policie-cr-prislusniky-armady-ceske-republiky-na-statnich-hranicich-220070/

Dvořáková, M. (2024). Pomoc vojáků při povodních dnes po třech měsících skončila. [online] Dostupné z: https://acr.mo.gov.cz/informacni-servis/zpravodajstvi/pomoc-vojaku-pri-povodnich-dnes-po-trech-mesicich-skoncila-255454/

Fajnor, J. (2021). *Vojáci dostanou mimořádné odměny za pomoc v boji s epidemií Covid-19*. [online] Dostupné z: https://mocr.mo.gov.cz/assets/informacni-servis/tiskove-zpravy/028_tz_vojaci-dostanou-mimoradne-odmeny-za-opatreni-proti-covid_210719.doc

Generální štáb. (2022). *Armáda České republiky v roce 2021*. Ministerstvo obrany České republiky – VHÚ Praha, ISBN 978-80-7278-835-4

Kramář., R. (2020). *Zásah ve Vrběticích je po dlouhých letech ukončen*. [online]. Dostupné z: https://hzscr.gov.cz/clanek/zasah-ve-vrbeticich-je-po-dlouhych-letech-ukoncen.aspx

Liberecký deník. (2012). *Výročí povodní: Povodně 2010 v číslech.* [online]. Dostupné z: https://liberecky.denik.cz/pribehy_vody/vyroci-povodni-povodne-2010-v-cislech-20120807.html

Lukáš, L. & Mrázková, L. & Šaur, D. (2020). Komparace způsobů varování před povodněmi ve vybraných evropských státech. Krízový manažment, 2020(1), 32-42. ISSN 1336-0019. DOI 10.26552/krm.C.2021.1.32-42.

Jurenka, M. (2023). *Použití ozbrojených sil České republiky* [PowerPoint]. Neuvedeno: [vlastní tvorba], [cit. 2025-08-10].

Ministerstvo vnitra. (2016). *Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu.* [online]. Dostupné z: https://mv.gov.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx

Modul – G (2020): integrovaný záchranný systém a požární ochrana. Praha: Ministerstvo vnitra – generální ředitelství Hasičského záchranného sboru ČR. ISBN 978-80-7616-071-2.

Natoaktual.cz. (2013). *Nasazení vojáků po povodních končí, vystřídalo se jich 10 tisíc.* [online]. Dostupné z: https://www.idnes.cz/zpravy/nato/vojaci-konci-pomoc-po-povodnich.A130715_115218_zpr_nato_inc

Natoaktual.cz. (2021). *Armáda stáhla vojáky z odklízení škod po červnovém tornádu.* [online]. Dostupné z: https://www.natoaktual.cz/zpravy/tornado-armada-vojaci-jihomoravsky-hodonin-breclav-zenijni.A210824_105055_na_zpravy_m00

Natoaktual.cz. (2023). *Na ochranu hranic nasadila armáda tisíce profesionálů a rekordní počet záložáků.* [online]. Dostupné z: https://www.natoaktual.cz/zpravy/armada-hranice-zaloh-aktivni-migrace-prevadec-policie.A230206_173638_na_zpravy_m00

Nařízení vlády č. 465/2008 Sb. o povolání vojáků Armády České republiky k plnění úkolů Policie České republiky při radiačních haváriích na jaderných elektrárnách

Právo a Novinky. (2016). *V Česku platí první stupeň ohrožení terorismem, Chovanec chce vojáky v ulicích.* [online]. Dostupné z: https://www.novinky.cz/clanek/domaci-v-cesku-plati-prvni-stupen-ohrozeni-terorismem-chovanec-chce-vojaky-v-ulicich-17786

Szaszo, Z. (2010) *Stručná historie profesionální požární ochrany v Českých zemích*. MV-GŘ HZS ČR. ISBN–978–80-86640-60-0.

Ústavní zákon č. 1/1993 Sb., Ústava České republiky.

Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky.

Vyhláška č. 122/2015 Sb., o způsobu vnějšího označení, služebních stejnokrojích a zvláštním barevném provedení a označení služebních vozidel, plavidel a letadel Policie České republiky a o prokazování příslušnosti k Policii České republiky (o policejním označení).

Zákon č. 222/1999 Sb., o zajišťování obrany České republiky a o změně některých zákonů.

Zákon č. 219/1999 Sb., o ozbrojených silách České republiky a o změně některých zákonů.

Zákon č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů.

Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon).
Zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých zákonů.
Zákon č. 273/2008 Sb. o Policii České republiky.

Jiří Kalenda, Ing.
Univerzita obrany, Kounicova 65, 66210 Brno, Česká republika
e-mail: jiri.kalenda@unob.cz

Jiří Barta, Ing., Ph.D.
Univerzita obrany, Kounicova 65, 66210 Brno, Česká republika
e-mail: jiri.barta@unob.cz

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.128-134
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

COST-BENEFIT ANALYSIS AS A TOOL TO STRENGTHEN ORGANISATIONAL CYBER RESILIENCE

KATARÍNA KAMPOVÁ, MATÚŠ MADLEŇÁK, TIMOTEJ MAČUHA, SAMUEL HUBOČAN, MARTIN HROMADA

ABSTRACT: Organisations face a wide range of cyber threats with significant operational, financial and reputational impacts. Strengthening resilience therefore requires not only technical and organisational measures, but also clear economic justification. Cost–Benefit Analysis (CBA) is a well-established method that compares the costs of security measures with their benefits, such as reducing the likelihood of incidents, limiting their impact or shortening recovery times. In line with NIS2 and ISO/IEC 27001:2022 and ISO/IEC 27005:2023, CBA supports proportionate, risk-based and cost-effective security. This paper outlines the methodology, its role in decision-making, and a practical example of its application in enhancing cyber resilience and trust.

KEYWORDS: *Risks. Resilience. Cybersecurity. Cost–Benefit Analysis. Measures.*

INTRODUCTION

Strengthening the cyber resilience of organisations has become a key challenge as they face many different types of threats. These threats can be intentional, such as cyberattacks or misuse of access rights, unintentional, such as human errors or misconfigurations, or caused by technical and natural factors, including infrastructure failures, power outages, or natural disasters. Such events may result in incidents with serious operational, financial, and reputational impacts. For this reason, effective risk management requires not only technical and organisational measures but also clear economic justification. One of the proven approaches is Cost–Benefit Analysis (CBA), which helps organisations evaluate whether investments in cybersecurity and resilience are adequate compared to the expected benefits. CBA compares the overall costs of introducing, operating, and maintaining security measures with the benefits they bring. These benefits include reducing the likelihood of a cyber incident, limiting its impact on the confidentiality, integrity, and availability of information, or shortening recovery time objectives (RTO, RPO). In practice, CBA can help organisations decide whether it is more efficient to implement multi-factor authentication, network segmentation, endpoint detection and response (EDR/XDR), or extended user training programs.

According to the NIS2 Directive and international standards ISO/IEC 27001:2022 and ISO/IEC 27005:2023, organisations are required to implement security measures that are proportionate to risks and cost-effective. CBA is one of the recommended methods that can support this requirement. It helps management make informed decisions, improves transparency in budget allocation, and provides evidence to regulators that measures follow the principle of proportionality. This paper explains the methodology of CBA and shows its use in evaluating organisational cyber resilience. It outlines how CBA can compare alternative security measures, identify those with the best balance of benefits and costs, and strengthen protection against cyber threats. A practical example demonstrates how CBA can support strategic decision-making and improve trust in the organisation among partners, customers, and regulators.

The main aim of this paper is to present a clear and structured application of CBA as a decision-support tool in cybersecurity, and to demonstrate its practical value in strengthening organisational cyber resilience. The contribution of the paper lies in linking risk management obligations under the NIS2 Directive and ISO/IEC standards with an economically justified methodology for selecting proportionate and cost-effective security measures. A practical model example illustrates how CBA can support transparent, evidence-based decision-making.

1. RISK ASSESSMENT AND ITS LINK TO THE RISK MANAGEMENT PLAN

Cyber risk management is a logical and systematic process of identifying, analysing, evaluating, and treating risks with the aim of minimising negative impacts or exploiting emerging opportunities. It is not just about methods and tools; according to Šimák, it also includes the culture, processes, and organisational structures that support the management of uncertainty and the continuous improvement of the quality of decision-making (Šimák, 2006). In a well-managed organisation, the process is embedded in strategic, operational, and project management and is supported by policies, procedures, and practices for communication and consultation, context determination, risk assessment, risk treatment, monitoring, documentation, and reporting (ISO/IEC 27001:2022).

The ISO/IEC 27005:2023 standard provides a specific framework for assessing information security risks and complements the requirements of ISO/IEC 27001:2022 for an ISMS management system. In accordance with the NIS2 Directive, essential and important entities have an obligation to implement appropriate and cost-effective technical, organisational and procedural measures, including proper incident management and top management accountability (European Union, 2022). Determining the context is a preliminary step in risk assessment, the organisation systematically evaluates external factors (legislation, technology, market, threats) and internal factors (structure, culture, resources, IS/IT architecture, existing controls), defines asset protection requirements and sets risk criteria (appetite, tolerance, consequence and probability metrics, time aspects, risk combinations). It includes the choice of analysis method (qualitative, quantitative or combined). Risk assessment consists of three steps (ISO 31000:2018), (ISO/IEC 27001:2022):

1. Risk identification: systematic search and description of risks (threats, vulnerabilities, causes, scenarios, affected assets).
2. Risk analysis: estimation of probability and severity of impacts on confidentiality, integrity and availability (CIA), taking into account the effectiveness of existing controls, working with uncertainty and input sensitivity.
3. Risk evaluation: comparison with acceptance criteria and setting priorities for treatment.

The output is a risk list, which is a direct input to the Risk Treatment Plan. This plan documents:

- risks to be treated;
- the chosen strategy (avoidance, reduction of probability/impact, sharing/transfer, acceptance);
- specific technical, organisational and procedural measures;
- responsibilities, deadlines, resources;
- and effectiveness metrics (e.g. incident rate, MTTD/MTTR, RTO/RPO compliance).

As the NIS2 Directive emphasises the principle of proportionality and cost-effectiveness, when selecting security measures, organisations are expected to be able to demonstrate their proportionality – that is, that the costs of the measures are in reasonable proportion to the risk reduction they bring. It is therefore not enough to have a technically effective solution, but also to have an economic justification for it. CBA thus forms a decision gateway between the risk assessment and the final design of the risk treatment plan. Since decision-making on measures often takes place in conditions of limited resources and multiple alternatives, it is necessary to ensure not only the technical effectiveness, but also the economic adequacy of the solutions. This is where CBA plays a key role, allowing to quantify and compare different risk treatment scenarios, for example whether it is more profitable to invest in technical measures (e.g. multi-factor authentication, EDR), organisational measures (user training, policy updates) or a combination of them. The results of CBA provide the basis for management to be able to transparently justify that the chosen measures are not only effective, but also cost-effective and in accordance with the principle of proportionality according to the NIS2 Directive (Figure 1).

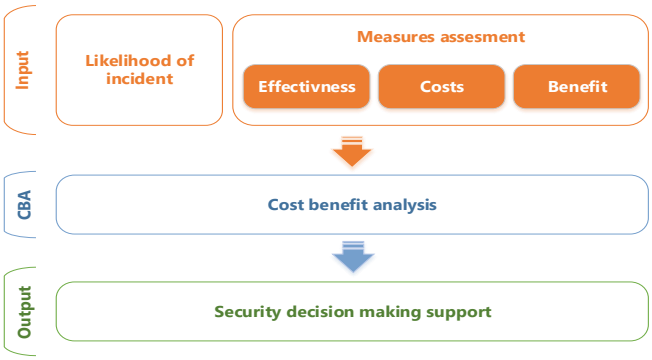


Figure 1 Cost–Benefit Analysis process within the security framework (Kampová, 2020)

As illustrated in Figure 1, CBA follows the risk assessment and is an input to the risk treatment plan. The process builds on the results of the threat identification, vulnerability assessment and impact assessment that are part of the risk analysis according to ISO/IEC 27005. CBA works with two main inputs:

- Incident probability – based on the combination of threats and vulnerabilities identified in the risk analysis and determines how often an incident is likely to occur.
- Evaluation of measures – involves assessing the proposed security measures in terms of their effectiveness in mitigating vulnerabilities and impacts, as well as the costs of their implementation and operation.

The output of CBA is an economically justified selection of measures that reduce risks to an acceptable level. At the same time, it meets the proportionality principle required by the NIS2 Directive – measures must not only be effective, but also appropriate and cost-effective.

2. COST-BENEFIT ANALYSIS

Strengthening the cyber resilience of organisations requires not only the implementation of technical and organisational security measures but also their clear economic justification. One of the proven methods is CBA, which makes it possible to compare the costs of implementing, operating, and maintaining security measures with the benefits they bring - from reducing the likelihood of cyber incidents, through limiting their impact on the confidentiality, integrity, and availability of information, to shortening recovery times (RTO, RPO). The CBA process typically includes the following steps:

- Definition of the problem and identification of alternatives.
- Identification and categorization of costs and benefits.
- Quantification and monetization of all impacts.
- Discounting future costs and benefits.
- Calculation of indicators such as NPV, BCR, ROI, and payback period.
- Conducting a sensitivity analysis.
- Selection of the most cost-effective and proportionate measure.

In accordance with the NIS2 Directive and the ISO/IEC 27001:2022 and ISO/IEC 27005:2023 standards, organisations are required to implement measures that are proportionate to risks while also being cost-effective. CBA provides a methodological framework that supports this principle of proportionality, increases transparency in budget allocation, and offers evidence for regulatory authorities. The article describes the CBA methodology and demonstrates its use in assessing the cyber resilience of organisations. It focuses on comparing alternative security measures, identifying those with the best cost-benefit ratio, and showing how CBA supports strategic decision-making and strengthens the trust of partners, customers, and regulatory authorities in the organisation (Sieber, 2004).

The fundamental principles of CBA rest on several conditions that determine its application in the evaluation of investment projects, policies, or security measures. One of the key principles is economic efficiency (Messonnier & Meltzer, 2002), (Boardman, 2018). CBA examines whether the proposed

project or measure represents an effective use of available resources, based on an estimate of social costs and benefits. Another principle is the quantification of costs and benefits. CBA makes it possible to translate even social effects - both positive and negative - into monetary units, thereby creating an objective basis for comparing alternative options. However, this approach also brings philosophical and ethical dilemmas, especially when it comes to valuing incomparable goods such as human life or the environment. Therefore, it is advisable to complement CBA with broader deliberative approaches when making decisions about public policies or security strategies. When applying CBA, it is necessary to distinguish between financial and economic analysis (Gunes, 2020).

- Financial analysis focuses on the actual financial costs and revenues of a project or measure. It assesses efficiency exclusively from the perspective of the organisation—that is, whether the investment is worthwhile in terms of cash flows, return on investment, or profitability. This approach does not take into account broader social consequences such as external costs or benefits. Its goal is to evaluate the financial sustainability of the project.
- Economic analysis, on the other hand, considers the overall societal effects. It includes in its calculations not only direct costs and benefits but also indirect and external impacts—for example, effects on employment, quality of life, reputation, or environmental factors. The focus is not on profit, but on the socio-economic benefits for the wider environment.

In the context of cybersecurity, an example can be given:

- Financial analysis will evaluate the costs of implementing multi-factor authentication (MFA) against the expected savings from preventing incidents.
- Economic analysis, however, will add a broader dimension: increased customer trust, improved organisational reputation in the market, greater stability of critical infrastructure, or savings in the form of reduced state expenditures for addressing the consequences of cyberattacks.

The combination of both approaches enables decision-makers to choose measures that are not only financially effective for the organisation but also bring broader societal benefits. CBA must take into account that individual costs and benefits occur at different stages of the project life cycle (Table 1). Their precise identification makes it possible to determine when the budget is most heavily burdened and when the benefits begin to materialize.

Table 1 Project life cycle phases and their characteristics (European Commission, 2014)

Project Phase	**Characteristics**
Pre-investment phase	Planning, preparatory analyses, decision-making; includes so-called “sunk costs.”
Investment phase	Implementation of the measure or project; high capital expenditures.
Operational phase	Regular operation of the project; generation of benefits and partial operating costs.
Post-operational phase	Project closure, sale or disposal of assets, evaluation of results.

The allocation of individual items to a specific phase enables a realistic assessment of the return and effectiveness of investments. For systematic and comparable processing of CBA, the categorization of costs and benefits is essential. This categorization increases transparency and allows for effective comparison of project or measure alternatives.

Table 2 Criteria for categorizing costs and benefits (Sieber, 2004)

Criterion	**Classification**
By affected entity	State, enterprises, households, non-profit organisations.
By project phase	Pre-investment, investment, operational, post-operational.
By nature of impact	Tangible (e.g., hardware), intangible (reputation), financial.
By measurability	Quantifiable, non-quantifiable.
By causality	Direct (e.g., technology purchase), indirect (secondary effects, reputational impacts).

3. EXAMPLE OF CBA APPLICATION IN CYBERSECURITY

In the practical application of CBA in the field of information and cybersecurity, standard financial analysis indicators are used to quantify the effectiveness of investments (European Commission, 2014):

- **NPV (Net Present Value):** the net present value, which expresses the difference between discounted benefits and costs. A positive NPV indicates that the project is economically beneficial.
- **BCR (Benefit–Cost Ratio):** the ratio of benefits to costs; a value greater than 1 confirms the efficiency of the project.
- **ROI (Return on Investment):** the return on investment, expressed as a percentage of the ratio of net benefit to total costs.
- **Payback period:** the time period within which the investment is recovered through the savings achieved.

These indicators provide a basis for the comparability of alternative measures and support transparent decision-making. The following model example illustrates how these CBA steps can be applied in practice. It shows the transition from risk-based justification to financial evaluation and demonstrates how CBA supports transparent and proportionate decision-making in line with the NIS2 Directive.

A model example can be given in the public administration environment, where accounting information systems represent critical infrastructure. The organisation is considering an investment in a security module that includes EDR (Endpoint Detection and Response) and automated data backup.

Table 3 Decision Parameters for the Implementation of a Security Module

Parameter	Value	Description/Calculation
Estimated annual loss before the measure	€250,000	System outages, manual processing, reputational losses
Estimated annual loss after the measure	€50,000	Impact reduction thanks to rapid detection and data recovery
Investment costs	€90,000	Licenses, implementation, training
Annual savings (Benefit)	€200,000	250,000 − 50,000
NPV (Year 1)	€110,000	200,000 − 90,000
BCR (Year 1)	2.22	200,000 / 90,000
ROI (Year 1)	122%	110,000 / 90,000 × 100
Payback period	0.45 year	90,000 / 200,000

The results show that the investment is economically effective (Table 3), with a short payback period and a significant reduction in operational risks. From the perspective of the NIS2 Directive, the organisation thus demonstrates the proportionality and cost-effectiveness of the implemented measures. To increase the robustness of the results, it is advisable to carry out a sensitivity analysis. Even with a +20% change in investment costs or a −20% decrease in expected savings, the BCR values remain greater than 1 in both cases, confirming that the measures continue to be economically justifiable.

CONCLUSION

The results of applying the CBA method in the field of information and cybersecurity highlight its significance in several dimensions:

- Financial transparency – Quantified indicators (NPV, BCR, ROI) enable management to effectively justify security investments to founders, shareholders, or regulatory authorities. CBA thus contributes to the rational allocation of limited financial resources.
- Compliance and regulatory requirements – In light of the NIS2 Directive, it is necessary to demonstrate that the implemented measures are proportionate to risks and economically justified. CBA provides an objective framework that supports the fulfillment of legislative obligations while minimising the risk of sanctions.

- Strategic management and priorities – With a limited budget, it is important to prioritize measures with higher BCR values and shorter payback periods. CBA enables the prioritization of investments and their alignment with the strategic goals of the organisation.
- Strengthening resilience and trust – Investments supported by CBA not only reduce the likelihood of incidents but also strengthen the trust of partners, customers, and regulatory authorities. Transparent economic justification contributes to building reputation and long-term organisational stability.
- Support for continuous improvement – The implementation of security measures is not a one-off process. CBA can be repeatedly used to monitor the effectiveness of measures and to guide decisions on their adjustment or modernization.

A significant implication for practice is that CBA links the technical and economic aspects of security. While technical measures are essential for risk reduction, economic rationality ensures that the organisation can maintain its security framework in the long term. This synergy is key to effective risk management in an environment of increasing digitalization and interconnected systems.

CBA is a useful and transparent method, but its results are influenced by several limitations. Estimates of incident probabilities may be inaccurate due to limited or low-quality data. It is also difficult to precisely quantify some intangible impacts, such as reputational damage or loss of trust. In addition, part of the benefits of security measures may appear only over a longer period, which complicates their exact evaluation.

Future research should focus on more accurate methods for estimating probabilities (e.g., using Bayesian approaches), on developing economic benchmarks for different NIS2 sectors, and on combining CBA with other decision-making methods. Another promising area is the application of CBA across various sectors of critical infrastructure to better assess the proportionality and long-term benefits of security measures.

ACKNOWLEDGEMENTS

This paper was supported by the Scientific Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic and the Slovak Academy of Sciences (VEGA) under project No. 1/0257/23 Cyber Risk Assessment as an Essential Tool for Enhancing Cybersecurity in Public Administration.

This publication has been produced thanks to support under the Operational Program Research and Innovation for the project: ICT for smart society, code ITMS2014 +: 313011T462, co-financed by the European Regional Development Fund.

REFERENCES

Boardman, A. E., Greenberg, D. H., Vining, A. R., & Weimer, D. L. (2018). Cost–Benefit Analysis: Concepts and Practice (5th ed.). Harlow: Pearson.

European Commission. (2014). Guide to Cost–Benefit Analysis of Investment Projects. Luxembourg: Publications Office of the European Union.

European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2), repealing Directive (EU) 2016/1148. Official Journal of the European Union, L 333, 80–152.

Gunes, N. (2020). Cost–benefit analysis. SAGE Publications. https://doi.org/10.4135/9781452229669.n858

International Organization for Standardization. (2018). ISO 31000:2018 – Risk management – Guidelines. Geneva: ISO.

International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO/IEC.

International Organization for Standardization & International Electrotechnical Commission. (2023). ISO/IEC 27005:2023 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks. Geneva: ISO/IEC.

Kampová, K., Mäkká, K., & Zvaríková, K. (2020). Cost–benefit analysis within organization security management. SHS Web of Conferences, 74, 01010. https://doi.org/10.1051/shsconf/20207401010

Messonnier, M. L., & Meltzer, M. I. (2002). Cost–benefit analysis. In Disease Control Priorities in Developing Countries (pp. 127–155). https://doi.org/10.1093/oso/9780195148978.003.0008

NIS2 Directive. (2022). NIS2 Directive – EU-wide cybersecurity rules. [Online] Available at: https://www.nis-2-directive.com [Accessed 11 Jun 2025].

Sieber, P. (2004). Methodological Guide: Cost–Benefit Analysis. Prague: Ministry for Regional Development.

Šimák, L. (2006). Manažment rizík. Žilina: Žilinská univerzita v Žiline, Fakulta špeciálneho inžinierstva. [Online] Available at: http://fsi.uniza.sk/kkm/old/publikacie/mn_rizik.pdf

Katarína Kampová, doc. Ing. PhD.

Faculty of security engineering, University of Zilina, Univerzitná 8215/1, 010 26 Žilina

e-mail: katarina.kampova@uniza.sk

Matúš Madleňák, Ing.

Faculty of security engineering, University of Zilina, Univerzitná 8215/1, 010 26 Žilina

e-mail: matus.madlenak@uniza.sk

Timotej Mačuha, Ing.

Faculty of security engineering, University of Zilina, Univerzitná 8215/1, 010 26 Žilina

e-mail: timotej.macuha@uniza.sk

Samuel Hubočan, Ing.

Faculty of security engineering, University of Zilina, Univerzitná 8215/1, 010 26 Žilina

e-mail: samuel.hubocan@uniza.sk

Martin Hromada, prof. Ing. PhD.

Faculty of Applied Informatics, Tomas Bata University in Zlín, Nad Stráněmi 4511, 760 05 Zlín, Czech Republic

e-mail: hromada@utb.cz

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.135-138
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

ŠPECIFIKÁ ZÁCHRANNÝCH PRÁC PRI ZDOLÁVANÍ NEŽIADÚCEJ UDALOSTI V ŽELEZNIČNEJ DOPRAVE

SPECIFICS OF RESCUE OPERATIONS IN MANAGING UNDESIRABLE EVENTS IN RAILWAY TRANSPORT

JAROSLAV KAPUSNIAK

ABSTRACT: *The article deals with the specifics of rescue operations in response to an undesirable event caused by a railway accident. Coordination and cooperation between the basic components of the Integrated Rescue System (hereinafter "IRS") during such an event are essential for effectively resolving the situation and providing the necessary assistance. The rapid and effective actions taken by IRS components in the first minutes after the occurrence of an undesirable event—especially one involving mass casualties—can have a significant impact on the outcome of the intervention. Each basic and supporting component of the IRS has its own specific tasks; however, it is crucial that they are well coordinated and maintain effective communication at the intervention site. The conclusion of the article focuses on the evaluation of current practices and offers proposals for improving cooperation and coordination among the components of the Integrated Rescue System when dealing with undesirable events.*

KEYWORDS: *Rescue operation, intervention, integrated rescue system, undesirable event, traffic accident.*

ÚVOD

Komunikácia medzi zložkami IZS počas nežiadúcej udalosti spôsobenej dopravnou nehodou je zásadne dôležitá pre efektívne riešenie situácie a poskytnutie potrebnej pomoci. Integrovaný záchranný systém (ďalej len „IZS“) zjednocuje a koordinuje činnosti rôznych zložiek záchranných služieb s cieľom poskytnúť efektívnu pomoc v prípade mimoriadnych udalostí, havárií, prírodných katastrof a iných situácií ohrozujúcich životy, zdravie, majetok alebo životné prostredie (Zákon 129, 2002). Záchranné práce sú činnosti na odvrátenie bezprostredného pôsobenia účinkov požiaru alebo inej nežiadúcej udalosti (Zákon 314, 2001).

1. ZLOŽKY INTEGROVANÉHO ZÁCHRANNÉHO SYSTÉMU

Do IZS v SR zaraďujeme základné záchranné zložky, medzi ktoré patria: Hasičský a záchranný zbor, záchranná zdravotná služba, kontrolné chemické laboratória civilnej ochrany, Horská záchranná služba, Banská záchranná služba a od 1. apríla 2023 aj Policajný zbor. Taktiež v IZS pôsobia aj ostatné záchranné zložky ako sú ozbrojené sily SR, dobrovoľné hasičské zbory obcí, závodné hasičské útvary, iné právnické osoby a fyzické osoby – podnikatelia, ktorým bola udelená akreditácia na úseku IZS (Zákon 129, 2002). Od 1.3.2025 bola legislatívne rozšírená pôsobnosť dobrovoľného hasičského zboru o banský špeciál, pričom výjazd tohto špeciálu od vyžiadania pomoci koordinačným strediskom alebo operačným strediskom je do 10 minút (Vyhláška 37, 2025).

2. ŠTATISTIKA UDALOSTÍ NA ŽELEZNICI V ŽILINSKOM KRAJI

Udalosti, ale najmä dopravné nehody na železniciach, nepatria medzi najčastejšie, ale v porovnaní s počtom dopravných nehôd v cestnej doprave, sú ich následky oveľa závažnejšie. Hlavne v počte ťažko zranených a usmrtených osôb. Preto je dôležité, aby sa pri zásahovej činnosti v prípade železničných nehôd uskutočnila spolupráca medzi zložkami IZS, operačným strediskom a ďalšími zainteresovanými osobami, ako napríklad: železničná spoločnosť, správca ciest, vrtuľníková záchranná zdravotná služba. V tabuľke 1 môžeme vidieť, príčiny pri ktorých zasahovali aj jednotky HaZZ za obdobie 2018 – 2024. Štatistické údaje sme získali od Železníc Slovenskej republiky (Miklovič, 2025).

Tabuľka 1 Nežiadúce udalosti na železnici za roky 2018 – 2024

Rok	Príčiny						
	Zrážka vlaku		Neoprávnený pohyb v koľajisku	Samovraždy	Zrážka vlaku s predmetmi (drevo, kamene a pod.)	Závady pri jazde a manipulácii posunu medzi dopravami	Ostatné príčiny
	s cestnými vozidlami	s chodcom (cyklistom)					
2018	12	1	3	18	3	0	1
2019	6	0	5	12	0	0	0
2020	9	1	6	12	1	0	1
2021	5	1	3	13	1	0	1
2022	13	1	3	18	3	1	4
2023	10	1	4	14	0	0	3
2024	9	0	5	16	1	0	2
Spolu	64	5	29	103	9	1	12

Na základe tabuľky je možno konštatovať, že na najčastejšia príčina nežiadúcich udalostí na železnici sú samovraždy. Ďalšou pomerne vyskytujúcou príčinou je zrážka vlaku s cestnými vozidlami a treťou najčastejšou príčinou sú neoprávnené pohyby mimo priecestia, tým sa chápe, každá osoba, ktorá sa nachádza v železničných priestoroch, kde je jej prítomnosť zakázaná.

3. ŠPECIFIKÁ SPOLUPRÁCE ZÁKLADNÝCH ZLOŽIEK IZS PRI ZDOLÁVANÍ NEŽIADÚCEJ UDALOSTI V DOPRAVE

Rýchla a efektívna činnosť zložiek IZS v prvých minútach po vzniku udalosti s hromadným postihnutím osôb môže mať zásadný vplyv na počet preživších a kvalitu ich ďalšieho života. Každá zo základných zložiek IZS má svoje špecifické úlohy, ale je dôležité, aby boli dobre koordinované a komunikovali medzi sebou na mieste zásahu. Policajný zbor má najmä za úlohu zabezpečiť bezpečnosť na mieste zásahu a pomôcť s organizáciou dopravy. HaZZ zasa zabezpečuje záchranu osôb a majetku z nebezpečných situácií a poskytuje prvú pomoc. Zdravotníci poskytujú odbornú lekársku starostlivosť a zabezpečujú prevoz pacientov do nemocníc.

Zdravotníci, ktorí sú prítomní na mieste udalosti, spolupracujú s príslušníkmi HaZZ a zabezpečujú základné ošetrenie ranených ešte pred transportom do zdravotníckeho zariadenia. Pri udalosti s hromadným postihnutím osôb sa veliteľ zásahu dohodne s veliteľom zdravotníckeho zásahu (ďalej len „VZS“) na spôsobe vzájomnej spolupráce, prioritných úlohách, organizácii miesta zásahu a na vedúcich zodpovedných za jednotlivé organizačné úseky zriadené VZS (Pokyn PHaZZ 20, 2007). Zdravotníci poskytujú informácie o stave a zraneniach pacientov príslušníkom HaZZ, pomáhajú pri určovaní priorít prenosu pacientov. Príslušníci HaZZ minimalizujú riziko vzniku požiaru, pri zhoršenej viditeľnosti zabezpečujú osvetlenie na mieste zásahu, pomáhajú pri transporte pacientov do odsunových prostriedkov a zabezpečujú ich prepravu na miesto ďalšieho ošetrenia.

Príslušníci PZ zabezpečujú priestor pre prácu záchranných zložiek na mieste zásahu, najmä pred prítomnosťou cudzích osôb, ktoré by mohli ohroziť ich bezpečnosť. Vykonávajú bezpečnostné opatrenia, ktoré sú nevyhnutné pre prevenciu hrozby ďalšieho nebezpečenstva na mieste zásahu. V spolupráci s HaZZ pomáhajú pri evakuácii obyvateľov z blízkych oblastí v prípade potreby. Zabezpečujú odsunové trasy, podľa cieľových zdravotníckych zariadení. V prípade, že sa plánuje použitie vrtuľníka na odsun zranených osôb, príslušníci PZ v spolupráci s HaZZ určia a vyznačia vhodnú

pristávaciu plochu. Taktiež zabezpečujú všetky relevantné informácie a dôkazy, ktoré by mohli pomôcť pri vyšetrovaní príčin.

4. KOORDINÁCIA ZLOŽIEK IZS PRI UDALOSTI NÁSLEDKOM ZRÁŽKY DVOCH VLAKOV

Analýza spolupráce zložiek IZS sa týka konkrétnej dopravnej nehody dvoch vlakov, a to osobného vlaku a rušňa na železničnej trati medzi Žilinou a Vrútkami, ktorá sa stala 3.6.2022 (piatok), krátko pred 19 hodinou. V čase nehody sa v osobnom vlaku nachádzalo 72 osôb a jedno dieťa. V druhej (náhradnej) lokomotíve sa nachádzal rušňovodič. Následkom nárazu došlo k zraneniu 32 osôb, ktoré boli prevezené do zdravotníckych zariadení. Ostatné osoby v počte 42 bolo vytriedených a prevezených na najbližšiu železničnú stanicu Vrútky. Kriticky boli zranené 4 osoby, ktoré boli transoprtované ako prvé, stredne ťažké poranenia malo 11 osôb a ostatní mali ľahké poranenia. Zásah vykonávalo 50 hasičov z 8-ich hasičských staníc (vrátane 18 členov DHZO), 11 ambulancií z okresov Martin a Žilina vrátane Vrtuľníkovej záchrannej služby a zložky PZ SR. Zásah záchranných zložiek na mieste udalosti trval takmer 7 hodín. Príčina nehody - v dôsledku nedorozumenia ohľadom súradníc pokazeného vlaku išiel rušeň za daným vlakom prirýchlo a keďže pokazený vlak bol odstavený tesne za neprehľadnou zákrutou, zrážke už rušňovodič nedokázal zabrániť a došlo k ich stretu (Šenšelová M., 2023). Veľmi dobrá bola spolupráca medzi jednotlivými zložkami IZS. Každá zo zložiek IZS sa snažila vykonať maximum pre pacientov a pomáhali si navzájom. Na danom mieste sa nachádzalo dostatok posádok, takže ošetrovanie a transport ranených bol veľmi rýchly a efektívny. Takisto nemocnice boli veľmi dobre pripravené, stiahli do služby lekárov, ktorí boli v čase osobného voľna a podarilo sa im otvoriť množstvo príjmových ambulancií, takže pacienti nemuseli čakať hodiny na ošetrenie.

Obrázok 1 Zrážka dvoch vlakov vo Vrútkach (Šenšelová M., 2023)

Problémy a nedostatky súvisiace so zásahovou činnosťou zložiek IZS a železničnej spoločnosti pri uvedenej mimoriadnej udalosti:

- zlé upresnenie polohy miesta mimoriadnej udalosti (prvé posádky ZZS a HaZZ išli na opačný smer),
- sťažená rádiová komunikácia medzi zložkami IZS (ZZS a HaZZ) na mieste mimoriadnej udalosti,
- okamžité neuzavretie železničnej trati počas príchodu prvých posádok ZZS v okolí miesta mimoriadnej udalosti prešiel po vedľajšej koľaji vlak;

Nedostatok v čase mimoriadnej udalosti, ktorý sa týkal železníc je, že na danom úseku nie je zriadené traťové rádiové spojenie medzi rušňovodičom, výpravcom a medzi jednotlivými vlakmi.

5. NÁVRHY OPATRENÍ NA ZLEPŠENIE SPOLUPRÁCE ZLOŽIEK IZS PRI MIMIORIADNEJ UDALOSTI V DOPRAVE

Kapitola je zameraná na vyhodnotenie a nvrhy opatrení na zlepšenie spolupráce a koordinácie činnosti pri zásahu medzi zložkami IZS. Technológie a systémy, ktoré sú súčasťou IZS, majú za cieľ zabezpečiť rýchlu odozvu záchranných zložiek a maximalizovať ich efektivitu.

Na základe zhrnutia poznatkov získaných z analýzy vybranej udalosti na železnici, navrhujeme riešenia týchto všeobecných oblastí v rámci IZS v SR:

- kompatibilita komunikačnej a informačnej infraštruktúry medzi zložkami IZS, s dôrazom na prenos získaných informácií dátovou vetou, čo spôsobuje časové oneskorenie pri poskytovaní potrebnej pomoci,
- je potrebné pravidlne aktualizovať geografický systém podpory operátora IZS, keďže v čase nehody bol neaktuálny (v systéme bola označená diaľnica D1 Turany – Martin ešte vo výstavbe),
- obmedzená lokalizácia volajúceho z mobilnej siete, spôsobené fyzickými překážkami, ktoré môžu oslabovať signál mobilnej siete (vzdialenosť od mobilních veží, terén a podobne), preto je potrebné sa zamerať na investície do modernizácie a rozšírenia infraštruktúry,
- takisto je potrebná aktualizácia aplikácii GINALITE tablet (komunikačný a informačný systém vo vozidlách HaZZ),
- tak, jako ukázala táto událost je potrebné zaviesť u operatorov LTV 112 kontrolné zoznamy, nakoľko operační důstojníci sú v čase udalosti vyťažení, systematické a komplexné získavanie informácií od volajúceho by minimalizovalo riziko vynechania dôležitých otázok a informácií;

Jedno z opatrení, ktoré prijala železničná spoločnosť po nehode bolo preskúšanie všetkých dispečerov a vlakvedúcich z interných predpisov, sprísnenie výberových konaní a najmä lepšie pokrytie železničných tratí, zo začiatku aspoň na najfrekventovanejších úsekoch, aby vlakvedúci medzi sebou komunikovali.

ZÁVER

Vlakových nešťastí je vo svete a na Slovensku v porovnaní s iným typom nehôd relatívne málo. Avšak nie raz končia s veľmi tragickým koncom. Našťastie si táto udalosť nevyžiadala obete na životoch iba zranenia rôzneho rozsahu. V konečnom dôsledku všetky zainteresované záchranné zložky odviedli veľmi dobrú prácu, súčinnosť medzi jednotlivými zložkami bola tiež výborná. Preto je veľmi dôležité sa aspoň raz do roka zúčastňovať rôznych typov cvičení, napríklad s témou udalosti s hromadným postihnutím osob. Taktiež je veľmi dôležitá efektívnosť informačných systémov v záchranných zložkách IZS. Operátori linky tiesňového volania zohrávajú v tomot procese kľúčovú úlohu, pretože sú prvou líniou informačného systému a sú zodpovední za prijímanie a spracovanie dôležitých informácií. Rýchlosť a najmä presnosť výmeny informácií sú nevyhnutné pre správne vyhodnotenie a nasadenie zložiek IZS.

POĎAKOVANIE

Príspevok vznikol za podpory projektu KEGA 035ŽU-4/2025 Inovatívne modulárne vzdelávacie kurzy ako efektívny nástroj na zvýšenie bezpečnosti na školách.

LITERATÚRA

MIKLOVIČ J., 2025. Nehodovosť železničnej dopravy za rok 2023 a za rok 2024. [Elektronická pošta]. Správa pre: Jaroslav KAPUSNIAK. 2025-07-30 [cit. 19-08-2025]. Osobná komunikácia.

Pokyn prezidenta Hasičského a záchranného zboru o vydaní Takticko-metodických postupov vykonávania zásahov č.20/2007

Vyhláška MV SR č. 37/2025, ktorou sa mení a dopĺňa vyhláška č. 611/2006 Z. z. o hasičských jednotkách.

ŠENŠELOVÁ M.2023. Činnosť koordinačného strediska a zložiek IZS pri riešení mimoriadnej udalosti spôsobenej dopravnou nehodou na železnici: diplomová práca. Žilina: ŽU, 2023. 57s.

Zákon NR SR č. 129/2002 Z. z. o integrovanom záchrannom systéme

Zákon NR SR č. 314/2001 Z. z. o ochrane pred požiarmi

Jaroslav Kapusniak, Ing. Ph.D.

Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, Ul. 1. mája 32, 010 01 Žilina,

e-mail: jaroslav.kapusniak@uniza.sk

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.139-146
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

DODÁVATEĽSKÝ REŤAZEC A KYBERNETICKÁ BEZPEČNOSŤ

SUPPLY CHAIN AND CYBERSECURITY

ĽUBOMÍRA SOKOLOVÁ, MATÚŠ MADLEŇÁK, TIMOTEJ MAČUHA

ABSTRACT: The NIS2 Directive is an updated version of the original 2016 NIS Directive and aims to strengthen the protection and security of the EU's cyberspace. Unlike the first directive, NIS2 focuses on the cybersecurity and resilience of key entities and entire sectors in the face of modern threats. EU Member States are required to transpose it into their national legal systems. In Slovakia, the requirements of NIS2 were implemented through an amendment to the Act on Cybersecurity. The amendment, prepared by the National Security Authority, entered into force on January 1, 2025. It modifies and supplements the original Act No. 69/2018 Coll. and introduces several fundamental changes. One of the key elements is the enhancement of supply chain security. This protection is ensured primarily through contractual mechanisms based on the Act and on Decree No. 227/2025 of the National Security Authority. Contractual obligations must also reflect the requirements of the GDPR.
The article focuses mainly on contractual protection within supply chains and its alignment with GDPR requirements.

KEYWORDS: *supply chain, cybersecurity, data protection, measures.*

ÚVOD

Smernica NIS2 predstavuje revidovanú a aktualizovanú verziu pôvodnej smernice NIS z roku 2016, pričom jej primárnym cieľom je posilnenie ochrany a zabezpečenia kybernetického priestoru Európskej únie. Na rozdiel od predchádzajúcej úpravy, ktorá sa sústreďovala primárne na zabezpečenie základných služieb, NIS2 rozširuje rozsah pôsobnosti smernice na širšie spektrum kľúčových subjektov a sektorov, pričom reflektuje dynamicky sa vyvíjajúce a komplexnejšie kybernetické hrozby. Členské štáty EÚ majú legislatívnu povinnosť transponovať ustanovenia smernice do svojich vnútroštátnych právnych poriadkov. V slovenskom právnom systéme bola smernica NIS2 implementovaná prostredníctvom novely zákona o kybernetickej bezpečnosti, ktorú vypracoval Národný bezpečnostný úrad. Novela bola schválená Národnou radou Slovenskej republiky a nadobudla účinnosť 1. januára 2025. Predmetná novela modifikuje a dopĺňa Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a prináša viacero koncepčných zmien. Jednou z významných inovácií je posilnenie ochrany bezpečnosti v rámci dodávateľských reťazcov, ktoré sú považované za kritický prvok v komplexnom systéme kybernetickej odolnosti.

1. DODÁVATEĹSKÝ REŤAZEC

Dodávateľský reťazec predstavuje proces, ktorý zahŕňa určité kroky a aktivity potrebné na vytvorenie a dodanie tovaru resp. určitých služieb konečnému odberateľovi.

V súčasnosti sa v komerčnom sektore čoraz častejšie uplatňuje model, v ktorom podniky delegujú činnosti, ktoré nepovažujú za súčasť svojho hlavného predmetu podnikania (tzv. core business) na externé subjekty. Tento prístup je všeobecne známy ako outsourcing. Organizácie týmto spôsobom separujú podporné a vedľajšie procesy, čím získavajú možnosť koncentrovať svoje kapacity a expertízu na strategicky kľúčové oblasti (Kampová, 2024).

Zatiaľ čo z pohľadu ekonomickej efektívnosti a optimalizácie procesov patrí hodnotenie takéhoto procesu do pôsobnosti odborníkov na ekonomiku a procesný manažment, z hľadiska informačnej bezpečnosti je potrebné poukázať na kľúčový aspekt. Každé obstarávanie tovarov alebo služieb, ktoré zasahuje do správy informačných aktív organizácie, predstavuje špecifický typ rizika. Tento rizikový faktor musí byť systematicky identifikovaný, analyzovaný a primerane riadený v súlade s princípmi riadenia kybernetickej a informačnej bezpečnosti.

Rozhodovanie o outsourcingu by nemalo byť založené výlučne na ekonomických aspektoch, ale musí reflektovať aj hľadiská informačnej a kybernetickej bezpečnosti.

Organizácia by mala vykonať dôkladnú analýzu, na základe ktorej určí:
- ktoré činnosti ponechá vo vlastnej réžii (insourcing),
- ktoré aktivity je možné outsourcovať čiastočne – najmä v prípade menej kritických podporných procesov,
- a či je vôbec vhodné presunúť všetky hlavné aktivity mimo organizácie.

Pri tomto rozhodovaní je nevyhnutné zohľadniť dopad na informačné aktíva organizácie a úroveň ich ochrany, keďže každé presunutie činnosti na externý subjekt-dodávateľa, so sebou prináša potenciálne bezpečnostné riziká.
Outsourcing zahŕňa aj cloudové služby. V praktickom kontexte možno väčšinu cloudových modelov považovať za formu outsourcingu (Kampová, 2024).

Z tohto dôvodu je potrebné pristupovať k ich hodnoteniu a riadeniu s rovnakou mierou dôslednosti a prísnosti, ako pri iných typoch externých služieb, najmä z hľadiska bezpečnosti a ochrany informačných aktív. Veľké množstvo subjektov zapojených do dodávateľského reťazca a jeho priestorové usporiadanie si nevyhnutne vyžadujú, aby boli tieto integrované reťazce riadené.

Ak sa bezpečnostné riziká hodnotia až po výbere dodávateľa, môže to byť pre organizáciu veľmi nebezpečné. Zrušenie zmluvy býva často nákladné a komplikované. Podrobná analýza dokáže odhaliť slabé zabezpečenie, chýbajúce bezpečnostné opatrenia či väzby na rizikové subjekty ešte pred podpisom zmluvy. Včasná identifikácia problémov umožňuje vybrať bezpečnejšieho dodávateľa alebo prijať ochranné opatrenia. Neseriózni dodávatelia predstavujú osobitnú hrozbu – môžu mať za sebou porušenia zmlúv, úniky dát či zneužitie osobných údajov, čo vedie k právnym následkom aj strate dôvery klientov (Hotwagner, 2008).

2. POŽIADAVKY PRÁVNYCH PREDPISOV

Povinnosť zabezpečiť informačné aktíva prostredníctvom zmluvných mechanizmov v dodávateľských reťazcoch je zakotvená vo viacerých právnych a normatívnych rámcoch.

Medzi najvýznamnejšie patria.
- **Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti - NIS 2,**
- **Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti**, ako aj **zákon č. 95/2018 Z. z. o informačných technológiách verejnej správy**,
- **Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov(ďalej len „GDPR“) (čl. 28, čl. 32)** – ktoré upravuje povinnosti prevádzkovateľa pri zverení spracúvania osobných údajov sprostredkovateľovi(dodávateľovi),
- **Medzinárodné technické normy**, ako napríklad **STN ISO/IEC 27001 a 27002**, ktoré definujú osvedčené postupy pre riadenie informačnej bezpečnosti.
- **Sektorovo špecifické právne predpisy**, ktoré stanovujú dodatočné požiadavky v regulovaných odvetviach.

Tieto predpisy spolu vytvárajú záväzný rámec, v ktorom je zmluvná úprava vzťahov s dodávateľmi kľúčovým nástrojom na ochranu informačných aktív (Kampová, 2025).

Smernica NIS2 vytvorila nielen potrebu aktualizácie Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti. Po novele zákona bola vytvorená i Vyhláška NBÚ č. 227/2025 o bezpečnostných opatreniach, ktorá stanovuje obsah riadenia rizík v dodávateľskom reťazci.

Riadeniu rizík sa venuje **§ 5 vyhlášky NBÚ č.227/2025**. Jej obsahom je:
- **identifikácia aktív** – systematické určenie všetkých relevantných informačných a technologických prostriedkov, ktoré podliehajú ochrane,
- **identifikácia rizík** – vrátane popisu existujúcich a realizovaných bezpečnostných opatrení, ktoré majú za cieľ eliminovať alebo zmierniť zistené hrozby,

- **analýza rizík** – v prípade, že prevádzkovateľ základnej služby využíva vlastnú bezpečnostnú metodiku, je potrebné zabezpečiť mapovanie rizík v súlade so štruktúrou uvedenou v referenčnej metodike dostupnej na oficiálnej webovej stránke príslušného úradu,
- **hodnotenie rizík** – kvantitatívne alebo kvalitatívne vyhodnotenie úrovne jednotlivých rizík na základe pravdepodobnosti výskytu a možného dopadu,
- **implementácia bezpečnostných opatrení** – na základe výsledkov hodnotenia rizík, vrátane zdokumentovania, ktoré opatrenia boli prijaté a ktoré nie, spolu s príslušným odôvodnením.
- **Pravidelné prehodnocovanie rizík** – minimálne raz ročne, s cieľom zabezpečiť aktualizáciu identifikovaných rizík a revíziu prijatých bezpečnostných opatrení v závislosti od zistených zmien a nových poznatkov (Vyhláška č.227/2025).

Súčasťou procesu riadenia rizík je aj analýza funkčného dopadu (Business Impact Analysis – BIA), ktorá zahŕňa hodnotenie potenciálneho vplyvu krízových scenárov na činnosť prevádzkovateľa základnej služby. Tieto scenáre môžu zasiahnuť kritické zdroje a aktíva, ktoré podporujú kľúčové procesy, a tým spôsobiť ohrozenie alebo prerušenie kontinuity poskytovania služieb. Neoddeliteľnou súčasťou analýzy funkčného dopadu je aj stanovenie cieľových úrovní obnovy a identifikácia prevádzkových a bezpečnostných požiadaviek, ktoré sú potrebné na zabezpečenie odolnosti organizácie.

- **Bezpečnostné opatrenia sú navrhované, implementované a realizované spôsobom, ktorý zabezpečuje elimináciu alebo zmiernenie všetkých rizík identifikovaných v rámci analýzy rizík.** Tieto opatrenia musia zároveň reflektovať strategické ciele kybernetickej bezpečnosti, byť v súlade s internou bezpečnostnou politikou a napĺňať legislatívne a normatívne požiadavky na informačnú a kybernetickú bezpečnosť (Vyhláška č.227/2025).

Bezpečnosť dodávateľského reťazca je zadefinovaná v zmysle povinností prevádzkovateľa základnej služby i priamo v zákone o kybernetickej bezpečnosti. Prevádzkovateľ základnej služby je povinný, ak vykonáva činnosť prostredníctvom tretej strany, ktorá priamo súvisí s dostupnosťou, dôvernosťou alebo integritou prevádzky jeho sietí a informačných systémov, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení. Pri uzatvorení zmluvy sa vykonáva analýza rizík. Počas trvania zmluvného vzťahu je tretia strana povinná vykonávať a uplatňovať bezpečnostné opatrenia v súlade s uzatvorenou písomnou zmluvou. V zmysle § 19 Zákona o kybernetickej bezpečnosti je prevádzkovateľ základnej služby povinný realizovať systematickú analýzu vzájomných závislostí svojich aktív, informačných systémov, využívaných produktov informačno-komunikačných technológií a služieb poskytovaných tretími stranami v rámci dodávateľského reťazca. Cieľom tejto analýzy je identifikácia a vyhodnotenie potenciálnych dopadov kybernetických bezpečnostných incidentov na prevádzku a poskytovanie služieb.

Analýza rizík slúži na určenie pravdepodobnosti výskytu škodlivej udalosti, ktorá môže nastať v dôsledku zneužitia existujúcej zraniteľnosti aktíva potenciálnou hrozbou, a to v kontexte aktuálne implementovaných bezpečnostných opatrení**.** Súčasťou tejto analýzy je aj identifikácia možných následkov narušenia základných bezpečnostných princípov – dôvernosti, integrity a dostupnosti daného aktíva. Výsledkom analýzy je kvalitatívne alebo kvantitatívne vyhodnotenie rizika, ktoré slúži ako podklad pre návrh a implementáciu adekvátnych opatrení na jeho elimináciu alebo zmiernenie. Analýza rizík podľa Filipa zahŕňa identifikáciu hrozieb, posúdenie pravdepodobnosti ich uskutočnenia a vyhodnotenie ich potenciálnych následkov. Je to komplexný nástroj manažmentu rizík, ktorý pomáha odpovedať na otázky, aké bezpečnostné riziká sa môžu vyskytnúť, aká je ich pravdepodobnosť a aké budú následky bezpečnostného konfliktu (Filip, 2011). Národný bezpečnostný úrad SR vypracoval metodiku analýzy rizík, ktorá je k dispozícii na ich webovej stránke (NBÚ, 2025).

Na základe výsledkov vykonanej analýzy rizík je prevádzkovateľ základnej služby povinný najneskôr do 12 mesiacov odo dňa zápisu do registra prevádzkovateľov základnej služby prijať, implementovať a udržiavať všeobecné bezpečnostné opatrenia minimálne v rozsahu stanovenom v § 20. Tieto opatrenia musia byť vykonávané s cieľom zabezpečiť primeranú úroveň kybernetickej bezpečnosti, odolnosti a kontinuity poskytovaných služieb (Zákon o kybernetickej bezpečnosti, 2025).

Zákon o kybernetickej bezpečnosti jasne stanovuje i ďalšie povinnosti, ktoré je potrebné v dodávateľskom reťazci dodržiavať. Prevádzkovateľ základnej služby je povinný realizovať systematickú analýzu vzájomných závislostí medzi vlastnými aktívami, informačnými systémami, využívanými produktmi a službami informačno-komunikačných technológií (IKT) tretích strán v rámci dodávateľského reťazca a poskytovaných služieb. Cieľom je identifikácia a hodnotenie potenciálnych dopadov kybernetických bezpečnostných incidentov na kontinuitu a integritu prevádzkovaných procesov.
Na základe výsledkov analýzy je prevádzkovateľ povinný prijať, implementovať a priebežne udržiavať bezpečnostné opatrenia v súlade s aktuálnymi bezpečnostnými metodikami a politikami príslušného úradu, pričom zohľadňuje najnovšie bezpečnostné trendy, príklady dobrej praxe a relevantné medzinárodné normy.

Tretia strana, ktorá má významný vplyv na zabezpečovanie kybernetickej bezpečnosti a je v zmluvnom vzťahu s prevádzkovateľom základnej služby vykonávajúcim kritickú základnú službu, nadobúda postavenie prevádzkovateľa základnej služby. Prevádzkovateľ kritickej základnej služby je povinný bezodkladne oznámiť príslušnému úradu uzatvorenie aj ukončenie zmluvného vzťahu s takouto treťou stranou. Táto tretia strana sa následne zapisuje do registra prevádzkovateľov základných služieb.
Zároveň je povinná uplatňovať a dodržiavať bezpečnostné opatrenia v súlade s platnou legislatívou a podlieha dohľadu a kontrole zo strany Národného bezpečnostného úradu (Zákon o kybernetickej bezpečnosti, 2025).

Vyhláška NBÚ č. 227/2025 o bezpečnostných opatreniach v § 7 stanovuje obsah zmluvy v dodávateľskom reťazci nasledovne:

a) záväzok dodávateľa vykonávať činnosti, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby (ďalej len „tretia strana“), a zároveň dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby,
b) potvrdenie súhlasu tretej strany s uvedenými bezpečnostnými politikami,
c) ustanovenie určujúce rozsah, spôsob a možnosti výkonu kontrolných činností a auditu, ktoré môže prevádzkovateľ základnej služby uskutočniť u tretej strany,
d) ustanovenie o povinnosti tretej strany informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach, ktoré môžu mať vplyv na úroveň kybernetickej bezpečnosti, ako aj o povinnosti poskytnúť súčinnosť pri riešení takýchto incidentov.

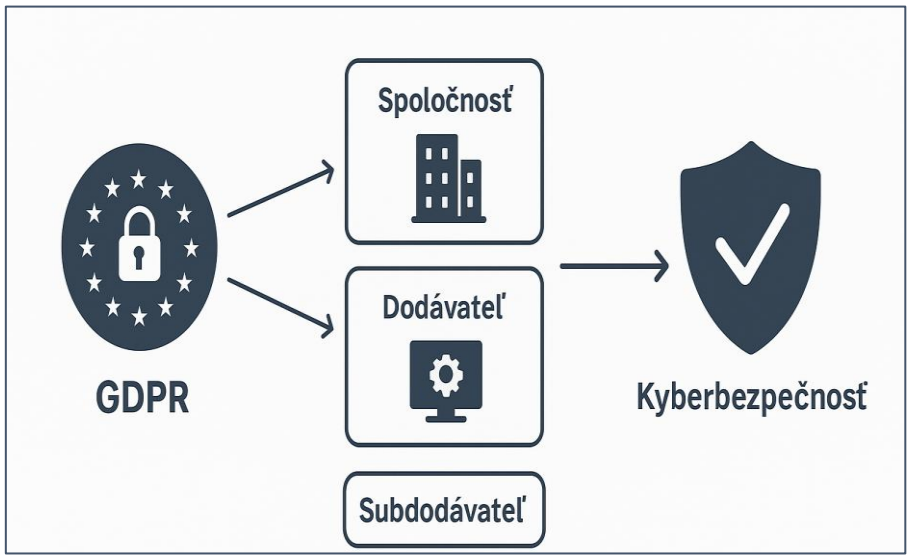
Rozsah bezpečnostných opatrení pre oblasť kybernetickej bezpečnosti podľa § 20 ods. 2 zákona sú upravené v **Prílohe č.1 k vyhláške č. 227/2025 Z. z.**

Tieto opatrenia sú stanovené pre:

- organizáciu a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti,
- správu zraniteľností a kybernetických hrozieb,
- správu aktív a riadenie kybernetických hrozieb a rizík,
- riadenie udalostí a kybernetických bezpečnostných incidentov,
- riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie,
- bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií,
- postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti,
- kryptografické opatrenia a zásady používania kryptografie,
- bezpečnosť a spôsobilosti ľudských zdrojov,
- správu identít a prístupov,
- bezpečnosť pri prevádzke sietí a informačných systémov,
- ochranu proti škodlivému kódu a nežiaducemu obsahu,
- systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť,
- monitorovanie, zaznamenávanie a hlásenie udalostí,
- fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení,
- ochranu záznamov, súkromia a označovanie informácií,
- dodávateľský reťazec.

3. GDPR A DODÁVATEĽSKÝ REŤAZEC V KYBERBEZPEČNOSTI

Do zmluvnej ochrany dodávateľského reťazca zasahujú nie len podmienky zákona o kybernetickej bezpečnosti a prislúchajúcej vyhlášky. Smernica NIS 2 upozorňuje i na požiadavky na bezpečnosť dodávateľského reťazca, ktoré kladie Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (GDPR).



Obrázok 1 GDPR a dodávateľský reťazec

GDPR dáva dôraz na zodpovednosť prevádzkovateľa aj sprostredkovateľa(dodávateľa) pri spracúvaní osobných údajov. To znamená, že ak si firma najme externého dodávateľa (napr. cloudové služby, IT podporu, hosting), nesie zodpovednosť za to, že tento dodávateľ dodržiava primerané bezpečnostné opatrenia na ochranu dát.

Prepojenia medzi dodávateľským reťazcom a GDPR:

- Zodpovednosť za dodávateľov – Organizácia musí preveriť, či jej partneri a dodávatelia dodržiavajú GDPR (tzv. due diligence).
- Zmluvné vzťahy – GDPR vyžaduje uzatvoriť so sprostredkovateľmi (dodávateľmi) *zmluvy o spracúvaní osobných údajov* (DPA), kde sa definujú bezpečnostné opatrenia (článok 28 GDPR).
- Kybernetická bezpečnosť – Článok 32 GDPR prikazuje zaviesť primerané technické a organizačné opatrenia. To sa vzťahuje aj na dodávateľský reťazec (napr. šifrovanie dát, bezpečný prenos, prístupové práva).
- Riziká dodávateľského reťazca – Ak dôjde k úniku údajov cez dodávateľa, zodpovednosť padá aj na firmu, ktorá ho využíva. V praxi sa často rieši cez bezpečnostné audity, certifikácie (ISO 27001) alebo hodnotenie dodávateľov.
- Incidenty a oznamovanie porušení – GDPR ukladá povinnosť nahlásiť únik dát do 72 hodín. Ak únik spôsobí dodávateľ, musí o tom okamžite informovať objednávateľa (GDPR, 2016).

Tabuľka 1 GDPR požiadavky a dodávateľský reťazec (Zdroj: GDPR, 2016)

GDPR požiadavka	Ako sa premieta do dodávateľského reťazca	Príklad z praxe
Zodpovednosť prevádzkovateľa (čl. 24, 28)	Firma je zodpovedná aj za svojich dodávateľov, ktorí spracúvajú dáta.	E-shop používa externý cloud – musí preveriť, či cloudový poskytovateľ dodržiava GDPR.
Zmluvy o spracúvaní údajov (DPA)	Povinnosť uzatvoriť so sprostredkovateľom zmluvu s jasne definovanými bezpečnostnými opatreniami.	Firma outsourcuje účtovníctvo – v zmluve sa špecifikuje, ako budú chránené osobné údaje klientov.
Primerané bezpečnostné opatrenia (čl. 32)	Dodávateľ musí zaviesť technické a organizačné opatrenia (šifrovanie, prístupové práva, monitoring).	Hostingová firma musí mať zabezpečené servery proti neoprávnenému prístupu.
Hodnotenie rizík	Prevádzkovateľ musí vyhodnotiť riziká dodávateľského reťazca.	Banka preveruje IT dodávateľov cez bezpečnostný audit pred podpisom zmluvy.
Oznamovanie incidentov (čl. 33)	Dodávateľ je povinný informovať prevádzkovateľa o úniku dát bez zbytočného odkladu.	Ak IT firma zistí únik hesiel, musí okamžite kontaktovať svojho klienta, aby ten stihol nahlásiť porušenie Úradu na ochranu osobných údajov.
Medzinárodné prenosy dát	Dodávatelia mimo EÚ musia dodržiavať špeciálne pravidlá (napr. štandardné zmluvné doložky).	Firma využíva call centrum v Indii – musí mať právne ošetrený prenos dát.

Článok 28 GDPR stanovuje podmienky zmluvy. Ak sa spracúvanie osobných údajov vykonáva v mene prevádzkovateľa, ten je povinný využívať výlučne sprostredkovateľov(ďalších dodávateľov) , ktorí poskytujú dostatočné záruky o prijatí primeraných technických a organizačných opatrení zabezpečujúcich, že spracúvanie bude v súlade s požiadavkami tohto nariadenia a zároveň bude chrániť práva dotknutých osôb. Sprostredkovateľ (dodávateľ) nesmie poveriť spracúvaním ďalšieho sprostredkovateľa(dodávateľa) bez predchádzajúceho osobitného alebo všeobecného písomného súhlasu prevádzkovateľa. V prípade všeobecného písomného súhlasu je sprostredkovateľ povinný informovať prevádzkovateľa o všetkých plánovaných zmenách týkajúcich sa pridania alebo nahradenia ďalších sprostredkovateľov, aby prevádzkovateľ mal možnosť uplatniť námietky voči týmto zmenám (GDPR, 2016).

Sprostredkovateľ(dodávateľ):

- dodržiava podmienky zapojenia ďalšieho sprostredkovateľa (dodávateľa),
- po zohľadnení povahy spracúvania v čo najväčšej miere pomáha prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti reagovať na žiadosti o výkon práv dotknutej osoby,
- po ukončení poskytovania služieb týkajúcich sa spracúvania na základe rozhodnutia prevádzkovateľa všetky osobné údaje vymaže alebo vráti prevádzkovateľovi a vymaže existujúce kópie, ak právo Únie alebo právo členského štátu nepožaduje uchovávanie týchto osobných údajov,
- dodržiava podmienky zapojenia ďalšieho sprostredkovateľa(dodávateľa),
- po zohľadnení povahy spracúvania v čo najväčšej miere pomáha prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti reagovať na žiadosti o výkon práv dotknutej osoby,
- po ukončení poskytovania služieb týkajúcich sa spracúvania na základe rozhodnutia prevádzkovateľa všetky osobné údaje vymaže alebo vráti prevádzkovateľovi a vymaže existujúce kópie, ak právo Únie alebo právo členského štátu nepožaduje uchovávanie týchto osobných údajov (GDPR, 2016).

Bezpečnosť spracúvania GDPR upravuje i prostredníctvom článku 32. Zaväzuje v ňom prevádzkovateľa a sprostredkovateľa (dodávateľa) prijať primerané technické a organizačné opatrenia:

- pseudonymizácia a šifrovanie;
- zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania a služieb,
- schopnosť včas obnoviť dostupnosť v prípade fyzického alebo technického incidentu,

- zabezpečiť pravidelné testovanie, posudzovanie a hodnotenie účinnosti technických a organizačných opatrení (GDPR, 2016).

ZÁVER

Zákon o kybernetickej bezpečnosti stanovuje opatrenia pre oblasť riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov, pričom je potrebné s dodávateľom uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby platnosti zmluvy. Obsah zmluvy je stanovený vyhláškou, pričom vzor bezpečnostnej dokumentácie a vzor zmluvy podľa § 19 ods. 2 zákona o kybernetickej bezpečnosti sa zverejnia na webovom sídle úradu. Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 (GDPR) významne ovplyvňuje riadenie dodávateľského reťazca. Organizácie nesú zodpovednosť za preverovanie svojich dodávateľov a musia mať s nimi uzatvorené zmluvy o spracúvaní osobných údajov. Celý reťazec musí dodržiavať primerané technické a organizačné bezpečnostné opatrenia podľa článku 32 GDPR, pričom konkrétne podmienky zmluvy, ktoré musia byť splnené, určuje článok 28 GDPR.
Predmetom tohto článku je sumarizácia zmluvných mechanizmov v rámci dodávateľských reťazcov v kybernetickej bezpečnosti, a to so zameraním na ich súlad s požiadavkami a zásadami stanovenými nielen zákonom o kybernetickej bezpečnosti ale i GDPR. Cieľom bolo identifikovať a zhodnotiť kľúčové prvky zmluvných vzťahov medzi prevádzkovateľmi a dodávateľmi, tzv. sprostredkovateľmi, ktoré zabezpečujú efektívne uplatňovanie zásad zákonnosti, minimalizácie údajov, transparentnosti a zodpovednosti v prostredí komplexných a viacúrovňových dodávateľských štruktúr.

POĎAKOVANIE

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

LITERATÚRA

Filip, S. Šimák, L., Kováč, M. 2011. Manažment rizika. ISBN 9788089393497.Učebnica.

Hotwagner, B.: Supply Chain Risk Management und dessen systemische Umsetzung im Unternehmen. In: Wirtschaft und Management, Band 8. Wien, Fachhochschule des BFI. 2008.ISSN 1812-9056

Kampová. K., 2024. In: Prednášky z predmetu Kontinuity manažment. 2024

Kampová. K., 2025. In: Prednášky z predmetu Kybernetická bezpečnosť. 2025

Metodika analýzy rizík. Riadenie kybernetických bezpečnostných rizík. 2025. [on line]. Dostupné na: https://www.nbu.gov.sk/metodika-analyzy-rizik/

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov.(GDPR) [on line]. Dostupné na:

https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32016R0679

Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti.(NIS 2) [on line]. Dostupné na:

https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=sk

Vyhláška č. 227/2025 Z.z. o bezpečnostných opatreniach podľa zákona o kybernetickej bezpečnosti. [on line].

Dostupné na: https://www.aspi.sk/products/lawText/1/104541/1/2/vyhlaska-c-227-2025-zz-o-bezpecnostnych-opatreniach/vyhlaska-c-227-2025-zz-o-bezpecnostnych-opatreniach

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. [on line]. Dostupné na:

https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/69/

Ľubomíra Sokolová, Ing., PhD.

Fakulta bezpečnostného inžinierstva, Žilinská univerzita v Žiline. 1. mája 32, Žilina, Slovensko
e-mail: lubomira.sokolova@uniza.sk

Matúš Madleňák, Ing.

Fakulta bezpečnostného inžinierstva, Žilinská univerzita v Žiline. 1. mája 32, Žilina, Slovensko
e-mail: matus.madlenak@uniza.sk

Timotej Mačuha, Ing.

Fakulta bezpečnostného inžinierstva, Žilinská univerzita v Žiline. 1. mája 32, Žilina, Slovensko
e-mail: timotej.macuha@uniza.sk

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.147-155
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online

ZÁCHRANA NA ZAMRZNUTÝCH VODNÝCH PLOCHÁCH: ŠTANDARDY, PRAX A MOŽNOSTI ZLEPŠENIA VÝCVIKU

RESCUE ON FROZEN WATERS: STANDARDS, PRACTICES AND OPPORTUNITIES FOR IMPROVING TRAINING

MAREK MIHALIČ, MAREK JAŠKO, PETER RUSNÁK

ABSTRACT: This article examines rescue operations on frozen freshwater surfaces, with particular emphasis on the procedures of the Fire and Rescue Corps in the Slovak Republic. It outlines the physical characteristics of ice formation, the factors influencing ice stability, and the risks associated with insufficient load-bearing capacity. Attention is given to personal protective equipment (PPE), rescue tools, and safety measures essential for both rescuers and casualties. The author describes specific intervention methods, including approach strategies, techniques for extricating a person from icy water, and the subsequent provision of first aid. The article also discusses the role of training, preparedness, and situational awareness in minimising operational risks. The aim of the paper is to provide a practical overview of rescue tactics and to highlight the importance of prevention, education, and the systematic development of rescue capabilities. The conclusions emphasise that effective rescue operations depend not only on technical equipment and procedures but also on the physical fitness, readiness, and coordination of the rescuers.

KEYWORDS: Ice Rescue. Frozen Water Surfaces. Fire And Rescue Corps. Safety Procedures. Personal Protective Equipment.

ÚVOD

Zásahy na zamrznutých vodných plochách patria medzi špecifické a mimoriadne rizikové činnosti príslušníkov Hasičského a záchranného zboru. V zimnom období dochádza každoročne k situáciám, keď sa osoby alebo zvieratá preboria cez ľad a ocitnú sa v ľadovej vode. Takéto udalosti si vyžadujú okamžitú a profesionálnu reakciu, pretože pobyt v studenej vode vedie veľmi rýchlo k podchladeniu a ohrozeniu života.

Problematika záchrany z ľadu je komplexná, zahŕňa poznanie fyzikálnych vlastností zamrznutej sladkej vody, posúdenie stability ľadovej plochy, ako aj správne použitie osobných ochranných pracovných prostriedkov a špeciálnych záchranných pomôcok. Úspešnosť zásahu závisí nielen od dostupného technického vybavenia, ale aj od pripravenosti, zručnosti a fyzickej kondície zasahujúcich jednotiek (Ashton, 2011; Gorman, 2019).

Cieľom článku je analyzovať špecifiká záchranných prác na zamrznutých vodných plochách, poukázať na základné faktory ovplyvňujúce bezpečnosť zásahu a predstaviť odporúčania pre efektívne a bezpečné vykonávanie týchto činností v podmienkach Slovenskej republiky. Príspevok vychádza aj z praktických skúseností jednotiek HaZZ a prináša odporúčania pre zlepšenie výcviku a vybavenia.

1. FYZIKÁLNE A BEZPEČNOSTNÉ ASPEKTY ZAMRZNUTÝCH VODNÝCH PLÔCH

Zamrznuté vodné plochy predstavujú pre zasahujúcich hasičov a záchranárov dynamické a nestabilné prostredie. Hrúbka a pevnosť ľadu sú ovplyvňované viacerými faktormi, medzi ktoré patria predovšetkým teplota vzduchu a vody, prúdenie pod hladinou, zrážky a dĺžka obdobia mrazu. Stabilita ľadovej plochy môže byť lokálne narušená aj v prípade, že na prvý pohľad pôsobí dostatočne pevne (Peterson, 2019).

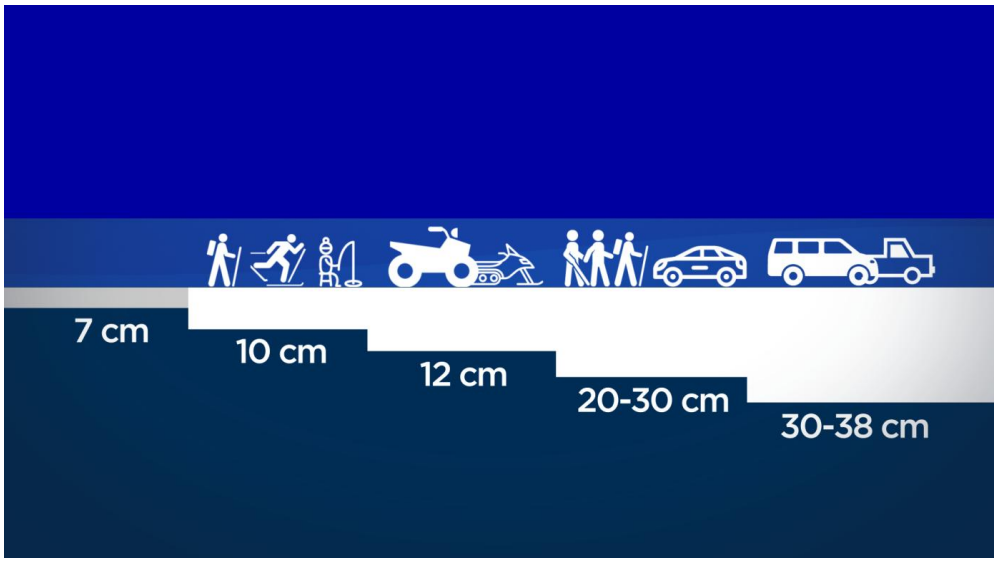
Za bezpečnú sa vo všeobecnosti považuje hrúbka ľadu minimálne 10 cm pre jednotlivca, 15 – 20 cm pre menšiu skupinu osôb a viac ako 25 cm pre motorové vozidlá (Tabuľka 1). V praxi je však hrúbka ľadu často nerovnomerná, čo spôsobuje, že tieto hodnoty nemožno aplikovať univerzálne. Obzvlášť nebezpečné sú miesta v blízkosti brehov, mostov, odtokov, prítokov a tam, kde je pod ľadom prúd alebo sa do jazera vlieva teplejšia voda (Chaplin, 2020).

Tabuľka 1 Odporúčaná hrúbka ľadu a jej únosnosť (vlastné spracovanie)

Hrúbka ľadu (cm)	Odporúčané zaťaženie
< 5	Veľmi nebezpečné, žiadna nosnosť
5 – 10	Jednotlivec v ohrození
10 – 15	Jednotlivec relatívne bezpečne
15 - 20	Menšia skupina osôb
25 +	Motorové vozidlá (osobné auto)
30 +	Ťažšie vozidlá (napr. dodávka)

Prepadnutie cez ľad nastáva najčastejšie pri jeho nedostatočnej únosnosti. Osoba vo vode čelí rýchlemu ochladzovaniu organizmu a hrozí u nej vznik hypotermie, ktorá v krátkom čase vedie k strate pohyblivosti a následnému utopeniu. Podľa lekárskych štúdií môže človek v studenej vode pri teplote 0–5 °C prežiť bez vážnej ujmy približne 15 až 30 minút, pričom rozhodujúcu úlohu zohráva oblečenie, fyzická kondícia a psychická odolnosť (Tipton & Golden 2011).

Tieto poznatky majú zásadný význam pre plánovanie a realizáciu zásahov Hasičského a záchranného zboru. Posúdenie rizík, správna voľba taktického postupu a využitie vhodných osobných ochranných pracovných prostriedkov sú kľúčové faktory na zníženie rizika ohrozenia života zasahujúcich aj zachraňovaných osôb.



Obrázok 1 Schéma únosnosti ľadu (vlastné spracovanie)

2. OSOBNÉ OCHRANNÉ PRACOVNÉ PROSTRIEDKY A ZÁCHRANNÉ POMÔCKY

Bezpečné vykonávanie zásahov na zamrznutých vodných plochách je neoddeliteľne spojené s používaním osobných ochranných pracovných prostriedkov (OOPP). Ich hlavnou úlohou je minimalizovať riziko podchladenia, úrazu a ohrozenia života zasahujúcich hasičov (Holmer & Kuklane. 2010; NFPA 1971, 2018; Holmer & Kuklane, 2010; NFPA, 2018).

Medzi základné OOPP pri zásahoch na ľade patria:

- ochranný zásahový odev a termálne vrstvy, ktoré zabezpečujú tepelný komfort,
- neoprénové alebo suché záchranárske obleky s integrovanou tepelnou izoláciou a vodeodolnosťou,
- ochranná prilba s integrovaným štítom, ktorá chráni pred úrazom pri pohybe po ľade alebo pri kontakte s výstrojom,
- plávacia záchranná vesta, ktorá udržuje záchranára nad hladinou aj v prípade vyčerpania,

- ochranné rukavice a obuv s protišmykovou úpravou, ktoré umožňujú bezpečný pohyb po klzkom povrchu (NFPA 1952, 2019).

Okrem osobnej výstroje sa pri zásahoch využívajú aj špeciálne záchranné pomôcky:

- záchranné hádzacie laná a kruhy,
- ľadové hroty a kliny, ktoré uľahčujú pohyb po ľade a umožňujú rýchly únik z otvoru,
- nafukovacie člny a plávajúce nosidlá na bezpečný transport zachraňovanej osoby,
- špeciálne sanie alebo plávajúce dosky, ktoré rozkladajú hmotnosť záchranára na väčšiu plochu (Novák, 2019).

Správne používanie uvedených prostriedkov zvyšuje bezpečnosť zásahu a zároveň umožňuje efektívnejšie vykonanie záchranných úkonov. Dôležitým predpokladom je pravidelný výcvik, ktorý pripravuje zasahujúcich hasičov na reálne podmienky a učí ich rýchlo a spoľahlivo ovládať výstroj a techniku.

3. TAKTICKÉ POSTUPY PRI ZÁCHRANE OSÔB Z ĽADOVEJ VODY

Taktika zásahov na zamrznutých vodných plochách sa riadi predovšetkým zásadou minimalizácie rizika pre záchranára a zrýchlenia zásahu. V praxi sa využívajú nasledovné postupy:

- prieskum a zabezpečenie miesta zásahu – určenie prístupovej cesty, posúdenie hrúbky ľadu, vytyčovanie bezpečnej zóny,
- priblíženie k zachraňovanému – odporúča sa plaziť alebo použiť plávajúce pomôcky, ktoré rozložia hmotnosť,
- kontakt so zachraňovanou osobou – upokojenie, inštrukcie na spoluprácu, podanie záchrannej pomôcky (lano, tyč, sanie),
- vytiahnutie z vody a transport – vždy v polohe ležmo, aby sa predišlo prelomeniu ľadu,
- prvá pomoc a odovzdanie ZZS – ošetrenie podchladenia, odstránenie mokrého odevu, tepelný komfort (IFSTA, 2017).

Po zvolení vhodného spôsobu záchrany osoby/osôb sú dôležité faktory ako hrúbka a celistvosť ľadu, vzdialenosť miesta preborenia od brehu, materiálne a technické vybavenie zložiek IZS a v neposlednom rade je, či sa na zamrznutej hladine nachádza vrstva snehu alebo v akom vizuálnom stave je ľadová plocha.

1. **Plazenie sa záchranára:** Jedná sa o základný spôsob pohybu po ľade, nakoľko je záchranca vybavený len zásahovým odevom hrozí pri ceste k preborenej osobe, že bude dochádzať z zvýšenému pocitu chladu záchranára. Pri vyťahovaní osoby späť na breh je veľmi pravdepodobné, že súčtom hmotnosti osôb bude dochádzať k prepadávaniu sa ľadu. Z tohto dôvodu je vhodné k rozloženiu hmotnosti použiť rôzne druhy materiálneho a technického vybavenia ako napríklad niektoré druhy nastavovacích rebríkov, nosidlá, dlahy a pod. V prípade využitia rebríkov, ak záchranu vykonávajú príslušníci HaZZ je preferovaný spôsob pohybu po ľade s využitím dvoch nastavovacích rebríkov, kedy príslušník rebríky posúva a prelieza medzi nimi. Jedná sa o veľmi fyzicky náročný spôsob pohybu, kde pri praktických meraniach sa rýchlosť pohybovala maximálne 20 metrov za minútu na hladkom povrchu a každé nezrovnalosti rýchlosť záchrany spomaľujú (Kováč, 2020; MV SR, 2017).

Obrázok 2 Schéma únosnosti ľadu (vlastné spracovanie)

Ako ďalší vyhovujúci spôsob pohybu po zamrznutej hladine s využitím rebríka je spôsob, kedy záchranca používa k posunu sekerku alebo bodce, kde pri tomto spôsobu sa rýchlosť pohybu pohybovala v rozmedzí 30 – 35 metrov za minútu. Obdobnú rýchlosť pohybu je možné podľa praktického výcviku dosiahnuť s nosidlami Spencer a nafukovacím člnom.

Obrázok 3 Pohyb po ľade s využitím sekerky a gumeného člna (vlastné spracovanie)

Obrázok 4 Využitie rebríka pri záchrane (vlastné spracovanie)

2. **Alternatívne využitie plávajúcich technických prostriedkov:** Čas, kedy je postihnutá osoba pri vedomí a schopná sa zachytiť o akýkoľvek predmet pomocou, ktorého môže byť vytiahnutá je veľmi individuálna a závisí na klimatických podmienkach, oblečení, veku, zdravotnému stavu, psychickému stavu a ďalších okolitých podmienok. Ak je osoba pri vedomí, je vhodné ju vytiahnuť pomocou akéhokoľvek plávajúceho predmetu priviazaného k lanu, aby záchranca nemusel zbytočne vstupovať na ľadovú plochu, čím by došlo k časovým stratám a taktiež k riziku preborenia. Ako alternatívne predmety možno využiť ťažné lano, bandasky na pohonné hmoty priviazané k ťažnému lanu a rôzne predmety vo technickom vybavení, ktoré majú zasahujúce zložky IZS na mieste zásahu (Canadian Red Cross, 2015).

Obrázok 5 Využitie alternatívnych predmetov k záchrane (vlastné spracovanie)

Obrázok 6 Využitie hadice C 52 k záchrane osoby (vlastné spracovanie)

3. **Záchrana osoby osobným zásahom záchranára:** Záchrana osoby osobným zásahom je metóda, ktorá sa využíva najčastejšie pri bezvedomí alebo v dôsledku účinku chladu na ľudský organizmus, kedy osoby nie sú schopné spolupráce a využívajú ju najčastejšie jednotky požiarnej ochrany, ktoré sú vybavené základnými technickými prostriedkami. Záchranca sa priblíži k otvoru, kde došlo k preboreniu osoby, sadne si na okraj, nohami chytí telo osoby a s použitím Rautekovho hmatu osobu zaistí. V prípade, že je okolo preborenej osoby veľký otvor, je potrebné sa k osobe doplaviť (Smith, 2016).

Obrázok 7 Záchrana osoby záchranárom (vlastné spracovanie)

4. **Záchrana špeciálnymi prostriedkami vo výbave HaZZ:** Vo výbave HaZZ na Slovensku a HZS v Českej republike sa na záchranu osôb využívajú špeciálne technické prostriedky:
    - nafukovacia záchranná lávka – určená na záchranu osôb na nestabilných plochách, ako napríklad ľadová triešť, bažinaté povrchy, ľadové povrchy na tečúcich tokoch a pod.,
    - nafukovacie záchranné nosidlá – určená na akékoľvek podmienky na vode, snehu a ľadu,
    - ľadové sane – plávajúci záchranná prostriedok, ktorý bol navrhnutý na základe skúseností jednotiek požiarnej ochrany v Škandinávií,
    - plastové plavidlo Relax Záchranár – plavidlo s vysokou stabilitou a odolnosťou voči prerazeniu. Jeho konštrukcia umožňuje kĺzanie po ľade pomocou vodiacich líšt,
    - Ponton Rescue Alive – používaný záchrannými zložkami v USA a Kanade,
    - plavák Marsars Ice Rescue – plastový plavák, na ktorom sú umiestnené úchyty,
    - záchranný raft RDC – záchranný raft, určený na celoročné používanie pri záchranných prácach na vode (Betuš, 2022).

Obrázok 8 Záchrana špeciálnymi prostriedkami vo výbave HaZZ (vlastné spracovanie)

Na základe analýzy zásahov HaZZ možno konštatovať, že najefektívnejšie postupy kombinujú využitie plávajúcich saní alebo nafukovacích člnov s adekvátnym OOPP. Pravidelné cvičenia ukázali, že zásahový čas možno skrátiť až o 30–40 % v porovnaní s improvizovanými technikami. Taktická pripravenosť preto výrazne ovplyvňuje úspešnosť a bezpečnosť zásahu.

4. VÝCVIK A PRIPRAVENOSŤ PRÍSLUŠNÍKOV HAZZ

Výcvik v oblasti záchrany z ľadu sa realizuje v rámci plánovaných cvičení a odbornej prípravy. Jeho cieľom je:

- osvojenie si správnych techník pohybu po ľade,
- bezpečné používanie OOPP a špeciálnych pomôcok,
- nácvik komunikácie a koordinácie v tíme,
- poskytovanie prvej pomoci pri podchladení (IFSTA, 2017).

Empirické poznatky potvrdzujú, že príslušníci, ktorí absolvovali pravidelný zimný výcvik, sú schopní vykonať zásah rýchlejšie, s menším rizikom vlastného ohrozenia a s vyššou mierou úspešnosti pri

záchrane osoby. Zavedenie povinného cyklického výcviku prispieva k štandardizácii zásahových postupov v podmienkach SR (Holmer & Kuklane, 2010).

Záchrana osôb z ľadovej vody predstavuje vždy vysoké riziko nielen pre zachraňovaných, ale aj pre zasahujúcich. Preto je nevyhnutné venovať pozornosť aj preventívnym opatreniam a osvete obyvateľstva.

Kľúčové preventívne opatrenia zahŕňajú:

- informovanie verejnosti prostredníctvom médií a školských programov o rizikách pohybu na zamrznutých vodných plochách,
- umiestňovanie výstražných tabúľ pri jazerách a vodných nádržiach počas zimného obdobia,
- zvýšený dohľad samospráv na frekventovaných miestach, kde hrozí vstup osôb na tenký ľad,
- spoluprácu so školami a mládežníckymi organizáciami, ktoré môžu významne prispieť k šíreniu osvetových aktivít.

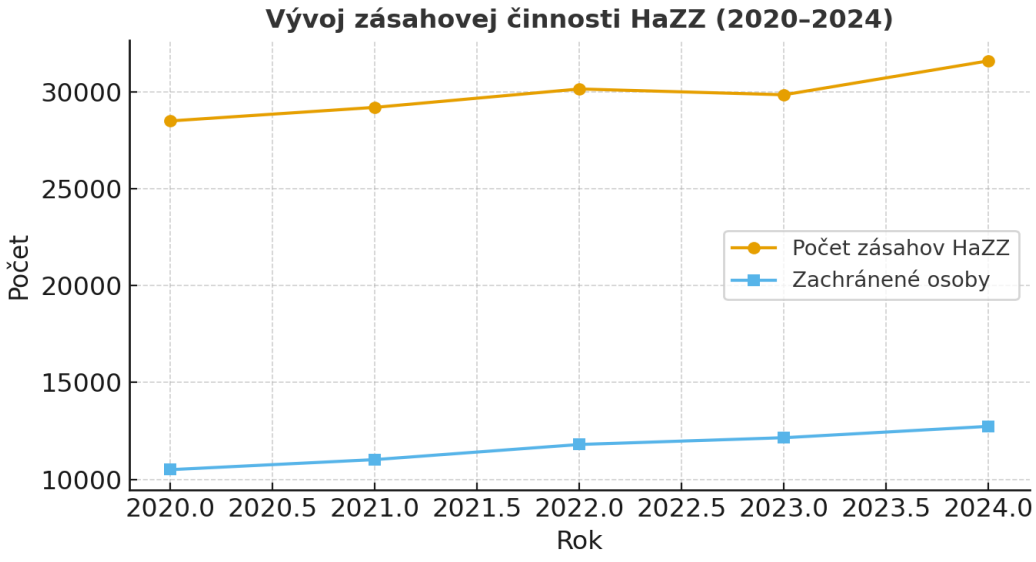
Prevencia dokáže výrazne znížiť počet zásahov HaZZ na zamrznutých plochách. Skúsenosti ukazujú, že v lokalitách, kde boli realizované cielené kampane (napr. letáky, informačné tabule, školenia), klesol počet incidentov až o 20 – 30 %. Z pohľadu HaZZ to znamená nielen zníženie operačnej záťaže, ale aj nižšie riziko pre samotných hasičov (Canadian Red Cross, 2015).

5. ŠTATISTICKÝ KONTEXT ZÁSAHOV HAZZ

Podľa správy o zásahovej činnosti Hasičského a záchranného zboru za rok 2024 zasahovali príslušníci HaZZ pri 31 602 udalostiach (nárast o 5,9 % oproti roku 2023). Z toho významný podiel predstavovala technická pomoc, ktorá zahŕňa aj zásahy na vodných plochách. V roku 2024 bolo počas zásahov zachránených 12 735 osôb, z toho 6 376 osôb utrpelo zranenia a 957 osôb zahynulo.

Špecifické údaje o zásahoch na zamrznutých vodných plochách nie sú samostatne vykazované, no HaZZ pravidelne rieši situácie spojené s preborením osôb alebo zvierat cez ľad. V priemere ide každú zimu o desiatky prípadov, pri ktorých hrá významnú úlohu rýchlosť zásahu a pripravenosť zasahujúcich jednotiek.

Tieto čísla potvrdzujú, že problematika záchrany z ľadovej vody má v praxi trvalý význam a opodstatnenie. Zároveň ukazujú potrebu systematickej prevencie a ďalšieho zlepšovania technického aj odborného zázemia HaZZ.



Obrázok 9 Vývoj zásahovej činnosti (2020-2024) (vlastné spracovanie)

ZÁVER

Zásahy na zamrznutých vodných plochách patria medzi najrizikovejšie činnosti Hasičského a záchranného zboru. Úspešnosť záchranných operácií závisí od kombinácie viacerých faktorov:

- znalosti fyzikálnych vlastností ľadu,
- správneho používania osobných ochranných pracovných prostriedkov,
- efektívnych taktických postupov a vysokej úrovne odbornej pripravenosti príslušníkov.

Analýza ukázala, že:

- bezpečnosť zásahu je úzko spätá s využitím špeciálneho vybavenia a s dôsledným dodržiavaním stanovených postupov,
- pravidelný výcvik významne skracuje zásahový čas a zvyšuje šance na záchranu postihnutých,
- preventívne opatrenia a edukácia obyvateľstva majú priamy dopad na zníženie počtu incidentov,
- najlepšie výsledky sa dosahujú kombináciou technickej pripravenosti a osvety verejnosti.

Prínosom článku je poskytnutie uceleného pohľadu na problematiku záchrany z ľadovej vody v podmienkach Slovenskej republiky, s dôrazom na praktické skúsenosti HaZZ. Výsledky potvrdzujú potrebu systematického prístupu – od technického zabezpečenia a výcviku až po preventívne aktivity v komunite.

Záverom možno konštatovať, že efektívna záchrana na zamrznutých vodných plochách je možná len pri súčinnosti techniky, taktiky a prevencie. Z dlhodobého hľadiska je preto kľúčové investovať do modernizácie výstroja, pravidelného vzdelávania hasičov a posilňovania preventívnych aktivít smerom k verejnosti.

LITERATÚRA

Ashton, G. D. (2011). Ice formation and properties. London: Springer. https://doi.org/10.1007/978-1-84882-333-0.

Ashton, G. D. (2011). River and lake ice engineering. Highlands Ranch: Water Resources Publications. ISBN 978-0918334596.

Betuš, M. (2022). Záchrana osôb pri preborení ľadovej pokrývky na vodných plochách. Civilná ochrana: revue pre civilnú ochranu obyvateľstva, 24(6), 14–18. ISSN 1335-4094.

Canadian Red Cross. (2015). Ice safety guidelines for public and emergency responders. Ottawa: Canadian Red Cross.

Chaplin, M. (2020). Water structure and anomalies. London: University College London.

Gorham, E. (2019). Ice formation and stability in freshwater bodies. Journal of Cold Regions Science, 45(2), 115–129. ISSN 0165-232X.

Gorham, P. (2019). Safety on ice: Physical properties and practical guidelines. New York: Wiley.

Holmer, I., & Kuklane, K. (2010). Protective clothing and thermal stress. Cambridge: Woodhead Publishing. ISBN 978-1-84569-730-9.

IFSTA. (2017). Essentials of fire fighting and fire department operations (7th ed.). Stillwater: Fire Protection Publications. ISBN 978-0879396443.

Kováč, L. (2020). Bezpečnosť pohybu a záchrana osôb na ľade. Bratislava: HaZZ.

Ministerstvo vnútra SR. (2017). Interná metodika Hasičského a záchranného zboru k zásahom na zamrznutých vodných plochách. Bratislava: MV SR.

NFPA. (2018). NFPA 1971: Standard on protective ensembles for structural fire fighting and proximity fire fighting. Quincy, MA: National Fire Protection Association. ISBN 978-1455920532.

NFPA. (2019). NFPA 1952: Standard on surface water operations protective clothing and equipment. Quincy, MA: National Fire Protection Association. ISBN 978-1455921591.

Novák, P. (2019). Zásahové prostriedky hasičov: Ochranné obleky a výstroj. Praha: Grada. ISBN 978-80-271-0296-1.

Peterson, R. (2018). Ice safety: Thickness guidelines and risk factors. Hanover: Cold Regions Research and Engineering Laboratory.

Smith, J. (2016). Rescue operations on frozen water bodies. New York: Fire Safety Press.

Tipton, M. J., & Golden, F. St. C. (2011). A proposed decision-making guide for the search, rescue and resuscitation of submersion (head under) victims based on expert opinion. Resuscitation, 82(7), 819–824. https://doi.org/10.1016/j.resuscitation.2011.02.021.

Marek Mihalič, práp., Ing.
Okresné riaditeľstvo Hasičského a záchranného zboru v Košiciach, Požiarická č. 4, 040 01 Košice
e-mail:marek.mihalic@student.tuke.sk

Marek Jaško, kpt., Ing.
Okresné riaditeľstvo Hasičského a záchranného zboru v Košiciach, Požiarická č. 4, 040 01 Košice
e-mail:marek.jasko@student.tuke.sk

Peter Rusnák, kpt., Ing.
Okresné riaditeľstvo Hasičského a záchranného zboru v Košiciach, Požiarická č. 4, 040 01 Košice
e-mail:peter.rusnak@student.tuke.sk

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.156-165
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

BEZPEČNOSTNÍ KULTURA ORGANIZACE JAKO NÁSTROJ FYZICKÉ BEZPEČNOSTI

SAFETY CULTURE IN AN ORGANISATION AS A PHYSICAL SECURITY TOOL

LUKÁŠ KOTEK, TEREZA MIČULKOVÁ, PAVEL KRÁL

ABSTRACT: This article examines the development of a safety culture within an organization, with the aim of applying it to more effective safety education, which subsequently serves as a key safety measure. The article introduces the authors' new concept of the pillars of physical security and the philosophy of the security system as an interconnected security ecosystem. It also outlines important areas of safety education that play a crucial role in managing security incidents and explains the core principles of a safety culture. Finally, using an example of implementation in a selected organization, it illustrates possible approaches to building such a culture and presents specific steps and elements that we used to cultivate it.

KEYWORDS: Physical Security. Safety Culture. Security Education.

ÚVOD

Fyzická bezpečnost je stále společensky významným tématem, kterému se věnuje řada odborníků jak v praxi, tak v akademické sféře. Ochrana osob a majetku je jedním ze základních segmentů bezpečnosti, který však musí reflektovat dynamicky se měnící dobu a nejnovější trendy. Čím dál větší váhu získává role vzdělávání, která se ukazuje jako zásadním bezpečnostním opatřením. V našem výzkumu se zabýváme způsoby, jak toto bezpečnostní vzdělávání zefektivnit tak, aby předávané informace byly zúročeny v maximální možné míře. Vzhledem k charakteru témat spadající do této oblasti nepovažujeme za vhodné jít cestou povinných školení, kde je ochota školených přijímat informace minimální, nehledě na vyšší účast. Mnohem efektivnější se nám jeví motivovat lidi k tomu, aby se školení účastnili dobrovolně a sami informace vyžadovali a aktivně je vyhledávali. Nástrojem, kterým lze takové motivace dosáhnout, je nastavení a pečlivé budování bezpečnostní kultury v organizaci, která je běžnou součástí některých společností. Pro fyzickou bezpečnost však dosud nebyla významněji využívána. Článek představuje vhled do této problematiky a náhled na přístup, kterým se pokoušíme bezpečnostní kulturu vybudovat v prostředí naší instituce.

1. FYZICKÁ BEZPEČNOST

Fyzická bezpečnost je jednou ze základních oblastí bezpečnostního systému subjektů, která se nachází na fyzické úrovni a zahrnuje celou řadu dílčích oblastí, které chrání aktiva jako majetek nebo lidé proti hrozbám fyzického charakteru – krádeži, poškození, újmě na zdraví či ztrátě na životě. Jedná se o tradiční segment bezpečnostní praxe často označovaný jako ochrana osob a majetku.

Základ praxe tohoto sektoru bezpečnostního managementu vychází z tradic počátku průmyslu komerční bezpečnosti v porevoluční České republice, která navázala na dostupné znalosti z předchozí historické etapy, kdy byla bezpečnost řešena výhradně státem a jeho bezpečnostními složkami. I když se tento obor neustále vyvíjí, zůstává v něm zakořeněna tendence k úzkému náhledu na problematiku a orientace zejména na objektovou bezpečnost a technická opatření. Aktualizace znalostní báze a modernizace přístupů mnohdy spočívá pouze v rozšíření bezpečnostních opatření o ta netechnická, zejména režimová.

Domníváme se, že je nutné koncept fyzické bezpečnosti zásadně změnit, reflektovat současné potřeby organizací a přinést nové perspektivy a paradigmata. Za tímto účelem jsme rozšířili klíčové prvky struktury fyzické bezpečnosti, které interpretujeme jako „pilíře fyzické bezpečnosti“.

1.1. PILÍŘE FYZICKÉ BEZPEČNOSTI

V pojetí našich vědecko-výzkumných i praktických aktivit prezentujeme pilíře fyzické bezpečnosti jako čtyři segmenty, které spolu vzájemně souvisí, doplňují se a zohledňují všechny aspekty, které se projevují v kvalitativní úrovni fyzické bezpečnosti.

Obrázek 1 Pilíře fyzické bezpečnosti (Kotek, 2024)

První z pilířů je bezpečnostní management, který zodpovídá za zajištění strategické, operativní i taktické úrovně řízení bezpečnosti. Jeho úkolem je kontinuálně vyhodnocovat bezpečnostní rizika, tvořit dlouhodobé plány bezpečnostního rozvoje, vytvářet a udržovat vhodnou bezpečnostní dokumentaci, plánovat bezpečnostní opatření a zajišťovat jejich realizaci a údržbu, provádět kontrolní činnost prvků bezpečnostního systému a jejich efektivity a v neposlední řadě plnit roli reakčního a operativního řízení.

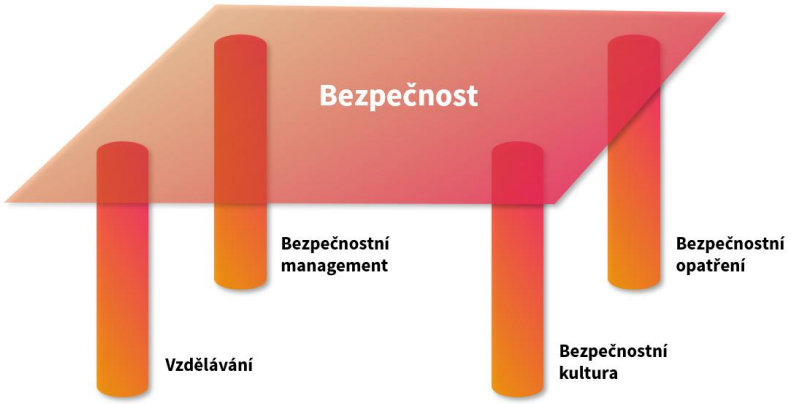
Druhým pilířem jsou bezpečnostní opatření, která jsou zpravidla nejviditelnějším pilířem, a proto se jim chybně přikládá nejvyšší váha. Spadá sem celá řada prvků jak technických (systém elektronické kontroly vstupu, kamerový systém, poplachový zabezpečovací a tísňový systém, mechanické zábranné systémy, krizové komunikační systémy aj.), tak netechnických (režimová opatření, fyzická ostraha, organizační opatření – dokumenty, samotná struktura bezpečnostního systému a nastavené procesy). U bezpečnostních opatření je nutné vyhodnocovat jejich vhodnost, kterou nelze plně přejímat z referenčních implementací, ale je nutné posuzovat je individuálně, zejména jejich efektivitu a vyřešit jejich vzájemnou provázanost a architekturu návazností.

Třetím pilířem je bezpečnostní vzdělávání, které je dle našeho výzkumu stále upozaděnou a nedostatečně rozpracovanou oblastí, která je však podle nás naprosto klíčová. Tento pilíř poskytuje osobám nacházejícím se v našem zájmovém referenčním objektu bezpečnostní povědomí a relevantní sadu znalostí a dovedností, které pozitivně působí na bezpečnost systému, např. znalost krizových procedur, ale také těch rutinních, které jsou nutné k běžnému provozu bezpečnostního systému. Na základě celosvětových zkušeností vyplývá, že dobře informovaný občan, který ví, co má dělat, je odhodlaný proaktivně reagovat a působí preventivně svým situačním povědomím, obezřetností a všímavostí, dokáže pozitivně působit na hrozby v oblasti fyzické bezpečnosti – jak těm interagujícím s materiálními aktivy (krádeže, poškozování), tak těmi lidskými (násilné napadení) (Kotek, 2018).

Čtvrtý, poslední, pilíř je bezpečnostní kultura v referenčním objektu. Tato oblast je ve fyzické bezpečnosti dosud neřešenou problematikou. Filozofie bezpečnostní kultury (nebo také „kultura bezpečnosti“) pochází z oblasti bezpečnosti a ochrany zdraví při práci (dále jen „BOZP“) a začala se rozvíjet zejména v segmentu energetiky po havárii jaderné elektrárny Černobyl v roce 1986. V České republice je definována Atomovým zákonem a povinná pro společnosti v nukleární oblasti. (Kultura bezpečnosti. Definice, pilíře, vytváření a rozvoj v organizaci, 2021) Pro jiné společnosti a organizace není povinnou, byť u velkých firem obvyklou. Výhradně však v oblasti BOZP. V našem pojetí je však důležitou součástí i oblasti fyzické bezpečnosti a zkoumáme způsoby, jak tento přístup implementovat k jejímu posílení, zefektivnění a zkvalitnění.

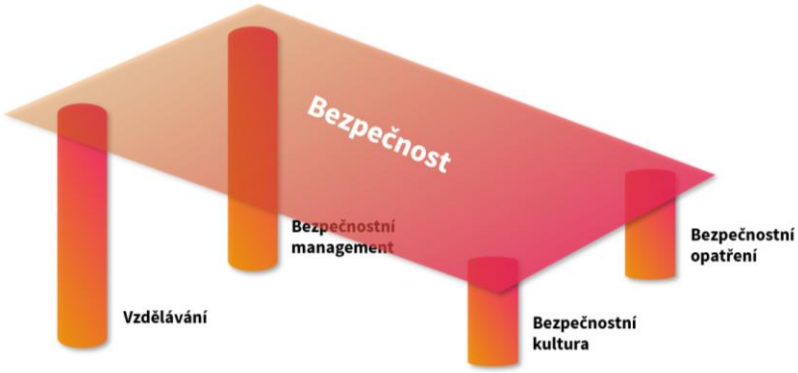
Náš koncept čtyř zmíněných pilířů fyzické bezpečnosti interpretujeme a vizualizujeme na ilustračním modelu čtyřnohého stolu, kde deska stolu reprezentuje úroveň bezpečnosti a každá z noh stolu jeden

z pilířů fyzické bezpečnosti. Dokud jsou nohy stolu přibližně stejně dlouhé, tedy všem pilířům je věnována stejná pozornost, je stabilní i deska stolu reprezentující úroveň fyzické bezpečnosti. Tu lze zvýšit při zachování efektivnosti a stability bezpečnostního systému souběžným zvyšováním všech čtyř noh, tedy rozvoji všech pilířů rovnoměrně a současně (Obrázek 2).



Obrázek 2 Vizualizace stability pilířů fyzické bezpečnosti (Kotek, 2024)

Dojde-li však k nerovnoměrné investici do těchto pilířů, způsobí to nerovnovážnost systému a destabilizaci bezpečnosti uvnitř organizace. Při extrémní nerovnovážnosti se pak stává systém nefunkčním a zcela závislým jen na některých z těchto pilířů. Toto však poskytuje jen imaginární bezpečnost a při prevenci, reakci a zmírňování dopadů bezpečnostního incidentu naprosto selhává. Tohoto stavu lze docílit buď přílišnou investicí do jedné nebo více oblastí, opomenutím některých oblastí nebo kombinací těchto faktorů (Obrázek 3).



Obrázek 3 Vizualizace nestability pilířů fyzické bezpečnosti (Kotek, 2024)

Jako příklad uveďme situaci, kdy dochází k velké finanční investici do technického zabezpečení (pilíř bezpečnostních opatření), ale není efektivně nastaven systém řízení, chybí postupy a reakce pro bezpečnostní i nebezpečnostní personál, nejsou nastaveny role a odpovědnosti, nejsou dořešeny návaznosti a propojení jednotlivých technických prvků (úloha pilíře bezpečnostního managementu), lidé nejsou dostatečně edukovaní, co mají v případě konkrétních situací dělat. V takovém případě může docházet k tomu, že je v objektu instalován moderní a sofistikovaný kamerový systém, který nikdo nemonitoruje, nikdo nereaguje na zaznamenané nežádoucí chování nebo bezpečnostní incidenty, lidé neví, co mají v případě nebezpečí nebo svědectví závadového jednání dělat, tudíž každý jedná podle svého nejlepšího uvážení, což může vést k nežádoucí nebo neefektivní reakci a samotná bezpečnostní opatření jsou chápána jako nechtěná omezení bez pochopení jejich významu.

1.2. FYZICKÁ BEZPEČNOST JAKO EKOSYSTÉM

Pro dosažení maximálního potenciálu bezpečnostního systému je nutné, aby bylo portfolio obsažených prvků co nejrůznorodější a fungovaly ve vzájemné symbióze. Se zaměřením na tento aspekt rozvoje

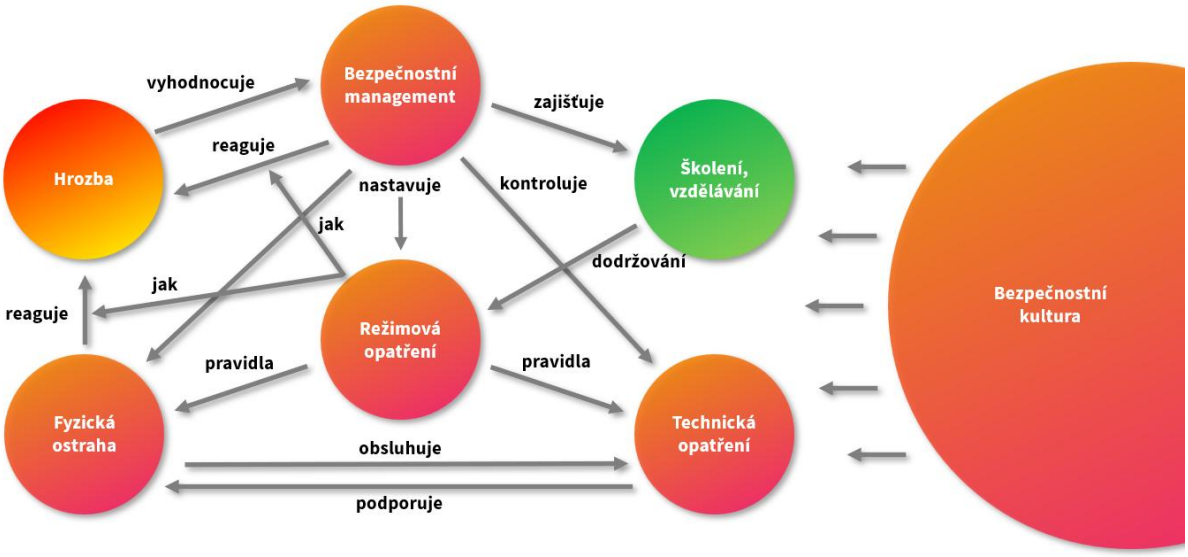
bezpečnostního systému se dá dosáhnout synergického efektu, kdy celek benefituje ze vzájemného precizního propojení a poskytuje větší efektivitu proti nežádoucímu chování, než je pouhý součet i efektivity individuálních prvků.

Tento princip, nazývaný „ekosystémová teorie“, pochází z přírodních věd a popisuje fungování vybraného biotopu a jeho odolnost proti změnám a přírodním katastrofám. Sledovanou vlastností systému je fakt, že čím různorodější a pestřejší je zastoupení biotických a abiotických prvků, tím lépe odolává negativním vlivům, jako je požár, vichřice aj. Vysoce heterogenní prostředí využívá zmíněné synergie k tomu, aby efektivně ustály jako celek externí vlivy, nehledě na dílčí škody, které událost způsobila. Prostředí pak dokonce ze situace vychází silnější a odolnější než před negativním zásahem. Příkladem může být tropický prales, který dokáže odolávat vnějším vlivům s vysokou efektivitou. Díky různě vysokým a hustým porostům je odolný proti větrným pohromám. Požár může zasáhnout značnou část, ale nevyhubí veškerou vegetaci, a dokonce některé druhy začnou těžit z chemických prvků vzniklých při požáru. Pokryjí místo požáru a podporují růst dalších vln rostlin, popadané stromy vyživují procesem trouchnivění okolní rostlinný pokryv atd. (Kotek, 2018)

Stanovená výzkumná hypotéza (Kotek, 2018) vychází z předpokladu založeném na praktických zkušenostech na různých bezpečnostních pozicích a deklaruje, že obdobný princip funguje i v oblasti fyzické bezpečnosti, kde různorodost bezpečnostních prvků zefektivňuje bezpečnostní standard a poskytuje mnohem větší variabilitu reakce na bezpečnostní hrozbu nebo nežádoucí událost. Díky této variabilitě se zvyšuje šance, že některým z prvků bude bezpečnostní hrozba eliminována v preventivní fázi (odrazení od provedení), bude dosaženo pohotové a účinné reakce (reakční fáze) anebo bude vytvořeno prostředí pro rychlé zastavení dopadů po ukončení působení zdroje hrozby (fáze zmírnění dopadů).

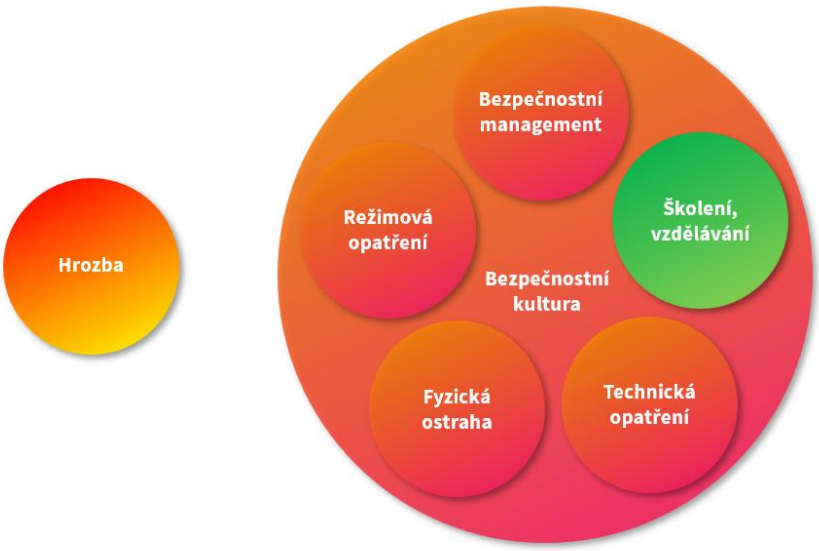
Nezbytným předpokladem je ale účinné provázání jednotlivých prvků, které spolu dokážou spolupracovat, podporovat své silné stránky a doplňovat ty slabé. Ve vhodně designovaném bezpečnostním ekosystému dokonce dochází k znásobení prevence, reakce a mitigace, kdy na hrozbu v různých fázích působí hned několik bezpečnostních prvků.

Takový ekosystém je velmi složitá architektura, která zabere značné množství práce a finančních prostředků, nicméně může být zdrojem inspirace pro nově budované nebo remodelované bezpečnostní systémy. Předpokladem je dostatečná odbornost zainteresovaných osob a dokonalé poznání procesů a struktury zkoumané organizace. Zjednodušená ilustrace provázání prvků bezpečnostního ekosystému je na obrázku níže.



Obrázek 4 Provázanost prvků ekosystému fyzické bezpečnosti (Kotek, 2024)

Cílem takového záměru je vytvořit provázaný synergický systém, který dokáže společným působením reagovat na širokou paletu hrozeb, efektivně je zvládat a napomáhat vyrovnat se s negativním působením. Hlavní motivací je fakt, že i přes důkladnou analýzu rizik může přijít nečekaná událost nebo nezohledněná varianta nebezpečí. Takový systém dokáže reagovat autonomně bez nutnosti akutní reakce pro úpravu aktuálním podmínkám dynamicky se měnící situace. Tento systém pak jako samostatný mechanismus reaguje na výskyt hrozby. Vizualizace níže prezentuje sílu spojení jednotlivých prvků do jednoho systému (Obrázek 5) přestože pro samostatné prvky by zvládnutí hrozby bylo mnohem obtížnějším problémem.



Obrázek 5 Resilience prvků fyzické bezpečnosti (Kotek, 2024)

2. BEZPEČNOSTNÍ KULTURA

Bezpečnostní kultura (může být označována také jako kultura fyzické bezpečnosti) v organizaci je kolektivním přístupem k řešení bezpečnostních otázek, kdy je plošně šířeno a zajišťováno vysoké povědomí o relevantních bezpečnostních tématech, postupech, znalostech a dovednostech a zároveň dochází k osobní angažovanosti každé osoby. K tomu je nutné pečlivě a dlouhodobě podporovat a kultivovat pozitivní vnímání bezpečnosti interním personálem a udržovat otevřenou komunikaci založenou na vzájemné důvěře.

Předpokladem je přijetí osobní odpovědnosti za osobní bezpečí, bezpečí svého okolí a celého systému každým jednotlivým člověkem. Organizace v takovém případě plní roli organizátora a mediátora tvorby bezpečnostního systému, kdy zejména:

- Vyhodnocuje rizika
- Realizuje bezpečnostní opatření
- Poskytuje vzdělávací servis

Je však nutné změnit vnímání osobního bezpečí jako odpovědnosti provozovatele místa, kde se právě nacházím (zaměstnavatele, školy, úřadu, nemocnice…), a přijmout fakt, že v případě nebezpečí bude ohrožená osoba ta, která je první v místě a čase incidentu a má tak jako jediná na incident reagovat. Sebelepší bezpečnostní opatření potřebuje určitou reakční dobu k tomu, aby se projevila. Tuto dobu je nutné překlenout vhodným působením právě dotčeného jedince. Spoléhat v prvních chvílích nelze ani na státní bezpečnostní složky (policie), které se o incidentu musí nejprve dozvědět, dopravit své síly na místo incidentu, zkoordinovat postup a teprve poté provést nutný zákrok. Takové uvědomění je pro běžného člověka nepříjemným zjištěním, mnohdy až zastrašujícím, je však nutné, aby proběhlo. Teprve po této změně přístupu mohou začít fungovat oblasti jako edukační příprava, praktické nácviky a jiné kvalifikační aktivity, které pomáhají lidem zvládat nebezpečné situace. Jak bylo zmíněno výše, právě adekvátní a pohotová reakce lidí v místě incidentu je naprosto klíčová.

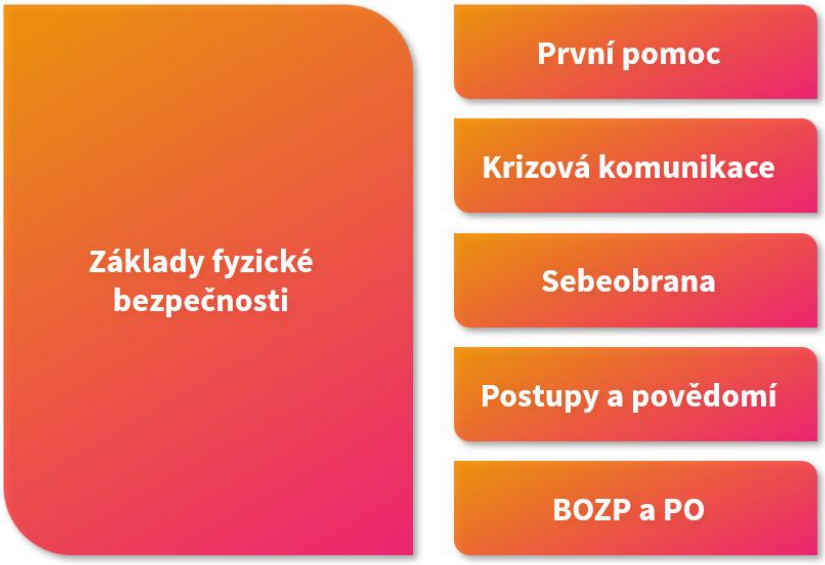
K tomu, aby lidé změnili svůj způsob uvažování na proaktivní, slouží právě bezpečnostní kultura, která vhodnou, nenásilnou formou otevírá důležitá témata, zvyšuje povědomí o bezpečnosti a transformuje uvažování lidí o bezpečnosti na něco, co je běžným a společensky důležitým tématem, kterému by se měli věnovat i mimo své profesní zaměření, a chápali ho jako soubor běžných lidských znalostí, jako je třeba znát dopravní předpisy nebo zákony své země. (Kotek, 2024)

3. DŮLEŽITÉ OBLASTI VZDĚLÁVÁNÍ

Během předchozího výzkumu (Kotek, 2018) byly identifikovány klíčové oblasti, které hrají důležitou roli při zvládání bezpečnostních incidentů. Tyto oblasti jsou v současně probíhající vědecko-výzkumné činnosti dále zkoumány, prohlubovány a kategorizovány na konkrétní znalosti, dovednosti a schopnosti.

V obecné rovině se však jedná o tyto tematické celky:

- **Základy fyzické bezpečnosti** – soubor školících materiálů, které účastníkům poskytují ucelený vzhled do této problematiky a seznamují se současným stavem fyzické bezpečnosti v zájmové organizaci tak, aby lidé vnímali prvky, ze kterých je bezpečnostní systém složen, a pozitivně je přijali jako součást bezpečného a komfortního prostředí. Současně obsahují základní postupy, které tvoří elementární znalost problematiky fyzického bezpečí. Obsaženy jsou témata, jako je aktivní útočník, komunikační postupy pro hlášení relevantních informací, rozvoj bezpečnostní všímavosti a myšlenky, které navádí účastníka školení k přijetí osobní odpovědnosti za svou bezpečnost a k proaktivní angažovanosti v jejím posilování.
- **První pomoc** – oblast, ve které by mělo být stupňovitým způsobem realizováno teoretické, ale i praktické vzdělávání v úkonech zachraňujících lidský život, jako je ošetření traumatických zranění, popálenin, vážných úrazů, zástavě krevní nebo dechové soustavy a stavy bezvědomí.
- **Krizová komunikace** – důležitá oblast, která se projevuje v preventivní fázi při deeskalaci konfliktu, ale i v reakční fázi při koordinaci činností vedoucích k zastavení hrozby, informování bezpečnostních složek a rychlému zastavení stále působcích dopadů incidentu.
- **Postupy a povědomí** – rozpracovávají se typové situace a postupy, jak se mají různé kategorie lidí zachovat v případě, že se v ní vyskytnou. Zohledněny jsou jak krizové situace, tak mimořádné incidenty, méně závažné bezpečnostní incidenty, ale i běžné rutinní bezpečnostně-relevantní činnosti.
- **Bezpečnost a ochrana zdraví při práci, požární ochrana** – oblast školení, která je uložena zákonem v předepsaném rozsahu.



Obrázek 6 Relevantní témata vzdělávání v oblasti fyzické bezpečnosti (Kotek, 2024)

Vzdělání v těchto oblastech je úzce propojeno právě s bezpečnostní kulturou. Vycházíme z předpokladu, že vhodně vytvořenou poptávkou (budováním a kultivací bezpečnostní kultury) dosáhneme reálného zájmu o bezpečnostní vzdělávání, které organizace nabízí. Účastníci školení, kurzů, webinářů, nácviků a seminářů tak budou pozitivně motivováni (vnitřní podnět) k získávání znalostí a dovedností ve výše uvedených oblastech, což se projeví na efektivitě procesu učení se u jednotlivých účastníků. Povinná školení vychází z vnějšího podnětu (stimulace zaměstnavatelem/institucí), kdy sice dochází k mnohem větší účasti na vzdělávacích akcích, ale s nízkou mírou učení se – účast u většiny osob bude pasivní bez vnitřní motivace získat předávané znalosti a dovednosti. (Mičulková, 2025)

Předpokladem však je nastavení synergie vzdělávacích možností, které realizuje organizace (poptávka), a vytvoření adekvátní nabídky školení, nácviků a jiných vzdělávacích akcí. Vhodné je zajistit větší nabídku různých formátů a způsobů vzdělávání, aby si zájemce mohl zvolit způsob, který je jeho potřebám odpovídající – fyzicky/online, s lektorem/bez lektora, teorie/praxe, různé dny a denní doby. (Mičulková, 2025)

4. ROZVOJ BEZPEČNOSTNÍ KULTURY

Nastavení bezpečnostní kultury v oblasti fyzické bezpečnosti je náročnou výzvou. V tomto tématu neexistuje dostatečně komplexní vědecký výzkum, který by byl aplikován v praxi a dlouhodoběji prezentován. Z tohoto důvodu vidíme vědecko-výzkumný potenciál tohoto tématu.

Referencí možného přístupu k rozvoji bezpečnostní kultury fyzické bezpečnosti může být přístup Univerzity Tomáše Bati ve Zlíně, která od ledna 2025 přijala novou vzdělávací a propagační strategii fyzické bezpečnosti zahrnující systematickou realizaci vzdělávacích aktivit ve výše zmíněných oblastech, doplněnou o propagační kampaň sloužící k šíření povědomí o vzdělávacích aktivitách, bezpečnostně významných tématech a vytvoření bezpečnostní kultury.

Ve svých aktivitách využívá principů a nástrojů marketingu, budovaní pozitivní image fyzické bezpečnosti a zlepšování veřejného i interního vnímání této oblasti. V tomto tématu bylo realizováno několik kroků:

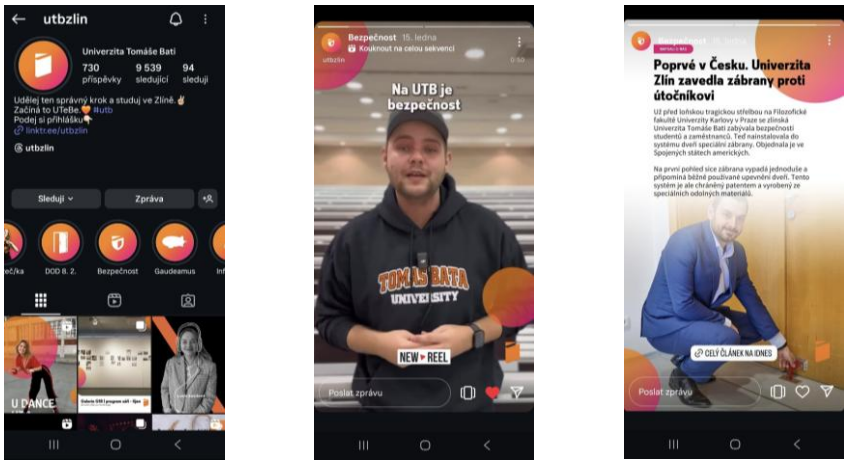
- **Vlastní značka zahrnující barevný design, logo a motto fyzické bezpečnosti** – cílem bylo vytvořit fyzické bezpečnosti vlastní značku, která by byla jasně identifikovatelná, rozpoznatelná, designově sladěná s univerzitním designem. Pro motto byla využita zkratka univerzity (UTB) a upraveno náborové motto do finálního: Bezpečnost začíná UTeBe. Logo fyzické bezpečnosti vychází z oficiálního loga univerzity, které je transformováno do stylizovaného štítu jako symbolu bezpečí.

Obrázek 7 Ukázka loga a motta fyzické bezpečnosti UTB (Mičulková, 2025)

- **Bezpečnostní newsletter** – pro rozšíření povědomí o činnosti univerzity v oblasti fyzické bezpečnosti byla zřízena speciální e-mailová adresa, která slouží výhradně pro komunikaci se zaměstnanci a studenty o bezpečnostních tématech. Přes ni je v nepravidelných intervalech rozesílán informační newsletter, který čtenáře stručnou formou seznamuje s proběhlými akcemi, novinkami v bezpečnosti na UTB a odkazy k dalšímu rozvoji.

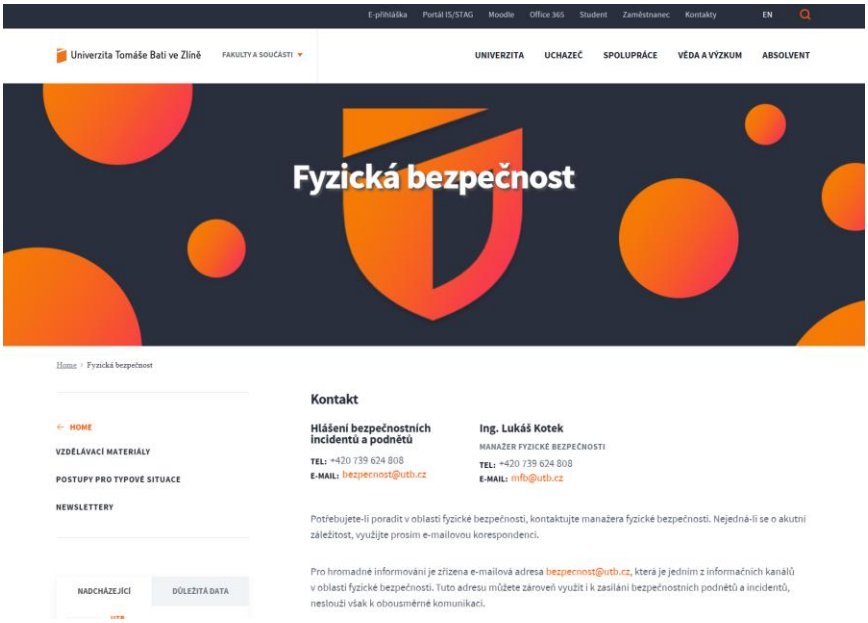
Obrázek 8 Bezpečnostní newsletter UTB (Bezpečnostní newsletter UTB, 2024)

- **Sociální sítě** – platformy jako Facebook, Instagram a YouTube jsou efektivními nástroji pro sdělování informací. Zejména díky tomu, že zhruba 90 % lidského faktoru na univerzitě tvoří studenti, z nichž většinu tvoří prezenční studenti ve věkovém rozmezí cca 20-25 let. Generace těchto lidí bere zmíněné platformy jako běžnou součást života a komunikace přes ně je efektivní cestou, jak zajistit dosah sdělovaných informací. Pro tento typ komunikace je nutné upravit i formát informací, kdy se jedná zpravidla o krátké videopříspěvky nebo fotky (s případným odkazem na delší stopáž).



Obrázek 9 Bezpečnostní témata na sociálních sítích UTB (Instagram UTB ve Zlíně, 2024)

- **Webové stránky** – základní platformou pro dostupnost informací o fyzické bezpečnosti jsou dedikované webové stránky. Ty slouží zejména jako vzdělávací nástroj, ale svou strukturou se snaží podporovat také rozvoj bezpečnostní kultury, proto je možné je zařadit i do tohoto pilíře fyzické bezpečnosti.



Obrázek 10 Webová stránka fyzické bezpečnosti UTB (Univerzita Tomáše Bati, 2025)

ZÁVĚR

Tento článek měl za cíl představit čtenářům problematiku bezpečnostní kultury a prezentovat myšlenku možnosti jejího využití ke zvýšení efektivity bezpečnostního vzdělávání. Představil nový, rozšířený koncept pilířů, z něhož je složena struktura fyzické bezpečnosti a také konceptuální model fyzické bezpečnosti jako vzájemně provázaného, variabilního a různorodého ekosystému, který díky své vzájemné synergii dokáže mnohem lépe reagovat na velkou škálu bezpečnostních hrozeb. Oproti běžné praxi je akcentována role vzdělávání a proaktivního přístupu osob v daném prostředí. Tato proaktivita je však závislá na přijetí osobní odpovědnosti za podílení se na tvorbě bezpečného prostředí a ochotě se v této oblasti vzdělávat a své dovednosti prohlubovat. Jako efektivní cestu, jak toto pozitivní smýšlení o bezpečnostních tématech šířit, se nám jeví cílené a systematické budování bezpečnostní kultury a její neustálá kultivace. Koncept bezpečnostní kultury není zcela novým tématem, v oblasti fyzické bezpečnosti však dosud nebyla v širší míře využita a jedná se o nedostatečně pokryté téma vědecko-výzkumných aktiv i praktických, bezpečnostně manažerských činností. Článek svým textem představil princip bezpečnostní kultury a autorský koncept možnosti jejího využití pro oblast fyzické bezpečnosti. Závěr práce prezentoval některé konkrétní kroky, kterými byla bezpečnostní kultura cíleně podporována a na kterou je navázáno dalšími strategickými činnostmi k rozvoji bezpečnostního povědomí a budování kultury bezpečnosti na Univerzitě Tomáše Bati ve Zlíně. Jedná se o nový, nevyzkoušený přístup, který je nutné dlouhodoběji zkoumat, vyhodnocovat a dostatečně akademicky i prakticky prozkoumat. Přesto se už nyní jeví jako inovativní přístup, který má potenciál posunout bázi vědeckého poznání o nové poznatky a rozšířit „dobrou praxi“ bezpečnostního managementu dalším směrem.

LITERATURA

Bezpečnostní newsletter Červen 2024. (2024).

Fyzická bezpečnost | UTB. (c2025). Univerzita Tomáše Bati ve Zlíně | UTB. Retrieved September 29, 2025, from https://www.utb.cz/fyzicka-bezpecnost/

Kotek, L. (2018). Status občana při zajištění osobní a komunitní bezpečnosti [Diplomová práce, Univerzita Tomáše Bati ve Zlíně]. http://hdl.handle.net/10563/43330

Kotek, L. (2024, November 27). Fyzická bezpečnost na VŠ [Prezentace]. Konference APUA, Praha.

Kultura bezpečnosti. Definice, pilíře, vytváření a rozvoj v organizaci. (2021, October 30). BOZP a PO - bezpečnost práce moderně a efektivně | BOZP.cz. Retrieved September 29, 2025, from https://www.bozp.cz/aktuality/kultura-bezpecnosti/

Mičulková, T. (2025). Informační a vzdělávací strategie fyzické bezpečnosti UTB [Diplomová práce]. Univerzita Tomáše Bati ve Zlíně.

Univerzita Tomáše Bati. https://www.instagram.com/utbzlin

Ing. Lukáš Kotek

Ústav bezpečnostního inženýrství, Univerzita Tomáše Bati ve Zlíně

e-mail: kotek@utb.cz

Ing. Tereza Mičulková

Ústav bezpečnostního inženýrství, Univerzita Tomáše Bati ve Zlíně

e-mail: t_miculkova@utb.cz

Ing. Pavel Král

Ústav bezpečnostního inženýrství, Univerzita Tomáše Bati ve Zlíně

e-mail: p_kral@utb.cz

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.166-173
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online

VYUŽITÍ ÚKOLOVÝCH KARET V KOORDINAČNÍCH PLÁNECH

THE USE OF TASK CARDS IN COORDINATION PLANS

PAVEL KRÁL, DORA KOTKOVÁ

ABSTRACT: *The article examines the use of task cards in the development of a coordination plan as an effective tool for accelerating and simplifying procedures in the event of security incidents. It is based on the premise that converting scenarios into a concise and graphical form significantly improves orientation within the plan and increases the overall clarity and efficiency of the established procedures. The aim is to present the essence of using task cards and to propose principles for their design, structure, and accessibility, including recommendations for regular training and exercises that continuously contribute to the gradual improvement of organisational preparedness and process efficiency.*

KEYWORDS: *Task cards. Coordination plan. Security. Security incidents.*

ÚVOD

Problematice bezpečnosti je v dnešní době věnována stále větší pozornost. Organizace se v řadě případů začínají aktivněji zajímat o vlastní bezpečnost. S tímto trendem souvisí rostoucí poptávka po různých bezpečnostních dokumentech, jako je například koordinační plán, od kterého si organizace slibují zvýšení reakceschopnosti na nečekané bezpečnostní incidenty. Článek se bude zabývat využitím úkolových karet v rámci koordinačního plánu, aby byl zajištěn požadovaný přínos na rychlost, efektivnost a správnost řešení vzniklé nežádoucí situace a byly odstraněny případné nedostatky, s nimiž se mohou organizace setkávat při snaze využít zpracovaný koordinační plán.

Článek nejprve popíše koordinační plán a jeho nezbytné součásti pro uvedení adekvátního kontextu problematiky, a následně se bude věnovat samotným bezpečnostním incidentům, jejichž postupy řešení má koordinační plán obsáhnout v rámci jednotlivých scénářů. Dále bude popsáno, jakým způsobem jsou úkolové karty tvořeny, aby byly přehledné, umožňovaly snadnou orientaci a obsahovaly logicky členěné kroky podle priority a fází incidentu. Budou rovněž zmíněny klíčové kroky pro zajištění efektivního využívání vytvořených karet, včetně jejich dostupnosti pro jednotlivé osoby. Současně je nutné zdůraznit proškolení a nacvičování postupů podle vytvořených scénářů s využitím úkolových karet.

1. KOORDINAČNÍ PLÁN

Koordinační plán je jedním z řady bezpečnostních dokumentů, které organizace může zpracovat za účelem zvýšení své připravenosti na nečekané a nežádoucí události. Staví na principu, že systematická příprava vedení organizace na možný vznik takových událostí a stanovení jasných postupů, jak v takových situacích postupovat, vede k výrazně efektivnějšímu řešení incidentů a k rychlejšímu obnovení standardního provozu organizace. Aby byl takový dokument efektivní a využitelný v praxi, je nutné jej zpracovat na míru konkrétního objektu tak, aby obsáhl veškeré specifické potřeby, jako je například organizační struktura, oblast působení nebo prostředí, ve kterém se organizace nachází (Ben David, 2025a).

Mezi další typy bezpečnostních plánů se v rámci České republiky řadí například také „Plán krizové připravenosti“, jehož náležitosti a součásti jsou pevně legislativně vymezeny nařízením vlády (Nařízení vlády č. 462/2000 Sb., 2000) a jeho zpracování je popsáno také v metodickém dokumentu „Metodika zpracování plánů krizové připravenosti podle § 17 až 18 nařízení vlády č. 462/2000 Sb., k provedení §27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů“ (Ryba, 2011). Tento dokument je zpracováván převážně subjekty kritické infrastruktury nebo dalšími subjekty, jímž tuto povinnost ukládají právní předpisy (Zákon

č. 240/2000 Sb., 2000). Významným rozdílem je také to, že tento dokument se zabývá řešením krizových situací a mimořádných událostí, ale neřeší jiné potenciálně škodlivé události. Další významný rozdíl spočívá v tom, že plán krizové připravenosti končí příjezdem složek Integrovaného záchranného systému (IZS) na místo (Ben David, 2025a, 2025b; Hromada, 2024). Za zmínku stojí také „Havarijní plán“, jehož obsah je opět legislativně upraven a který je zpracováván povinně subjekty, jímž tuto povinnost ukládá relevantní právní předpis (Zákon č. 224/2015 Sb., 2015). Týká se výhradně otázky závadných látek a závažných havárií či mimořádných událostí, které jsou s nimi spojeny. Neřeší však jiné potenciálně škodlivé události (Ben David, 2025a, 2025b).

Zpracování koordinačního plánu není legislativně upraveno, ale je popsáno například v metodickém dokumentu „Metodika koordinace měkkého cíle pro fáze po závažném incidentu aneb jak se vyrovnat s nastalou závažnou situací“ (Ben David, 2025a) nebo v navazujícím metodickém dokumentu „Jak se připravit na závažnou situaci? Koordinační plány pro měkké cíle“ (Ben David, 2025b). Tyto metodiky se konkrétně věnují tvorbě a využití koordinačního plánu a jeho aplikaci u měkkých cílů. Koordinační plán je však dokument, který může být značně užitečný pro všechny typy objektů, ale vypracovává se organizacemi čistě z jejich vlastní iniciativy, a proto se může přístup k jeho tvorbě výrazně lišit. Tímto se značně odlišuje od jiných již zmíněných plánů. Dalším významným rozdílem je, že i když se tato metodika značně věnuje spolupráci a komunikaci organizace se složkami IZS, postupy určené v plánu končí až návratem do běžného provozu, nikoliv příjezdem složek IZS na místo (Ben David, 2025a, 2025b).

Aby dokument splnil svůj účel, musí být zpracován ve stručné a přehledné formě tak, aby umožnil předání všech nutných informací relevantním osobám i bez hlubších znalostí v oblasti bezpečnosti. Plán musí být zároveň dostatečně konkrétní a pokrývat celou řadu možných incidentů, přičemž by jeho forma měla umožňovat rychlý přístup k potřebným informacím bez nutnosti pročítání rozsáhlého textu. Měl by obsahovat pouze stručné definice klíčových pojmů a krátký úvod objasňující význam dokumentu. Důležité je také na začátku koordinačního plánu zavést klíčové zkratky, které umožní rychlejší orientaci v textu (Král, 2025).

Dále je nutné zahrnout seznam incidentů, pro které bude plán zpracovávat konkrétní scénáře a které tak povedou k jeho aktivaci. Tyto incidenty by měly zahrnovat nejen násilné útoky, ale také jiné, pro organizaci relevantní události (Ben David, 2025a; Král, 2025). Pro účely zjištění možných incidentů je vhodné využít například vyhodnocení ohroženosti na základě metodického dokumentu „Vyhodnocení ohroženosti měkkého cíle aneb co, kdy, kde a od koho vám hrozí“ (Kavlach, 2025). Metodika se konkrétně věnuje dané problematice z pohledu měkkých cílů, je však možné ji využít i pro jiné typy objektů.

Důležitou součástí je také určení osob, typicky členů vedení organizace, kteří budou zodpovědní za provádění jednotlivých kroků stanovených koordinačním plánem. Takto určenou skupinu lze například nazývat jako „koordinační štáb“ (Ben David, 2025a; Král, 2025).

V rámci plánu je jasně stanoveno, kdo jsou členové tohoto štábu, jaké jsou jejich pozice a odpovědnosti v případě aktivace koordinačního plánu, včetně podrobného popisu úkolů specifických pro určené incidenty. Koordinační štáb je často inspirován organizační strukturou dané organizace a z tohoto důvodu se může mezi subjekty výrazně lišit. Při jeho sestavování je také nutné individuálně posoudit osobnost každého potenciálního člena z hlediska schopnosti zvládat rozhodování a jednání ve stresových situacích, a na základě tohoto posouzení zvážit obsazení jednotlivých rolí ve štábu. Mezi pozice, ze kterých se může koordinační štáb skládat, patří například:

- předseda koordinačního štábu,
- koordinační manažer,
- zapisovatel,
- koordinátor komunikace,
- tiskový mluvčí,
- koordinátor informační a technické podpory (Král, 2025).

Součástí plánu musí být také popis procesu aktivace koordinačního štábu. Především je nutné stanovit, kdo a jakým způsobem toto rozhodnutí provádí. Je zde kladen důraz na skutečnost, že je vždy lepší

provést i potenciálně chybné rozhodnutí, které lze později pozměnit či zrušit, než zůstat u nečinnosti, která může mít závažné nenapravitelné následky. Současně je nutné vhodné nastavení komunikace jak uvnitř koordinačního štábu (informování o aktivaci a následná komunikace při řešení incidentu), tak i s ostatními členy organizace a s vnějším prostředím (s médii, veřejností a státním aparátem) (Ben David, 2025a).

Samozřejmostí jsou také přílohy, které musejí poskytovat všechny podstatné informace určeným osobám v přehledné a snadno využitelné formě. Jedná se nejčastěji o mapy a plány budov, seznam všech členů koordinačního štábu a kontaktní informace na všechny zainteresované osoby (například členy koordinačního štábu nebo různé dodavatele). Pravděpodobně nejdůležitější jsou zde však úplné postupy (scénáře) pro vybrané incidenty, určené jednotlivým členům (Ben David, 2025a).

2. ZÁVAŽNÉ BEZPEČNOSTNÍ INCIDENTY

V rámci koordinačního plánu je nutné definovat, na jaké situace se dokument vztahuje a pro jaké události budou zpracovávány detailní scénáře. Lze je vymezit například jako „závažné bezpečnostní incidenty“, u nichž se předpokládá, že při jejich vzniku dochází k bezprostřednímu ohrožení životů a zdraví osob, popřípadě k závažnému narušení standardního provozu organizace. Společným rysem všech takových situací je, že je nelze efektivně zvládnout bez využití koordinovaného postupu členů organizace s využitím koordinačního plánu. Dalším typickým společným rysem je také nepředvídatelnost jejich vzniku (Král, 2025).

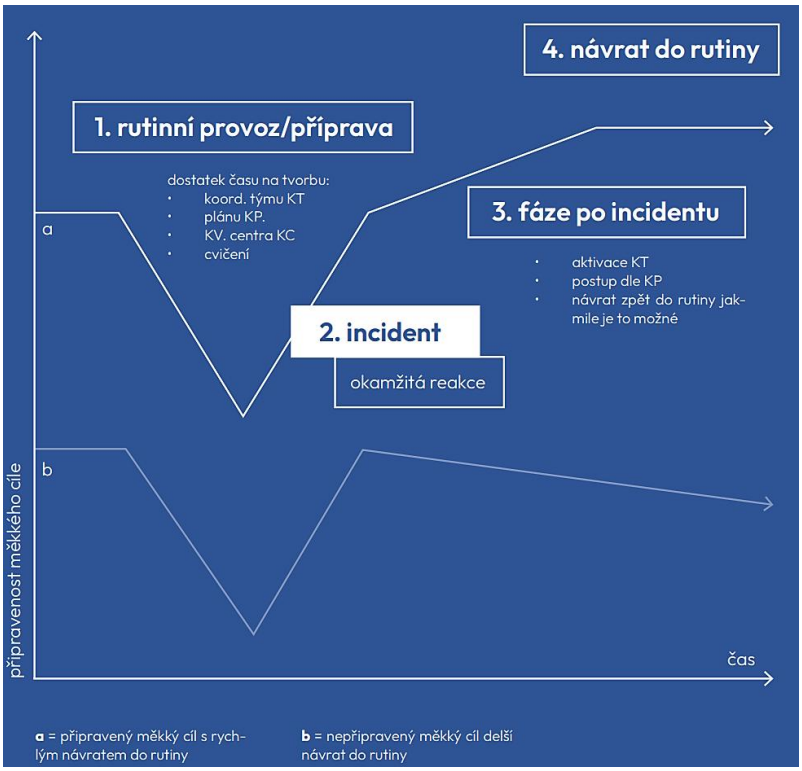
Z takto definovaných incidentů je nutné vytvořit seznam událostí, pro které organizace zpracuje jednotlivé postupy. Seznam závažných bezpečnostních incidentů může například obsahovat tyto situace:

- ozbrojený útok v objektu,
- závažný požár v objektu,
- výhružka útoku nebo nástražným výbušným zařízením v objektu,
- agrese beze zbraně v objektu,
- závažná havárie v objektu (různé typy),
- kybernetický útok nebo jeho zvýšené riziko (Král, 2025).

Seznam i samotná definice musí vždy odrážet především potřeby, specifika a možnosti konkrétní organizace. Je rovněž doporučeno vytvořený seznam konzultovat s relevantními složkami IZS (Ben David, 2025a).

Pro incidenty v takto vytvořeném seznamu jsou následně zpracovávány konkrétní scénáře. Ty jsou vždy rozděleny podle jednotlivých členů koordinačního štábu a obsahují všechny významné kroky, které má daná osoba provádět, aby bylo možné efektivně zvládnout řešený incident a minimalizovat jeho dopady (Král, 2025). Je zároveň důležité obsáhnout i na první pohled samozřejmé kroky, protože právě ty mohou být pod vlivem stresu snadno opomenuty (Ben David, 2025a).

V případě vzniku závažného incidentu jsou často nejkritičtější první desítky minut od jeho vypuknutí, kdy každá reakce může významně ovlivnit další vývoj situace. Správně připravený scénář tak představuje základ rychlé a efektivní reakce, přičemž by měl předcházet tápání, nerozhodnosti či chybám při řešení vzniklého incidentu. Tím lze minimalizovat potenciální následky nežádoucích událostí a současně urychlit návrat organizace do běžného provozu (Ben David, 2025a).



Obrázek 1 Rozdíl mezi připraveným a nepřipraveným měkkým cílem (Ben David, 2025a)

Je důležité také podotknout, že efektivitu i u dobře vytvořeného scénáře může snižovat jeho forma zpracování. Z důvodu nutnosti zahrnout velké množství informací a obsáhlých postupů pro řadu scénářů a členů štábu může velmi snadno docházet k obtížné orientaci v dokumentu. V textové podobě jsou jednotlivé scénáře pro jednotlivé členy často nepřehledné, zmatečné a neumožňují rychlou orientaci. Zároveň je také velmi nepraktické, aby daný člen štábu musel ve stresové situaci při vzniku závažného bezpečnostního incidentu listovat celým dokumentem, hledat příslušný scénář pro vzniklou situaci a teprve poté vyhledávat konkrétní postup relevantní pro jeho pozici. Takto může dojít ke ztrátě drahocenných minut, které by mohly být využity k provádění zásadních kroků nezbytných pro zvládnutí daného incidentu.

3. VYUŽITÍ ÚKOLOVÝCH KARET JAKO NÁSTROJE V KOORDINAČNÍCH PLÁNECH

Problém s přehledností, přístupností a orientací ve zpracovaných scénářích lze významně zlepšit převedením informací do grafické podoby, například ve formě úkolových karet. V této podobě vzniká kompaktní celek informací, ve kterém má daná osoba po ruce veškeré potřebné informace pro efektivní zvládnutí situace.

ZÁKLADNÍ PRINCIPY VYUŽITÍ ÚKOLOVÝCH KARET

Samotné úkolové karty musejí být vždy vytvořeny tak, aby splňovaly několik důležitých principů, které zajistí jejich efektivní využití v případě potřeby. Každá úkolová karta by měla být ve formátu, který obsáhne všechny kroky pro konkrétního člena koordinačního štábu a pro daný scénář. Tímto způsobem jsou pro daného člena dostupné všechny relevantní informace na jednom místě, což zajišťuje rychlou orientaci, přehlednost a efektivní provádění jednotlivých kroků při řešení incidentu.

Žádoucí je také vytvoření sady úkolových karet pro všechny scénáře pro každého člena koordinačního štábu. Při vzniku závažného bezpečnostního incidentu a aktivaci koordinačního plánu tato osoba pouze vybere konkrétní úkolovou kartu ze sady, která odpovídá danému incidentu. Není zde důvod, aby jednotliví členové měli pohromadě úkolové karty všech členů, avšak v případě potřeby by měly být tyto karty k dispozici v příloze samotného koordinačního plánu.

Na jednotlivých úkolových kartách je nutné uvádět všechny důležité kroky, včetně těch, které mohou působit samozřejmě. Cílem je zabránit možnosti opomenutí jakéhokoli kroku, ke kterému by mohlo dojít vlivem stresového působení. Jednotlivé kroky by měly být uspořádány podle priority jejich provedení a logické posloupnosti tak, aby umožňovaly systematický postup. Některé kroky je možné provádět současně s jinými, je však nutné zachovat jejich logické seřazení pro udržení přehlednosti.

Současně je nutné logické rozdělení jednotlivých kroků do fází incidentu, a to na základě toho, kdy je daný krok nutné provést. Takto lze efektivně oddělit kroky různé priority. Jednou z možností je rozdělit kroky do dvou fází podle aktuálního stavu závažného bezpečnostního incidentu. A to například na fáze:

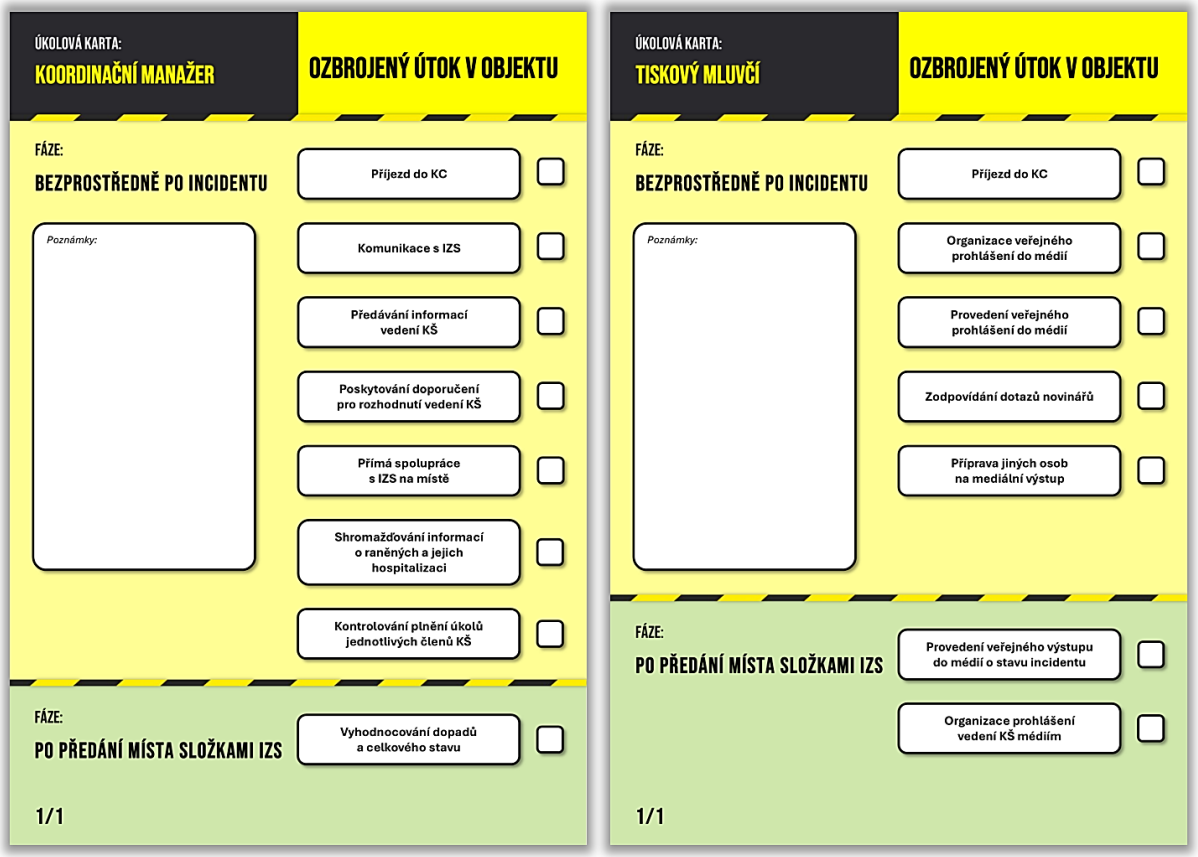
- Bezprostředně po incidentu – tato fáze zahrnuje kroky, které je nutné provádět v řádech minut či hodin od vzniku incidentu a které primárně směřují k zastavení působení nežádoucího incidentu.
- Po předání místa složkami IZS – v této fázi se předpokládá, že hlavní nebezpečí je již zažehnáno, a tyto kroky lze provádět v delších časových intervalech (v některých případech i týdnech), s cílem směřovat k obnově běžného provozu v organizaci (Král, 2025).

ROZLOŽENÍ ÚKOLOVÝCH KARET

Jednotlivé úkolové karty musejí obsahovat řadu informací, které umožní snadnou orientaci v celé sadě karet a přehlednost obsahu na jednotlivé kartě. Jedná se například o jasné určení funkce v rámci koordinačního štábu, pro kterou je daná karta určena, a zřetelný název scénáře, na který se karta vztahuje. Současně je nutné uvést stránkování úkolové karty, aby bylo naprosto zřejmé, zda se skládá z více stran či nikoliv. Jednotlivé fáze, do kterých jsou kroky v rámci daného scénáře rozděleny, je také nutné jasně označit, přičemž je vhodné používat jednotné označení těchto fází, aby byla zajištěna konzistence mezi různými scénáři.

Samostatné kroky je vhodné na kartě umístit v oddělených buňkách, kde by měly být uspořádány v logické posloupnosti. I v případech, kdy je nutné některé kroky provádět současně, je vhodné je na kartě uvádět samostatně pod sebe, aby byla zachována přehlednost. Tyto kroky musejí být také jasně formulované, stručné a bez zbytečných detailů. Pro zlepšení přehlednosti mezi již splněnými a zbývajícími úkoly je žádoucí vedle jednotlivých kroků umístit pole pro odškrtávání provedených úkolů. Na úkolové kartě je také vhodné vyhradit dostatečný prostor pro poznámky člena štábu, který umožní zaznamenávat všechny potřebné doplňující informace či připomínky.

Dalším významným prvkem, který může usnadnit orientaci v úkolových kartách, je využití vizuálních prvků a jednotného designu. Vhodně zvolené barvy či symboly mohou urychlit identifikaci úkolových karet oproti jiným dokumentům a zároveň přispět k rychlejší orientaci v rámci samotné karty. Například je možné využít rozdílné barvy pro jednotlivé fáze postupu nebo zvýraznit nejdůležitější kroky. Nezbytné je však zachovat jednotný vizuální styl napříč celou sadou karet, aby nedocházelo ke zbytečnému matení členů koordinačního štábu. Je také důležité dbát na to, aby vizuální prvky byly využívány cíleně tak, aby rozdílné barvy, podtržení či symbol měly mít jasný účel. Nadměrné využívání těchto prostředků by naopak mohlo vést k nechtěnému zmatku a komplikovat pochopení úkolové karty.



Obrázek 2 Ukázka úkolových karet pro scénář „Ozbrojený útok v objektu“ (Král, 2025)

V případě fyzické verze úkolové karty je rovněž důležité zvolit vhodnou velikost karty. Je nutné, aby všechny informace na kartě byly dobře čitelné, přičemž menší rozměry umožňují větší flexibilitu umístění a umožní členovi štábu mít kartu vždy u sebe. V případech, kdy scénář vyžaduje pro obsažení informací využití dvou stran, je vhodné úkolové karty tisknout oboustranně, aby byla zachována přehlednost a ucelenost postupu. Pozornost by měla být věnována také odolnosti fyzických kopií úkolových karet. Aby nedocházelo k jejich poškození vlivem nepříznivých podmínek, je vhodné karty například zalaminovat nebo vytisknout na kvalitnější a odolnější papír. Takto lze docílit lepší životnosti karet při současném zachování jejich čitelnosti i v případě používání v náročnějších podmínkách. Při využití laminace je nutné počítat s omezenou možností zapisování poznámek nebo odškrtávání splněných kroků.

PRÁCE S ÚKOLOVÝMI KARTAMI

Obecně je jedním z nejpodstatnějších kroků celého koordinačního plánu průběžné školení a nacvičování všech postupů se všemi zainteresovanými osobami. Toto samozřejmě platí i pro vytvořené scénáře ve formě úkolových karet. Je proto nutné zajistit seznámení členů koordinačního štábu s kartami samotnými, ale také s postupy na nich uvedenými. Dále je nutné pravidelně provádět nácviky závažných bezpečnostních incidentů a simulovat postupy dle scénářů s využitím úkolových karet. Tento bod je zásadní, protože nástroje, které nejsou využívány při nácvicích, pravděpodobně budou opomenuty i při reálném spuštění daných procesů. Důležitou součástí je rovněž využití testovacích nácviků pro ověření efektivity, identifikaci chyb či nedokonalostí v připravených úkolových kartách a jejich následné vylepšování. Konkrétní způsoby testování se v současnosti dále rozpracovávají, přičemž probíhající výzkum se zaměřuje na výběr hodnotících parametrů a stanovení rozsahu testování. Obecně platí, že školení, nácviky i doplňování nedostatků by měly tvořit pravidelně se opakující cyklus, který směřuje k postupnému zdokonalování připravenosti organizace na možné výskyty závažných bezpečnostních incidentů (Ben David, 2025b; Král, 2025).

Zároveň je nezbytné zajistit dostupnost úkolových karet pro všechny členy koordinačního štábu. Je nutné počítat s tím, že vzhledem k nepředvídatelnosti vzniku závažného bezpečnostního incidentu se může stát, že k nim dojde i mimo standardní pracovní dobu, nebo v případě kdy je některý z členů štábu například na pracovní cestě, či jiném místě mimo své obvyklé pracoviště. S ohledem na charakter, možnosti a potřeby organizace je proto důležité vybrat vhodnou formu a rozmístění úkolových karet zajišťující jejich dostupnost.

Úkolové karty ve fyzické podobě je vhodné rozmisťovat v několika kopiích na různá místa, kde lze předpokládat výskyt dané osoby v co nejširším spektru situací. Typicky se jedná například o:

- pracoviště či kancelář osoby,
- osobní nebo firemní automobil,
- recepci objektu,
- domov daného člena koordinačního štábu.

V případě převedení úkolové karty do digitální podoby lze významně zvýšit pravděpodobnost, že člen štábu bude mít přístup ke kartám ve všech možných situacích. Jednou z nejjednodušších možností je uložení elektronické podoby karet (například ve formě PDF dokumentu) na mobilních zařízeních a počítačích členů koordinačního štábu. Další možností je vytvoření mobilní nebo webové aplikace, případně implementace této funkce do již existující aplikace využívané v rámci organizace. Pokud organizace používá specifický krizový systém, například Krizový informační a svolávací systém (KISS), pro aktivaci koordinačního plánu nebo jiných zavedených procesů, lze rozesílání konkrétních úkolových karet propojit se samotným informováním členů o vzniku závažného bezpečnostního incidentu.

Důležité je rovněž zdůraznit, že při využití elektronické podoby úkolových karet je vhodné upřednostňovat nástroje, se kterými jsou členové koordinačního štábu již obeznámeni a které běžně využívají. Platí totiž, že pokud například danou aplikaci téměř nepoužívají, může se objevit odpor k její instalaci nebo tendence ignorovat upozornění, které aplikace zasílá. Je proto nezbytné brát v úvahu konkrétní specifika organizace a jednotlivých členů štábu, protože řešení, které se osvědčí v jedné organizaci, nemusí být efektivní v jiné (Ben David, 2025a).

ZÁVĚR

Závěrem lze shrnout, že cílem článku bylo představit možnosti využití úkolových karet jako praktického nástroje, který významně přispívá k rychlosti, přehlednosti a správnosti provádění postupů stanovených v koordinačním plánu. Jejich hlavní přínos spočívá v tom, že výrazně zkracují čas potřebný k orientaci v komplexních scénářích a umožňují členům koordinačního štábu provádět jednotlivé kroky v potřebné posloupnosti, čímž předcházejí opomíjení dílčích úkolů i ve vysoce stresových situacích. Grafická forma rovněž eliminuje riziko vzniku chyb způsobených nepřehledností textu nebo rozsáhlostí samotného bezpečnostního dokumentu.

Úspěšné využití tohoto nástroje je však podmíněno jeho správným návrhem, pravidelnými aktualizacemi a systematickým zasazením do širšího systému bezpečnosti organizace, včetně začlenění do pravidelných nácviků a školení. V rámci organizace je také nutné zajistit, aby byly karty pro všechny relevantní členy štábu snadno dostupné bez ohledu na denní či pracovní dobu nebo místo, kde se aktuálně nacházejí. Stejně důležité je dlouhodobé prověřování jejich funkčnosti v praxi a následné odstraňování zjištěných nedostatků. Při dodržení všech důležitých zásad lze zajistit, že úkolové karty nebudou pouze formální přílohou koordinačního plánu, ale užitečným nástrojem, který přispěje k vyšší úrovni bezpečnostní připravenosti organizace a k efektivnímu zvládání závažných bezpečnostních incidentů.

LITERATURA

Ben David, G. (2025a). *Metodika koordinace měkkého cíle pro fáze po závažném incidentu aneb jak se vyrovnat s nastalou závažnou situací*. Ministerstvo vnitra České republiky. https://www.mvcr.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx

Ben David, G. (2025b). *Jak se připravit na závažnou situaci? Koordinační plány pro měkké cíle*. Ministerstvo vnitra České republiky. https://www.mvcr.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx

Hromada, M. (2024). *Přednáška z předmětu Krizové plánování a řízení – Plán krizové připravenosti* [Přednáška]. Univerzita Tomáše Bati ve Zlíně.

Kavlach, Z. (2025). *Vyhodnocení ohroženosti měkkého cíle aneb co, kdy, kde a od koho vám hrozí*. Ministerstvo vnitra České republiky. https://mv.gov.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx

Král, P. (2025). *Návrh koordinačního plánu vybrané univerzity* [Diplomová práce]. Univerzita Tomáše Bati ve Zlíně.

Nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení (krizový zákon). (2000). Sbírka zákonů.

Ryba, D. (2011). *Metodika zpracování plánů krizové připravenosti podle § 17 až 18 nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů*. Krizport. https://www.krizport.cz/system/files/files/download/pkp-metodika-2011.pdf

Zákon č. 224/2015 Sb., o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými směsmi a o změně zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů (zákon o prevenci závažných havárií). (2015). Sbírka zákonů.

Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). (2000). Sbírka zákonů.

Pavel Král, Ing.

Ústav bezpečnostního inženýrství, Univerzita Tomáše Bati ve Zlíně

e-mail: p_kral@utb.cz

Dora Kotková, Ing., Ph.D.

Ústav bezpečnostního inženýrství, Univerzita Tomáše Bati ve Zlíně

e-mail: kotkova@utb.cz

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.174-180
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online

SYSTÉM BEZPEČNOSTNÍHO VZDĚLÁVÁNÍ S VYUŽITÍM MODERNÍCH TRENDŮ

SECURITY AND SAFETY EDUCATION SYSTEM USING MODERN TRENDS

TEREZA MIČULKOVÁ, LUKÁŠ KOTEK

ABSTRACT: The article highlights the importance of education in physical security, based on the premise that security begins with each individual. In the event of a security incident, professional assistance is not immediately available, leaving individuals to rely solely on themselves. They must depend on their own preparedness, which includes specific knowledge and skills. In this way, their personal readiness is strengthened while also contributing to a safer overall environment.
The aim is to design an effective educational system that, through a well-structured approach, can motivate individuals to actively engage with this issue. However, education itself may present a number of challenges, which can be addressed by drawing on modern trends. The article also discusses the advantages of applying artificial intelligence in the development of educational materials.

KEYWORDS: *Safety. Education. Educational materials. Modern trends. Artificial intelligence.*

ÚVOD

Fyzická bezpečnost je nedílnou součástí ochrany organizací i jednotlivců. Tradičně bývá spojována především s technickými opatřeními, jako jsou např. přístupové, zabezpečovací či kamerové systémy. Přestože tato složka hraje zásadní roli, skutečná úroveň bezpečnosti je vždy podmíněna také lidským faktorem. Žádná infrastruktura ani technologie nedokážou plně eliminovat rizika, pokud jedinci nedisponují potřebnými znalostmi, dovednostmi a schopností adekvátně reagovat na vzniklé situace. Navíc právě lidský faktor stojí často za tím, že jsou technické systémy obcházeny například z důvodu umístění nábytku před detektory pohybu apod. Článek se tedy bude zabývat problematikou vzdělávání, přičemž pozornost bude věnována také moderním trendům, které lze v tomto kontextu využívat.

Článek se nejprve zaměří na zdůvodnění, proč by se každý jedinec měl aktivně zabývat tématem fyzické bezpečnosti, a jak je toto téma obecně vnímáno v České republice. Následně představí běžné formy vzdělávání a upozorní na úskalí, která jsou s nimi spojena, včetně požadavků kladených na samotný proces vzdělávání. Článek následně nabídne možná řešení těchto úskalí a doporučí využití současných moderních trendů.

1. PROČ JE POTŘEBA VZDĚLÁVAT

Bezpečnost je součástí každodenního života každého člověka. I když se o ni stará celá řada subjektů, jako je organizace, ve které je jednotlivec zaměstnáván, jeho bezprostřední okolí a stát, je důležité, aby hlavní iniciativu za sebe převzal především samotný jedinec. V případě bezpečnostního incidentu není odborná pomoc k dispozici okamžitě a jedinec je tak právě často odkázán pouze sám na sebe. Musí proto spoléhat na svou vlastní připravenost, což zahrnuje určité znalosti a dovednosti. Z toho důvodu je tak nezbytné navrhnout efektivní systém vzdělávání v oblasti fyzické bezpečnosti, jenž prostřednictvím vhodně sestavené struktury dokáže v jednotlivcích vzbudit zájem o aktivní zapojení do této problematiky. Tímto způsobem se zvyšuje jejich osobní připravenost a zároveň se podporuje i spoluvytváření celkově bezpečnějšího prostředí. To se může týkat mnoha situací, od požáru až po fyzické napadení. Proto ačkoli je technické zabezpečení důležité, pouze samotné nestačí a je zásadní, aby byl v rámci fyzické bezpečnosti kladen důraz také i na vzdělávání osob.

Odborná veřejnost se v České republice začala významu vzdělávání v oblasti ochrany měkkých cílů věnovat již v roce 2017 v rámci vydání metodiky *Koncepce ochrany měkkých cílů pro roky 2017-2020*,

ve které se zmiňuje, že *„Dobré vyškolení pak plní svojí úlohu při útoku samotném, kdy může správná reakce zachránit mnoho lidských životů.“* (Ministerstvo vnitra České republiky, 2017). Ačkoli se tato metodika zabývá pouze ochranou měkkých cílů, její hlavní myšlenka má přesah do všech oblastí bezpečnosti. Kromě toho metodika popisovala také plán o vytvoření série vzdělávacích kurzů zajišťovaných Ministerstvem vnitra ČR, jejichž smyslem by bylo rozšíření základních znalostí v této problematice nejen představitelům měkkých cílů, ale také široké veřejnosti. Avšak důležitost tohoto tématu do povědomí široké veřejnosti přišlo především až po incidentu na *Filozofické fakultě Univerzity Karlovy* z 21. 12. 2023 (Deml, 2023).

Přitom právě osobní angažovanost každého jedince (ať už rozvojem znalostí, všímavosti či reakcí na podezřelé jevy) přispívá nejen k prevenci a včasné reakci, která může pomoci předejít eskalaci problémů, ale také k rozvoji a podpoře bezpečnostní kultury.

2. STANDARDNÍ MODEL A ZPŮSOBY VZDĚLÁVÁNÍ

Běžné vzdělávání probíhá obvykle při nástupu na pracoviště v rámci zákonem stanovených pravidelných školení, jako je tomu například u bezpečnosti a ochraně zdraví při práci, anebo dodatečně po tom, co dojde k určité události (např. pracovní úraz, útok aktivním útočníkem aj.) s cílem předejít opakování podobné situace v budoucnosti.

Školení však často probíhá pouze jednorázově formou teoretického výkladu vedeného odborným lektorem na stanoveném místě a v předem stanovený čas, přičemž po uplynutí stanovené doby školení končí a k dalšímu vzdělávání již nedochází. V mnoha případech se tak jedná pouze o teoretickou formu bez aktivního zapojení účastníků. V lepších případech jsou účastníci alespoň na závěr školení povinni absolvovat test sloužící k ověření jejich právě získaných znalostí. Takový formát školení bývá typický například pro bezpečnost a ochranu zdraví při práci nebo pro požární ochranu.

Ovšem existují i aktivnější způsoby vzdělávání, při kterých je vyžadována už i určitá míra aktivity samotné školené osoby. Mezi běžně využívané patří například:

- **stínování**, při kterém školená osoba pečlivě sleduje svého lektora a následně napodobuje jeho jednotlivé kroky,
- **counching** předávající znalosti a dovednosti v dlouhodobějším měřítku,
- **mentoring** v podobě lektora, jenž je školené osobě neustále na blízku a v případě potřeby podává pomocnou ruku,
- **counselling** kombinující pozici lektora a školené osoby, při níž se obě osoby pomocí vzájemného konzultování ovlivňují,
- **rotace práce,** při které dochází ke školení pomocí různých činností napříč různými odděleními z důvodu rozšíření obzoru i v jiných oblastech (Dobaka, 2022).

3. POTŘEBY A POŽADAVKY NA VZDĚLÁVÁNÍ

Kvalitní a úspěšné vzdělávání závisí na celé řadě faktorů. Klíčovou roli v tomto procesu hraje především lektor, který by měl být nejen odborníkem na danou problematiku, ale zároveň by měl disponovat i schopností předat své znalosti a zkušenosti účastníkům školení v kvalitní podobě. Zároveň je žádoucí, aby takovýmto vzděláváním prošel co největší počet osob – v ideálním případě všechny osoby, které se pohybují v daném prostředí či organizaci. To ovšem v praxi často znamená nutnost proškolit velmi vysoký počet účastníků, což sebou přináší řadu komplikací. Hlavním problémem bývá nejen omezená kapacita prostor, ve kterých se má školení konat, ale také časové možnosti jednotlivých účastníků. Neméně významným faktorem je však i časová dostupnost samotného lektora, který nemusí mít možnost opakovat školení tak často, aby se jej zúčastnily opravdu všechny osoby. Navíc ne každé školení je přímo vyžadováno zákonem. V takových případech je pak účast závislá pouze na dobrovolnosti osob, což může vést k výrazně nižšímu počtu proškolených osob a následně i k nižší efektivitě celého vzdělávacího systému.

Ačkoli se samozřejmě nabízí varianta online webináře nebo aby lektor celý obsah svého školení převedl do videonahrávky a vytvořil tak vzdělávací materiál, který by si následně osoby určené k proškolení mohly projít formou samostudia, je ovšem i tato možnost spojena s řadou problémů. Nejenže je velice

časově náročné připravit, natočit a následně zpracovat kvalitní výukový materiál, ale téměř nemožné je zajistit kvalitu řeči během celého záznamu stále na stejné úrovni, a to dokonce i v případě využití profesionálního dabéra. Kvalita lidského hlasového projevu není konzistentní z důvodu neustálého působení nejrůznějších fyziologických a psychologických vlivů na lektora (např. zadrhávání, využívání slovní vaty apod.). Stejné obtíže nastávají i v okamžiku, kdy je potřeba materiál aktualizovat. To bývá také velmi časově náročné, a to nejen v rámci postprodukce, která musí zajistit stejnou kvalitu nové části nahrávky oproti původnímu záznamu, ale je závislá také na dostupnosti samotného lektora. Protože v případě, že daný lektor nebude mít časový prostor na to vytvořit novou část nahrávky, přestože by byla aktualizace obsahu opravdu nezbytná, nezbývalo by nic jiného než připravit zcela nový vzdělávací materiál. Problémem však může být i samotné přimění účastníků, aby si nahrávku školení přehráli.

Mimo jiné není vhodné v rámci vzdělávání spoléhat na příliš obecné vzdělávací materiály, protože je potřeba daný obsah přizpůsobit nejen konkrétním podmínkám či situacím, které mohou být pro dané prostředí typické (například prosklené stěny, veřejný přístup do objektu, otevírání dveří směrem ven z místnosti aj.), ale také i případným změnám. To může postupem času nevyhnutelně vést právě k potřebě tyto materiály pravidelně obměňovat, aby zůstaly stále aktuální a použitelné.

4. ŘEŠENÍ

Řešením problémů zmíněných v předchozí kapitole je vytvoření promyšlené vzdělávací strategie. Je důležité klást důraz na vytvoření takové struktury vzdělávání, která by zahrnovala co nejvíc různorodých možností, ale zároveň nebyla příliš rozsáhlá. Jen tak si totiž dokáže zachovat přehlednost, funkčnost a v konečném důsledku především také i efektivitu.

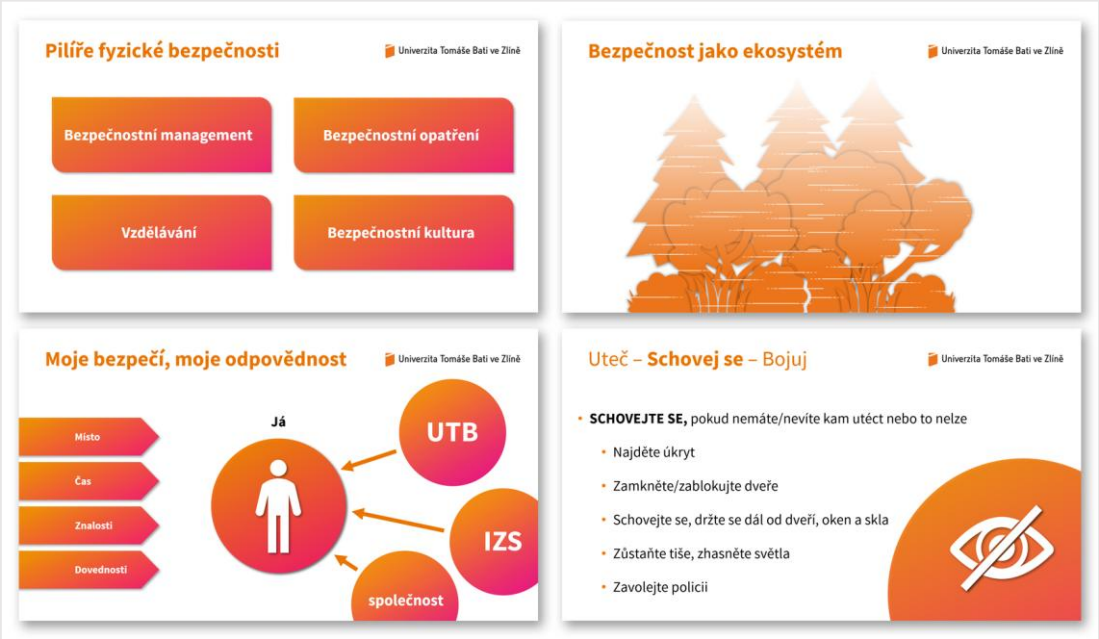
Taková struktura může obsahovat mnohem více prvků než jen pouhé klasické fyzické školení. Klíčovým prvkem celkové struktury jsou zejména vlastní vzdělávací materiály v podobě různých typů prezentací, které lze následně využívat mnoha způsoby (Mičulková, 2025). Tyto prezentace lze zpravidla rozdělit na dva hlavní typy – na plnou verzi a na zkrácenou verzi.

Plná verze prezentace představuje kompletní soubor informací a může tak posloužit k samostudiu, protože díky plnohodnotné formulaci textu, tedy informacím formulovaných v celých srozumitelných a snadno pochopitelných větách, není zapotřebí žádný dodatečný výklad lektora. Příklad takto koncipované prezentace je možné vidět na obrázku č. 1.

Obrázek 1 Příklad plné verze vzdělávací prezentace (Mičulková, 2025)

Zkrácená verze prezentace, jak už napovídá samotný název, je oproti plné variantě výrazně stručnější. Obsahuje totiž pouze klíčové informace, které jsou zpracovány do podoby záchytných bodů, které jsou dále rozvedeny mluveným projevem. Takovýto projev však nemusí mít nutně pouze podobu klasického prezenčního školení. Lze jej snadno nahradit digitální hlasovou nahrávkou, a to nejen namluvením samotného lektora, ale nabízí se zde také i možnost využití syntetického hlasu generovaného umělou inteligencí (více viz následující kapitola). Propojením prezentace s audio nahrávkou hlasového doprovodu pak vzniká vzdělávací video prezentace.

Na obrázku č. 2 je ukázka této zkrácené prezentace se záchytnými body místo plného textu. Klíčové je dbát na vizuální podobu celé prezentace, aby dokázala udržet pozornost školených osob. Je tak žádoucí, aby prezentace byla nejen obsahově atraktivní, ale i vizuálně poutavá. Je tak vhodné ji doplnit o nejrůznější grafické prvky v podobě obrázků, ilustrací, animací, efektů či přechodů mezi jednotlivými snímky.



Obrázek 2 Příklad zkrácená verze vzdělávací prezentace (Mičulková, 2025)

Zároveň je vhodné vytvořit více prezentací rozdělených podle jednotlivých témat vzdělávání, protože je potřeba myslet také na to, aby tyto vzdělávací materiály nebyly příliš dlouhé a dokázaly tak nejen udržet pozornost školených osob, ale současně v nich i vzbuzovat zájem o další dobrovolné rozvíjení znalostí. Přespříliš obsáhlé materiály by naopak mohly od vzdělání odrazovat. Délku prezentace je tak vhodné orientovat spíše podle času potřebného k jejich kompletnímu projití. Jako optimální se doporučuje časový rozsah okolo 15 až 30 minut právě z důvodu, že delší trvání vede k neschopnosti člověka udržet plnou pozornost a soustředění.

Tyto prezentace je poté ideální umístit na vhodné online úložiště, odkud si ji potenciální zájemci o vzdělání mohou kdykoli otevřít, případně stáhnout, a následně pomocí ní rozvíjet své znalosti odkudkoli a v jakýkoli čas. Tyto dvě popsané verze prezentací tak lze považovat za samonosný typ vzdělávacího materiálu, protože nevyžadují přítomnost odborného lektora, jelikož obsahují všechny nezbytné informace.

Ovšem i v opačném případě, kdy je zapojení lektora žádoucí, lze tyto prezentace efektivně využít. A to využitím zkrácené varianty, která poslouží jako doprovodná prezentace k mluvenému výkladu živého lektora (samozřejmě bez použití digitální nahrávky). Tuto prezentaci je tak možné využít jak při fyzickém školení, tak i při její alternativní variantě – během online webináře. Přičemž právě online webináře mohou oproti klasickému prezenčnímu školení představovat významnou výhodu zejména z hlediska

kapacitní flexibility. Odpadá zde nutnost zabývat se organizačními záležitostmi, jako je zajištění prostor pro konání školení a jeho kapacitní omezeností, díky čemuž lze jednorázově proškolit výrazně více osob. Na druhou stranu nevýhodou může být omezený nebo zcela chybějící osobní kontakt lektora s účastníky, který v prezenčním školení přirozeně posiluje interakci a zapojení.

Vzdělávací struktura však nemusí být omezena pouze na prezentace. V rámci některých témat se nabízí možnost doplnit školení také o pořádání praktických nácviků a kurzů, během kterých si účastníci mohou sami vyzkoušet aplikaci získaných znalostí z předchozích absolvovaných školení. To může vést k lepšímu zapamatování informací a zároveň k rozvoji schopností nezbytných pro jejich smysluplné uplatnění. Přičemž u některých témat, například první pomoci nebo barikádování v rámci procedury *„Uteč, schovej se, bojuj“* (USB) apod., je to dokonce přímo žádoucí. Dále lze vzdělávací strukturu obohatit o další podpůrné prvky, jako je například vytvoření samostatných webových stránek určených výhradně k ukládání a sdílení vzdělávacích materiálů.

Ty mohou zahrnovat:

- stručné přehledové materiály obsahující souhrn pouze klíčových informací, které umožní rychlou orientaci a okamžitou reakci bez nutnosti pročítat kompletní prezentaci,
- vlastní názorná videa natočená za účelem lepšího pochopení a doplnění určité problematiky,
- odkazy na materiály třetích stran, které mohou sloužit jako vhodné rozšiřující zdroje,
- a mnoho dalších prvků, které mohou podporovat různorodé styly učení.

Kromě všech zmíněných prvků je však nutné zohlednit také samotný zájem o toto vzdělávání. Nestačí vytvořit pouze promyšlenou a pestrou strukturu vzdělávání. Klíčová je rovněž i její samotná propagace. Proto je potřeba vytvořit takovou propagaci, která dokáže u potenciálních účastníků vzbudit zájem se v dané problematice dobrovolně a aktivně angažovat. Pro dosažení maximální efektivnosti je vhodné všechny jednotlivé prvky struktury a propagace zasadit do uceleného harmonogramu. Tím vznikne komplexní systém vzdělávání, který nejen udržuje kontinuitu, ale zároveň zajišťuje, že se vzdělávací proces stává systematickým a dlouhodobě funkčním. Odpadá tak i riziko zahlcení účastníků, ke kterému by mohlo dojít například při příliš častém školení s neustále se měnícími tématy prezentací.

5. VYUŽITELNOST MODERNÍCH TRENDŮ

Současné vzdělávací prostředí prochází dynamickými změnami, které jsou úzce spjaty s rozvojem moderních technologií a společenských trendů, mezi než patří například to, že si lidé zvykli na online formu v důsledku pandemie COVID-19, mnoho firem stále využívá home office a některé zaměstnance tak ani nemá na pracovišti atd. Ať už jde o digitalizaci, umělou inteligenci, personalizované vzdělávání či využití atraktivních interaktivních prvků, všechny tyto nástroje zásadně mění způsob, jakým jsou znalosti předávány, osvojovány a prakticky aplikovány. V dnešní době se tak otevírá stále více možností, jak efektivně využívat moderní trendy, jež by mohly být přínosné pro účel vzdělávání.

Mezi takové patří například následující:

- **rozšířená** a **virtuální realita** otevírající možnosti vzdělávání v situacích, které by byly v běžném prostředí obtížně realizovatlené nebo zcela neproveditelné,
- **umělá inteligence** umožňující personalizované vzdělávání,
- **gamifikace** doplňující učení o zajímavé herní prvky,
- **microlearning** a **nanolearning** představující rychlou formu předání vzdělávacího obsahu v časovém rozsahu do pěti a do dvou minut,
- **blended learning** propojující prvky klasického vzdělávání s distančními nástroji,
- **učení založené na scénářích**, **platformy pro sociální učení**, **reverzní mentorství** aj (Mičulková, 2025).

Využití umělé inteligence (AI) pro tvorbu vzdělávacích materiálů

Za jeden z nejefektivnějších moderních trendů dnešní doby, využívaných pro potřeby vzdělávání, lze považovat umělou inteligenci. Přestože existuje celá řada nástrojů využívajících AI, je vhodné zmínit technologii *Text to speech (TTS) (Text-to-speech, c2025)*, která umožňuje převádět psaný text do

syntetické řeči pomocí umělé inteligence. Ačkoli se jedná o uměle generovaný hlas, díky moderním systémům, které využívají neuronové sítě a strojové učení, je možné vytvářet kvalitní výstupy, které znějí velice plynule, přirozeně a jsou mnohdy k nerozeznání od lidského projevu. Aby však výsledná nahrávka dosahovala takové vysoké kvality, je zapotřebí zohlednit několik důležitých faktorů, jež mohou konečný efekt značně ovlivnit.

První z těchto faktorů nastává při zohlednění výslovnosti (Mičulková, 2025). Každý scénář určený pro generování hlasu je nutné psát foneticky, jelikož AI převádí text přesně tak, jak je uveden ve scénáři. V praxi to znamená, že aby se dosáhlo požadovaného zvukového výsledku, je potřeba v určitých případech text záměrně zapisovat s chybným pravopisem, gramatikou, interpunkcí nebo diakritikou. Jako ilustrativní příklad lze uvést zkratku názvu *Univerzita Tomáše Bati*, která se správně zapisuje jako *„UTB“.* Aby však byla vygenerována správná výslovnost, je nutné ji ve scénáři zapsat foneticky, tedy jako *„útébé“*. Neméně důležitým aspektem je také správné značení pauz, pomocí kterého jsou poté v mluveném projevu zachovány přirozené rytmy a intonace. V některých případech lze tohoto efektu docílit pouze prostřednictvím špatného použití interpunkčních znamének, tedy vložit je i v místech, kde správně nepatří.

Dále je nutné věnovat pozornost správnému výběru hlasu, při kterém je možné ovlivnit také hloubku hlasu, rychlost projevu, zvolit mužský/ženský hlas apod., tak, aby odpovídal zamýšlenému účelu a působil přirozeně v kontextu daného vzdělávacího materiálu. Různé zabarvení hlasu se hodí pro různé situace – například jiný typ hlasu je vhodný pro odborný výklad, jiný zase pro motivační obsah. V rámci tvorby vzdělávacích materiálů je tak klíčové vybírat takové hlasy, které dokážou udržet pozornost posluchače po celou dobu výkladu. Z toho důvodu je lepší se vyhnout hlasům, které znějí příliš tiše, pomalu anebo monotónně, protože mohou u posluchače vyvolat únavu a vést k tomu, že postupně přestane věnovat výkladu plnou pozornost.

Ačkoli je nezbytné brát v úvahu určité faktory, využití této technologie při tvorbě vzdělávacích materiálů má spoustu výhod. Mnohé problémy spojené s požadavky a nároky na vzdělávání, jež byly zmíněny v 3. kapitole, lze vyřešit právě prostřednictvím umělé inteligence, která v určitých případech může dokonce zcela nahradit živého lektora, což v konečném důsledku může být i finančně výhodnější, přestože jde o placenou technologii. Zejména při vytváření materiálů obsahující mluvený projev. Nejen, že je tvorba audio nahrávky pomocí syntetické řečí mnohem rychlejší a flexibilnější než nahrávání skutečným člověkem, ale zároveň je také i mnohem kvalitnější, protože na rozdíl od lidského hlasu nepodléhá žádným fyziologickým ani psychologickým faktorům. Každý generovaný výstup si tak udržuje stejné hlasové charakteristiky (barvu hlasu, hlasitost, tempo, intonaci), pokud nedojde k cílené úpravě jednotlivých parametrů. V případě nutnosti jakékoli aktualizace vzdělávacích materiálů pak stačí nahradit konkrétní část novou verzí, aniž by byl patrný jakýkoli rozdíl. Tím odpadá nutnost vytvářet vzdělávací materiál zcela znovu, přičemž veškeré úpravy lze provádět kdykoli a odkudkoli.

Celkově tak lze říci, že využití této technologie vede k významné úspoře finančních prostředků i času, a také k zajištění konstantní kvality. Zároveň výrazně zjednodušuje případné úpravy a aktualizace. Na rozdíl od zapojení skutečného lidského lektora je tak vzdělávací prezentace závislá výhradně na obsahu, nikoli na osobních faktorech či momentálním rozpoložení lektora, které by jinak mohli průběh a efektivitu školení jakýmkoli způsobem negativně ovlivnit. Lze tak snadno připravit vzdělávací materiály určené k samostudiu, které mohou plnohodnotně nahradit omezení spojená s tradičním prezenčním školením. Nyní už zbývá pouze přesvědčit účastníky, aby si tyto materiály skutečně prostudovali.

ZÁVER

Cílem článku je zdůraznit širší veřejnosti důležitost vzdělávání v oblasti fyzické bezpečnosti. Zvláštní důraz je přitom kladen na potřebu vytvářet systematické vzdělávání založené na pestré a vyvážené vzdělávací struktuře a nebát se pro tyto účely využívat i moderních trendů. Tyto nástroje totiž mohou výrazně zvýšit efektivitu vzdělávání a stát se užitečnou oporou jak při tvorbě, tak i při samotném využívání vzdělávacích materiálů.

LITERATÚRA

Deml, O. (2023). *Střelba na pražské filozofické fakultě má čtrnáct obětí, 25 lidí je zraněných*. ČT24. Retrieved September 29, 2025, from https://ct24.ceskatelevize.cz/clanek/domaci/sledujte-policejni-prezident-a-ministr-vnitra-ke-strelbe-na-karlove-univerzite-344375

Dobaka, E. (2022). *Aktuální trendy využívání digitálních nástrojů ve firemním vzdělávání* [Rigorózní práce, Univerzita Karlova]. https://dspace.cuni.cz/bitstream/handle/20.500.11956/179246/150058188.pdf

Koncepce ochrany měkkých cílů pro roky 2017-2020. (2017). Ministerstvo vnitra České republiky. Retrieved September 29, 2025, from https://www.mvcr.cz/soubor/koncepce-ochrany-mekkych-cilu-pro-2017-2020-pdf.aspx

Mičulková, T. (2025). *Informační a vzdělávací strategie fyzické bezpečnosti UTB* [Diplomová práce]. Univerzita Tomáše Bati ve Zlíně.

Text-to-speech. (c2025). NVIDIA. Retrieved September 29, 2025, from https://www.nvidia.com/en-us/glossary/text-to-speech/

Ing. Tereza Mičulková

Ústav bezpečnostního inženýrství, Univerzita Tomáše Bati ve Zlíně

e-mail: t_miculkova@utb.cz

Ing. Lukáš Kotek

Ústav bezpečnostního inženýrství, Univerzita Tomáše Bati ve Zlíně

e-mail: kotek@utb.cz

KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2025.2.181-183
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online

PREDSTAVENIE PROJEKTU APVV-24-0153: VYTVORENIE DÁTOVÉHO MODELU A JEHO IMPLEMENTÁCIA DO GEOGRAFICKÝCH INFORMAČNÝCH SYSTÉMOV NA ZVÝŠENIE PRIPRAVENOSTI VEREJNEJ SPRÁVY ZVLÁDAŤ MIMORIADNE UDALOSTI

INTRODUCTION OF THE APVV PROJECT APVV-24-0153: DEVELOPMENT OF A DATA MODEL AND ITS IMPLEMENTATION INTO GEOGRAPHIC INFORMATION SYSTEMS TO ENHANCE THE PREPAREDNESS OF PUBLIC ADMINISTRATION FOR MANAGING EMERGENCY EVENTS

JOZEF KUBÁS

ABSTRACT: *A crisis management system is employed to ensure the protection of property, health, and lives. The required level of safety can be achieved through measures that prevent emergency events. If an emergency event occurs, the system should be prepared and apply appropriate procedures to address it. Subsequently, it must be capable of mitigating its negative impacts. To ensure the protection of the population, the first step is to assess the risks affecting individual elements and the monitored area. Therefore, it is essential to have relevant data and information about the area and to use them effectively. The project focuses on analysing the information needs of crisis management in the field of territorial risk assessment and their further usability within the data model. It enables the implementation of data management, which focuses on creating a data model and integrating it into geographic information systems to enhance the preparedness of public administration authorities. Such a data model within geographic information systems allows for the proper assessment of the negative impact of an emergency event on the affected area and the options for effective resolution.*

KEYWORDS: *Security, Civil protection, Crisis management, GIS, Data model, Emergency event, Disaster, Public administration*

ÚVOD

Mapovanie rizík je proces zobrazenia rizík, ich rozsahu, následkov, zraniteľnosti alebo pripravenosti prostredníctvom priestorových údajov. Výsledným produktom je mapa rizika, ktorá môže obsahovať rôzne štatistiky a informácie pre krízových manažérov. Mapy rizika je možné využívať v tlačenej verzii alebo pomocou softvérových nástrojov a webových aplikácií. Tlačené verzie sú používané najmä v dokumentoch krízového riadenia. Príkladom takéhoto dokumentu môže byť „analýza územia z hľadiska vzniku možných mimoriadnych udalostí“ a „plány ochrany obyvateľstva“, ktoré sa vytvárajú na základe analýzy. Na Slovensku sa aktuálne analýzy územia spracovávajú na neaktuálnych mapách a nereflektujú všetky dáta a potreby územia. Na základe analýzy územia sa vypracováva plán ochrany obyvateľstva, ktorý ale, ak nemá relevantné dáta z analýz územia, nemôže byť úplne správny. Ministerstvo vnútra SR (ďalej MV SR) v oblasti krízového riadenia a posudzovania rizík nemá žiadne informačné systémy. Práve novo vytvorený dátový model a proces dátového manažmentu by bolo možné využívať ako takýto informačný systém, avšak je potrebné aby reflektoval na aktuálne nedostatky. Novo navrhnutý dátový model a proces dátového manažmentu by bol koncipovaný tak, aby ako celok a zároveň jeho jednotlivé časti bolo možné využiť aj v iných štátoch. Výsledný dátový model a proces riadenia údajov tak umožní zvýšiť pripravenosť na mimoriadne udalosti nielen v podmienkach Slovenskej republiky ale i v ďalších štátoch, čo reflektuje na požiadavky Sendai. Vzhľadom na to, že mimoriadne udalosti môžu vplývať na viacero štátov existuje predpoklad, že okolité štáty by využili výsledky projektu alebo sa nimi inšpirovali. Aplikovanie výsledkov projektu do praxe bude mať pozitívny spoločenský dopad s dôrazom na životy, zdravie a majetok.Projekt sa zameriava na implementáciu efektívneho dátového manažmentu v celom cykle krízového riadenia, pričom hlavným dôrazom je proces posudzovania rizík územia. Účelom je poskytnúť verejnej správe nástroje a metodické postupy na zlepšenie pripravenosti na mimoriadne udalosti.

1. CIELE A PRÍNOSY PROJEKTU

Hlavným cieľom projektu je zavedenie dátového manažmentu v cykle krízového riadenia s dôrazom na proces posudzovania rizík územia pre potreby verejnej správy na zvýšenie pripravenosti na mimoriadne udalosti. Hlavný cieľ je precizovaný do nasledujúcich parciálnych cieľov:

1. Analýza informačných potrieb krízového manažmentu s dôrazom na fázu posudzovania rizík.
2. Navrhnutie štruktúry dátového modelu pre potreby posudzovania rizík.
3. Vytvorenie metodického postupu riadenia údajov pre potreby dátového modelu
4. Vytvorenie zloženého indexu a metodiky hodnotenia územnej odolnosti
5. Vytvorenie digitálnych máp územnej odolnosti pomocou dátového modelu a GIS
6. Vytvorenie metodiky využitia dátového modelu a mapovania územnej odolnosti pre potreby krízových manažérov vo verejnej správe
7. Implementácia digitálnych máp územnej odolnosti do dokumentov krízového manažmentu
8. Publikovanie vedeckej monografie zameranej na využitie dátového modelu a GIS v krízovom manažment.

Predpokladané prínosy nadväzujú na stanovený hlavný cieľ a parciálne ciele vedeckého projektu. Riešenie projektu vytvára predpoklad na zvýšenie pripravenosti miest a obcí voči mimoriadnym udalostiam, čím sa zvyšuje ich celková úroveň odolnosti. Vlastné prínosy je možné rozdeliť do dvoch skupín a to na teoretické a praktické. Za jeden z hlavných teoretických prínosov je možné považovať spracovanie prehľadného metodického postupu tvorby a využitia dátového modelu pre potreby krízového manažmentu a GIS v rámci prípravy dokumentov krízového riadenia. Zároveň budú spracované rôzne prístupy využitia priestorových údajov pomocou softvérových nástrojov pre potreby analýzy rizikových faktorov územia. Predpokladané teoretické prínosy je možné zhrnúť nasledovne:

- prehľadné zosumarizovanie dostupných dát a zdrojov vhodných na detailnú analýzu územia s ohľadom na ohrozenia majetku, životného prostredia a obyvateľov,
- prehľadné spracovanie aktuálnych teoretických základov pre mapovanie rizík územia s využitím GIS,
- rozšírenie poznatkovej bázy charakteristík územia a ich vplyvu na odolnosť,
- prehľadné spracovanie všeobecne záväzných právnych predpisov a technických noriem v oblasti posudzovania rizík a využívania informačných systémov,
- rozšírenie poznatkovej bázy skúmanej problematiky odolnosti územia,
- identifikovanie nedostatkov a navrhnutie odporúčaní v oblasti tvorby dokumentov krízového riadenia,
- spracovanie návrhu dátového modelu pre spracovanie dostupných dát a ich možné využitie v softvérovej podpore a GIS,
- využitie pre pedagogickú činnosť, ako aj pre ďalšiu vedecko-výskumnú činnosť.

Významným praktickým prínosom bude vytvorenie procesného a dátového modelu, ktorý bude možné využiť v procese posudzovania rizík územia a jeho implementovanie do GIS. To umožní pracovníkom obcí a okresných úradov sekcie krízového riadenia spracovanie priestorových údajov, ich analýzu a tvorbu rizikových máp. Ďalším dôležitým prínosom bude navrhnutie spôsobu využitia analýz a máp rizika pri tvorbe krízovej dokumentácie, čo umožní dosiahnuť vyššiu úroveň odolnosti v obciach a mestách. Tieto výstupy umožnia efektívne využitie síl a prostriedkov na analyzovanom území v súlade s novo vytvoreným indexom územnej odolnosti. Ako dôležitý prínos bude schopnosť využitia dátového manažmentu v prípade vzniku mimoriadnej udalosti, nakoľko bude možné správne aplikovať riešenie, ktoré bude reflektovať aktuálnu náročnosť udalosti. Predpokladané praktické prínosy je možné zhrnúť nasledovne:

- vytvorenie dátového modelu pre potreby posudzovania rizík územia,
- návrh dátového manažmentu pre potreby posudzovania rizík územia (metodický postup),
- posudzovanie rizík vybraného územia s využitím GIS,
- vytvorenie máp rizika a ich implementácia do dokumentov krízového manažmentu konkrétneho územia,
- vytvorenie indexu odolnosti územia potrebného na efektívnu prípravu na mimoriadne udalosti,
- zvýšenie pripravenosti územia obce, okresu a štátu na mimoriadne udalosti,

- zvýšenie efektívnosti zvládania mimoriadnych udalostí s využitím, dátového manažmentu,
- vytvorenie metodiky využitia dátového modelu a mapovania rizík pre potreby krízových manažérov.

ZÁVER

Za krízové riadenie a civilnú ochranu na Slovenku zodpovedá MV SR prostredníctvom Sekcie krízového riadenia. Sekcia krízového riadenia je odborným útvarom MV SR pre integrovaný záchranný systém, civilnú ochranu, krízové riadenie, civilné núdzové plánovanie, ochranu kritickej infraštruktúry, hospodársku mobilizáciu, správu materiálu civilnej ochrany a humanitárnu pomoc. MV SR stanovuje náležitosti, povinnosti a úlohy ďalších subjektov. Z pohľadu hierarchie krízového riadenia MV SR riadi civilnú ochranu a krízové riadenie. Na nižšej úrovni je okresný úrad v sídle kraja, okresný úrad a následne obec. Prijatie výsledkov na základe zmluvy o budúcej zmluve, sekciou krízového riadenia MV SR, okresným úradom v sídle kraja Žilina a mestom Žilina, zabezpečí efektívne implementovanie výsledkov projektu. Z ticho odberateľov výstupov je najdôležitejšia práve sekcia krízového riadenia, nakoľko jednotlivé výstupy projektu sprístupni ako odporúčacie alebo záväzne podľa uváženia pod všetky subjekty, ktoré sú na nižšej úrovni.

Výstupy projektu majú ambíciu zlepšovať problematiku aj v zahraničí. Jednotlivé štáty v prípade tvorby strategických dokumentov, metodík ale aj iných výstupov sa často inšpirujú zo skúsenosti dobrej praxe v zahraničí alebo iných dostupných materiálov. Slovenská republika je súčasťou medzinárodných organizácií krízového manažmentu a spolupracuje s okolitými a ďalšími štátmi na tejto úrovne. Práve preto prijatie výsledkov projektu a ich zverejnenie na oficiálnych stránkach ministerstva rôznych medzi štátnych stretnutiach jen vhodný spôsob ako dať k dispozícií výsledky projektu na využitie aj iným štátom. Zároveň zodpovedný riešiteľ a aj ďalší riešitelia spolupracujú o odborníkmi a organizáciami riešiace podobné problematiky na Slovensku a v zahraničí. Táto spolupráca bude využívaná počas tvorby výstupov a zároveň zahraničné subjekty budú mať povedomie o čiastkových výstupoch, budú mať možnosť pripomienkovať spracovanie projektu tak aby bol univerzálne využitý v zahraničí a zároveň môžu tieto výsledky využiť v plnej miere alebo nadviazať na ne v ich ďalšej činnosti.

POĎAKOVANIE

Táto práca bola podporená Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-24-0153 s názvom Vytvorenie dátového modelu a jeho implementácia do geografických informačných systémov na zvýšenie pripravenosti verejnej správy zvládať mimoriadne udalosti.

Jozef Kubás, doc. Ing., PhD.

Katedra krízového manažmentu, Fakulta bezpečnostného inžinierstva, Žilisnká univerzita v Žiline, Univerzitná 8215/1, 010 26 Žilina,Slovensko

email: jozef.kubas@uniza.sk

KRÍZOVÝ MANAŽMENT
DOI
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

NÁZOV PRÍSPEVKU

NÁZOV PRÍSPEVKU V ANGLICKOM JAZYKU

MENO A PRIEZVISKO AUTORA, MENO A PRIEZVISKO AUTORA

ABSTRACT: *Nahraďte tento text anotáciou **v anglickom jazyku (britská angličtina)** v rozsahu 5-10 riadkov. Abstrakt oboznamuje s obsahom článku. Autor v ňom uvádza aj **aké ciele a postupy použil** a **k akým záverom** dospel. Odporúča sa v dĺžke 100 - 250 slov.*
(voľný riadok Arial 8)
KEYWORDS: *Nahraďte tento text kľúčovými slovami v anglickom jazyku v rozsahu 3 až 5 výrazov. Každý výraz písať veľkým začiatočným písmenom a ukončiť bodkou.*
(voľný riadok Arial 8)

ÚVOD (ARIAL 11)

Elektronickú formu tohto vzoru nájdete na stránke https://www.fbi.uniza.sk/stranka/sablona-clanku. Vlastný text píšte v Arial 10, bez odsadenia prvého riadku v odseku, odseky oddeliť jedným voľným riadkom (písmo Arial 10). Text zarovnať do bloku.

1. KAPITOLA (ARIAL 11)

Používať jednoúrovňové alebo viacúrovňové automatické číslovanie kapitol. V texte používať jednoduché odrážky zarovnané na ľavý okraj alebo viacúrovňové odrážky rovnakého typu odlíšené veľkosťou odrážky:

- xxxx,
- xxxx,
- xxxx.

(voľný riadok Arial 10)

Na citácie použitej literatúry používajte túto formu (Autor, rok).

Tabuľka 1 Názov tabuľky (Autor & Autor, rok)

Názov stĺpca	Parameter 1	Parameter 2
Text, text, text...	Text – číslo	06.02.2020
Text, text, text...	Text – číslo	06.02.2020

(voľný riadok Arial 10)

Číslo a názov tabuľky (Tabuľka 1) písať podľa vyššie uvedeného vzoru. Za číslo tabuľky bodku nedávať. Pred číslom tabuľky dávať pevnú medzeru (ctrl-shift-medzerník). Odkaz na tabuľku v texte uvádzať ako odkaz na tabuľku 1. Šírku tabuľky prispôsobiť šírke okna. Doplniť typ a veľkosť písma v tabuľke. Hodnoty v tabuľkách nesmú byť prepojené na iné programy (napr. Excel).

(voľný riadok Arial 10)

Text, text...

(voľný riadok Arial 10)

Vzorce písať cez editor vzorcov.

(voľný riadok Arial 10)

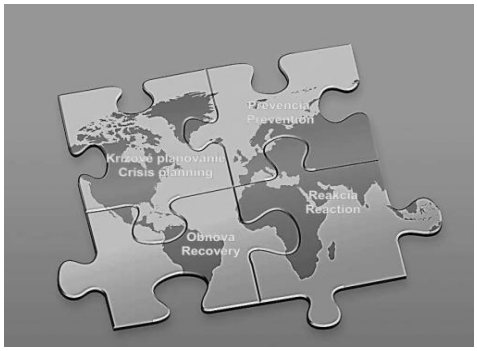
$$S = \pi . r^2 \quad (1)$$

Kde: S – obsah,
π – konštanta,
r – polomer.

(voľný riadok Arial 10)

Text, text....

(voľný riadok Arial 10)



Obrázok 1 Názov obrázku (Autor, Autor & Autor, rok)

Číslo a názov obrázku písať podľa vyššie uvedeného vzoru. Pred a za číslom obrázku dávať pevnú medzeru (ctrl-shift-medzerník). Názov – text pod obrázkom – začíname písať vždy s veľkým písmenom ako na začiatku vety. Na konci textu bodku nedávame. Odkaz na obrázok v texte uvádzať ako odkaz na obrázok 1. Veľkosť obrázka nesmie presiahnúť okraje. Obrázok je zarovnaný na stred. Doplniť kvalitu. Obrázky a grafy nesmú mať prepojenie na iné programy (napr. Excel).

ZÁVER (ARIAL 11)

Autor zodpovedá za vecnú a jazykovú správnosť príspevku. Odporúčaná štruktúra príspevku vychádza z modelu IMRaD (IMRD).

POĎAKOVANIE (ARIAL 11)

Projekt, financovanie, autorskému kolektívu a pod.

LITERATÚRA (ARIAL 11)

Blakey, N., Guinea, S., & Saghafi, F. (2017). Transforming undergraduate nursing curriculum by aligning models of clinical reasoning through simulation. In R. Walker, & S. Bedford (Eds.), HERDSA 2017 Conference: Research and Development in Higher Education: Curriculum Transformation (pp. 25-37). Hammondville, NSW: Higher Education Research and Development Society of Australasia. Retrieved from http://www.herdsa.org.au/research-and-development-higher-education-vol-40-25 (článok z konferencie)

Carey, B. (2019, March 22). Can we get better at forgetting? The New York Times. https://www.nytimes.com/2019/03/22/health/memory-forgetting-psychology.html (článok z novín)

Fagan, J. (2019, March 25). Nursing clinical brain. OER Commons. Retrieved September 17, 2019, from https://www.oercommons.org/authoring/53029-nursing-clinical-brain/view (web stránka)

Grady, J. S., Her, M., Moreno, G., Perez, C., & Yelinek, J. (2019). Emotions in storybooks: A comparison of storybooks that represent ethnic and racial groups in the United States. *Psychology of Popular Media Culture*, *8*(3), 207–217. https://doi.org/10.1037/ppm0000185 (časopis)

Sapolsky, R. M. (2017). Behave: The biology of humans at our best and worst. Penguin Books. (kniha)

Zákon č. 131/2002 Z. z. o vysokých školách a o zmene a doplnení niektorých zákonov. (zákon)

Zoznam literatúry zoradiť abecedne. Pre viac informácií postupujte podľa citačného formátu APA - https://apastyle.apa.org/style-grammar-guidelines/references/examples (Arial 8,5)

(voľný riadok 10)

Meno a priezvisko autora - 1, tituly

Kontaktné údaje (pracovisko, adresa,)

e-mail:

Meno a priezvisko autora - 2, tituly

Kontaktné údaje (pracovisko, adresa,)

e-mail:

POSTUP NA PRIJÍMANIE ČLÁNOV DO ČASOPISU „KRÍZOVÝ MANAŽMENT“

1. Redakcia prijíma príspevky doteraz nepublikované, v textovom editore MS Word vo formáte docx. v rozsahu max. 10 strán, bez číslovania, upravené podľa pokynov na písanie článkov (šablóna článku).

2. Príspevok prosíme poslať e-mailom na adresu: ***michal.ballay@uniza.sk*** alebo doručiť poštou na CD na adresu: **Fakulta bezpečnostného inžinierstva Žilinskej univerzity, redakcia časopisu KRÍZOVÝ MANAŽMENT, Ulica 1.mája 32, 010 26 Žilina, Slovakia**.

3. Príspevky, ktorých úprava nesplní požiadavky redakcie, alebo budú v rozpore s etickými zásadami na publikovanie, nebudú redakciou prijaté. Prijaté rukopisy budú vytlačené bez poplatku, v čiernobielom prevedení. Príspevky nie sú honorované.

4. Redakcia prijíma príspevky písané v anglickom, českom alebo slovenskom jazyku.

5. Redakcia si vyhradzuje právo zaradiť články na návrh oponentov do vedeckej alebo informatívnej časti časopisu.

6. Na hodnotenie článkov doručených redakčnej rade sa používa systém ***Double-blind peer review***[1]. Rozhodovanie o publikovaní článkov prebieha vo viacerých kolách:
   - V prvom kole sú články posúdené po formálnej stránke technickou redakciou časopisu. Pokiaľ články nespĺňajú formálne požiadavky sú autorom vrátené na prepracovanie.
   - V druhom kole stanoví predseda redakčnej rady anonymných oponentov, ktorými sú nezávislí odborníci z odboru do ktorého články patria.
   - V treťom kole vypracujú oponenti posudky, v ktorých odporučia publikovanie (nepublikovanie) článkov. Zároveň odporučia zaradenie článkov do vedeckej alebo informačnej časti časopisu. Publikovanie článkov môžu podmieniť úpravami. Posudky sú archivované technickou redakciou časopisu.
   - V štvrtom kole doručí technická redakcia posudky tým autorom, ktorých články vyžadujú dopracovanie a požiada autora o dopracovanie článku.
   - V piatom kole odsúhlasí redakčná rada štruktúru, zaradenie a počet článkov, ktoré budú zverejnené v nasledujúcom čísle časopisu.

[1] *Double-blind peer review* je systém posudzovania, založený na hodnotení nezávislými odborníkmi.

OPONENTSKÝ POSUDOK ČLÁNKU DO ČASOPISU KRÍZOVÝ MANAŽMENT

Elektronická forma posudku je vyhotovené ako formulár, na pohyb vo formulári používajte tabelátor.
VZOR

Názov článku:

Tento posudok bude poskytnutý autorovi za účelom prípadnej úpravy článku bez uvedenia oponenta. Redakčná rada časopisu žiada oponentov o hodnotenie príspevku v nasledujúcej tabuľkovej a textovej časti. Pripomienky, návrhy a odporúčania možno vyznačiť priamo v texte článku alebo uviesť v bode 5 a poslať s posudkom. Technický redaktor poskytne článok s poznámkami autorom.

Hodnotenie článku (zaškrtnite zodpovedajúce možnosti)

1. Odborná úroveň

a) aktuálnosť témy
- ☐ téma nová,
- ☐ téma bežná, ale aktuálna,
- ☐ téma neaktuálna,
- ☐ téma nekorešponduje so zameraním časopisu,

b) vedecké poznatky
- ☐ článok obsahuje aplikáciu vedeckých metód,
- ☐ článok obsahuje nové vedecké poznatky,
- ☐ článok obsahuje nové odborné poznatky,
- ☐ článok obsahuje nové informácie,
- ☐ článok neobsahuje nové poznatky alebo informácie,

b) citácie
- ☐ pôvod prevzatých častí sa cituje v súlade s normou,
- ☐ pôvod prevzatých častí sa cituje nedostatočne alebo vôbec.

2. Úroveň spracovania
- ☐ článok je zostavený prehľadne, logicky a zrozumiteľne,
- ☐ prehľadnosť a zrozumiteľnosť článku je priemerná,
- ☐ článok je nevhodne usporiadaný a málo zrozumiteľný.

a) jazyková úroveň	☐ výborná,	☐ priemerná,	☐ nevyhovujúca
b) odborná terminológia	☐ správna,	☐ drobné nedôslednosti,	☐ závažné nedostatky,
c) grafická úroveň obrázkov a grafov	☐ výborná,	☐ priemerná,	☐ nevyhovujúca.

3. Odporúčanie oponenta
- ☐ odporúčam článok publikovať v pôvodnej verzii,
- ☐ odporúčam článok publikovať po odstránení uvedených pripomienok a nedostatkov,
- ☐ článok nie je vhodný na publikovanie.

- ☐ odporúčam článok zaradiť do vedeckej časti časopisu,
- ☐ odporúčam článok zaradiť do odbornej časti časopisu,
- ☐ odporúčam článok zaradiť medzi informácie.

4. Pripomienky, návrhy a odporúčania oponenta

Prosíme uviesť krátky komentár k vyššie uvedeným bodom hodnotenia. Pripomienky, návrhy a odporúčania možno vyznačiť priamo v texte článku a poslať s posudkom. Technický redaktor poskytne článok s poznámkami oponenta autorom.

Táto časť posudku sa autorovi článku neposkytuje

Dátum: Podpis oponenta: _____

PROCEDURE FOR SUBMITTING ARTICLES
'CRISIS MANAGEMENT' JOURNAL

The editorial board accepts only previously unpublished papers, written in text editor MS Word within max. 10 – even number of pages, without page numbering, processed as per the directions for writing articles.

1. The paper should be sent by e-mail to: ***michal.ballay@uniza.sk*** or sent by post on a CD, USB to the address **Fakulta bezpečnostného inžinierstva Žilinskej university v Žiline, redakcia časopisu KRÍZOVÝ MANAŽMENT, Ulica 1. mája 32, 010 26 Žilina, Slovakia**

2. Papers, which do not fulfil the requirements of the editorial board or are in conflict with the ethical principles of publishing, will not be accepted. Accepted manuscripts will be printed free of charge, in monochrome. Papers are not remunerated.

3. The editorial board accepts papers in the English, Czech and Slovak language.

4. The editorial board reserves the right to move papers to the scientific, professional and informative parts of the journal.

5. For reviewing of articles received by the editorial board a peer-review system is in place.
   The decision making on publishing of a paper is done in the following stages:
   - In the first stage, the paper is reviewed by the technical board. If the paper does not meet the formal requirements it is returned to the authors for revision.
   - In the second stage, the chairman of the editorial board assigns anonymous peer-reviewers who are independent experts from the field in which the paper belongs to.
   - In the third stage, the peer-reviewers review the paper and recommend publishing or rejection of the paper. They also recommend the inclusion of the paper into the scientific, professional, or informative part of the journal. Publishing of the paper may be conditional, requiring the recommended modifications. Reviews are archived by the technical board of the journal.
   - In the fourth stage, the technical board delivers the reviews to the authors, whose papers require further modifications or finalization, and requests the author to implement the recommendations.
   - In the fifth stage, the editorial board approves the structure, classification and number of papers which will be published in the next issue of the journal.

PAPER REVIEW REPORT
FOR CRISIS MANAGEMENT JOURNAL

The electronic form of the review template is designed as a form; use Tab for navigation.
TEMPLATE

Title of paper:

This report will be made available to the author for any corrections or modifications of the paper without stating the name of the reviewer. The editorial board kindly asks reviewers to use the fields below for the paper evaluation. Comments, suggestions and recommendations may be either marked directly in the text of the paper or specified in Part 4. The Technical Editor will provide a paper with reviewer's comments to the authors.

Paper rating (check the appropriate option)

1. Professional level

a) Topicality
- ☐ new topic,
- ☐ common topic, but actual,
- ☐ outdated topic,
- ☐ topic is beyond the scope of the journal,

b) Scientific value
- ☐ paper applies scientific methods,
- ☐ paper contains new scientific knowledge,
- ☐ paper contains new expert knowledge,
- ☐ paper contains new information,
- ☐ paper does not contain new knowledge or information.

c) Citations
- ☐ sources of citations are referenced in accordance with the standard,
- ☐ sources of citations are referenced poorly or not at all

2. Quality of processing

- ☐ The paper is structured intelligibly, logically and clearly.
- ☐ Intelligibility and clarity of the article is on an average level.
- ☐ The paper is inappropriately structured and difficult to understand.

a) Language level	☐ excellent,	☐ average,	☐ inappropriate
b) Terminology	☐ correct,	☐ minor inconsistencies,	☐ serious shortcomings,
c) Layout of graphs and figures	☐ excellent,	☐ average,	☐ unsatisfactory.

4. Reviewer's recommendations

- ☐ I recommend publishing the original version of the paper.
- ☐ I recommend publishing the paper with minor corrections.
- ☐ The paper is not suitable for publishing.

- ☐ I recommend the paper to be included in the scientific part of the journal.
- ☐ I recommend the paper to be included in the professional part of the journal.
- ☐ I recommend the paper to be included in the section Information.

5. Comments, suggestions and further recommendations of the reviewer

Please, provide brief comments on the above points. Comments, suggestions, and recommendations can be directly marked in the text and sent with a review. The Technical Editor will provide a paper with reviewer´s comments to the paper's author.

This part of the report is not provided to the author of the paper.

Date: Signature of reviewer: _____