Hrozby 21. století a jejich vliv na společnost a její obyvatele

Bc. Terézia Valeková

Diplomová práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Terézia Valeková**
Osobní číslo:	**L21212**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Hrozby 21. století a jejich vliv na společnost a její obyvatele**

Zásady pro vypracování

1. Charakterizujte bezpečnostní prostředí (hrozba, riziko, zranitelnost, opatření) a mimořádné události.
2. Proveďte analýzu a popis vybraných hrozeb (terorismus, kybernetické hrozby, hybridní hrozby, organizovaný zločin, migrace, přírodní hrozby a epidemie).
3. Implementujte analýzu vybraných hrozeb pomocí metod analýzy rizik.
4. Na základě dosažených výsledků analýzy proveďte vyhodnocení.

Forma zpracování diplomové práce: **tištěná/elektronická**
Jazyk zpracování: **Slovenština**

Seznam doporučené literatury:

1. FRÜHLING, Stephan a Andrew O'NEIL. *Alliances, Nucear Weapons and Escalation*. Canberra: ANU Press, 2021. ISBN 978-1-76046-491-2.
2. JUŘÍČEK, Ludvík a Petr ROŽŇÁK. *Bezpečnost, hrozby a rizika v 21. století*. Ostrava: Key Publishing, 2014. ISBN 978-80--7418-201-3.
3. MAREŠ, Miroslav, Jaroslav REKTOŘÍK a Jan ŠELEŠOVSKÝ. *Krizový management: případové bezpečnostní studie*. Praha: Ekopress, 2013. ISBN 978-80-86929-92-7.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Lukáš Pavlík, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2022**
Termín odevzdání diplomové práce: **28. dubna 2023**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2022

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 28. 4. 2023

Jméno a příjmení studenta: Bc. Terézia Valeková

.....
podpis studenta

ABSTRAKT

Diplomová práca je vytvorená so zameraním na aktuálne hrozby 21. storočia, ktoré môžu ovplyvniť bezpečnosť obyvateľstva. Cieľom práce je zistenie momentálnych postojov občanov v otázke rizík, plynúcich zo zvolených hrozieb pomocou využitia kvantitatívnej metódy dotazníka s následným rozšírením a analýzou rizík prostredníctvom metód What-if a matice rizík. Práca taktiež obsahuje vyhodnotenia jednotlivých metód a návrhy opatrení do budúcnosti.

Kľúčové slová: bezpečnosť, hrozba, terorizmus, kybernetické hrozby, migrácia, prírodné hrozby, epidémie

ABSTRACT

The thesis is created with a focus on the current threats of the 21st century that may affect the safety of the population. The aim of the thesis is to find out the current attitudes of citizens regarding the risks arising from the selected threats by using a quantitative questionnaire method, followed by an extension and analysis of the risks through What-if and risk matrix methods. The thesis also includes evaluations of each method and suggestions for future action.

Keywords: security, threat, terrorism, cyber threats, migration, natural threats, epidemics

Týmto chcem venovať moju vďaku vedúcemu školiteľovi mojej diplomovej práce Ing. Lukášovi Pavlíkovi, Ph.D., za odborné znalosti, cenné rady, trpezlivosť, ochotu a čas, ktoré mi poskytol počas tvorby celej práce.

Taktiež ďakujem svojej rodine, za všetku podporu, pochopenie a povzbudenie počas celého štúdia.

Prehlasujem, že odovzdaná verzia diplomovej práce a elektronická verzia nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD

Hrozby, bezpečnosť a riziká sú odbory, ktoré sa neustále formujú a rozvíjajú. Tieto 3 základné pojmy sú navzájom späté a sú súčasťou ľudstva už od jeho počiatkov. Úroveň bezpečnosti obyvateľov nezávisí len na orgánoch zaisťujúcich bezpečnosť, ale tiež na samotných obyvateľoch. Hrozby a riziká v spoločnosti vždy boli, sú aj budú, nedokážeme ich úplne eliminovať. Čo však dokážeme, je ich minimalizácia na najnižší možný level.

Žijeme v 21. storočí, hrozby a riziká sa menia spolu s dobou. Niektoré sú stále toho istého charakteru, iné pribúdajú na základe technologického rozvoja. Z historických udalostí a skúseností vyplýva množstvo ponaučení, ktoré dopomôžu k pripravenosti čeliť hrozbám aktuálneho storočia.

Diplomová práca s názvom „*Hrozby 21. století a jejich vliv na společnost a její obyvatele*“ je zameraná na aktuálnu problematiku týkajúcu sa bezpečnostných hrozieb a rizík, ktorým môže byť spoločnosť vystavená. Terorizmus, migrácia, organizovaný zločin, ozbrojený konflikt, prírodné hrozby, epidémie a pandémie, to všetko sú hrozby dnešnej epochy. S narastajúcou elektronizáciou sa aj kybernetické hrozby dostávajú na popredné priečky, čo sa vyvolávajúceho nebezpečenstva týka.

Cieľom tejto diplomovej práce je charakterizovať základné pojmy z oblasti predmetnej problematiky. Poskytnúť prehľad možných hrozieb 21. storočia, ktoré môžu ovplyvniť bezpečnosť spoločnosti a jej obyvateľov. Poukázať na možné nebezpečenstvá a hrozby, ktoré môžu nastať v blízkej budúcnosti. Umožniť pohľad na vnímanie obyvateľov Slovenskej republiky na bezpečnosť v spoločnosti. A v neposlednom rade pomocou metód analýzy rizík určiť mieru vybraných hrozieb na obyvateľov.

I. TEORETICKÁ ČASŤ

1 BEZPEČNOSTNÉ PROSTREDIE

Prostredie, v ktorom môžu prebiehať akékoľvek bezpečnostné deje a udalosti s potenciálnym alebo reálnym dopadom do bezpečnosti pre zúčastnené objekty či subjekty so vznikom škôd alebo rôznych foriem ujmy sa označuje ako **bezpečnostné prostredie**. (Porada a kol., 2019)

Bezpečnostné prostredie Karaffa a kolektív charakterizujú ako prostredie, ktoré je vyznačené štátmi, medzinárodnými organizáciami, neštátnymi aktérmi a ďalšími subjektami, ktoré z hľadiska bezpečnosti sú poprepájané vzájomnými reláciami a aktivitami. „*Jedná sa o priestor, ktorý sa nedá presne geograficky vymedziť, kde dochádza alebo môže dochádzať k ovplyvňovaniu alebo ohrozovaniu bezpečnostných záujmov referenčného objektu*.“ (Karaffa, Hrinko, Zůna a kol., 2022)

Ivančík bezpečnostné prostredie zase definuje ako určité územie, geopoliticky relatívne ucelené, ktoré je spravidla podmienené ďalšími činiteľmi, napr. vojensko-strategickými, kultúrno-historickými, či socioekonomickými. (Ivančík, 2022)

Z hľadiska geografického a geopolitického rozsahu je bezpečnostné prostredie definované:

a) VONKAJŠIE BEZPEČNOSTNÉ PROSTREDIE

Ide o priestor, ktorý sa nachádza mimo hraníc referenčného objektu. Na úroveň jeho bezpečnosti majú alebo môžu mať rozhodujúci vplyv činitele, ktoré sa tam nachádzajú a procesy, ktoré sa v ňom odohrávajú. Toto prostredie pozostáva z prírodných, sociálnych a technogénnych prvkov, ktoré môžu pozitívne alebo negatívne vplývať na plnenie jeho funkcií a taktiež úroveň jeho bezpečnosti. K vymedzeniu vonkajšieho bezpečnostného prostredia je potrebná identifikácia geografickej dimenzie a v rámci nej špecifikácia spoločenských subjektov. (Ivančík, 2022)

b) VNÚTORNÉ BEZPEČNOSTNÉ PROSTREDIE

Ide o priestor, ktorý sa nachádza vo vnútri hraníc referenčného objektu. Na úroveň jeho bezpečnosti majú alebo môžu mať rozhodujúci vplyv činitele, ktoré sa tam nachádzajú a procesy, ktoré sa v ňom odohrávajú. Toto prostredie pozostáva z prvkov štruktúry referenčného objektu a jeho prírodným prostredím, ktoré môžu vo vzájomnej interakcii vytvárať pozitívne alebo negatívne účinky na jeho bezpečnostné záujmy. (Ivančík, 2022)

Stabilita bezpečnostného prostredia môže byť zásadne ovplyvnená ambíciami jednotlivých aktérov, ktorí pri presadzovaní svojich záujmov neváhajú použiť vojenskú silu

alebo hrozbu jej použitím. Častokrát bývajú vo forme kybernetických prostriedkov, zbraní hromadného ničenia, rastúcim dopytom po kľúčových surovinách, aktivitou na finančných trhoch, súperením o vplyv v strategických oblastiach alebo agresívnym presadzovaním vlastných politických ambícii. (Porada a kol., 2019)

1.1 Základná terminológia

Pre kvalitné a správne pochopenie danej problematiky je nutné, vytýčiť si primárne a súvisiace pojmy, s ktorými sa počas práce budeme stretávať. V úvode kapitoly je esenciálne objasnenie referenčného objektu a aktérov bezpečnosti.

1.1.1 Referenčný objekt

Je to jednotka, ktorú je potrebné chrániť, ak by sa nachádzala v existenčnom ohrození. Všetky dôležité rozhodnutia v oblasti bezpečnostnej politiky sú odôvodnené v mene referenčného objektu a jeho záujmu. (Karaffa, Hrinko, Zůna a kol., 2022)

Porada a kol. dopĺňa, že tradične za referenčný objekt môžeme považovať štát, národ, ale taktiež jedinca, civilizáciu, náboženskú skupinu, organizáciu apod. (Porada a kol., 2019)

1.1.2 Aktéri bezpečnosti

„*Sú to všetky subjekty, ktoré sa buď nachádzajú alebo pôsobia v systéme a procese ovplyvňovania bezpečnosti na referenčný objekt. Pričom referenčný objekt je sám o sebe aktérom bezpečnosti a môže mať aktívnu alebo pasívnu rolu*.“ (Karaffa, Hrinko, Zůna a kol., 2022)

Porada a kol. opisujú bezpečnostných aktérov (alebo geostrategických hráčov) ako subjekty bezpečnosti, ktorí dokážu previesť zmeny vo fáze vývoja bezpečnostného prostredia vo svoj prospech, k plneniu svojich cieľov či zámerov. Ide o dominantné subjekty bezpečnosti, o významné, ekonomicky, politicky a vojensky silné zeme, napr. USA, Ruská federácia, Francúzsko, Čína atď. (Porada a kol., 2019)

1.1.3 Bezpečnosť

Presná definícia bezpečnosti je ťažko stanoviteľná, pretože je individuálna a závisí na rôznych faktoroch. Bezpečnosť má základný význam pre fungovanie štátu a existenciu človeka ako indivídua. Práve aj to môže byť dôvodom vzniku rozporu bezpečnosti štátu

a bezpečnosti jednotlivých ľudí a spoločnosti. Pre porovnanie uvediem nižšie v texte niekoľko rôznych definícii od rôznych zdrojov.

Pojem **bezpečnosť** sa dá vymedziť ako stav, kedy sú na najnižšiu možnú mieru eliminované hrozby pre objekt a jeho záujmy a tento objekt je k eliminácii existujúcich aj potenciálnych hrozieb efektívne vybavený a ochotný pri nej spolupracovať. Bezpečnosť sa nedá zmerať, preto sa nedá povedať, že je bezpečnosť zaistená úplne. Pocit bezpečia patrí medzi základné ľudské hodnoty a potreby. (Juříček a Rožnák, 2014)

Slovník súčasného slovenského jazyka popisuje definíciu bezpečnosti ako „*stav bez reálnej hrozby nebezpečenstva, alebo ako vlastnosť toho, čo nepredstavuje nijakú hrozbu, nebezpečenstvo*.“ (Slovník súčasného slovenského jazyka, 2015)

Cambridgeský výkladový slovník zasa definuje bezpečnosť ako „*stav, pri ktorom sú osoby, budovy, organizácie alebo krajiny chránené pred hrozbami, ako je napríklad trestný čin alebo útoky zahraničných krajín, alebo ako stav, kedy nie je pravdepodobné, že niečo zlyhá alebo sa stratí*.“ (Security, 2022)

Bezpečnosť môže byť ohrozená v rôznych dimenziách, eventuálne ich kombináciou. Týka sa to bezpečnosti: sociálnej, kybernetickej, systémovej, prírodnej, spirituálnej, environmentálnej, energetickej, potravinovej, finančnej, ekonomickej, jadrovej a vojenskej. (Sak, 2018)

V súčasnom svete sú prepojené faktory, javy a udalosti, ktoré ovplyvňujú bezpečnosť. Výstižné znázornenie, viď. Obrázok 1. (Karaffa, Hrinko, Zůna a kol., 2022)

1.1.4 Nebezpečnosť

Ivančík charakterizuje **nebezpečnosť** ako „*stav bezpečnostnej situácie a činiteľov, javov, procesov a hrozieb tento stav ovplyvňujúcich, ktorý nevytvára vhodné, priaznivé podmienky pre existenciu, pretrvanie, plnenie požadovaných funkcií a rozvoj referenčného objektu. Je to stav nerovnováhy, v ktorom, resp. počas trvania ktorého potenciál ohrození prevažuje nad možnosťami systému ochrany (obrany) referenčného objektu odvrátiť hroziace nebezpečenstvo*.“ (Ivančík, 2022)

O nebezpečnosti môžeme hovoriť aj ako o vnútornej vlastnosti spoločenského, prírodného alebo technogénneho systému alebo jeho prvkov, ktorá môže ohroziť, narušiť bezpečnosť iných systémov alebo prvkov vo svojom okolí. (Porada a kol., 2019)

1.1.5 Opatrenia

Pomocou bezpečnostných opatrení sa v zásade nedajú vyriešiť bezpečnostné problémy. Pretože sa jedná len o čiastočné reakcie na konkrétne hrozby. Podstatu alebo zdroj ohrozenia nijak neriešia. (Karaffa, Hrinko, Zůna a kol., 2022)

Hlavným cieľom opatrení je schopnosť riešiť vzniknuté mimoriadne udalosti, byť na ne adekvátne pripravený, prípadne do budúcnosti predchádzať vážnejším problémom vďaka prevencii. Preventívne opatrenia sa môžu týkať rôznych odvetví, napr. preventívne opatrenia v boji proti terorizmu alebo organizovanému zločinu, opatrenia proti šíreniu ochorení, preventívne opatrenia voči kybernetickým útokom atď.

Opatrenia vznikajú v súvislosti s mimoriadnymi udalosťami. Management rizík identifikuje možné hrozby, ktoré hrozia obyvateľom, analyzuje ich a následne prijíma opatrenia na ochranu života, zdravia, majetku a životného prostredia. **Opatrenia civilnej ochrany** sa prijímajú v rámci fáz krízového riadenia: *prevencia – pripravenosť – reakcia – obnova*. (Bezpečnostné riziká, 2022)

1.1.6 Hrozba

Ide o akýkoľvek prejav jednania alebo fenomén, ktorý má potenciálnu schopnosť poškodiť záujmy alebo priamo spôsobiť škody na strane ohrozeného. (Juříček a Rožnák, 2014)

Definícia hrozby v Slovníku medzinárodných vzťahov je opísaná ako „*subjekt, jav alebo udalosť, ktoré môžu svojím pôsobením poškodiť alebo úplne zničiť chránenú hodnotu alebo záujem iného subjektu*.“ (Novotný, 2004)

Bezpečnostné hrozby môžeme rozlíšiť z rôznych hľadísk, a to na: priame, nepriame a skryté hrozby; naliehavé a latentné hrozby; úmyselné a neúmyselné hrozby; vojenské a nevojenské hrozby; symetrické a asymetrické hrozby; globálne a individuálne hrozby; vonkajšie a vnútorné hrozby; systémové a nesystémové hrozby; prírodné a spoločenské hrozby; stabilné a nestabilné hrozby; a v neposlednom rade na vojenské, politické, ekonomické, sociálne, energetické, kybernetické, environmentálne a zdravotné hrozby. (Ivančík, 2022)

Pre porovnanie, Karaffa a kolektív klasifikujú bezpečnostné hrozby podľa pôvodcu (zámerné a nezámerné hrozby), sektorovej príslušnosti (vojenské, politické, ekonomické, environmentálne a kultúrne), geopolitiky (priame a nepriame hrozby) a času (latentné

a naliehavé hrozby). Taktiež tvrdia, že hrozby vznikajú a pôsobia úplne nezávisle na prostredí, v ktorom pôsobia. (Karaffa, Hrinko, Zůna a kol., 2022)

Pre prehľadnejšie rozdelenie hrozieb je použité ich umiestnenie v Tabuľka 1.

Tabuľka 1 – rozdelenie hrozieb (Zdroj: vlastný, 2022)

HROZBY				
Prírodné		**Antropogénne**		
biotické	**abiotické**	**technogénne**	**sociogénne**	**ekonomické**
-epidémia -epifýtia -epizótia	-povodeň -dlhodobé sucho -svahový zosuv -krupobitie -snehová kalamita -extrémne teploty -požiare v prírode -zemetrasenie -lavíny -búrka -dlhodobá inverzia	-únik nebezpečnej chemickej látky -radiačná havária -závažné nehody v doprave -závažná priemyselná havária -environmen-tálna záťaž	-rozsiahla a neregulárna migrácia -narušenie zákonnosti veľkého rozsahu vrátane terorizmu -vojenské napadnutie SR -narušenie verejného zdravotníctva -narušenie školského systému	-narušenie menového, devízového a finančného hospodárstva štátu -narušenie menového, devízového a finančného hospodárstva štátu

1.1.7 Riziko

Riziko je udalosť, ktorú považujeme z bezpečnostného hľadiska za nežiadúcu. Dá sa vždy odvodiť z konkrétnej hrozby a má subjektívny charakter. Na základe analýzy rizík,

ktorá vychádza aj z posúdenia pripravenosti čeliť hrozbám, je možné posúdiť mieru rizika. (Juříček a Rožnák, 2014)

Riziko vyjadruje pravdepodobnosť, závažnosť a naliehavosť realizácie deštrukčného potenciálu hrozby. Ide teda o možnosť, kedy s určitou pravdepodobnosťou vznikne udalosť, ktorá sa líši od stavu žiadúceho. (Karaffa, Hrinko, Zůna a kol., 2022)

Bezpečnostné rizika sú odvádzané od hrozieb a kategorizované na: vojenské, politické, ekonomické, ekologické, sociálne a kultúrne. (Juříček a Rožnák, 2014)

Úroveň rizika alebo kombinácie rizík sa dosiahne vyjadrením kombinácie následkov udalosti a pravdepodobnosti, že nejaká udalosť nastane. Zatiaľ čo v minulosti sa úrovne rizika delili na prijateľné a neprijateľné, v súčasnosti sa kategorizuje do troch skupín: neprijateľné, prijateľné a riziká, ktoré sú na pomedzí dvoch predchádzajúcich kategórií. V bezpečnostnej praxi sa však môžeme stretnúť aj s ďalšími úrovňami a to: minimálna úroveň rizika, zostatkové (reziduálne) riziko a nulové riziko.

Ivančík označuje bezpečnostné riziká ako „*súhrnný pojem používaný pre označenie rizík spojených s bezpečnosťou osôb, sociálnych skupín, štátov, zoskupením štátov, ľudstvom, resp. s bezpečnosťou majetku, systémov, procesov, informácií a pod.* “ (Ivančík, 2022)

V oblasti krízového riadenia či krízového managementu, existuje zjednodušené, objektivizované a operacionalizované vysvetlenie, kedy je **riziko kalkulované ako súčin pravdepodobnosti a dopadu**. (Karaffa, Hrinko, Zůna a kol., 2022)

1.1.8 Zraniteľnosť

„*Zraniteľnosť znamená vlastnosť ľubovoľného materiálneho objektu, technického prostriedku alebo sociálneho subjektu stratiť schopnosť plniť svoju prirodzenú alebo stanovenú funkciu v dôsledku pôsobenia vonkajších alebo vnútorných ohrození rôznej povahy a intenzity.*“ (Porada a kol., 2019)

Môžeme ňou označiť slabé miesto informačného aktíva, slabinu informačného systému. Zraniteľnosťou sa rozumie problematické, ľahšie napadnuteľné miesto systému či prekonateľné miesto bezpečnostných opatrení. Taktiež môže ísť o nevhodný spôsob implementácie systému alebo jeho ochrany. Práve zraniteľnosti sa stávajú terčom útokov nositeľov hrozieb. (Makatura, 2021)

Príkladom napadnutia zraniteľnosti, je tzv. „*zero day attack*“ vo voľnom preklade znamenajúci *napadnutie nultého dňa*. Útok nultého dňa nastáva vtedy, keď hackeri využijú zraniteľnosť softvéru alebo siete, o ktorej vývojári nevedia. (Brooks, 2021)

Zraniteľnosť je „*vlastnosť aktíva v návrhu, vyhotovení alebo prevádzke infraštruktúry, ktorá sa prostredníctvom ohrozenia stáva citlivou na zničenie alebo uvedenie do stavu nespôsobilosti*.“ (Pravidlá pre hlásenie incidentu a zraniteľnosti, 2021)

1.2 Charakteristika mimoriadnych udalostí

Mimoriadnou udalosťou sa rozumie škodlivé pôsobenie síl a javov vyvolaných činnosťou človeka, prírodnými vplyvmi a tiež havárie, ktoré ohrozujú život, zdravie, majetok a životné prostredie a vyžadujú prevedenie záchranných a likvidačných prác. (Česko, 2000)

Môže sa taktiež jednať o závažnú situáciu, ktorá spôsobuje množstvo negatívnych následkov. Zároveň sa dá definovať ako náhla, neočakávaná, časovo a priestorovo obmedzená udalosť, ktorá vznikne v súvislosti s prevádzkou technických zariadení, neodborným či neopatrným zachádzaním s chemickými a inými nebezpečnými látkami alebo iným nebezpečím spôsobeným ľudskou či technickou chybou. (Mimořádná událost. Definice, druhy a řešení prostřednictvím IZS, 2022)

S mimoriadnou udalosťou sú späté aj stupne poplachu, ktoré vyhlasuje veliteľ zásahu po príjazde na miesto danej udalosti, na základe poplachového plánu. Existujú 3 stupne poplachu a zvláštny stupeň poplachu. V prípade vzniku mimoriadnej udalosti, dochádza k aktivácii traumatologický plán, ktorý vypracováva zdravotnícka záchranná služba, ktorá popri tom určí stupeň aktivácie plánu podľa počtu postihnutých osôb: 1. stupeň = 0 až 10 postihnutých osôb; 2. stupeň = 11 až 100 postihnutých osôb; 3. stupeň = 101 až 1 000 postihnutých osôb a zvláštny stupeň = nad 1 000 postihnutých osôb. (Mimořádná událost. Definice, druhy a řešení prostřednictvím IZS, 2022)

Druhy mimoriadnych udalostí

K mimoriadnej udalosti môže dôjsť rôznymi cestami, najčastejšie však činnosťou človeka (napr. dopravné havárie, sabotáž, vojna, teroristický útok, únos...), prírodnými vplyvmi (napr. záplavy, lesný požiar, zosuv pôdy, snehová kalamita...) ale zároveň aj v súvislosti s výkonom práce (napr. výbuch, radiačná havária, únik nebezpečnej látky...). (Mimořádná událost. Definice, druhy a řešení prostřednictvím IZS, 2022)

2 VYBRANÉ HROZBY 21. STOROČIA

Hrozby 21. storočia, ktorým čelí súčasná spoločnosť má priame a nepriame dopady na jej obyvateľov. Dokážu negatívne vplývať na rôzne sektory, ako trebárs zdravotníctvo, ekonomiku, kybernetické či environmentálne prostredie. V posledných rokoch dochádza k zmene bezpečnostnej situácie v Európe a vznikajú tak nové otázky bezpečnosti. Na Obrázok 2 sú zobrazené globálne CBRN hrozby a aktivity za rok 2022. Ide o mapu sveta s vyobrazením aktuálnych hrozieb, farebne rozlíšených na chemické, biologické, rádiologické či nukleárne.

2.1 Terorizmus

Terorizmus neodmysliteľne patrí medzi hrozby 21. storočia. Jeho pôsobenie sa netýka len bezpečnosti štátu, ale dosahuje až globálnu úroveň. Moderný terorizmus nemá žiadne morálne obmedzenie.

Americký kódex federálnych nariadení definuje terorizmus ako nezákonné použitie sily a násilia voči osobám alebo majetku s cieľom zastrašiť alebo donútiť vládu, civilné obyvateľstvo alebo akúkoľvek jeho časť na podporu politických alebo sociálnych cieľov. Prostredníctvom extrémnych násilných činov sa väčšina teroristov snaží presadiť agendu, či už ide o politickú zmenu alebo o náboženskú dominanciu. (Hesterman, 2019)

V súčasnosti je známe množstvo typov terorizmu. Jedným z možných rozdelení je klasifikácia podľa motivácie a to na terorizmus politický, náboženský, monotematický, kriminálny a psychopatologický. (Filipec, 2017)

V spojitosti s terorizmom je termín **teroristická skupina**. Ide o organizáciu, ktorá systematicky používa teroristické taktiky, ktoré sú motivované politickými, environmentálnymi, alebo náboženskými motiváciami s cieľom spôsobiť chaos v spoločnosti alebo funkčnej organizácii. (What are Terrorist Groups?, 2019)

Profilovanie teroristu nepatrí medzi jednoduché záležitosti. Neexistuje pojem ako „typický terorista“. Teroristom môže byť ktokoľvek – žena, muž, človek s rôznym vzdelaním, rôznej rasy, rôzneho vierovyznania apod. Množstvo novodobých názorov je spájaných s predstavou teroristu, ako predstaviteľom Islamského štátu, čo je samozrejme len odrazom určitého všeobecného „škatuľkovania“. (Filipec, 2017)

Vývoj teroristických útokov priniesol aj fenomén „*alone wolves*“, vo voľnom preklade známych ako **osamelí vlci**. „*Jedná sa o autonómnych jednotlivcov, ktorí operujú*

nezávisle, bez direktívneho vedenia, či podpory formálnej organizácie.“ Útočníci si sami vyberajú svoj cieľ a dátum, vrátane *modu operandi*. Obyčajne sa jedná o uzavretých, ničím z davu nevyčnievajúcich, relatívne inteligentných a vysoko motivovaných jedincov, ktorí svojvoľne dospejú k rozhodnutiu učiniť teroristický útok. Alarmujúcim zistením je fakt, že útoky osamelých vlkov, či už bez napojenia na organizáciu alebo vzdialene riadenú skupinu, sú náročnejšie k odhaleniu a dá sa im len obťažne predchádzať. (Vegrichtová, 2019)

Čo sa týka výberu cieľa teroristov, ten nie je náhodný. Najmä radikálne náboženské skupiny, ktoré hľadajú zvýšený počet osôb, zviditeľnenie v spravodajstve/médiách a zastrašené obyvateľstvo k presadeniu svojich cieľov. Práve tieto spomenuté aspekty môžu teroristom poskytnúť tzv. *soft targets*, známe ako ***mäkké ciele***. Mäkké ciele by sa dali označiť ako nedostatočne chránené civilné objekty, v ktorých sa zhromažďuje veľké množstvo osôb. Typicky medzi také miesta radíme školy, obchodné centrá, kostoly, divadlá, kina, bary, reštaurácie, úrady, letiská, nemocnice, autobusové či vlakové stanice, taktiež športové alebo kultúrne verejné udalosti atď. Na druhej strane stoja tzv. *hard targets*, známe ako ***tvrdé ciele***. Sú presným opakom mäkkých cieľov. Ide o výborne strážené a chránené objekty, napr. vládne budovy, vojenské priestory atď. (Hesterman, 2019)

V terajšej dobe v rámci terorizmu už existuje množstvo nových taktík a vznikajúcich hrozieb. K vykonaniu teroristického útoku dokážu teroristi použiť rôzne formy, napr. vozidlá, zbrane hromadného ničenia či dokonca drony.

Drony slúžia teroristom k presadzovaniu svojich cieľov na bojisku. ISIS v súčasnosti používa drony na videozáznamy a sledovanie, na nepriame pozorovanie paľby a dodávanie zbraní. Drony môžu byť naprogramované a použité na nečestné účely, ako sa práve ukazuje na bojovom poli. Odhliadnuc od terorizmu a trestnej činnosti, drony so sebou nesú aj potenciál narušiť súkromie, zraniť ľudí a spôsobiť škody na majetku, aj keď sa používajú správne a legálne. (Hesterman, 2019)

2.2 Migrácia

Migrácia je spojená s ľudstvom už od prvopočiatku. Ide o pohyb skupiny osôb za účelom zmeny bydliska, získania práce, nadobudnutia vzdelania, útekom pred politickým alebo vojenským konfliktom. Z toho dôvodu môžeme migráciu rozdeliť na dobrovoľnú alebo nútenú. Z iného uhla pohľadu na vnútroštátnu a medzinárodnú. (Rožnák, Kubečka a kol., 2018)

Migráciu môžeme označiť ako globálny jav, ktorý môže byť spôsobený ekonomickými, sociálnymi, kultúrnymi, politickými, environmentálnymi, vzdelávacími a dopravnými faktormi. (Rožnák, Kubečka a kol., 2018)

„*Z demografického hľadiska sa dá migrácia vyjadriť niekoľkými ukazovateľmi. Jedným z nich je migračné saldo, ktoré vyjadruje rozdiel počtu prisťahovaných (imigrantov) a vysťahovaných (emigrantov) v danej oblasti. V závislosti na výsledku sa potom hovorí, buď o migračnom raste alebo migračnom úbytku.*“ (Rožnák, Kubečka a kol., 2018)

Umberto Eco rozlišuje pojmy migrácia a imigrácia nasledovne. K **imigrácii** podľa neho dochádza vtedy, ak sa určité množstvo osôb presúva z jednej zeme do druhej. Taktiež tento fenomén sa dá politicky kontrolovať, obmedzovať, povzbudzovať, plánovať či akceptovať. Čo sa týka **migrácie**, či už prebieha násilne alebo mierumilovne, jedná sa o prirodzený jav. O migráciu ide vtedy, keď sa celý národ postupne presúva z jedného územia na druhé. O imigrácii hovoríme iba v prípade, že imigranti z veľkej časti akceptujú zvyky zeme, do ktorej imigrujú, čo sa však už nedá povedať o migrantoch, ktorý radikálne zmenia kultúru územia, do ktorého migrujú. (Eco, 2021)

S medzinárodnou migráciou sú spojené aj tzv. **PUSH** a **PULL faktory**. Typické *PUSH* faktory, alebo faktory, ktoré migráciu z daného územia vytláčajú, reprezentujú napr. vojna, konflikt, chudoba, nízka životná úroveň či prenasledovanie z rôznych dôvodov. Na druhú stranu ako *PULL* faktory, alebo faktory, ktoré migráciu na dané územie priťahujú, môžeme označiť napr. mier, bezpečie, uplatnenie na trhu práce či prístup k zdravotnej starostlivosti. (Karaffa, Hrinko, Zůna a kol., 2022)

Európska únia pomocou sledovania pohybu migrantov identifikovala niekoľko hlavných migračných ciest do EÚ. Tieto trasy sú kombináciou pozemných a morských. Ide o: západoafrickú trasu, trasu západného a východného Stredomoria, stredomorskú trasu, trasu Apúlie a Kalábrie, kruhovú trasu z Albánska do Grécka, západo-balkánsku trasu a trasu cez východnú hranicu EÚ. (Rožnák, Kubečka a kol., 2018)

2.3 Hybridné hrozby

Koncept hybridnej vojny nie je úplne nový. Mnohí odborníci tvrdia, že je starý ako samotná vojna. Napriek tomu v posledných rokoch nadobudol značnú aktuálnosť a význam, keďže štáty využívajú neštátnych aktérov a informačné technológie na potlačenie

svojich protivníkov počas priameho ozbrojeného konfliktu alebo - čo je dôležitejšie - bez neho.

Hybridná vojna zostáva sporným pojmom a neexistuje jej všeobecne prijatá definícia. Zjednodušene povedané, hybridná vojna zahŕňa súhru alebo spojenie konvenčných, ako aj nekonvenčných nástrojov moci a nástrojov rozvratu. (Bilal, 2021)

Skoršie koncepcie ju definovali ako hrozby, ktoré zahŕňajú celú škálu rôznych spôsobov vedenia vojny vrátane konvenčných spôsobilostí, nepravidelných taktík a formácií, teroristických činov vrátane nerozlišujúceho násilia a nátlaku a kriminálnych nepokojov, ktoré vedú obe strany a rôzne neštátne subjekty. Prebiehajú rôzne diskusie o definíciách hybridnej vojny, hybridných hrozbách a súvisiacom pojme „konflikty v šedej zóne“. Okrem toho dochádza aj k prekrývaniu alebo spájaniu s ďalšími pojmami, ako sú napríklad vojna na diaľku, asymetrická vojna, nová vojna apod. (Freedman, Hoogensen Gjørv a Razakamaharav, 2021)

Aktualizovaná austrálska Obranná stratégia do roku 2020 popisuje „šedú zónu“ ako „*jeden z viacerých pojmov používaných na opis činností určených na donucovanie krajín spôsobom, ktorý sa snaží vyhnúť vojenskému konfliktu. Medzi príklady patrí využívanie polovojenských síl, militarizácia sporných prvkov, využívanie vplyvu, rušivé operácie a nátlakové využívanie obchodných a hospodárskych nástrojov*.“ (2020 Defence Strategic Update, 2020)

Cieľom hybridnej vojny je narušiť procesy právneho štátu, chod demokratických inštitúcií a vnútornú bezpečnosť štátu pomocou politických, ekonomických, vojenských, finančných či ďalších nástrojov. Zámerom útočníka hybridnej vojny je ovládnuť myseľ politického vedenia a obyvateľov napadnutého štátu pomocou propagandy a taktiež zastrašovanie terorom. (Karaffa, Hrinko, Zůna a kol., 2022)

Postupom času sa nevojenské metódy hybridnej vojny, najmä dezinformačné kampane a iné prístupy k destabilizácii spoločnosti (napríklad kybernetické útoky na infraštruktúru), stali kľúčovými prvkami hybridnej vojny a hrozbami. (Freedman, Hoogensen Gjørv a Razakamaharav, 2021)

Vplyv a rozsah hybridných hrozieb poskytuje veľa informácií o tom, ako ľudia, komunity a národy zvládajú krízu alebo konflikt. Testuje odolnosť spoločnosti a ilustruje, do akej miery môžu byť spoločnosti destabilizované nevojenskou hrozbou. (Freedman, Hoogensen Gjørv a Razakamaharav, 2021)

Hlavné znaky a podmienky hybridnej vojny:

Charakteristické znaky hybridnej vojny:

- zapojenie alebo využívanie jednotlivcov, skupín, organizácií a strán na účely agresorského štátu, ich schopností, a to prostredníctvom otvorenej a/alebo skrytej manipulácie ich názorov a presvedčení,
- nasadenie a začatie rozsiahlej informačnej vojny na psychologickú a ideologickú prípravu vlastného obyvateľstva, obyvateľstva a personálu ozbrojených síl krajiny, proti ktorej sa pripravuje a vedie hybridná vojna, svetového spoločenstva s cieľom zavádzať o skutočných zámeroch agresora,
- vytváranie separatistických hnutí v štáte, ktorý je predmetom hybridnej vojny, z politických, etnických alebo náboženských dôvodov,
- blokovanie alebo prerušenie komunikácie. (Bratko, Zaharchuk a Zolka, 2021)

Podmienky hybridnej vojny:

Analýza názorov popredných vojenských vedcov a reálnych udalostí okolo Ukrajiny umožňuje načrtnúť jej hlavné črty a podmienky hybridnej vojny:

- existencia jedného centra, ktoré plánuje, organizuje a kontroluje vedenie konfrontácie vo všetkých oblastiach,
- kombinácia konvenčných a nekonvenčných vojenských operácií a široký okruh účastníkov vojny (ozbrojené sily, teroristi, žoldnieri, partizáni, milície, gangy, špeciálne jednotky bez zodpovednosti akéhokoľvek štátu, ako aj novinári, diplomati, ekonómovia atď.),
- sústrediť sa na boj o povedomí ľudí, t. j. informačný boj, kde hlavné subjekty nie sú prezentované armádou, ale civilnými cestami, ako sú médiá, televízia, internet, iné masmédiá,
- konfrontácia vo všetkých sférach ľudského života, spoločnosti a štátu. (Bratko, Zaharchuk a Zolka, 2021)

2.4 Organizovaný zločin

Hrozba organizovaného zločinu predstavuje riziko nielen určitým štátom, ale celosvetovo. Ide o miliardový biznis, ktorý ťaží najmä z pôsobenia v trestnej činnosti.

Tieto činnosti môžu zahŕňať obchodovanie s ľuďmi, ilegálny predaj drog, obchod s nezákonným tovarom a zbraňami, falšovanie peňazí, korupciu atď.

Opakujúce sa páchanie cieľavedome koordinovanej závažnej trestnej činnosti, ktorej subjektom sú zločinecké skupiny alebo organizácie, a ktorej hlavným cieľom je dosahovanie maximálnych nelegálnych ziskov pri minimalizácii rizika nazývame **organizovaný zločin**. (Smolík, Šmíd a kol., 2010)

Úzko spätým pojmom s organizovaným zločinom je **organizovaná skupina**, ktorou sa rozumie „*spolčenie najmenej troch osôb na účel spáchania trestného činu, s určitou deľbou určených úloh medzi jednotlivými členmi skupiny, ktorej činnosť sa v dôsledku toho vyznačuje plánovitosťou a koordinovanosťou, čo zvyšuje pravdepodobnosť úspešného spáchania trestného činu.“* (Slovensko, 2005)

Ďalším významným pojmom je **zločinecká skupina**, ktorou sa rozumie *„štruktúrovaná skupina najmenej troch osôb, ktorá existuje počas určitého časového obdobia a koná koordinovane s cieľom spáchať jeden alebo viacej zločinov, trestný čin legalizácie výnosu z trestnej činnosti alebo niektorý z trestných činov korupcie na účely priameho alebo nepriameho získania finančnej alebo inej výhody*.“ (Slovensko, 2005)

Niektoré nadnárodné zločinecké skupiny môžu považovať menšie štáty alebo krajiny len ako *tranzitné*, t. j. že si tam vytvárajú určitú predprípravu k expanzii, pokúšajú sa o legalizáciu ziskov z trestnej činnosti apod. Medzi oblasti, ktoré organizovaný zločin poškodzuje či ohrozuje radíme politiku, právny systém, ekonomiku, občanov a spoločnosť. (Smolík, Šmíd a kol., 2010)

Obchodovanie s ľuďmi môže mať niekoľko foriem, ide napr. o sexuálne vykorisťovanie, nútené sobáše, nelegálne adopcie, nútené práce, nútené žobranie, nelegálny obchod s ľudskými orgánmi či zneužitie sociálneho systému. (Aktivity, 2020)

V momentálnej dobe existuje niekoľko kampaní v prevencii obchodovania s ľuďmi. Ministerstvo vnútra v kolaborácii so Slovenskou katolíckou charitou, vládnymi organizáciami a občianskymi združeniami vypracovalo množstvo letákov a plagátov v snahe pomôcť obetiam obchodovania s ľuďmi, viď. Obrázok 3, Obrázok 4 a Obrázok 5.

Okrem obchodovania s ľuďmi je tak isto formou organizovaného zločinu falšovanie peňazí. Pod týmto pojmom sa rozumie falošná mena, ktorú zločinci vytvárajú v snahe napodobniť skutočnú menu, ktorú vyrába a za ktorú ručí zvrchovaná vláda. Takáto mena je vždy navrhnutá tak, aby sa vydávala za skutočné peniaze a presvedčila ľudí o svojej

legitímnosti. Existujú zriedkavé prípady, keď sa takéto falzifikáty nevyrábajú na nákup služieb a tovaru, ale namiesto toho sa snažia v ekonomike vyvolať infláciu. Moderné falošné peniaze napodobňujú bankovky rôznych hlavných mien, ako sú doláre, eurá, libry a švajčiarske franky. Vďaka vývoju technológií sa dnes peniaze dajú čoraz ľahšie napodobňovať. Stále je to však ťažké účinne robiť, keďže väčšina peňazí a bankoviek je vytlačená na materiáli, ktorý nie je dostupný širokej verejnosti. Napriek tomu pokrok a rozšírenie technológie komerčných tlačiarní umožnili falšovateľom dobre napodobniť textúry skutočných bankoviek. (What is Counterfeit Money?, 2022)

Ďalšou formou je aj korupcia, ktorú definujeme ako zneužitie zverenej moci na súkromný prospech. Korupcia narúša dôveru, oslabuje demokraciu, brzdí hospodársky rozvoj a ďalej prehlbuje nerovnosť, chudobu, sociálne rozdelenie a environmentálnu krízu. Korupcia sa môže vyskytnúť kdekoľvek: v podnikaní, vo vláde, na súdoch, v médiách a v občianskej spoločnosti, ako aj vo všetkých odvetviach od zdravotníctva a vzdelávania až po infraštruktúru a šport. Môže sa týkať kohokoľvek: politikov, vládnych úradníkov, štátnych zamestnancov, podnikateľov alebo občanov. Môže mať dopad na: politiku, ekonomiku, spoločnosť či životné prostredie. (What is corruption?, 2022)

Korupcia môže mať rôzne podoby: štátni zamestnanci požadujú alebo prijímajú peniaze alebo výhody výmenou za služby, politici zneužívajú verejné peniaze alebo udeľujú verejné pracovné miesta alebo zákazky svojim sponzorom, priateľom a rodinám, podplácanie úradníkov korporáciami s cieľom získať lukratívne zmluvy.

Korupcia sa prispôsobuje rôznym kontextom a meniacim sa okolnostiam. Môže sa vyvíjať v reakcii na zmeny pravidiel, právnych predpisov a dokonca aj technológií. (What is corruption?, 2022)

2.5 Extrémizmus

Spoločnosť sa s prejavmi fenoménu známeho ako extrémizmus stretáva každý deň. Formy jeho prejavu nemusia zákonite vykazovať prvky trestného činu, niekedy môže ísť o nemiestnu poznámku, či nevhodný vtip.

Ministerstvo vnútra Slovenskej republiky klasifikuje extrémizmus ako „*konanie a prejavy vychádzajúce z postojov krajne vyhrotenej, demokratickému systému nepriateľskej ideológie, ktoré či už priamo, alebo v určitom časovom horizonte deštruktívne pôsobia na existujúci demokratický systém a jeho základné atribúty*.“ (Základné informácie, 2022)

Extrémizmus môžeme tiež vysvetliť ako jednanie, ideológiu či skupiny mimo hlavný prúd spoločnosti, ktorým je pripisované porušovanie či neuznávanie základných, etických, právnych a iných spoločensky dôležitých štandardov, najmä v spojení s verbálnou alebo fyzickou agresivitou, násilím alebo hrozbou násilia, historickým revizionizmom, sociálnou demagógiou, motivované hlavne rasovou, náboženskou, národnostnou alebo inou sociálnou nenávisťou. (Juříček a Rožnák, 2014)

Pojmom **extrémistické aktivity** sa vyznačujú tie aktivity, ktoré sa stavajú proti demokratickému ústavnému štátu a jeho základným hodnotám, normám a pravidlám a ktorých cieľom je zvrhnúť liberálny demokratický poriadok a nahradiť ho poriadkom v súlade s ideami príslušnej skupiny. (Extremism, 2022)

Extrémistická skupina je skupina ľudí, ktorých hodnoty, ideály a presvedčenia sa vymykajú tomu, čo spoločnosť považuje za normálne. Extrémistická skupina sa často spája s násilnými taktikami, k presvedčeniu svojich názorov outsiderom; preto sa v mnohých definíciách môžu tieto skupiny označovať ako „násilné extrémistické skupiny“. Odborníci sa zhodujú na niektorých charakteristických črtách extrémistických skupín: neveria v žiadnu formu kompromisu, démonizujú druhú stranu, sú si jednoznačne istí svojim postojom, obhajujú použitie násilia ako prostriedku na dosiahnutie svojich cieľov a sú netolerantní voči odlišným názorom v rámci skupiny. (Norwood, 2022)

Za strategické ciele extrémistov môžeme označiť spochybňovanie, ohrozovanie a snahu o odstránenie demokratických pilierov spoločnosti. Základná klasifikácia extrémizmu obsahuje národnostný, náboženský, politický, ekologický, etnický alebo islamský extrémizmus. (Vegrichtová, 2013)

Jednou zo zložiek v boji proti extrémizmu je mimo ministerstva vnútra, polície a nevládnych organizácií aj antikonflitkný tím (alebo AKT tím). AKT tím sa riadi heslom *Verbum non arma*, čo znamená slovom miesto zbrane. Z toho vyplýva, že hlavným cieľom takéhoto tímu je predchádzať agresívnemu jednaniu osôb prostredníctvom transparentnej komunikácie. Filozofiou AKT tímu je tzv. *Low Profile Policing* a *3D stratégia*. Low Profile Policing znamená, prezentáciu policajných zložiek v takom množstve a s takou výstrojou, aby nevzbudzovala negatívne emócie a tým pádom neupozorňovala na možný zákrok. Jej opakom je tzv. *Hard Profile Policing*, pri ktorom sú klasicky známi ťažkoodenci. 3D stratégia znamená skratku 3 slov, discussion (diskusia, rozhovor), deescalation (deeskalácia, zmiernenie), determination (rozhodujúci zákrok). (Vegrichtová, 2013)

2.6 Kybernetické hrozby

V prítomnom svete plného moderných technológií, je nutné rátať aj s vysokou mierou zraniteľnosti bezpečnosti, akú kybernetické hrozby predstavujú. Práve kybernetická bezpečnosť naberá v posledných rokoch na dôležitosti, a to najmä z dôvodu expanzie moderných technológií v spoločnosti.

Kybernetická bezpečnosť je ochrana počítačov, serverov, mobilných zariadení, elektronických systémov, sietí a údajov pred škodlivými útokmi. Je známa aj ako bezpečnosť informačných technológií alebo elektronická informačná bezpečnosť. (What is Cyber Security?, 2022)

Hrozby, ktorým čelí kybernetická bezpečnosť, sú trojaké:

1. Kybernetická kriminalita jedná sa o trestnú činnosť spáchanú v kyberpriestore, v ktorej figuruje počítač ako súhrn technického a programového vybavenia vrátane dát alebo iba niektorý z jeho komponentov, prípadne väčšie množstvo počítačov, či už samostatných alebo prepojených do počítačovej siete. (Smejkal, 2022)

2. Kybernetický útok je súbor činností vykonávaných aktérmi hrozieb, ktorí sa snažia získať neoprávnený prístup, ukradnúť údaje alebo spôsobiť škody na počítačoch, počítačových sieťach alebo iných počítačových systémoch. Kybernetický útok sa môže začať z akéhokoľvek miesta. Útok môže vykonať jednotlivec alebo skupina s použitím jednej alebo viacerých taktík, techník a postupov. (Cyber Attack, 2022)

3. Kyberterorizmus zahŕňa teroristické útoky, ktoré sa odohrávajú v kyberpriestore, pričom cieľom alebo nástrojom útokov teroristov je informačný alebo telekomunikačný systém. Taktiež môžu teroristi využiť informačné a komunikačné systémy k realizácii aktu násilia s cieľom vyvolať určitú reakciu. (Smejkal, 2022)

Nižšie si uvedieme niekoľko používaných metód k ohrozeniu kyberbezpečnosti:

A) Malware - je akýkoľvek typ softvéru vytvorený na poškodenie alebo zneužitie iného softvéru alebo hardvéru. Skratka pre "*malicious software*", vo voľnom preklade *škodlivý softvér,* je súhrnný termín používaný na označenie vírusov, spyware, ransomware, trójskych koní a akéhokoľvek iného typu kódu alebo softvéru vytvoreného so škodlivým zámerom. (Regan a Belcic, 2022)

B) SQL injection - injekcia SQL (angl. *structured language query*) je typ kybernetického útoku, ktorý sa používa na prevzatie kontroly nad databázou a krádež údajov z nej.

Kyberzločinci využívajú zraniteľnosti v aplikáciách riadených údajmi na vloženie škodlivého kódu do databázy prostredníctvom škodlivého príkazu SQL. Tým získajú prístup k citlivým informáciám obsiahnutým v databáze. (What is Cyber Security?, 2022)

C) Phishing - je počítačová kriminalita, pri ktorej cieľ alebo ciele sú kontaktované e-mailom, telefonicky alebo textovou správou osobou, ktorá sa vydáva za legitímnu inštitúciu, s cieľom aby nalákala jednotlivcov na poskytnutie citlivých údajov, ako sú osobné identifikačné údaje, údaje o bankových a kreditných kartách a heslá. (What is phishing, 2022)

D) Man-in-the-middle attack - predstavuje kybernetický útok, pri ktorom sa škodlivý hráč vloží do konverzácie medzi dvoma stranami, vydáva sa za obe strany a získa prístup k informáciám, ktoré sa obe strany snažili zdieľať. Škodlivý hráč zachytí, odošle a prijme údaje určené pre niekoho iného - alebo údaje, ktoré vôbec nemali byť odoslané, pričom ani jedna z vonkajších strán o tom nevie. (Georgescu, 2021)

E) Denial-of-service attack - pri tomto type útoku kyberzločinci bránia počítačovému systému v plnení legitímnych požiadaviek tým, že zahlcujú siete a servery prevádzkou. Tým sa systém stáva nepoužiteľným a organizácia nemôže vykonávať dôležité funkcie. (What is Cyber Security?, 2022)

Rok 2020 predstavoval pre hackerov množstvo príležitostí k rôznym typom útokov. Kľúčová pre nich bola aj pandemická situácia spojená s Covid-19. Práve zdravotnícke zariadenia sa stali pre hackerov lukratívnym cieľom. Dôvodom je veľké množstvo citlivých údajov, či sa už jedná o zdravotné záznamy pacientov, osobné údaje pracovníkov alebo software zaisťujúci fungovanie prístrojov, ktorými tieto zariadenia disponujú. (Bínek, 2020)

Jedným z poučných príkladov ohľadom kyberzabezpečenia, je slovenská nemocnica v Novom Meste nad Váhom. Vzhľadom k tomu, že nemocnica generuje veľké množstvo dát, ktoré musia byť neustále k dispozícii, zvolili v spolupráci s firmou COMTEC službu Acronis Cyber Backup Cloud, ktorá ponúka bezpečné úložisko dát mimo firmy. V prípade akejkoľvek katastrofy alebo hackerského útoku na nemocnicu vedia, že o uložené dáta v cloude neprídu a v prípade potreby ich obnovia, bez toho aby bolo ohrozené ich fungovanie. Toto riešenie dokonca obsahuje aj ochranu proti ransomwaru, ktorá každý podobný útok zastaví už v zárodku, čím minimalizuje šírenie nákazy po sieti a potenciálnu možnosť výpadku lekárskych prístrojov. (Bínek, 2020)

Počas koronakrízy sa celosvetovo zvýšil aj počet tzv. *homeoffice*. S nárastom práce z domu došlo tiež k výraznému zvýšeniu prevádzky cez zabezpečené VPN siete. Problémom tohto využitia homeoffice je najmä to, že zamestnanci nemajú prístup ku všetkým firemným dátam či kritickým aplikáciám. K dispozícii je viac možností, avšak mnoho z nich nespĺňa bezpečnostné štandardy a tzv. *virtual private network* (VPN) je jednou zo zabezpečených ciest. Vytvorením tejto VPN siete môžu vzdialení pracovníci naplno pracovať z pohodlia domova a využívať všetky firemné dostupné údaje, či aplikácie. (Bínek, 2020)

Nový trend BYOD:

Ako už spomenutý homeoffice, so sebou prináša aj vzostup tzv. BYOD (Bring-Your-Own-Device) vo voľnom preklade *prines svoje vlastné zariadenie*. Tento trend prináša na jednu stranu pozitíva, no na druhú so sebou nesie aj negatíva. Podľa niekoľkých štatistík sa ukázalo, že BYOD dokázalo zamestnávateľom ušetriť výrazné množstvo financií, zamestnanci preukázali väčšiu produktivitu a efektivitu a taktiež si zamestnanci pochvaľovali úsporu času, ktorú boli schopní docieliť. (Šabata, 2022)

BYOD môže so sebou niesť právne, bezpečnostné a praktické problémy, či riziká. Kybezločinci stále hľadajú príležitosti k získaniu súkromných informácii. Preto software vyvinutý pre správu BYOD môže prispieť k ochrane dát tým, že technikom umožní získať prehľad o spravovaných zariadeniach, aby mohli vynútiť nasadenie správcu hesiel, odhaliť podozrivé aktivity atď. Ďalším rizikom je fakt, že zamestnanci využívajú svoje zariadenia nielen pre firemné aj osobné účely, čo môže viesť k neželanému stiahnutiu vírusu alebo malware. Takto získaný malware by sa potom mohol preniesť do firemnej siete a poškodiť údaje. Stratené alebo odcudzené zariadenia tak isto radíme medzi hrozby, ktoré súvisia s BYOD. Ak zamestnanec pri používaní svojho zariadenia nedodržiaval firemné bezpečnostné protokoly, môže strata alebo krádež spôsobiť závažné narušenie bezpečnosti. (Šabata, 2022)

2.7 Ozbrojený konflikt

Neoddeliteľnou hrozbou súdobého sveta je taktiež ozbrojený konflikt. Slovom konflikt môžeme vyjadriť určitý spoločenský stav, ktorý vzniká, keď dvaja alebo viac aktérov sledujú vzájomne nezlučiteľné ciele. Konflikt býva často spájaný s vojnou. Faktom však je, že každá vojna je konflikt, no nie každý konflikt je vojnou. (Karaffa, Hrinko, Zůna a kol., 2022)

Vojna môže byť vykreslená ako ozbrojený zápas alebo použitie ozbrojených síl vo vzťahu medzi dvoma alebo viacerými aktérmi. O vojne smieme hovoriť iba v prípade takého ozbrojeného konfliktu, kedy dôjde k usmrteniu najmenej 1 000 ľudí za rok. O ozbrojený konflikt ide vtedy, ak je počet obetí nižší. (Karaffa, Hrinko, Zůna a kol., 2022)

Za **ozbrojený konflikt** môžeme považovať použitie ozbrojených síl medzi štátmi (medzinárodný ozbrojený konflikt) alebo intenzívnu mieru ozbrojeného násilia, buď medzi vládnymi ozbrojenými silami a neštátnymi organizovanými ozbrojenými skupinami alebo ozbrojenými skupinami navzájom (ozbrojený konflikt nemedzinárodný alebo vnútroštátny). Akonáhle vypukne ozbrojený konflikt, potom jednanie jeho strán upravuje medzinárodné právo. (Ditrichová a Jukl, 2017)

Uppsala Conflict Data Project je hlavným svetovým poskytovateľom údajov o organizovanom násilí a ozbrojený konflikt delí do troch kategórií:

1. **menší ozbrojený konflikt**, kde počet mŕtvych v súvislosti s bojom behom konfliktu dosiahol najmenej 25, najviac však 1 000,
2. **stredný ozbrojený konflikt**, v ktorom počet mŕtvych v súvislosti s bojom presiahol 1 000, ale bolo to menej než 1 000 v každom roku konfliktu,
3. **vojna**, v ktorej počet mŕtvych v súvislosti s bojom presahuje každý rok 1 000. (Karaffa, Hrinko, Zůna a kol., 2022)

Príčiny ozbrojených konfliktov súčasnosti:

Klasické príčiny ozbrojených konfliktov z minulosti, prakticky až do konca studenej vojny pretrvávajú, no v postmodernej dobe naberajú aj novú podobu. Typicky medzi ne radíme politicky nestabilné vlády, diktátorské režimy, separatizmus, dominanciu, boj o zdroje surovín, zrútené štáty, náboženský extrémizmus a izraelsko-arabské vzťahy. (Karaffa, Hrinko, Zůna a kol., 2022)

Rusko-Ukrajinský ozbrojený konflikt:

Ruský agresívny akt násilia na Ukrajine je čiastočne ospravedlňovaný na základe údajného amerického programu biologických zbraní v krajine. V skutočnosti, však ide o ruskú dezinformačnú kampaň, ktorá sa datuje už od roku 2009 a ktorá po invázii nadobudla nový účel. (Petersen, 2022)

Obavy pochádzajú z možného použitia Ruska, jeho chemických a biologických zbraní k porazeniu Ukrajiny. NATO, WHO a G7 varovali pred rizikom chemickej

a biologickej vojny. NATO aktivovalo svoju *Spoločnú kombinovanú pracovnú skupinu pre CBRN obranu* (*Combined Joint CBRN Defense Task Force*) a spolu s vládou Spojených štátov amerických dodávajú Ukrajine ochranné vybavenie pre vojakov a civilistov. Európska únia zhromažďuje zásoby ochranných prostriedkov a liekov pre prípad potreby. (Petersen, 2022)

Hlavným dôvodom ruskej dezinformačnej kampane o útočnom americkom programe biologických zbraní na Ukrajine, je podľa ruských predstaviteľov fakt, že tieto biologické zbrane majú za účel zničiť ruských obyvateľov. Práve tieto obvinenia sa stali neoddeliteľnou súčasťou ruskej *casus belli* pre vojnu s Ukrajinou. (Petersen, 2022)

2.8 Prírodné hrozby a epidémie

Okrem vyššie uvedených antropogénnych hrozieb, čiže hrozieb vyvolaných vplyvom človeka, sú neoddeliteľnou súčasťou aj naturogénne alebo prírodné hrozby. Medzi stále aktuálne prírodné hrozby jednoznačne radíme sucho a povodne. Globálne otepľovanie, topenie permafrostu, či stret Zeme s mimozemskými telesami už nepokladáme za hrozby budúcnosti, ale za hrozby dobového charakteru.

A) Sucho

Jedná sa o určitú formu mimoriadnej situácie, ktorá sa prejavom nedostatku vody môže zmeniť na situáciu krízovú. Dôsledkom je ohrozovanie bytia biotopu, teda vymieranie živých organizmov, čo môže viesť k ohrozeniu existencie ekosystému ako takého. Príčiny vzniku sucha môžu byť podmienené buď prírodnými procesmi (napr. nedostatok zrážok), alebo procesmi ovplyvňované človekom (napr. skleníkový efekt, budovanie hrádzí). (Mareš a kol., 2013)

B) Povodne a záplavy

Povodne nastávajú, keď sa voda preleje cez územie, ktoré je za normálnych okolností suché, alebo ho podmáča. Môžu sa vyvinúť mnohými spôsobmi. Najčastejšie sa vyskytujú, keď sa rieky alebo potoky vylejú z brehov. (Boudreau et al., 2022)

Silný dážď, pretrhnutá hrádza alebo hrádza, rýchle topenie ľadov v horách alebo dokonca bobria hrádza na zraniteľnom mieste môžu rozvodniť rieku, rozliať sa po okolitom území a spôsobiť tým záplavy. (Boudreau et al., 2022)

Povodne erodujú pôdu, odnášajú ju spod základov budov, čo spôsobuje ich praskanie a zrútenie. Povodne môžu spôsobiť ešte väčšie škody, keď ich voda ustúpi. Voda a krajina

môžu byť kontaminované nebezpečnými materiálmi, ako sú ostré úlomky, pesticídy, palivo a nespracované odpadové vody. Potenciálne nebezpečné plesne môžu rýchlo zaplaviť vodou nasiaknuté stavby. Ako sa povodňová voda šíri, prenáša taktiež choroby. Obete záplav môžu zostať celé týždne bez čistej vody na pitie alebo hygienu. (Boudreau et al., 2022)

C) Globálne otepľovanie

K tomuto javu dochádza v súvislosti so skleníkovým efektom. Planéta stráca funkciu dokonalého žiariča v momente, kedy má atmosféru, ktorej plyny ako vodná para, oxid uhličitý, metán a oxid dusný dokážu selektívne pohlcovať časť odchádzajúceho infračerveného žiarenia a naďalej ich vyžarovať smerom nahor i nadol. Taká absorpcia infračerveného žiarenia je známa ako *skleníkový efekt*. (Smil, 2017)

Miznúce ľadovce, stúpajúca hladina morí, narušenie biotopov, alergie, epidémie, vlny horúčav, suchá a záplavy, sú len zlomkom toho, čo nám globálne otepľovanie môže priniesť, ak sa táto otázka nezačne adekvátne a prioritne riešiť. (MacMillan a Turrentine, 2021)

D) Stret Zeme s mimozemskými telesami

Naša Zem sa neustále míňa s riedkymi, ale početnými masívnymi oblakmi menších kozmických telies. Rozsah veľkostí takýchto meteoritov je radovo od mikroskopických častíc po telesá s priemerom až do 10 m. Dopadom je fakt, že planéta je stále zasypávaná mikroskopickým prachom. Tento spád tvorí cca 5 ton denne, prekvapivo to však pre život a modernú civilizáciu nepredstavuje významné riziko, a to vďaka tomu, že sa tieto objekty pri prechode atmosférou rozpadajú a na povrch Zeme sa tak dostanú len drobné fragmenty či prach. Čo už však pre našu planétu predstavuje riziko, sú telesá omnoho väčšie, predovšetkým planétky s priemerom od 10 m po desiatky kilometrov. Dopad planétky na povrch Zeme, či už na súš alebo do morí či oceánov, by predstavoval nielen globálne straty, ale aj ekonomické škody. (Smil, 2017)

E) Epizootia

Vzťahuje sa na hromadný výskyt choroby zvierat, ktorý je časovo a miestne obmedzený. Môže sa tu uskutočniť liečba. Na rozdiel od panzootického ochorenia, kde výskyt ochorenia je extrémne vysoký, nie je žiadne časové ani miestne obmedzenie a liečba nie je možná. (Jozefová, Večerek a Večerková, 2015)

Úbytok biodiverzity:

V súčasnej dobe pomaly, ale iste dochádza k úbytku biodiverzity, napr. vymieranie určitých druhov živočíchov. Akokoľvek sú tieto straty ohrozených druhov zvierat hrozné, straty ekonomicky významných bezstavovcov má oveľa väčšie následky. Nenahraditeľnou ekosystémovou službou je opeľovanie včelami. Problém nastáva vo chvíli, akonáhle dôjde k úbytku opeľovačov, a to ako domestikovaných včiel, tak voľne žijúcich druhov hmyzu. K úbytku biodiverzity môže dôjsť ničením alebo podstatnou zmenou prírodného prostredia. K poklesu výrazne prispelo aj umelé vytvorenie poľnohospodárskej pôdy, či enormný výrub stromov, ktoré poskytujú domov širokému spektru živočíšstva a rastlinstva. Mimoriadne devastujúce účinky má aj bioinvázia na ostrovoch, ktorá núti faunu a flóru, buď k asimilácii, migrácii alebo uhynutiu. (Smil, 2017)

F) Epidémia

Centrum pre kontrolu a prevenciu chorôb (CDC) opisuje epidémiu ako neočakávaný nárast počtu prípadov ochorenia v určitej geografickej oblasti. Žltá zimnica, kiahne, osýpky a detská obrna sú hlavnými príkladmi epidémií. Epidemické ochorenie nemusí byť nevyhnutne nákazlivé. Za epidémiu sa považuje aj rýchly nárast miery obezity. (Epidemic, Endemic, Pandemic: What are the Differences?, 2021)

Rezistencia voči antibiotikám

V momentálnej spoločnosti sa vyskytuje hneď niekoľko baktérií (napr. *Salmonella typhimurium, Vibrio cholerae, Escherichia coli* atď.), ktoré sú rezistentné na antibiotiká. K odolnosti voči antibiotikám prispelo aj ich nadmerné predpisovanie lekármi, ďalej nedostatok hygieny v nemocniciach či masívne užívanie profylaktických antibiotík vo veterinárnom zdravotníctve. (Smil, 2017)

G) Pandémia

Pandémia, vypuknutie infekčného ochorenia, ktoré sa vyskytuje v rozsiahlej geografickej oblasti a ktoré má vysokú prevalenciu, spravidla postihujúcu značnú časť svetovej populácie, zvyčajne v priebehu niekoľkých mesiacov. Pandémie vznikajú z epidémií, ktoré sú ohniskami choroby obmedzenými na jednu časť sveta, napríklad na jednu krajinu. Pandémie, najmä tie, ktoré sa týkajú chrípky, sa niekedy vyskytujú vo vlnách, takže po postpandemickej fáze, ktorá sa vyznačuje zníženou aktivitou ochorenia, môže nasledovať ďalšie obdobie vysokého výskytu ochorenia. (Rogers, 2022)

Lloviu vírus (LLOV):

Výskumníci z farmaceutickej Medway school objavili, že Lloviu má potenciál infikovať ľudské bunky a replikovať sa. Práve to zvyšuje obavy z rozšírenia v Európe a urguje žiadosť o vykonanie štúdii patogenity a antivírusové štúdie. Výskumy tiež neodhalili žiadnu reaktivitu protilátok medzi LLOV a ebolou, čo naznačuje, že existujúce vakcíny proti ebole nemusia chrániť pred LLOV, ak sa prenesie na ľudí. (CBRNews, 2022)

Ide o filovírus, ktorý je úzko spojený s vírusmi Marburg a Ebola a cirkuluje v Schreiberových netopieroch (*Miniopterus schreibersii*) v Európe. Tento vírus bol identifikovaný v roku 2002 v Španielsku a následne bol zistený u netopierov v Maďarsku. Vírus teda predstavuje reálnu hrozbu nakazenia ľudí a primátov. Preto sa radí medzi hrozby 21. storočia. (Kemenesi et al., 2022)

Opičie kiahne:

Infekcia opičích kiahní je väčšinou zapríčinená prenosom zo zvierat ako primáty, veverice alebo hlodavce. Ide teda o zoonózu. Taktiež sa však môžu prenášať z človeka na človeka úzkym kontaktom, telovými tekutinami alebo kvapôčkami. (Rutherford, 2022)

Prirodzene sa toto ochorenie vyskytuje v centrálnej a západnej Afrike. Tridsaťdeväť rokov od posledného prípadu sa znovuobjavil v Nigérii v roku 2017. Najväčšie vypuknutie tejto epidémie zažila Demokratická republika Kongo, kedy od januára do septembra 2020 zaznamenali 4 594 infikovaných a 171 úmrtí v dôsledku nakazenia. V súčasnej dobe, 2022, boli zaznamenané jednotlivé prípady aj v Európe, konkrétne aj v Česku a Slovenskej republike. (Rutherford, 2022)

Bolo preukázané, že tento vírus sa líši 40 a viac mutáciami, od vírusu pred štyrmi rokmi. To, čo sa však nachádza v súčasnosti je úplne nový druh ochorenia. Objavili sa tiež správy, že príznaky tohto konkrétneho kmeňa sa môžu javiť miernejšie a jemnejšie ako tie, ktoré sa vyskytovali predtým. (Rutherford, 2022)

V roku 2020 tím výskumníkov z Pasteurovho Inštitútu zistilo, že opičie kiahne majú epidemický potenciál a s klesajúcou imunitou voči ortopoxvírusom môžu predstavovať stále väčšiu hrozbu pre zdravie spoločnosti. Ďalší výskum, ktorý sa uskutočnil vo februári 2022 dospel k záveru, že slabnúca imunita obyvateľstva vytvorila podmienky pre opätovný výskyt opičích kiahní. (Rutherford, 2022)

3 ANONYMNÉ HROZBY

Anonymné hrozby alebo taktiež hrozby neznáme, či hrozby budúcnosti. Týmto pomenovaním môžeme označiť hrozby, ktorým spoločnosť zatiaľ len môže čeliť. Jedná sa o hrozby, ktoré doposiaľ vyvolávajú iba polemiku v spoločnosti, no v kruhoch odborníkov sa až tak nereálne nezdajú. Podobne ako asteroidy, storočné záplavy a pandémie chorôb je termonukleárna vojna hrozbou s nízkou frekvenciou výskytu a veľkým dopadom.

3.1 Jadrové hrozby

Jadrové zbrane zostávajú najvyšším prostriedkom odstrašovania a kontroly eskalácie a sú ústredným prvkom spojenectiev USA v Európe a v Indopacifiku. Samotní spojenci sa však musia lepšie pripraviť na riadenie eskalácie v geostrategicky a technologicky čoraz náročnejšom prostredí pre USA a ich spojencov. (Frühling a O'Neil, 2021)

Ľudia hodnotia nebezpečenstvo ako väčšie, keď je jeho dopad dramatický a šokujúci. Dalo by sa očakávať, že jadrové zbrane budú pôsobiť obzvlášť hrozivo vzhľadom na desivé účinky ich použitia. Mnohým ľuďom však môžu chýbať konkrétne predstavy, ako by jadrová vojna mohla vyzerať, preto pre nich nepredstavuje až tak veľkú hrozbu. (Rendall, 2022)

Zatiaľ čo v prípade zmeny klímy, kedy by došlo k otepleniu planéty o 4 až 5 stupňov Celzia, v prípade nukleárnej zimy, ktorá hrozí, ak by nastala potenciálna jadrová vojna, by to znamenalo ochladenie o 12 až 13 stupňov. Dôsledkom by nastal kolaps oceánov a poľnohospodárstva a následný hladomor. (Aj malá nukleárna vojna..., 2022)

3.2 Umelá inteligencia (*AI*, z angl. *Artificial Intelligence*)

Metódy ako umelá inteligencia alebo strojové učenie sa používajú najmä pri pokročilejšej analýze údajov a výrobných procesoch. Umožňujú prepojiť obrovské množstvá údajov vo forme čísel, obrázkov, textov, zvukov alebo videí s cieľom odhaliť skryté súvislosti a prepojenia. (Artificial intelligence..., 2022)

V súčasnej dobe existuje tzv. "Turingov test", v ktorom by sa ľudský vyšetrovateľ pokúsil rozlíšiť medzi počítačovou a ľudskou textovou odpoveďou. V tomto prípade je nutné aj rozdelenie samotnej AI. Na „*Silnú AI*“, ktorá popisuje skutočne mysliace stroje. A „*Slabú AI*“, ktorá je určená k tomu, aby ľudskú inteligenciu neprekračovala, skôr doplňovala. (Watson, 2014)

Dnes bezprostrednejšiu hrozbu nepredstavuje superinteligencia, ale užitočné, no potenciálne nebezpečné aplikácie, na ktoré sa umelá inteligencia v súčasnosti používa. Niektoré pracovné miesta budú kvôli technológii AI stratené. Umelá inteligencia zmení spôsob vedenia konfliktov z autonómnych dronov, robotických rojov a útokov na diaľku a nanorobotov. Technológia AI umožňuje veľmi ľahko vytvárať "falošné" videá skutočných ľudí. Tie sa dajú použiť bez súhlasu jednotlivca na šírenie falošných správ, vytváranie porna s podobizňou osoby, ktorá v ňom v skutočnosti nevystupuje, a ďalšie na poškodenie nielen povesti, ale aj živobytia jednotlivca. (Marr, 2020)

3.3 Topenie permafrostu

Permafrost je územie, ktoré je zamrznuté najmenej dva roky a pozostáva z pôdy, skál a sedimentov, ktoré sú spojené do jedného celku ľadom, ktorý pôsobí ako tmel. Jeho hĺbka sa môže pohybovať od niekoľkých centimetrov až po stovky metrov a je pokrytý tzv. aktívnou vrstvou, vrstvou zeme na povrchu, ktorá sa v lete topí, hoci sa večne zamrznutá pôda niekedy nachádza aj na povrchu. (Melting permafrost: why is it a serious threat to the planet?, 2022)

Väčšina dnešného permafrostu vznikla počas doby ľadovej a po nej a vzhľadom na svoj vek akumuluje veľké množstvo metánu a uhlíka, hlavných skleníkových plynov, z rozkladajúcich sa organických látok v ňom. Podľa niektorých zdrojov je množstvo uhlíka zadržaného v permafroste takmer dvojnásobné oproti množstvu v atmosfére. Preto jeho rozmrazovanie a následné uvoľňovanie plynov predstavuje vážnu hrozbu v boji proti zmene klímy. Odhaduje sa, že do roku 2100 by sa mohlo uvoľniť až 92 miliárd ton uhlíka. Hlavným dôvodom topenia permafrostu je zvyšovanie priemernej teploty na Zemi. (Melting permafrost: why is it a serious threat to the planet?, 2022)

Tak ako permafrost zadržiava uhlík a iné skleníkové plyny, môže tiež zachytávať a uchovávať staroveké mikróby. Predpokladá sa, že niektoré baktérie a vírusy môžu v chladných a tmavých priestoroch permafrostu spať tisíce rokov, kým sa po oteplení pôdy prebudia. Otázkou odborníkov ostáva, akú hrozbu môžu tieto „spiace“ baktérie a vírusy predstavovať. (Denchak, 2018)

4 ZHRNUTIE TEORETICKEJ ČASTI

V predchádzajúcich kapitolách teoretickej časti sa rozobrali najhorúcejšie hrozby 21. storočia, ktorým čelí spoločnosť. Nevyhnutnou súčasťou bola charakteristika samotných pojmov spojených s bezpečnosťou ako sú hrozby, riziká, bezpečnostné prostredie a mimoriadna udalosť. Definovanie týchto pojmov slúžilo k lepšiemu porozumeniu práce, pretože predstavujú kľúčové faktory.

Nasledoval detailnejší opis jednotlivých hrozieb, medzi ktoré boli radené terorizmus, migrácia, hybridné hrozby, organizovaný zločin, extrémizmus, kybernetické hrozby, ozbrojený konflikt a v neposlednom rade prírodné hrozby s epidémiami a pandémiami. V samotných hrozbách boli identifikované základné pojmy spojené s danou problematiku, ich bližšie priblíženie a taktiež vplyv na obyvateľstvo.

Posledná kapitola teoretickej časti, anonymné hrozby, sa venovala nebezpečenstvám, ktorým môže byť spoločnosť v blízkej budúcnosti ešte len vystavená. Jednalo sa o hrozby, ktoré nemajú už len „science-fiction“ charakter, ale o hrozby reálneho pôvodu, ktoré sa môžu naplno prejaviť, ak sa im nebude venovať dostatočné množstvo pozornosti. Spomenuté boli jadrové hrozby, umelá inteligencia a topenie permafrostu. Súčasťou bol ich opis a prípadné predstavujúce nebezpečenstvo.

5 CIELE DIPLOMOVEJ PRÁCE

Cieľom diplomovej práce je identifikácia a posúdenie jednotlivých bezpečnostných hrozieb, ktorým môže čeliť spoločnosť Slovenskej republiky a ktoré môžu vplývať na bezpečnosť spoločnosti ako takej. Vyplnenie dotazníka obyvateľmi Slovenskej republiky, konkrétne mesta Gelnica, pomôže pri vytvorení predstavy aktuálnych postojov a názorov jeho obyvateľov na momentálnu situáciu v oblasti bezpečnosti. Pomocou zvolenej metódy analýzy rizík - What-if, ktorej výstupom bude matica rizík, bude uskutočnené vyhodnotenie najzávažnejších globálnych hrozieb.

5.1 Hlavný cieľ a čiastkové ciele

Základným cieľom práce bolo, vyobrazenie momentálnej situácie v oblasti bezpečnosti z pohľadu obyvateľstva, aký majú aktuálne globálne hrozby vplyv na danú spoločnosť. Pre splnenie tohto cieľa bolo nutnosťou splnenie niekoľkých čiastkových cieľov:

- charakteristika bezpečnostného prostredia,
- analýza a popis vybraných hrozieb,
- implementácia vybraných hrozieb pomocou metód analýzy rizík.

5.2 Metódy použité v práci

V uvedenej práci bolo použitých niekoľko rôznych metód, ako napríklad:

- **Analýza** – využitie tejto metódy je esenciou práce. Pomocou tejto metódy sa skúmali bezpečnostné hrozby momentálne ovplyvňujúce bezpečnosť slovenského obyvateľstva. Vďaka metódy syntézy sa dokázalo spojenie poznatkov získaných analytickým postupom.
- **Dedukcia** – v danej metóde sa vychádzalo zo známych, overených a všeobecne platných záverov, ktoré boli následne aplikované na zatiaľ neznáme, nepreskúmané jednotlivé kauzy, v tomto prípade hrozby.
- **Abstrakcia** – pomocou tejto metódy sa dokázalo získať odpovede na už konkrétne otázky, ktoré boli nevyhnutné k dosiahnutiu vytýčených cieľov. To sa docielilo pomocou dotazníkovej techniky a vybraných metód analýzy rizík (metóda What-if a matica rizík).

II. PRAKTICKÁ ČASŤ

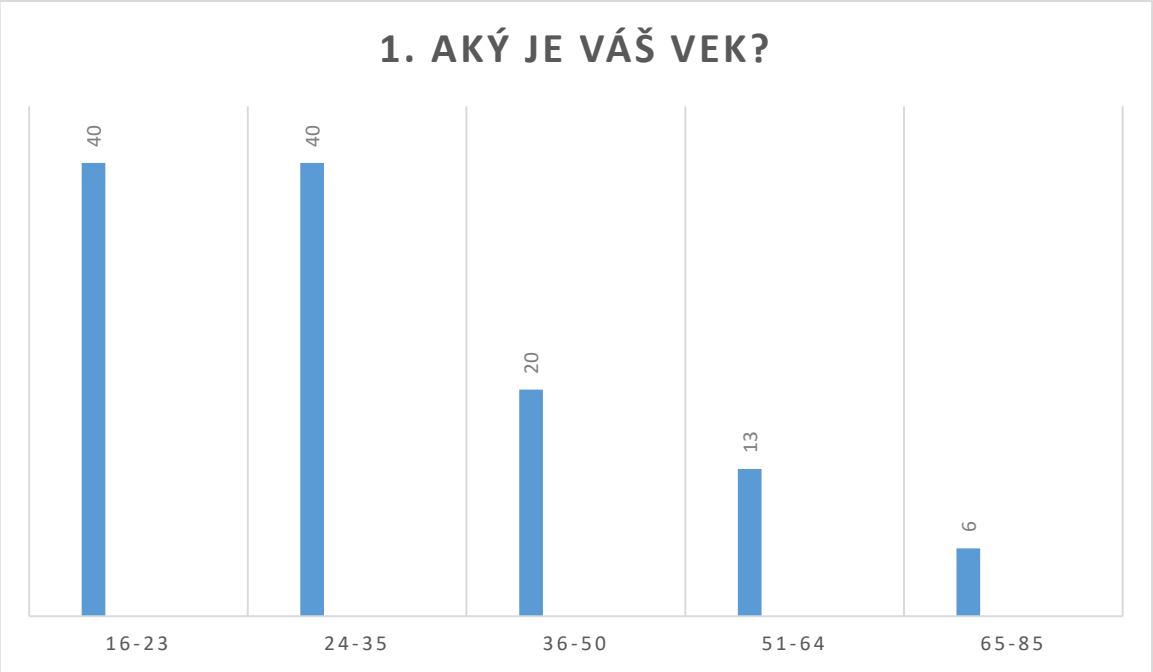
6 DOTAZNÍK OBČANOV

V praktickej časti bola použitá kvantitatívna metóda písomného dotazovania občanov Slovenskej republiky. Vzhľadom k tomu, aby bol dotazník efektívny a dosiahol výpovednú hodnotu, bolo vybrané mesto Gelnica na východe Slovenska. Mesto malo ku dňu 31.12.2021 5 886 obyvateľov. Dôvodom výberu práve tohto mesta bola jeho lokalita na východnom Slovensku, ktorá bola medzi najviac ohrozenými lokalitami ozbrojeným konfliktom na Ukrajine, taktiež masívnou vlnou migrácie a samozrejme aj inými globálnymi hrozbami.

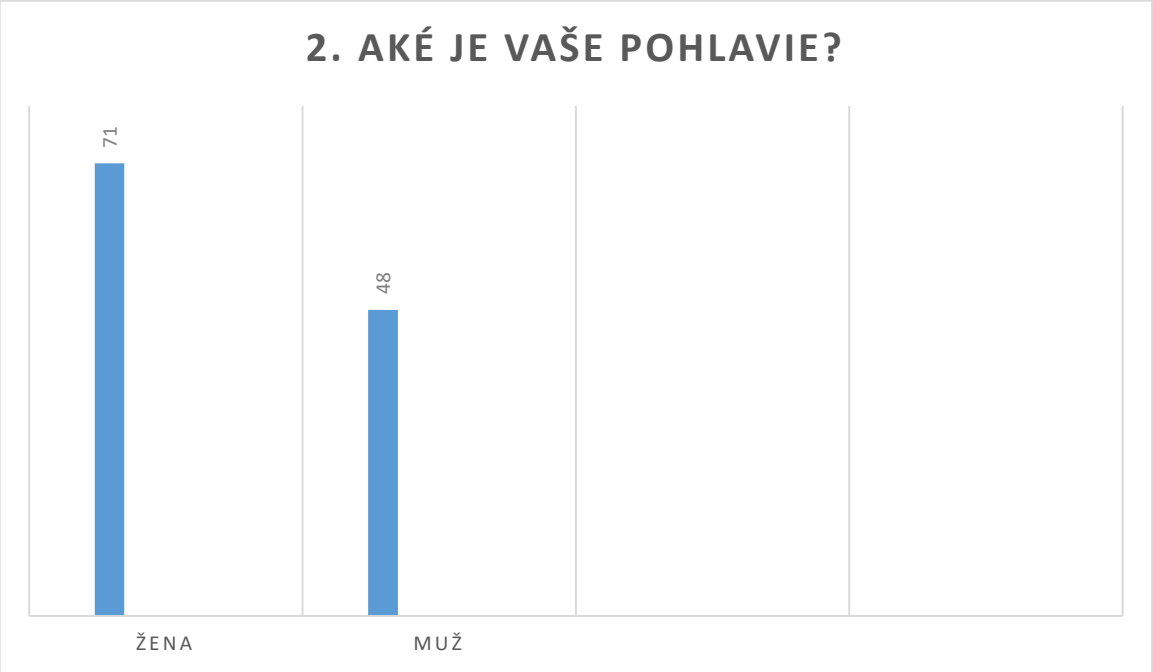
Čo sa týka samotnej tvorby dotazníka, tá mala spĺňať hlavné kritérium, časový harmonogram, ktorý sme docielili pomocou:

- predvýskumu – jednalo sa o analýzu a následné určenie cieľovej skupiny, v ktorej bol uskutočnený kvalitatívny výskum. Toto prebehlo v období november až december.
- dotazovania samotného – v ktorom šlo o reálny zber odpovedí od respondentov. Trvanie bolo od decembra po január.
- analýzy, hodnotenia a formulácie výsledkov – týkalo sa to evaluácie a rozboru získaných odpovedí. Časové obdobie tejto fázy prebehlo počas mesiaca február.
- a zapracovania výsledkov do diplomovej práce – v tejto poslednej fáze došlo k finálnemu spracovaniu nadobudnutých výsledkov do uceleného celku v trvaní počas mesiaca február.

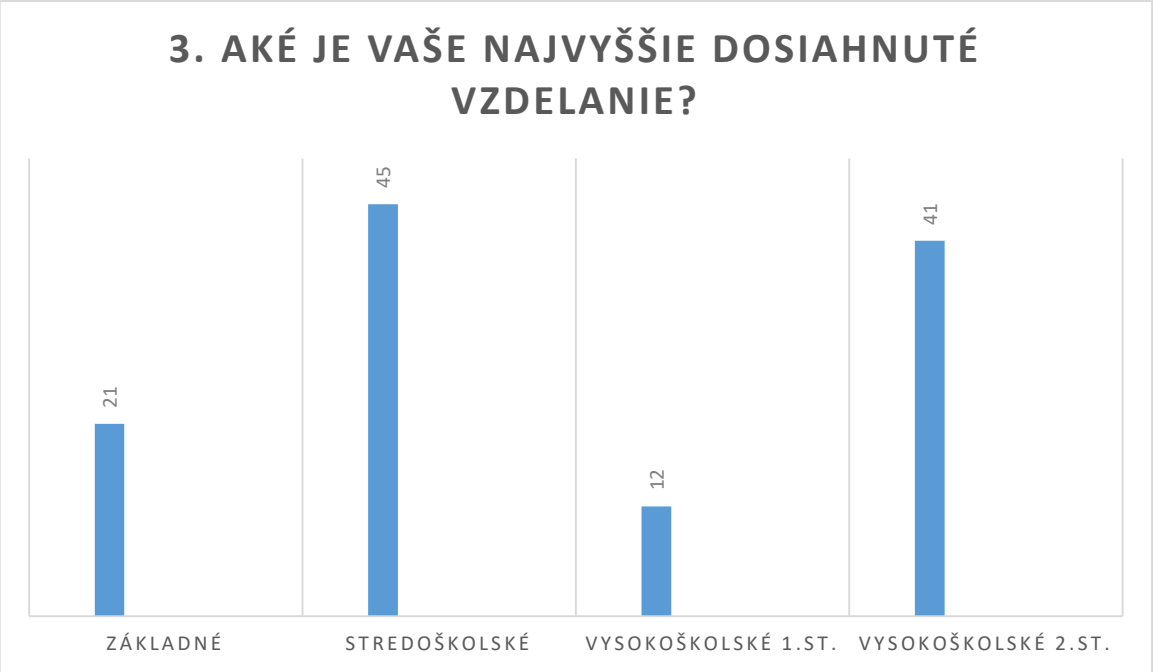
Zo štatistického hľadiska boli obyvatelia mesta Gelnica, ako celkovo oslovené subjekty. Počet subjektov, ktorých sa na dotazovaní zúčastnilo bolo 119, čiže tzv. návratnosť dotazníka bola v prepočte vyše dvoch percent. Nižšie sa v jednotlivých grafoch nachádza prehľad získaných odpovedí.



Graf 1 – vek obyvateľov (Zdroj: vlastný, 2023)

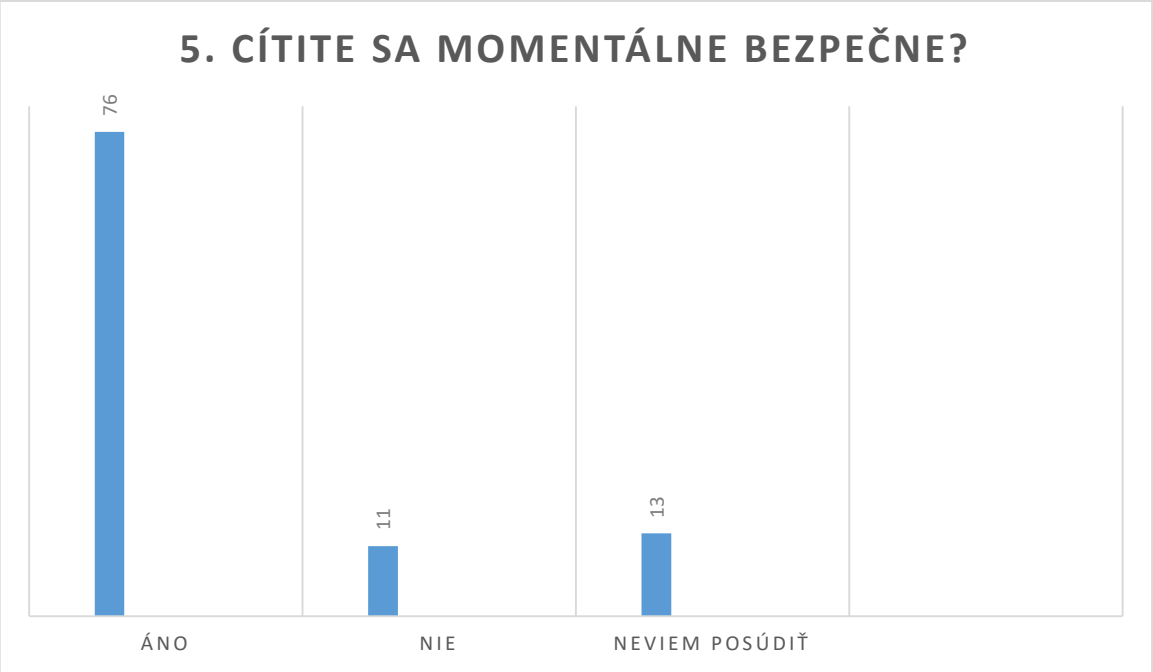


Graf 2 – pohlavie obyvateľov (Zdroj: vlastný, 2023)

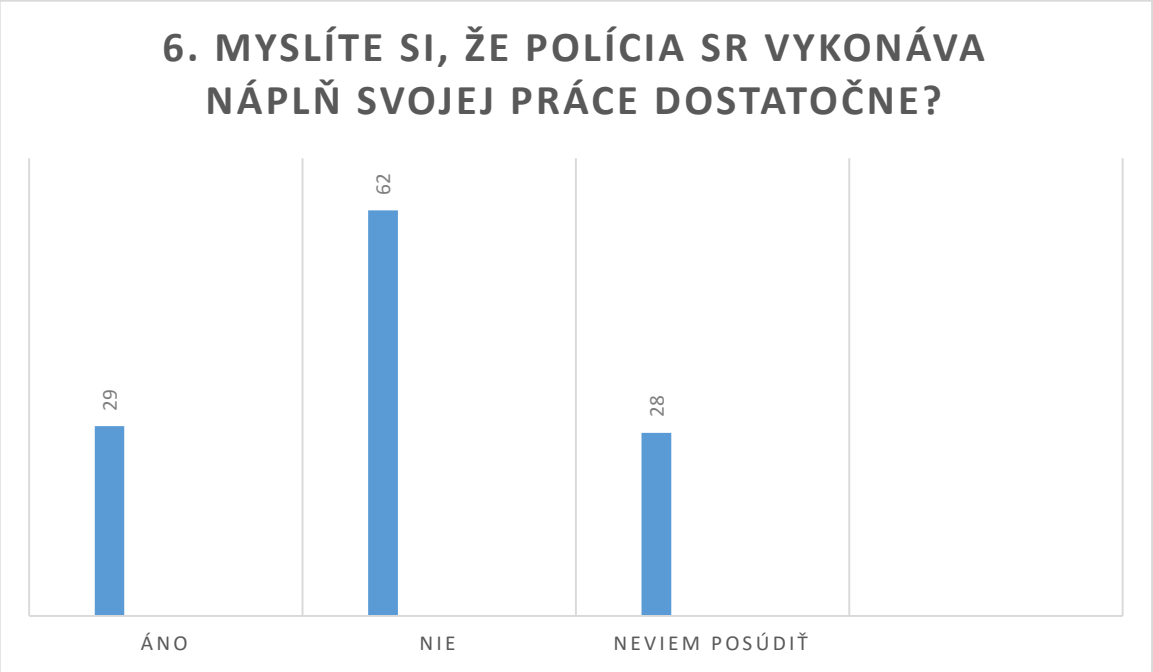


Graf 3 – vzdelanie obyvateľov (Zdroj: vlastný, 2023)

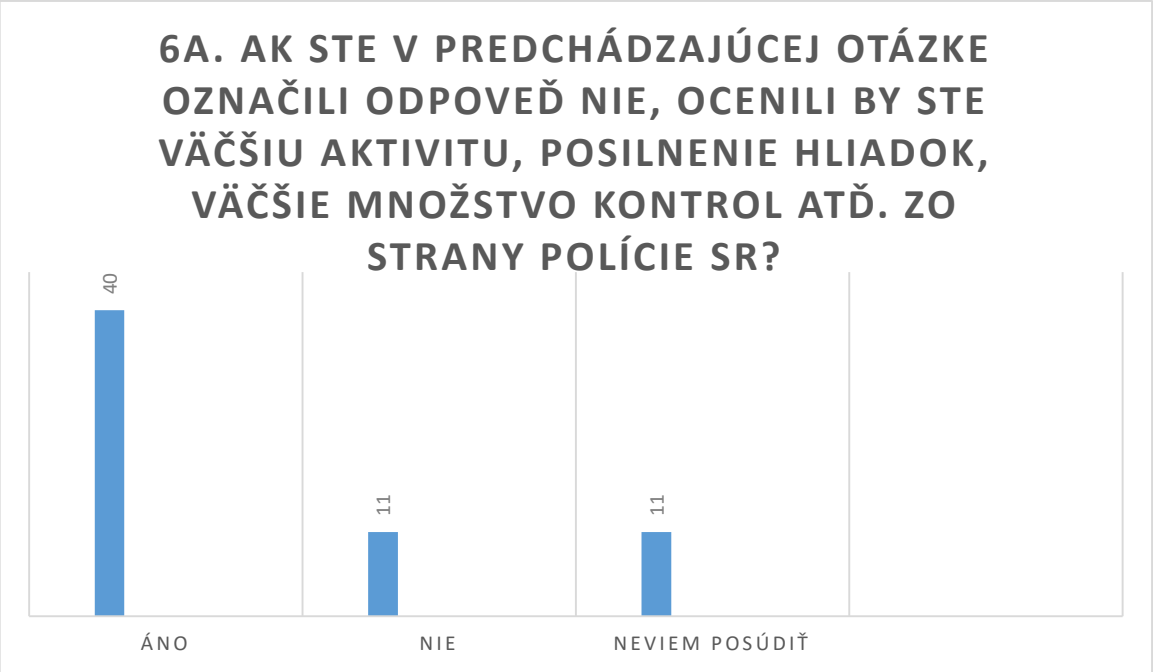
Graf 4 – bydlisko obyvateľov (Zdroj: vlastný, 2023)



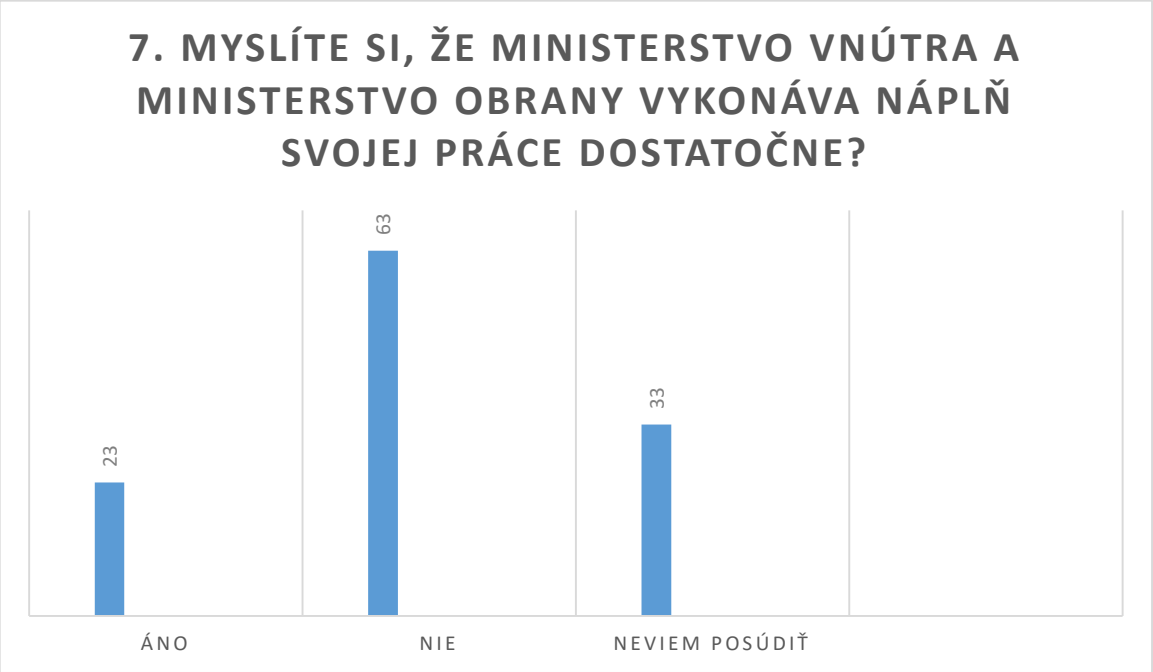
Graf 5 – otázka č. 1 (Zdroj: vlastný, 2023)



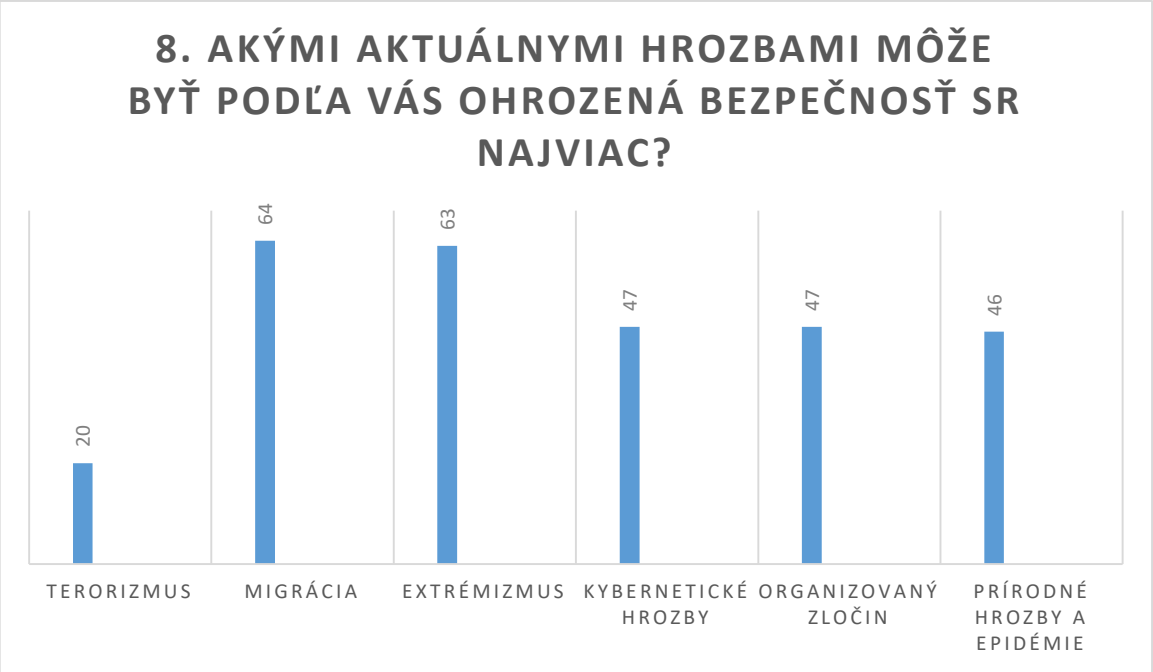
Graf 6 – otázka č. 2 (Zdroj: vlastný, 2023)



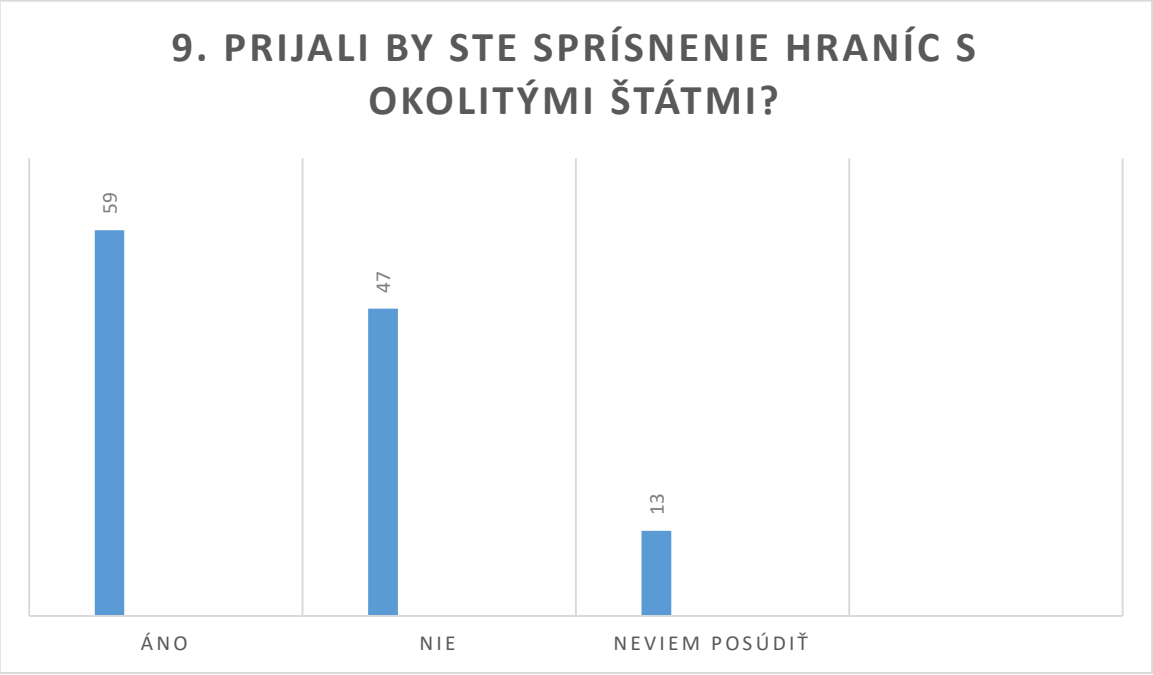
Graf 7 – otázka č. 3 (Zdroj: vlastný, 2023)



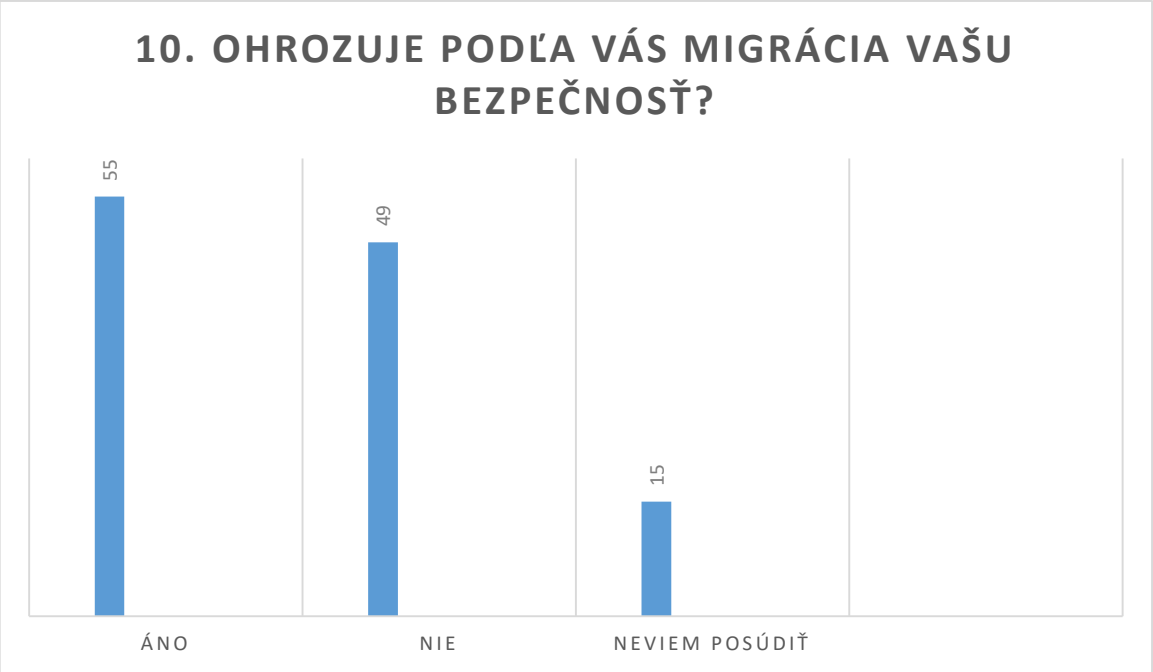
Graf 8 – otázka č. 4 (Zdroj: vlastný, 2023)



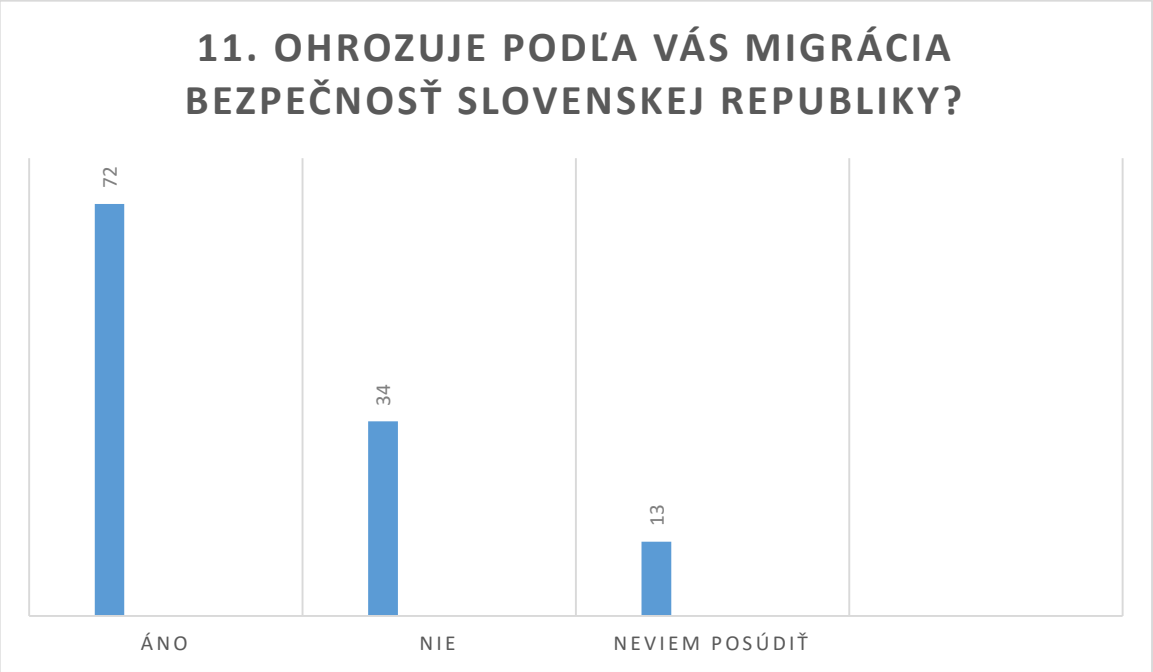
Graf 9 – otázka č. 5 (Zdroj: vlastný, 2023)



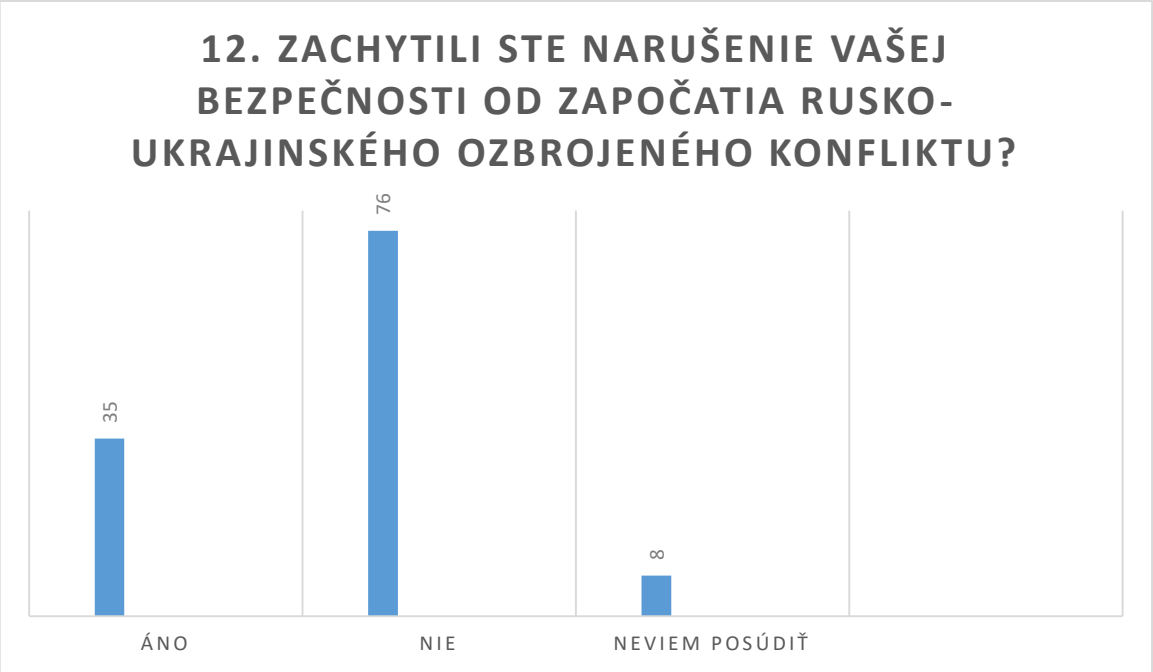
Graf 10 – otázka č. 6 (Zdroj: vlastný, 2023)



Graf 11 – otázka č. 7 (Zdroj: vlastný, 2023)

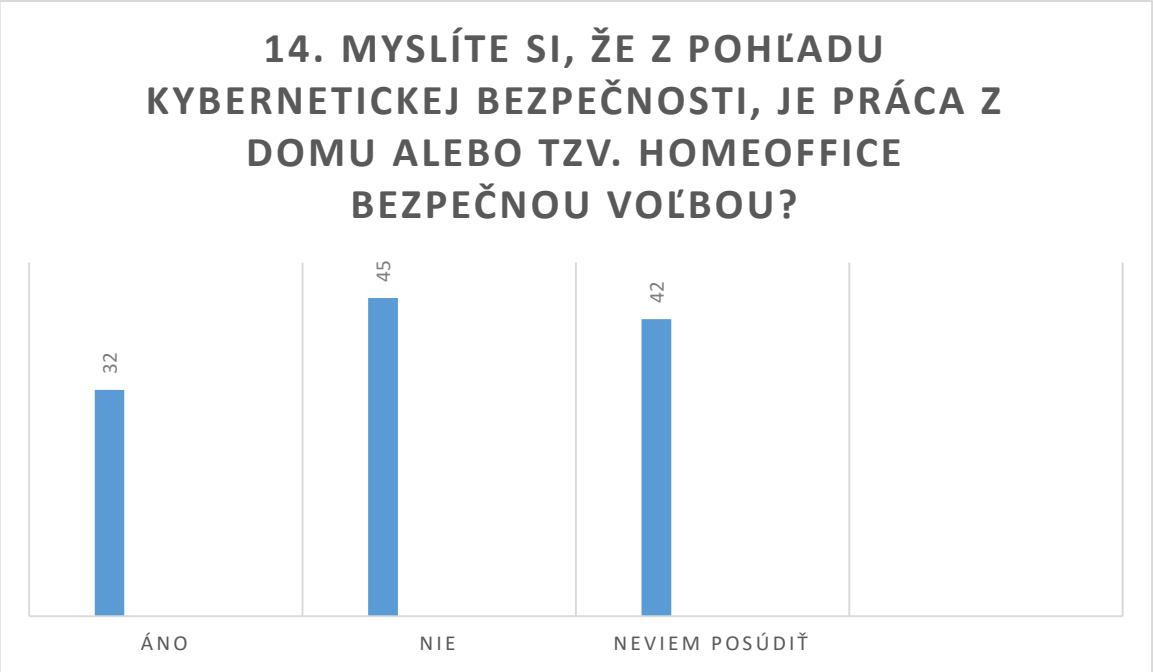


Graf 12 – otázka č. 8 (Zdroj: vlastný, 2023)

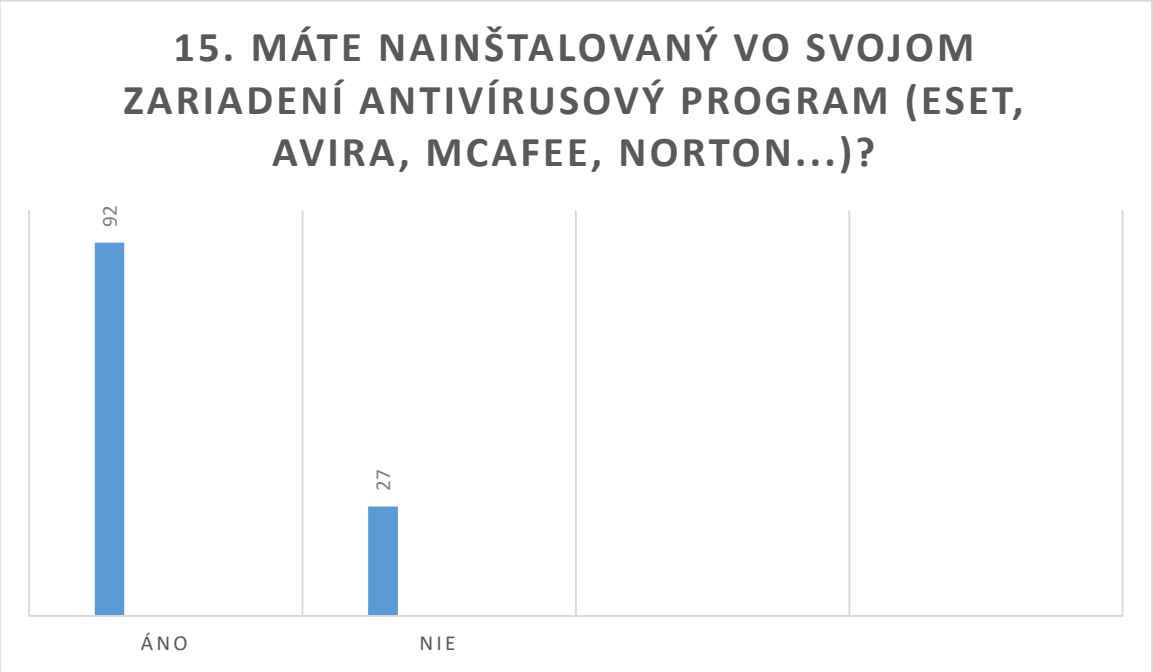


Graf 13 – otázka č. 9 (Zdroj: vlastný, 2023)

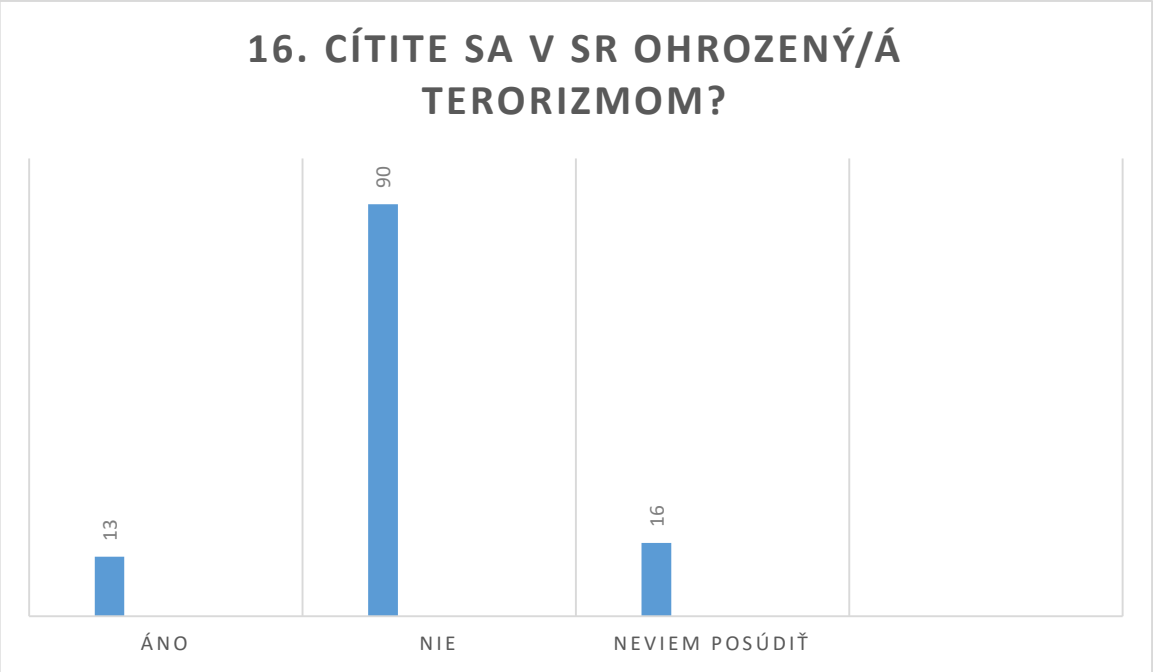
Graf 14 – otázka č. 10 (Zdroj: vlastný, 2023)



Graf 15 – otázka č. 11 (Zdroj: vlastný, 2023)



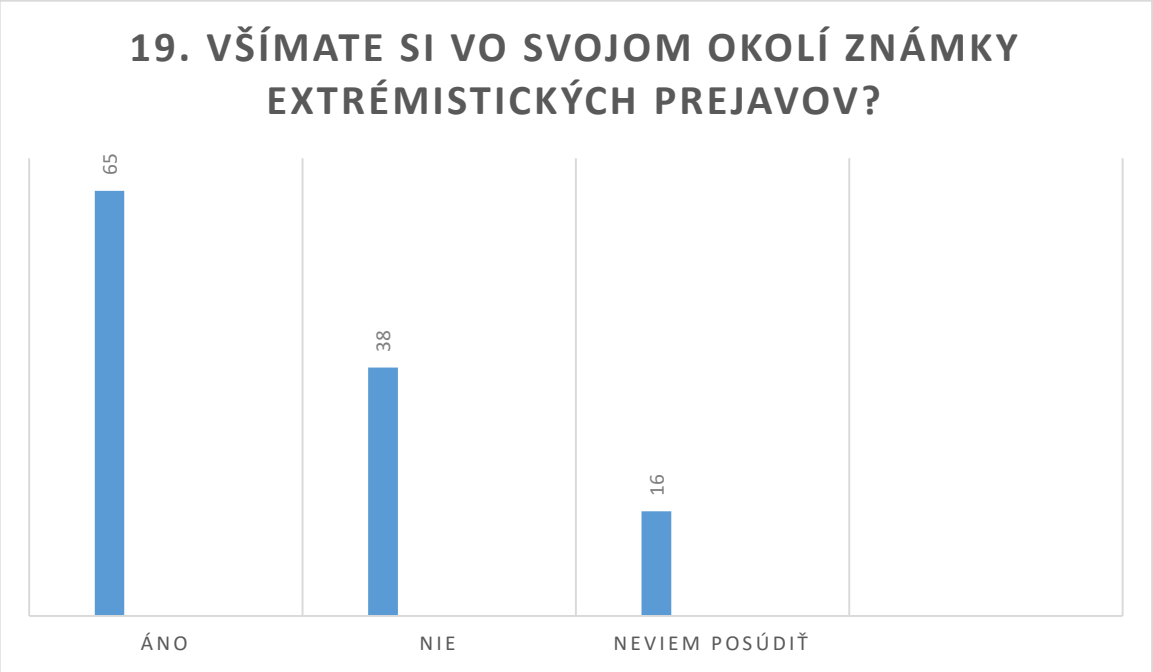
Graf 16 – otázka č. 12 (Zdroj: vlastný, 2023)



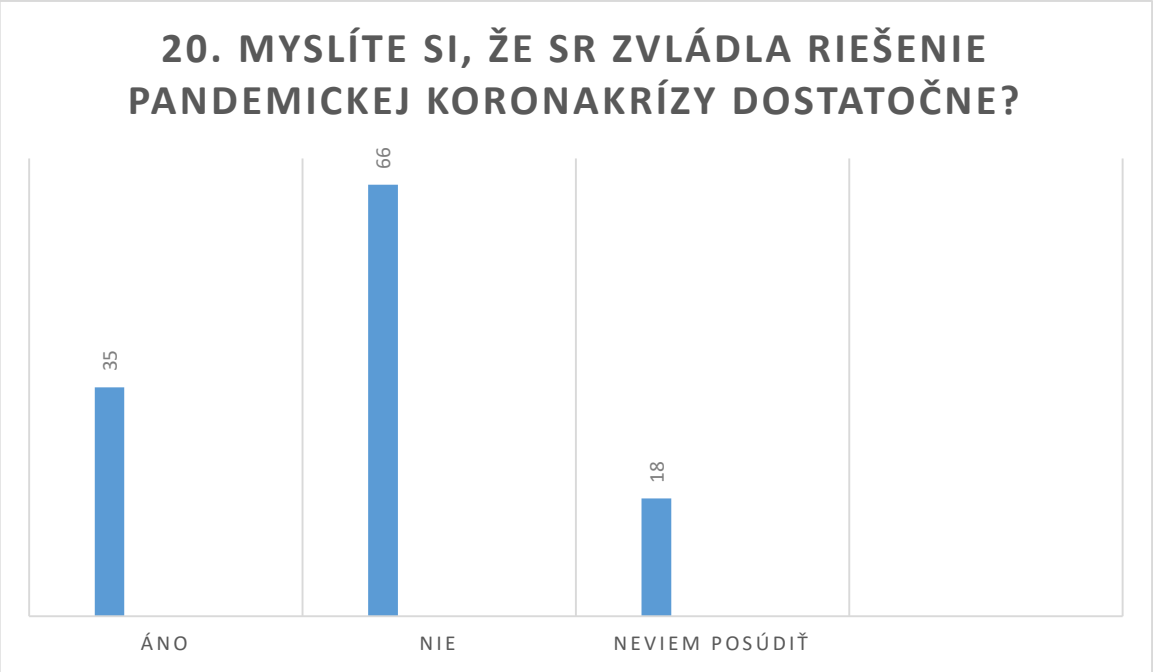
Graf 17 – otázka č. 13 (Zdroj: vlastný, 2023)

Graf 18 – otázka č. 14 (Zdroj: vlastný, 2023)

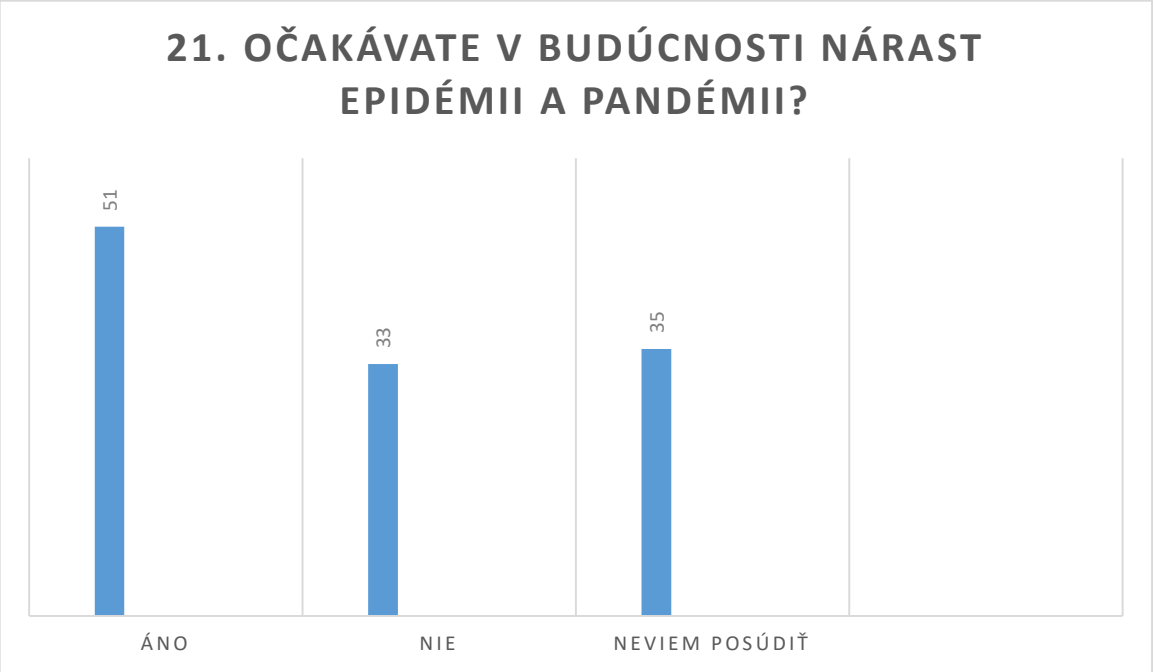
Graf 19 – otázka č. 15 (Zdroj: vlastný, 2023)



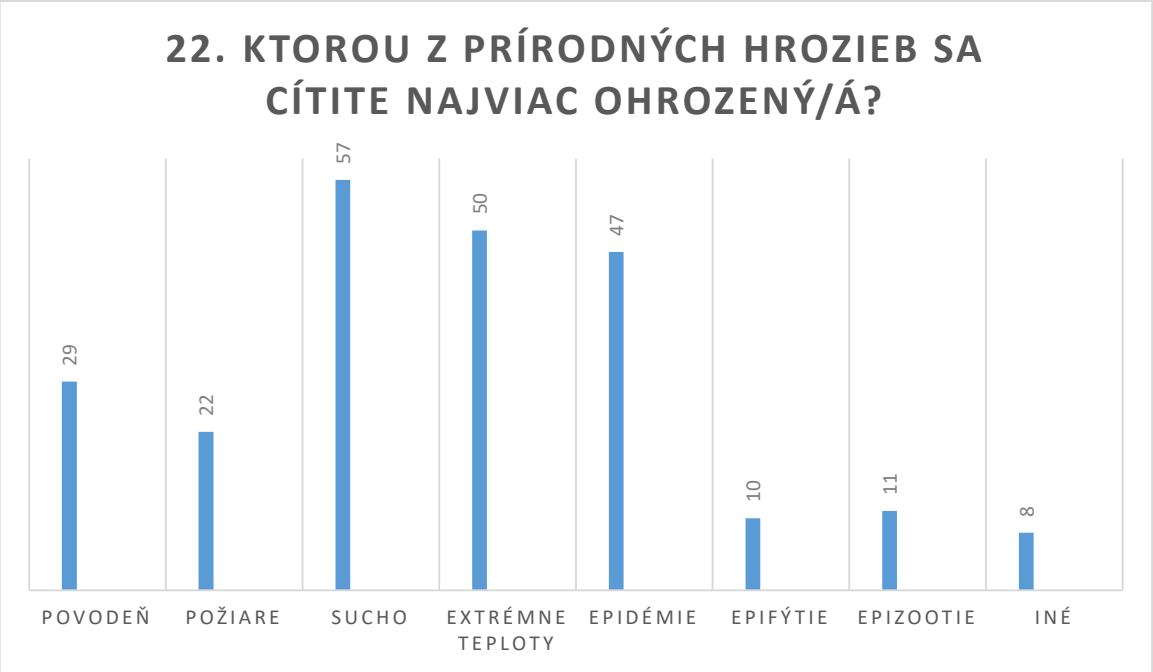
Graf 20 – otázka č. 16 (Zdroj: vlastný, 2023)



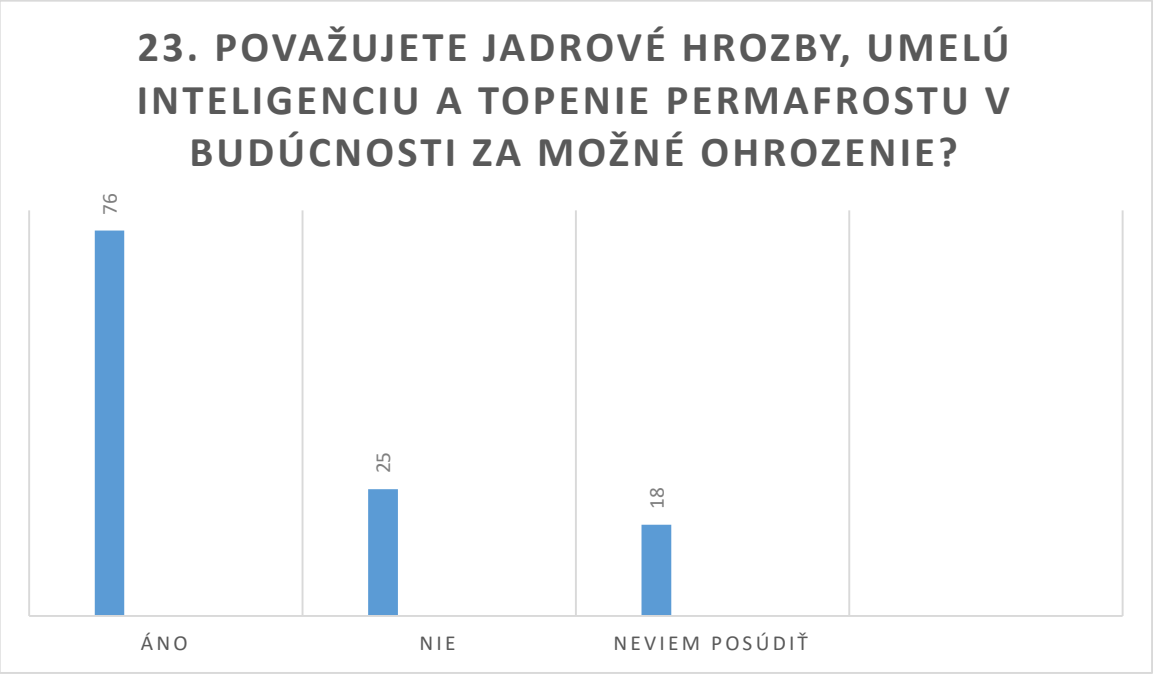
Graf 21 – otázka č. 17 (Zdroj: vlastný, 2023)



Graf 22 – otázka č. 18 (Zdroj: vlastný, 2023)



Graf 23 – otázka č. 19 (Zdroj: vlastný, 2023)



Graf 24 – otázka č. 20 (Zdroj: vlastný, 2023)

7 VYHODNOTENIE DOTAZNÍKOVEJ TECHNIKY

Zvolenie dotazníkovej techniky napomohlo k získaniu všeobecného prehľadu o názoroch a postojoch obyvateľov mesta Gelnica na východnom Slovensku, na súčasnú situáciu z pohľadu bezpečnostných hrozieb. Zvolenie tejto dotazníkovej techniky bolo pre prácu esenciálne. Táto technika dokáže vyhovujúco zhodnotiť názory a postoje opýtaných občanov. Dotazník obsahuje otázky z oblasti bezpečnosti a globálnych hrozieb, ktoré majú alebo môžu mať vplyv na bezpečnosť obyvateľstva. Zisťovalo sa, či sa obyvatelia cítia momentálne bezpečne, či podľa nich Polícia SR a Armáda SR vykonáva náplň svojej práce dostatočne alebo či v budúcnosti rátajú s výskytom nových hrozieb atď.

Zber odpovedí bol uskutočnený pomocou elektronickej a papierovej formy. Dotazník bol tvorený podobou dvadsiatich troch uzavretých výberových otázok. Zúčastnilo sa ho 119 obyvateľov vo veku od 16 do 85, z toho bolo 71 žien a 48 mužov. Úroveň vzdelania jednotlivých respondentov, viď. Graf 3, zavážila pri posudzovaní odpovedí respondentov. Zatiaľ, čo ľudia s nižším vzdelaním pociťovali väčšiu mieru nebezpečenstva z migrácie a korupcie, ľudia s vyšším vzdelaním sa viac obávali kybernetických hrozieb a hrozieb prírodného charakteru. Vzhľadom však na aktuálnu situáciu, sa väčšina opýtaných cíti momentálne bezpečne, viď. Graf 5.

Až 52,1 % respondentov vyjadrilo nespokojnosť s vykonávaním náplne práce Policajného zboru SR a 52,9 % vyjadrilo nespokojnosť s vykonávaním náplne práce Ministerstva obrany a Ministerstva vnútra SR, viď. Graf 6, Graf 7, Graf 8. Občania by privítali vyššiu mieru angažovanosti a aktivity daných orgánov vo sfére bezpečnosti.

So zreteľom na aktuálne globálne hrozby, sa zúčastnení cítia byť najviac ohrození migráciou a extrémizmom a najmenej terorizmom, viď. Graf 9. Až 49,6 % opýtaných by prijalo sprísnenie hraníc so susednými štátmi vplyvom migrácie, viď. Graf 10. Rovnako si opýtaní myslia, že migrácia ohrozuje nie len ich, ale aj bezpečnosť SR, viď. Graf 11, Graf 12. Príčinou zvolených odpovedí bolo podľa všetkého vplyv Rusko-Ukrajinského konfliktu, ktorý vyvolal hustú vlnu migrácie, a tá následne vyvolala strach u občanov východného Slovenska.

Znalosť odboru kybernetickej bezpečnosti sa prejavila u 83,2 % opýtaných, viď. Graf 14. Otázka bezpečnosti práce z domu, tzv. homeoffice, priniesla u vyššieho percenta respondentov voľbu odpovede „NIE“ a „NEVIEM POSÚDIŤ“, viď. Graf 15.

Faktor, ktorý mohol zapríčiniť tak vysoké číslo odpovede „neviem posúdiť“, môže byť spojený s nedostatočnými skúsenosťami s prácou z domu alebo z oblasti kyberbezpečnosti. Na druhú stranu má dostatočne vysoké percento respondentov nainštalovaný antivírusový softvér vo svojom zariadení, čo je viac než uspokojivé zistenie, viď. Graf 16.

Vysoké percento opýtaných občanov, konkrétne 75,6 %, uviedlo, že sa celkovo necítia byť ohrození terorizmom, viď. Graf 17, a taktiež hrozbu terorizmu na území SR považujú za skôr nižšiu (55,5 %) a strednú (40,3 %), než vysokú (4,2 %), viď. Graf 18. Dôvodom prečo to tak je, môže byť fakt, že tento typ hrozby nemá v histórii Slovenska obdoby, a preto občania nevedia, čo táto hrozba môže obnášať a aké dôsledky môže priniesť.

V otázke organizovaného zločinu nenastali žiadne prekvapivé zvraty. Podľa stanovenej hypotézy, kde korupcia spolu s výrobou a distribúciou drog mala predstavovať najvyšší podiel, sa to aj potvrdilo. Korupcia jednoznačne prevýšila ostatné činnosti organizovaného zločinu, ako napr. pranie špinavých peňazí či predaj zbraní, viď. Graf 19. Po diskusii s jednotlivými respondentmi sa ukázalo, že hrozbu korupcie vnímajú na Slovensku dlhodobo, najmä medzi vyššími verejnými činiteľmi a nemyslia si, že tak skoro vymizne.

Zarážajúce percento opýtaných označilo odpoveď „ÁNO“ v otázke, či sa v ich okolí vyskytuje extrémizmus alebo či sa už stretli s extrémistickými prvkami, viď. Graf 20. Prejavy extrémizmu práve v tejto lokalite na východe Slovenska majú zväčša rasový charakter a nebývajú ojedinelé.

Čo sa týka otázky z oblasti pandémii a epidémii, ktoré môžu ohroziť bezpečnosť spoločnosti v budúcnosti, v nej sa ukázalo takmer rovnocenné rozloženie odpovedí medzi „ÁNO“, „NIE“ a „NEVIEM POSÚDIŤ“, viď. Graf 22. Na druhú stranu, popredné priečky medzi hrozbami, ktorými sa obyvatelia cítia byť najviac momentálne ohrození sú sucho, extrémne teploty a epidémie, pričom za najmenej ohrozujúce považujú epifýtie a epizootie, viď. Graf 23.

Jadrové hrozby, umelá inteligencia, topenie permafrostu, súhrnným názvom označené ako hrozby budúcnosti vďaka dotazníku ukázali, že dokážu mať vplyv na predpoklad ohrozenia bezpečnosti spoločnosti do budúcnosti, viď. Graf 24.

8 METÓDA WHAT IF A MATICA RIZÍK

Proces analýzy rizík predstavuje v diplomovej práci nevyhnutný krok. Slúžiť bude v rámci prípravy na mimoriadne či krízové situácie v oblasti globálnych hrozieb. V nadväznosti na dotazníkovú techniku sú metódy What-if a matica rizík, ktoré sú v úzkej korelácii. Vďaka dotazníkovej technike sa zvolili najzávažnejšie hrozby z pohľadu opýtaného obyvateľstva. Tieto vybrané hrozby sa následne aplikovali do metódy What-if. Dôvodom výberu vyššie spomenutých metód bol fakt, že metóda What-if dokáže nadviazať na získané odpovede z dotazníkovej techniky a ďalej ich v konkrétnom smere rozvinúť.

8.1 Metóda What-if

Ide o induktívnu metódu, ktorá pracuje na báze slov „čo sa stane ak“. Metóda What-if sa využíva na vyhľadávanie potenciálnych scenárov. Tvorba tejto metódy býva často spojená aj s využitím metódy brainstormingu, ktorá funguje na princípe využitia kreativity pri práci v tíme a rôznorodosti odpovedí, s cieľom dosiahnutia čo najkvalitnejších výsledkov. Kvalita spracovania metódy odpovedá skúsenostiam, znalostiam a vedomostiam jednotlivých členov tímu.

Metóda bola zvolená s cieľom vytvorenia prehľadu globálnych hrozieb, ktoré môžu ohroziť bezpečnosť obyvateľstva. Do metódy bolo zahrnutých deväť globálnych hrozieb, konkrétne terorizmus, migrácia, hybridná vojna, organizovaný zločin, extrémizmus, kybernetické hrozby, ozbrojený konflikt, epidémie a pandémie a nové hrozby budúcnosti. Vybrané boli priame príklady možných scenárov s vytvorenými dôsledkami a následnými návrhmi opatrení k minimalizácii dopadov či prevencii jednotlivých hrozieb do budúcnosti.

Vďaka vypracovaniu tejto metódy sa získal určitý prehľad o daných globálnych hrozbách, ktoré boli spracované pomocou dotazníkovej techniky. V nadväznosti na túto metódu je matica rizík, ktorej závery a vyhodnotenia sú zahrnuté v kap. 9.2. a 9.4.

Tabuľka 2 – evidencia hrozieb a metóda What-if (Zdroj: vlastný, 2023)

p.č.	Čo sa stane ak...?	Dôsledok	Návrh opatrenia k minimalizácii	P	D	R
1.	vznikne teroristický útok v letiskovej hale	vyvolanie strachu, panika, straty na majetkoch a životoch	prísnejšie kontroly vstupu do priestorov letiska	B	III.	8
2.	sa zvýši medzinárodná migrácia	väčšia pravdepodobnosť vzniku medzinárodnej kriminality	zavedenie podrobných kontrol na hraniciach jednotlivých štátov	C	II.	9

3.	dôjde k vzniku hybridnej vojny	narušenie procesov právneho štátu, chod demokratických inštitúcií a vnútornej bezpečnosti	boj proti dezinformáciám, zabezpečenie štátu pomocou vojenských i nevojenských techník	C	IV.	14
4.	narastú rôzne formy organizovaného zločinu	ekonomické straty, ujmy na zdraví, úmrtia ľudí	posilnenie hliadok a policajného zboru, náhodné kontroly podozrivých budov, zariadení, osôb atď.	D	III.	15
5.	expanduje vznik extrémistických aktivít	zvrhnutie liberálneho demokratického poriadku a nahradenie ho poriadkom v súlade s ideami príslušnej extrémistickej skupiny	zásah AKT tímu, novelizácia Koncepcie pre boj proti extrémizmu, vznik Národnej jednotky boja proti extrémizmu	D	II.	13
6.	obyvatelia nebudú dostatočne edukovaní v oblasti kybernetickej bezpečnosti	vznik a rozšírenie kybernetických hrozieb	zvýšenie povedomia medzi občanmi SR v danej problematike, školenia, workshopy atď.	B	II.	5
7.	sa rozšíri ozbrojený konflikt za hranice štátu	možné rozpútanie svetovej vojny	podpísanie mierových dohôd, medzinárodných zmlúv o zákaze používania, výroby, skladovania ZHN	B	IV.	11
8.	vzniknú nové a neznáme epidémie a pandémie	straty na ľudských životoch	zavedenie povinnej vakcinácie, globálne zdravotnícke opatrenia	C	IV.	14
9.	sa vytvoria nepravé videá skutočných ľudí prostredníctvom technológie AI	narušenie dôstojnosti, živobytia, integrity ľudských bytostí	dôsledný dohľad nad technológiou AI	C	II.	9

Tabuľka 3 – matica rizík (Zdroj: vlastný, 2023)

D/P	A	B	C	D
I.	1	3	6	10
II.	2	5	9	13
III.	4	8	12	15
IV.	7	11	14	16

Tabuľka 4 – kategórie pravdepodobnosti (Zdroj: vlastný, 2023)

ozn.	názov	popis
A	nepravdepodobné	nestane sa nikdy
B	málo pravdepodobné	1x za 5 rokov
C	pravdepodobné	1x za rok
D	vysoko pravdepodobné	1x za mesiac

Tabuľka 5 – kategórie závažnosti dopadu (Zdroj: vlastný, 2023)

ozn.	názov	popis	kvalitatívne hodnotenie dopadu
I.	bezvýznamné	nemá dopad, nedôjde k ohrozeniu	Aktívum je dostatočne odolné voči pôsobeniu hrozieb a dopad je zanedbateľný.
II.	významné	ľahký dopad na život a zdravie obyvateľov	Aktívum je mierne ohrozené hrozbami a dopad je vyšší než minimálny.
III.	kritické	stredný dopad na život a zdravie obyvateľov	Aktívum je vysoko náchylné k hrozbám a dopad je značný.
IV.	katastrofické	fatálny dopad na život a zdravie obyvateľov	Aktívum nie je vôbec chránené voči vplyvom hrozieb a dopad je tragický.

Tabuľka 6 – kategórie prijateľnosti (Zdroj: vlastný, 2023)

ozn.	názov	popis
1 až 7	prijateľné	riziko je prijateľné, nepredstavuje žiadnu výraznú hrozbu
8 až 13	stredne prijateľné	riziko je v stredne prijateľnej kategórii, je potrebné vypracovanie náhradného plánu v prípade zhoršenia situácie
14 až 16	neprijateľné	riziko je neprijateľné, opatrenia k náprave musia byť zahájené ihneď

Tabuľka 7 – matica rizík evidovaných hrozieb podľa poradového čísla (Zdroj: vlastný, 2023)

D/P	A	B	C	D
I.				
II.		6	2,9	5
III.		1		4
IV.		7	3,8	

8.2 Matica rizík

Matica rizík slúži k posúdeniu rizika súvisiaceho s analyzovanými hrozbami. Pomocou nej sa dajú kombinovať kvalitatívne a semikvantitatívne klasifikácie dopadov a následkov s cieľom vytvorenia hodnoty úrovne vzniknutého rizika. Pri tejto metóde je potrebné si uvedomiť, že matica rizík nebezpečie/ohrozenie neidentifikuje. Slúži len k posúdeniu do akej miery je riziko ešte prijateľné, resp. bez následkov, a kedy už naberá neprijateľný charakter. Vďaka matici rizík sme schopní určiť, ktoré hrozby si vyžadujú podrobnejšiu analýzu alebo ktoré potrebujú byť riešené prioritne.

Matica rizík, vytvorená pre túto prácu obsahuje štvorbodovú stupnicu dopadov a rovnako štvorbodovú stupnicu pravdepodobnosti. Stupnica prijateľnosti bola navrhnutá tak, aby čo najvernejšie dokázala opísať mieru adekvátnosti, v tomto prípade číselným rozsahom 1 až 16 spolu so slovným popisom.

8.3 Vyhodnotenie metódy What-if a matice rizík

V tejto práci sa došlo ku kvalitatívnej analýze a hodnoteniu hrozieb a rizík. V Tabuľka 2 sa nachádza 9 vybraných hrozieb s následkami a možnými návrhmi opatrení do budúcna. K splneniu výpovednej hodnoty danej metódy boli využité kategórie pravdepodobnosti P (A,B,C,D), dopadu D (I.,II.,III.,IV.) a prijateľnosti R (1 až 16). Následne sa vďaka takto vypracovaným kategóriám mohli priradiť jednotlivé statusy, ktoré boli vyberané z Tabuľka 4, Tabuľka 5, Tabuľka 6.

Ku klasifikácii boli použité slovné pojmy, ktoré definovali stupnicu dopadov hrozieb. Vybrané slovné pojmy boli zvolené tak, aby čo najlepšie dokázali pokryť danú situáciu, stupnicu dopadov hrozieb a stanoviť prijateľné medze. V tomto prípade šlo o bezvýznamné, významné, kritické, katastrofické, prijateľné, stredne prijateľné a neprijateľné slovné hodnotenie.

V Tabuľka 3 je vypracovaná matica rizík, ktorú horizontálne tvorí kategória pravdepodobnosti, vertikálne kategória závažnosti dopadu a vo vnútri sú obsiahnuté hodnoty ich vzájomného vzťahu. Zelenou farbou sú označené polia v kategórii prijateľné, žltou farbou stredne prijateľné a červenou farbou neprijateľné riziká, ktoré majú katastrofálny dopad.

V Tabuľka 7 sa nachádza finálne zobrazenie evidovaných hrozieb v matici rizík. Každá hrozba bola jednotlivo a objektívne posúdená zároveň aj s možnými dôsledkami

a návrhmi opatrení do budúcna. Na základe tohto boli hrozbám priradené konkrétne hodnoty. Ich dopad sa následne odčítal z matice rizík s tým sa získali požadované medze nebezpečnosti.

Z Tabuľka 7 vyplýva, že hrozba č. 6, z oblasti kybernetickej bezpečnosti, mala posúdenie P (B) a D (II.). Tým získala číselnú hodnotu 5, ktorá má v matici rizík umiestnenie v zelenej časti, tzn. že táto hrozba predstavuje prijateľné riziko. Na druhej strane, hrozby č. 3, 4 a 8, z oblasti hybridnej vojny, organizovaného zločinu, epidémii a pandémii sa umiestnili v červenej časti matice. Z toho vyplýva, že tieto hrozby sú považované za najzávažnejšie, predstavujú neprijateľné riziko a ich dopad na aktívum, čo je v našom prípade zdravie a život človeka, je katastrofický.

Hrozby č. 1, 2, 5, 7 a 9 (teroristický útok v letiskovej hale, medzinárodná migrácia, extrémistické aktivity, ozbrojený konflikt a negatívny vplyv umelej inteligencie) sa vyskytujú v žltej zóne, čo vypovedá o tom, že tieto hrozby majú stredne prijateľný potenciál v rozmedzí hodnôt od 8 po 13. Vyšší dôraz je najmä kladený na hrozbu expanzie extrémistických aktivít, ktorá už hraničí s červenou oblasťou matice rizík. V prípade tejto hrozby, by bolo vhodné mať na zreteli možné potenciálne následky a pomaly sa pripravovať na preventívne opatrenia, aby sa nedostala do najvyššieho stupňa ohrozenia aktíva.

Záverom vyhodnotenia metód What-if a matice rizík je pozitívum, že len jedna tretina rozoberaných hrozieb predstavuje pre aktívum ten najhorší možný scenár, aj to sa tieto hrozby nenachádzajú v poslednom červenom poli, ale na prelome so žltým poľom.

9 NÁVRHY OPATRENÍ

V rámci tejto diplomovej práci boli spomenuté, objasnené a identifikované globálne hrozby, ktoré aktuálne môžu ohroziť, resp. narušiť bezpečnosť obyvateľstva Slovenskej republiky. Nižšie je poskytnutý výber najzávažnejších hrozieb. K týmto hrozbám je vhodné vytipovanie určitých návrhov opatrení do budúcnosti, či už v rámci prevencie alebo k minimalizácii ich dopadov.

Ad A) Terorizmus

Hrozba teroristických útokov je v dnešnej dobe na veľmi vysokej úrovni. Odhalenie teroristických útokov je náročné a častokrát neuskutočniteľné, vzhľadom na nedostatok informácii. V súčasnosti je mnoho orgánov činných v boji proti terorizmu. Presne definované tabuľky či postupy k odhaleniu budúcich teroristických útokov neexistujú. Je však pár možných preventívnych krokov, ktoré môžu viesť k minimalizácii dopadu teroristických útokov. Medzi ne sa dá zaradiť sprísnenie hraničných kontrol, odrezanie teroristických skupín od finančných prostriedkov, získavanie interných dát od leteckých spoločností o prepravených cestujúcich, prístup k osobným informáciám z rôznych externých databáz, redukovanie prístupu občanov k nebezpečným zbraniam či prevencia šírenia radikalizmu na sociálnych sieťach.

Ad B) Migrácia

Vo svete, kde sa migrácia stala fenoménom dnešnej doby a má potenciál stále narastať, je potrebné prísť s krokmi, ako s týmto javom do budúcna pracovať. Z výsledkov vypracovaného dotazníka sa zistilo, že obyvatelia sa cítia byť ohrození migráciou a taktiež vnímajú migráciu ako hrozbu pre slovenský štát. Preto je vhodné prísť s niekoľkými návrhmi, aby tomu tak nebolo. Bude esenciálne riešiť príčiny nedobrovoľnej migrácie, vytvoriť viac legálnych a bezpečných ciest migrácie a uvedomiť si pozitívne prínosy migrácie napr. obohatenie kultúry, zvykov, tradícii, skúseností, myšlienok, vzdelania, pracovných miest atď.

Ad C) Hybridné hrozby

Hybridné hrozby sú kombináciou konvenčných a nekonvenčných metód vedenia vojny, ako sú propaganda, klamstvo, sabotáž a iné nevojenské taktiky. Z toho vyplýva, že nemožno sa sústrediť len na vojenské propagovanie hybridných hrozieb, ale taktiež aj iné formy nevojenských taktík. Jednou z ciest, ako čeliť hybridným hrozbám je to, že sa im

predchádza "pasívnymi" prvkami, ako je zvýšená odolnosť voči šoku alebo prekvapeniu, ako aj aktívnejšími prvkami vrátane spoľahlivých opatrení na prípravu a ochranu funkcií a štruktúr, ktoré sa s najväčšou pravdepodobnosťou stanú terčom hybridných útokov. Vytvorenie podporných tímov pre boj proti hybridným hrozbám, posilnenie globálnej dôvery a globálneho finančného systému, odborná príprava a cvičenia v prevencii proti hybridným hrozbám aj to sú návrhy k minimalizácii dopadu hybridných hrozieb.

Ad D) Organizovaný zločin

Organizovaný zločin nepredstavuje enormnú hrozbu len pre občanov, ale aj pre podniky, inštitúcie a hospodárstvo. Zločinecké skupiny nepôsobia len na území daného štátu, ale dokážu presahovať do iných nielen okolitých štátov, tým pádom zvyšujú riziko nebezpečenstva. Momentálne je funkčných množstvo organizácii, agentúr, inštitúcii a projektov v rámci boja proti organizovanému zločinu. V prevencii proti organizovanému zločinu je možné podstúpiť nasledujúce kroky, ako napr. zlepšenie medzinárodnej justičnej spolupráce, zdieľanie osvedčených a overených postupov medzi jednotlivými štátmi, posilnenie frekventovaných hliadok policajných jednotiek, či vyšší výskyt náhodných, neohlásených kontrol. Názor opýtaných občanov v dotazníku jasne preukázal, že obyvatelia považujú za najzávažnejšiu formu organizovaného zločinu korupciu. Cesty ako postupovať v boji proti korupcii sú rôzne a zapojiť sa k nim dokážu aj samotní obyvatelia. Monitorovanie peňazí či majetku v danej inštitúcii, počítanie hmotných alebo nehmotných zásob v komunitách, používanie sociálnych sietí k zdieľaniu podozrení z korupcie a taktiež vytvorenie falošnej peňažnej meny môže byť efektívnou cestou k zisteniu osôb podporujúcich prijímanie úplatkov.

Ad E) Extrémizmus

Jednou z ďalších foriem nebezpečenstva, ktorá predstavuje pre opýtaných občanov hrozbu, bol extrémizmus. Ako sa aj preukázalo v dotazníku, mnoho opýtaných sa priamo stretlo s prejavmi nenávistného charakteru. Niektoré spôsoby boja proti terorizmu zahŕňajú: nahlasovanie podozrivých aktivít príslušným orgánom činným v trestnom konaní, emočnú či finančnú podporu obetiam extrémistických útokov, edukáciu o príčinách extrémizmu a ako mu predchádzať, či vyvíjanie tlaku na vedúcich predstaviteľov k prijatiu opatrení proti extrémistickým skupinám a ideológiám.

Ad F) Kybernetické hrozby

Pri kybernetickej bezpečnosti je nutné si uvedomiť, ako zraniteľná je táto oblasť a aké škody môže priniesť jej narušenie. Táto kyber-oblasť je veľmi úzko spätá s ľudským faktorom. K porušeniu kybernetickej bezpečnosti, ale môže dôjsť aj vplyvom prírodných podmienok. Treba však poukázať na fakt, že v tomto prípade by v najhoršom scenári došlo k strate alebo poškodeniu údajov. V druhom prípade, ak sa jedná o ovplyvnenie kybernetickej bezpečnosti človekom, je nutné počítať s oveľa katastrofickejšími následkami. Do úvahy pri takomto narušení je potrebné vziať poškodenie, úplné zničenie, krádež, zneužitie či zmenu osobných dát. Proti kybernetickej kriminalite sa dá bojovať rôznymi spôsobmi, ako napr. aktívne využívať balíky bezpečnostných služieb, používať silné heslá, pravidelne si aktualizovať softvér na zariadeniach, spravovať bezpečnostné nastavenia na webových stránkach, konzultovať o nástrahách na internete s deťmi a staršími ľuďmi a taktiež informovať a zdieľať informácie o závažných narušeniach bezpečnosti.

Ad G) Ozbrojený konflikt

Hrozba ozbrojeného konfliktu nie je pre Slovensko až tak nereálna, keďže od februára 2022 prebieha Ruská invázia na Ukrajine, ktorá je východným susedom Slovenskej republiky. Existuje niekoľko opatrení, ktoré možno prijať na predchádzanie ozbrojeným konfliktom a ich zmiernenie. Všetky strany konfliktu by mali prijať opatrenia na minimalizáciu škôd spôsobeným civilistom a civilným objektom a nesmú vykonávať útoky, pri ktorých sa nerozlišuje medzi civilistami a bojovníkmi alebo ktoré spôsobujú neprimerané škody civilistom.

Ad H) Prírodné hrozby a epidémie

Čo sa týka prírodných hrozieb snaha o návrhy opatrení, alebo snaha o minimalizáciu dopadov na obyvateľstvo, či životné prostredie, je koniec koncov márna. Nie sme schopní byť na prírodné hrozby adekvátne pripravení. Miera zásahu environmentálnych hrozieb môže svojou silou a rozsahom vždy prekvapiť. Jedinou cestou ako sa teoreticky brániť pred naturogénnymi hrozbami môže byť poučenie z historických udalostí, či prevencia. To isté sa týka epidémii a pandémii. Voči novým epidemiologickým hrozbám sme v podstate bezbranní. Stále sa objavujú úplne nové hrozby, s ktorými naša spoločnosť nemá skúsenosti s tým pádom na ne nie sme dostatočne vybavení, či pripravení.

Ad I) Anonymné hrozby

Hrozby nového storočia, neznáme hrozby, či anonymné hrozby patria neoddeliteľne do skupiny hrozieb vyvolávajúcich potenciálne nebezpečenstvo. Čo však tieto hrozby budúcnosti dokážu priniesť a ako presne ohroziť bezpečnosť ľudstva sa bohužiaľ nedá presne stanoviť, dokážu sa však predikovať možné následky a vytvárať preventívne kroky. U jadrovej vojny by sa mohlo jednať o obmedzenie spravovania a nakladania s tak nebezpečným materiálom alebo na druhú stranu vytvoriť dostatočne silné antilátky. Napredovanie vývoja umelej inteligencie sa zastaviť nedá, s takým rýchlym postupom v technike zároveň aj narastá možné riziko. Na jednu stranu je myšlienka skvelá, na strane druhej sa dokáže veľmi ľahko vymaniť spod kontroly a spôsobiť nemalé škody, nielen na majetku ale čo je horšie na zdraví a živote človeka. Konkrétnym cieľom ako bojovať proti „temnej“ stránke umelej inteligencie by sa napríklad mohlo dosiahnuť prostredníctvom naprogramovaných autonómnych systémov a aj prísnejšími zákonmi o ochrane osobných údajov.

ZÁVER

Témou diplomovej práce boli hrozby 21. storočia a ich vplyv na ľudstvo. Hlavným cieľom práce bolo zistenie postojov a pocitov opýtaných obyvateľov, ktorí reprezentovali určitú vzorku slovenského národa. Práve obyvatelia okresného mesta Gelnica boli zvolení k dotazovaniu, z dôvodu tesnej blízkosti s ukrajinskými hranicami. Ako sa ukázalo v dotazníkovej technike, hrozba medzinárodnej migrácie obyvateľom nie je cudzia a predstavuje vysokú mieru nebezpečnosti.

Mnohokrát pri vnútroštátnych a regionálnych konfliktoch, ktoré negatívne ovplyvňujú bezpečnosť, dochádza najmä v dôsledku nedostatočného zaistenia bezpečia vlastnej obrany a bezpečnosti svojich obyvateľov. Nielen hrozby, ktoré ohrozujú majetok, zdravie a život ľudí sú závažné. Poškodzovanie životného prostredia ohrozuje blahobyt, zdravie a prežitie miestneho obyvateľstva, čo zvyšuje jeho zraniteľnosť na roky a dokonca desaťročia. Keďže ľudstvo vždy počítalo svoje vojnové obete v podobe mŕtvych a zranených vojakov a civilistov, zničených miest a živobytia, životné prostredie je často skrytou obeťou vojny. V priebehu rokov strany ozbrojených konfliktov znečisťovali vodu, podpaľovali úrodu, vyrubovali lesy, otrávili pôdu a zabíjali zvieratá, aby získali vojenskú výhodu. Zhoršovanie a ničenie životného prostredia v dôsledku konfliktov si vyberá daň nielen na samotnej prírode, ale tiež zhoršuje potravinovú a vodnú neistotu a ničí zdroje obživy.

V teoretickej časti práce som sa venovala základným pojmom, ako sú bezpečnosť, hrozba, riziko, bezpečnostné prostredie apod. z dôvodu lepšej, jednoduchšej orientácie a porozumeniu diplomovej práce. Definícia vybraných hrozieb 21. storočia, ako terorizmus, migrácia, hybridné hrozby, organizovaný zločin, extrémizmus, kybernetické hrozby, prírodné hrozby a epidémie, bola pre prácu taktiež esenciálna. Samostatná kapitola bola venovaná anonymným hrozbám alebo hrozbám budúcnosti. Čo však treba podotknúť je fakt, že tieto hrozby už v spoločnosti majú svoje miesto, je len otázkou času, kedy začnú pre obyvateľstvo predstavovať nebezpečie.

Praktická časť bola založená na vytvorení dotazníka, ktorý obsahoval 23 otázok z oblasti bezpečnosti. Cieľom tejto metódy bolo získanie obrazu o tom, ako obyvatelia mesta Gelnica vnímajú hrozby 21. storočia, ktoré z hrozieb považujú za najzávažnejšie a či sa momentálne cítia bezpečne. Zarážajúcim zistením bolo, že hrozba extrémizmu získala tak vysoký podiel odpovedí. O malé percento bola pred hrozbou extrémizmu,

hrozba migrácie, čo však vyplýva zo súčasnej situácie na blízkych východných hraniciach, ktorá súvisí s ozbrojeným konfliktom na Ukrajine. Vďaka získaným odpovediam z dotazníka som sa presunula k vytvoreniu metódy What-if, v ktorej som pracovala s deviatimi najzávažnejšími hrozbami, s následnými dôsledkami a návrhmi opatrení do budúcna. Hodnotenie metódy What-if som dosiahla pomocou spracovania metódy matice rizík. Hodnotenie bolo uskutočnené objektívnym názorom a prostredníctvom vytvorených tabuliek.

Posledná kapitola praktickej časti bola venovaná návrhom opatrení k deviatim vytýčeným hrozbám. Každej hrozbe boli priradené určité návrhy krokov či už k prevencii alebo minimalizácii dopadov.

Záverom tejto diplomovej práce by som zhodnotila, že obyvatelia na Slovensku sa v rámci možností cítia bezpečne, uvítali by však väčšiu mieru angažovanosti bezpečnostných zložiek a pociťujú prirodzené obavy, či už z nových pandemických a epidemiologických hrozieb, prírodných hrozieb, hrozieb súčasnosti alebo anonymných hrozieb budúcnosti. Čo však treba mať na pamäti je fakt, že najväčším zdrojom ohrozenia pre našu civilizáciu, je táto civilizácia sama.

ZOZNAM POUŽITEJ LITERATÚRY

2020 Defence Strategic Update [online], 2020. Canberra: © Commonwealth of Australia [cit. 2022-11-25]. ISBN 978-1-925890-26-6. Dostupné z: https://www.defence.gov.au/sites/default/files/2020-11/2020_Defence_Strategic_Update.pdf

Aj malá nukleárna vojna by spôsobila hladomor. Naše modely sú zastarané, 2022. *Trend* [online]. Bratislava: © News and Media Holding, a.s [cit. 2022-12-09]. Dostupné z: https://www.trend.sk/spravy/aj-mala-nuklearna-vojna-sposobila-hladomor-nase-modely-su-zastarane?itm_brand=trend&itm_template=other&itm_modul=topic-articles&itm_position=1

Aktivity: Boj proti obchodovaniu s ľuďmi, 2020. *Medzinárodná organizácia pre migráciu* [online]. Bratislava: © Medzinárodná organizácia pre migráciu (IOM) [cit. 2022-12-08]. Dostupné z: https://www.iom.sk/sk/aktivity/presidlovanie-utecencov/28-aktivity/boj-proti-obchodovaniu-s-ludmi.html#:~:text=Medzi%20formy%20obchodovania%20s%20%C4%BEu%C4%8Fmi%20patr%C3%AD%20n%C3%BAten%C3%A1%20pr%C3%A1ca%2C,pracovnej%20sile%20a%20na%20dopyt%20po%20sexu%C3%A1lnych%20slu%C5%BEb%C3%A1ch.

Artificial intelligence, machine learning, neural networks, 2022. *Data Mind* [online]. Praha: © Data Mind [cit. 2022-12-11]. Dostupné z: https://www.datamind.cz/en/services/Artificial_intelligence_machine_learning_deep_neural_networks?msclkid=cf96bdb7ed4f1b1d466dde222a53e5b7

Bezpečnostné riziká, 2022. *Ministerstvo vnútra Slovenskej republiky* [online]. Bratislava: © Ministerstvo vnútra SR [cit. 2022-11-19]. Dostupné z: https://minv.sk/?Bezpecnostne_rizika

BILAL, Arsalan, 2021. Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. *NATO Review* [online]. NATO Review © [cit. 2022-11-22]. Dostupné z: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

BÍNEK, Zdeněk, 2020. Začátek roku 2020 v kyberbezpečnosti: útoky na nemocnice, spolupráce na dálku, VPN provoz. *Security Magazín*. Praha: © Security Media, **26**(124-2), s. 19-21. ISSN 1210-8723.

BOUDREAU, Diane et al., 2022. Flood. *National Geographic* [online]. Washington D.C.: ©National Geographic Society [cit. 2022-11-28]. Dostupné z: https://education.nationalgeographic.org/resource/flood

BRATKO, Artem, Denys ZAHARCHUK a Valentyn ZOLKA, 2021. Hybrid warfare – a threat to the national security of the state. *Revista de Estudios en Seguridad Internacional* [online]. 7(1), 147-160 [cit. 2022-11-23]. Dostupné z: doi:10.18847/1.13.10

BROOKS, Ashley, 2021. What Is a "Zero-Day" Attack? A Cybersecurity Nightmare Explained. *Rasmussen university* [online]. © Rasmussen College [cit. 2022-11-20]. Dostupné z: https://www.rasmussen.edu/degrees/technology/blog/zero-day-attack/

Brožúry a letáky, 2022. In: *Ministerstvo vnútra SR* [online]. Bratislava: ©Ministerstvo vnútra SR [cit. 2022-12-08]. Dostupné z: https://www.minv.sk/?brozury-a-letaky

CBRNews, 2022. *CBRNe WORLD*. Winchester: © Falcon Communication, **17**(3), s. 4-6. ISSN 2040-2724.

ČESKO, 2000. Zákon č. 239/2000 Sb. Zákon o integrovaném záchranném systému a o změně některých zákonů. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-239

Cyber Attack, 2022. *Imperva* [online]. © Imperva. [cit. 2022-12-09]. Dostupné z: https://www.imperva.com/learn/application-security/cyber-attack/

DE MULINEN, Frédéric, 2017. *Příručka práva ozbrojeného konfliktu pro ozbrojené síly*. Vyd. 2. Praha: Ministerstvo obrany České republiky. ISBN 978-80-7278-692-3.

DENCHAK, Melissa, 2018. Permafrost: Everything You Need to Know. *NRDC* [online]. © Natural Resources Defense Council [cit. 2022-12-16]. Dostupné z: https://www.nrdc.org/stories/permafrost-everything-you-need-know

DITRICHOVÁ, Petra a Marek JUKL, 2017. *Základní prameny mezinárodního humanitárního práva*. Praha: Ministerstvo obrany České republiky. ISBN 978-80-7278-698-5.

ECO, Umberto, 2021. *Migrace, nesnášenlivost: Věčný fašismus*. Vyd. 1. Praha: Argo. ISBN 978-80-257-3379-0.

Epidemic, Endemic, Pandemic: What are the Differences?, 2021. *Columbia* [online]. New York: © Columbia University [cit. 2022-11-28]. Dostupné z:

https://www.publichealth.columbia.edu/public-health-now/news/epidemic-endemic-pandemic-what-are-differences

Extremism, 2022. *Federal Ministry of the Interior and Community* [online]. Berlín: © Federal Ministry of the Interior and Community [cit. 2022-11-26]. Dostupné z: https://www.bmi.bund.de/EN/topics/security/extremism/extremism-node.html

FILIPEC, Ondřej, 2017. *Fenomén terorismus: česká perspektiva*. Olomouc: Univerzita Palackého v Olomouci. ISBN 978-80-244-5040-7.

FREEDMAN, Jane, Gunhild HOOGENSEN GJØRV a Velomahanina RAZAKAMAHARAV, 2021. Identity, stability, Hybrid Threats and Disinformation. *Icono14* [online]. 19(1), 38-69 [cit. 2022-11-22]. ISSN 1697-8293. Dostupné z: doi:10.7195/ri14.v19i1.1618

FRÜHLING, Stephan a Andrew O'NEIL, 2021. *Alliances, Nucear Weapons and Escalation*. Canberra: ANU Press. ISBN 978-1-76046-491-2.

GEORGESCU, Elena, 2021. Man-in-the Middle (MITM) Attack. *Heimdal Security* [online]. Kodaň: ©Heimdal Security [cit. 2022-11-30]. Dostupné z: https://heimdalsecurity.com/blog/man-in-the-middle-mitm-attack/#:~:text=A%20man-in-the-middle%20attack%20represents%20a%20cyberattack%20in%20which,that%20the%20two%20parties%20were%20trying%20to%20share.

HESTERMAN, Jennifer, 2019. *Soft Target Hardening*. Vyd. 2. New York: Routledge. ISBN 978-1-138-39108-6.

IVANČÍK, Radoslav, 2022. *Bezpečnosť: Teoreticko-metodologické východiská*. Plzeň: Aleš Čeněk. ISBN 978-80-7380-873-0.

JOZEFOVÁ, Jana, Vladimír VEČEREK a Lenka VEČERKOVÁ, 2015. *Základy veterinární péče* [online]. In:. Brno [cit. 2022-11-29]. Dostupné z: https://www.vfu.cz/files/2390_71_vecerkova_skripta-zaklady-veterinarni-pece.pdf

JUŘÍČEK, Ludvík a Petr ROŽNÁK, 2014. *Bezpečnost, hrozby a rizika v 21. století*. Ostrava: Key Publishing. ISBN 978-80-7418-201-3.

KARAFFA, Vladimír, Martin HRINKO, Jaromír ZŮNA a kol., 2022. *Vybrané kapitoly o bezpečnosti*. Praha: Vysoká škola CEVRO Institut. ISBN 978-80-87125-35-9.

KEMENESI, G. et al., 2022. Isolation of infectious Lloviu virus from Schreiber's bats in Hungary. *Nature Communications* [online]. **13**(1706) [cit. 2022-11-11]. Dostupné z: doi:https://doi.org/10.1038/s41467-022-29298-1

MACMILLAN, Amanda a Jeff TURRENTINE, 2021. Global Warming 101. *NRDC* [online]. New York: © Natural Resources Defense Council [cit. 2022-11-28]. Dostupné z: https://www.nrdc.org/stories/global-warming-101

MAKATURA, Ivan, 2021. Zraniteľnosti systémov a zariadení. *Bezpečnosť v praxi* [online]. Žilina: S-EPI [cit. 2022-11-20]. Dostupné z: https://www.bezpecnostvpraxi.sk/clanok-z-titulky/zranitelnosti-systemov-a-zariadeni-ttbvp.htm

MAREŠ, Miroslav a kol., 2013. *Krízový management: Případové bezpečnostní studie*. Praha: Ekopress. ISBN 978-80-86929-92-7.

MARR, Bernard, 2020. Is Artificial Intelligence (AI) A Threat To Humans?. *Forbes* [online]. © Forbes Media LLC. [cit. 2022-12-11]. Dostupné z: https://www.forbes.com/sites/bernardmarr/2020/03/02/is-artificial-intelligence-ai-a-threat-to-humans/?sh=3861e9dc205d

Melting permafrost: why is it a serious threat to the planet?, 2022. *Iberdrola* [online]. Bilbao: © Iberdrola, S.A [cit. 2022-11-28]. Dostupné z: https://www.iberdrola.com/sustainability/what-is-permafrost

Mimořádná událost. Definice, druhy a řešení prostřednictvím IZS, 2022. *BOZP.cz* [online]. Praha: ©CRDR spol. s r.o. [cit. 2022-11-20]. Dostupné z: https://www.bozp.cz/aktuality/mimoradna-udalost/

NORWOOD, Melanie, 2022. Extremist Groups in Criminology: Definition & Overview. *Study.com* [online]. ©Study.com [cit. 2022-11-26]. Dostupné z: https://study.com/academy/lesson/extremist-groups-definition-criminology-lesson.html

NOVOTNÝ, Adolf, 2004. *Slovník medzinárodných vzťahov*. Bratislava: Magnet Press. ISBN 80-8916-901-5.

PETERSEN, Robert, 2022. Lies, damned lies and Russian statistics. *CBRNe WORLD*. Winchester: © Falcon Communication, **17**(3), s. 57-61. ISSN 2040-2724.

PORADA, Viktor a kol., 2019. *Bezpečnostní vědy*. Plzeň: Aleš Čeněk. ISBN 978-80-7380-758-0.

Pravidlá pre hlásenie incidentu a zraniteľnosti, 2021. *CSIRT* [online]. Bratislava: Ministerstvo investícií, regionálneho rozvoja a informatizácie SR [cit. 2022-11-20]. Dostupné z: https://www.csirt.gov.sk/en/pravidla-pre-hlasenie-incidentu-a-zranitelnosti/index.html

REGAN, Joseph a Ivan BELCIC, 2022. What Is Malware? The Ultimate Guide to Malware. *AVG* [online]. © Copyright Avast Software [cit. 2022-11-30]. Dostupné z: https://www.avg.com/en/signal/what-is-malware

RENDALL, Matthew, 2022. Nuclear war as a predictable surprise. *Global Policy* [online]. **13**(5), s. 782-791 [cit. 2022-12-09]. ISSN 1758-5880. Dostupné z: doi:10.1111/1758-5899.13142

ROGERS, Kara, 2022. Pandemic. *Britannica* [online]. ©Encyclopædia Britannica [cit. 2022-11-28]. Dostupné z: https://www.britannica.com/topic/World-Health-Organization

ROŽNÁK, Petr, Karel KUBEČKA a kol., 2018. *Země Visegrádu a migrace: Fenomén procesu migrace, integrace a reintegrace v kontextu bezpečnosti zemí V4*. Ostrava: Key Publishing. ISBN 978-80-7418-292-1.

RUTHERFORD, Zoe, 2022. Monkeypox: A Prophecy fulfilled?. *CBRNe WORLD*. Winchester: © Falcon Communication, **17**(3), s. 46-49. ISSN 2040-2724.

SAK, Petr, 2018. *Úvod do teorie bezpečnosti*. Praha: Petrklíč. ISBN 978-80-7229-652-1.

Security, 2022. *Cambridge Dictionary* [online]. Cambridge: © Cambridge University Press [cit. 2022-11-15]. Dostupné z: https://dictionary.cambridge.org/dictionary/english/security

SLOVENSKO, 2005. Zákon č. 300/2005 Z. z. Trestný zákon. In: *Zbierka zákonov Slovenskej republiky*. Dostupné také z: https://www.zakonypreludi.sk/zz/2005-300

Slovník súčasného slovenského jazyka, 2015. *Slovníkový portál Jazykovedného ústavu Ľ. Štúra SAV* [online]. Bratislava: © Jazykovedný ústav Ľ. Štúra SAV [cit. 2022-11-15]. Dostupné z: https://slovnik.juls.savba.sk/?w=bezpe%C4%8Dnos%C5%A5&s=exact&c=9939&cs=&d=kssj4&d=psp&d=ogs&d=sssj&d=orter&d=scs&d=sss&d=peciar&d=ssn&d=hssj&d=bernolak&d=noundb&d=orient&d=locutio&d=obce&d=priezviska&d=un&d=pskfr&d=pskcs&d=psken#

SMEJKAL, Vladimír, 2022. *Kybernetická kriminalita*. Vyd. 3. Plzeň: Aleš Čeněk. ISBN 978-80-7380-849-5.

SMIL, Vaclav, 2017. *Globální katastrofy a trendy*. Praha: Kniha Zlin. ISBN 978-80-7473-528-8.

SMOLÍK, Josef, Tomáš ŠMÍD a kol., 2010. *Vybrané bezpečnostní hrozby a rizika 21. století*. Brno: Masarykova univerzita, Mezinárodní politologický ústav. ISBN 978-80-210-5288-8.

ŠABATA, Ondřej, 2022. 7 rizik používaní osobních IT zařízení v zaměstnání (BYOD). *Security Magazín*. Praha: © Security Media, **27**(131-4), s. 13-14. ISSN 1210-8723.

VEGRICHTOVÁ, Barbora, 2013. *Extremismus a společnost*. Plzeň: Aleš Čeněk. ISBN 978-80-7380-427-5.

VEGRICHTOVÁ, Barbora, 2019. *Hrozba radikalizace*. Praha: Grada. ISBN 978-80-271-2031-4.

What are Terrorist Groups?, 2019. *Laws* [online]. © LAWS.COM [cit. 2022-12-02]. Dostupné z: https://criminal.laws.com/terrorism/terrorist-groups#:~:text=A%20terrorist%20group%20is%20an%20organization%20that%20systematically,to%20inflict%20mayhem%20on%20a%20society%20or%20functional

What is corruption?, 2022. *Transparency International* [online]. © Transparency International [cit. 2022-12-08]. Dostupné z: https://www.transparency.org/en/what-is-corruption

What is Counterfeit Money?, 2022. *Herold Financial Dictionary* [online]. ©Herold Financial Dictionary [cit. 2022-12-08]. Dostupné z: https://www.financial-dictionary.info/terms/counterfeit-money/

What is Cyber Security?, 2022. *Kaspersky* [online]. © AO Kaspersky Lab [cit. 2022-11-30]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

What is phishing, 2022. *Phishing* [online]. © KnowBe4 [cit. 2022-11-30]. Dostupné z: https://www.phishing.org/what-is-phishing

WATSON, Richard, 2014. *Budoucnost: 50 myšlenek, které musíte znát*. Bratislava: Slovart. ISBN 978-80-7391-823-1.

Základné informácie, 2022. *Ministerstvo vnútra SR* [online]. Bratislava: ©Ministerstvo vnútra SR [cit. 2022-11-26]. Dostupné z: https://www.minv.sk/?zakladne-informacie-1

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

AKT tím	antikonfliktný tím
CBRN	chemické, biologické, rádiologické a nukleárne
Casus belli	*z lat*. „prípad vojny“ alebo „dôvod na vojnu“
EÚ	európska únia
G7	medzivládne politické fórum pozostávajúce z Kanady, USA, Francúzska, Talianska, Nemecka, Japonska, Spojeného kráľovstva
ISIS	islamský štát
NATO	North Atlantic Treaty Organisation Severoatlantická aliancia
SR	Slovenská republika
WHO	World Health Organisation Svetová zdravotnícka organizácia
ZHN	zbrane hromadného ničenia

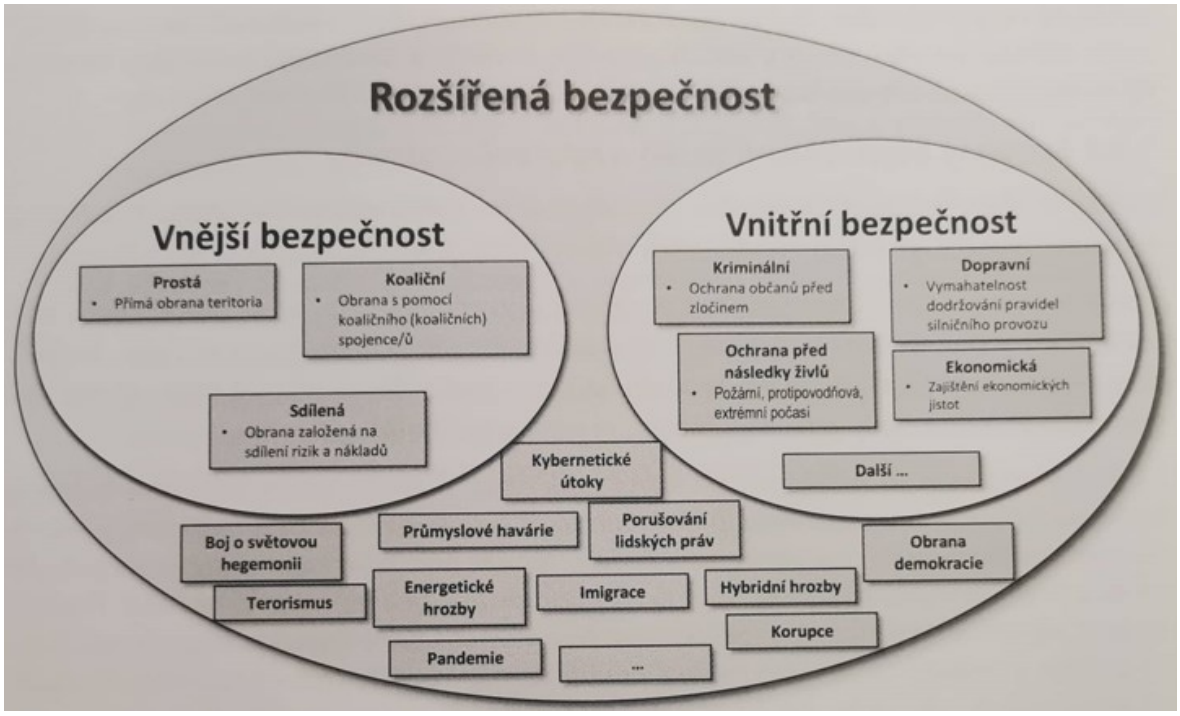
ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM GRAFOV

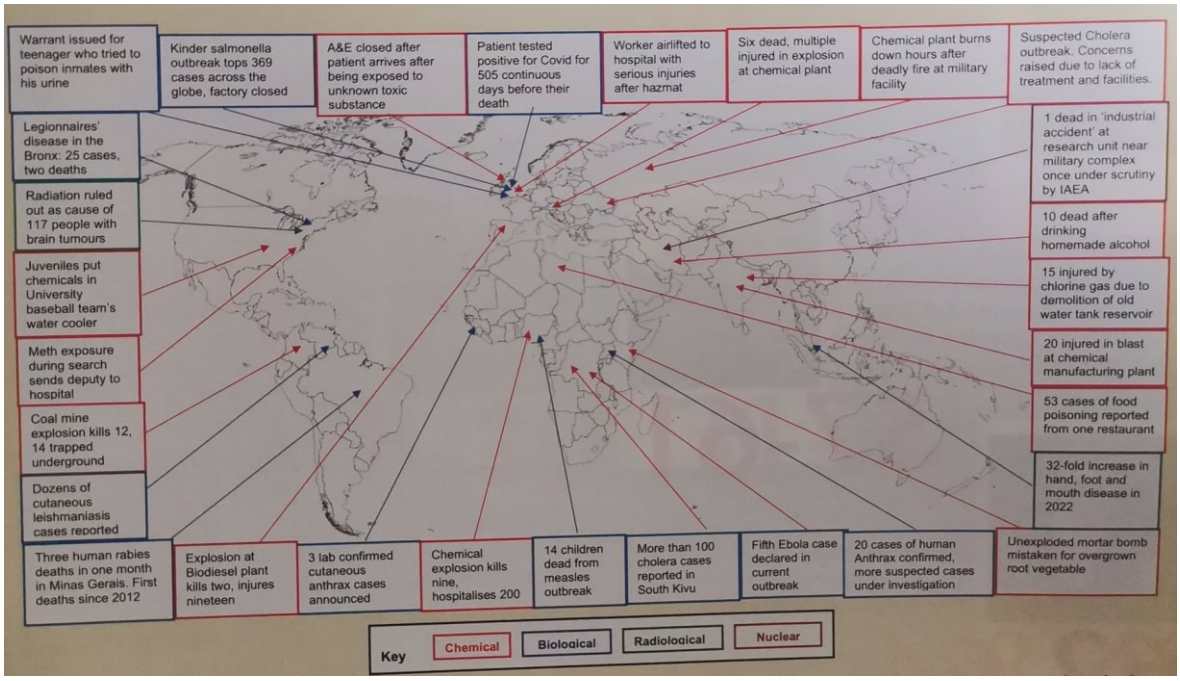
ZOZNAM PRÍLOH

PRÍLOHA P I: HORIZONTÁLNA ŠTRUKTÚRA ROZŠÍRENEJ BEZPEČNOSTI



Obrázok 1 - Horizontálna štruktúra rozšírenej bezpečnosti (Karaffa, Hrinko, Zůna a kol., 2022)

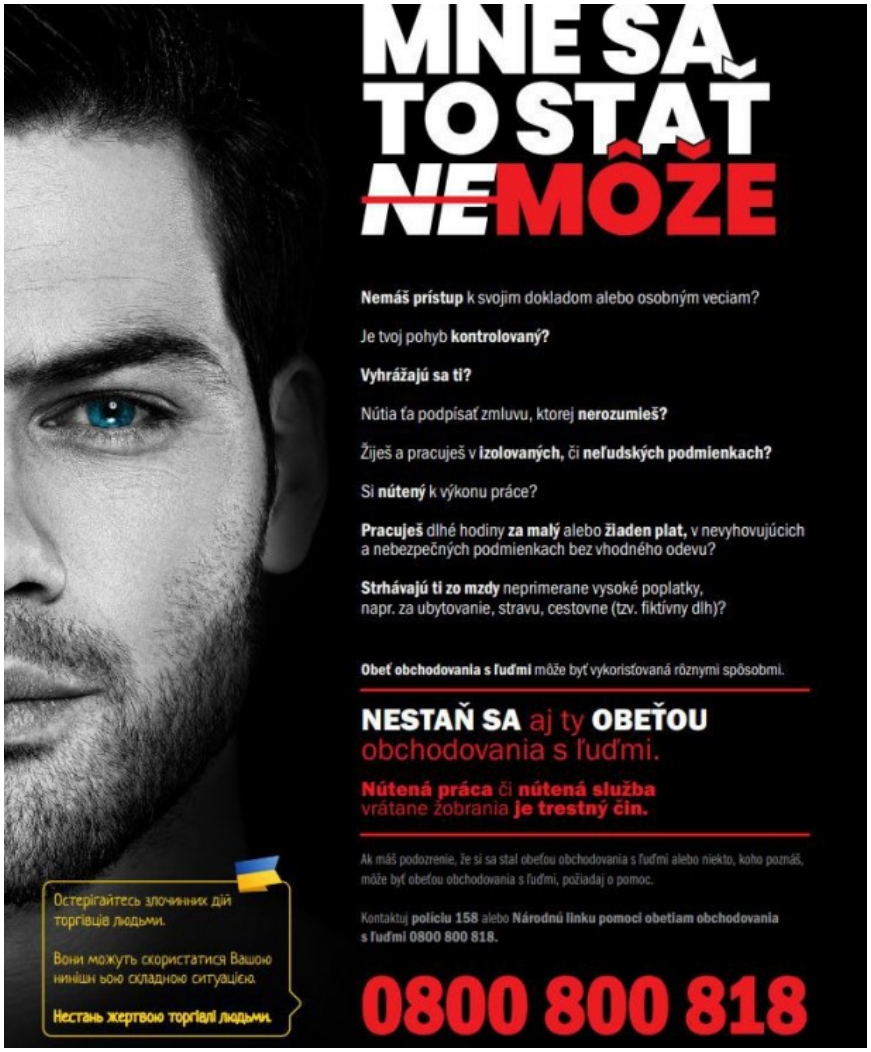
PRÍLOHA P II: GLOBÁLNE CBRN HROZBY A AKTIVITY



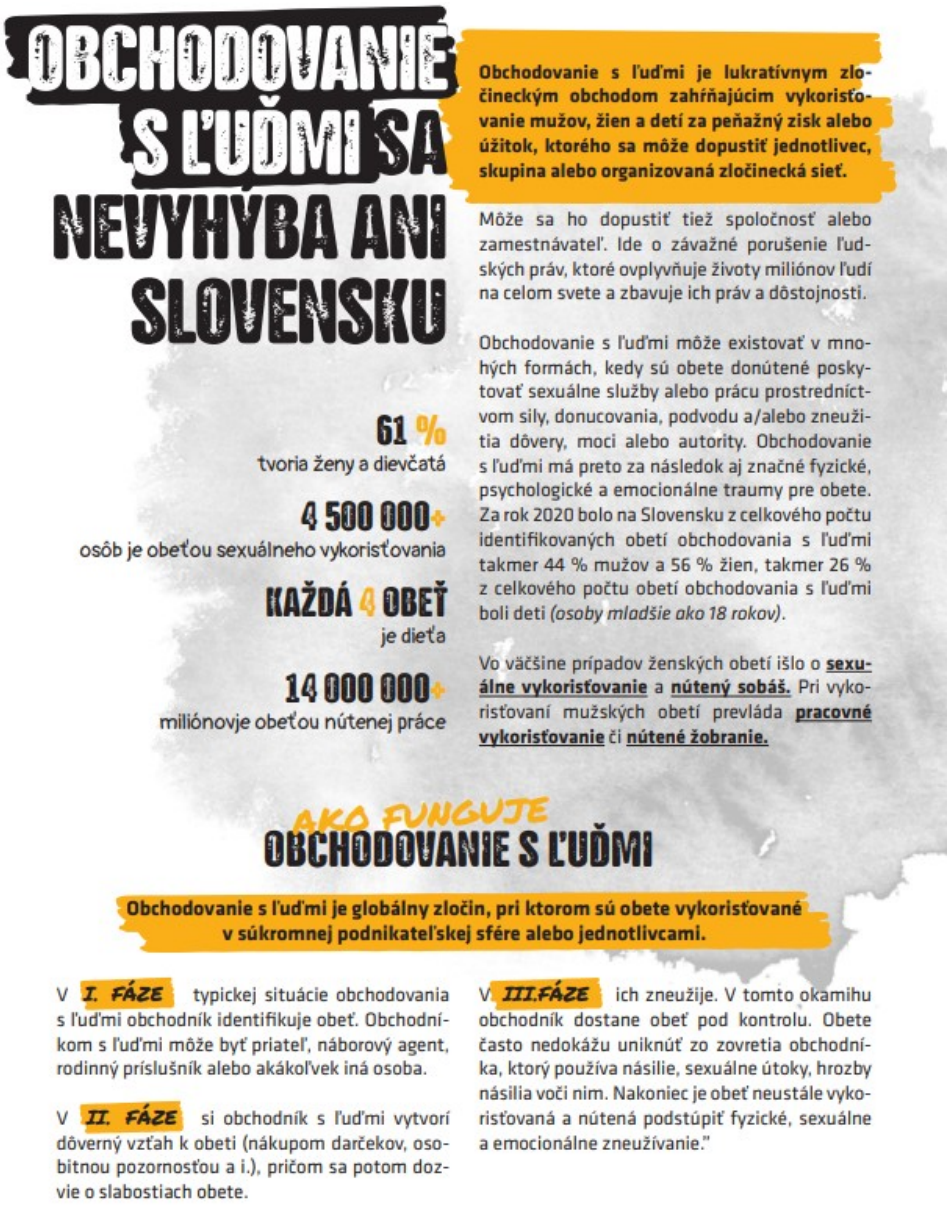
Obrázok 2 - globálne CBRN hrozby a aktivity (Zdroj: CBRNews, 2022)

PRÍLOHA P III: LETÁKY V PREVENCII BOJA PROTI OBCHODOVANIU S ĽUĎMI

Obrázok 3 - informačný leták pre vojnových utečencov z Ukrajiny (Zdroj: Brožúry a letáky, 2022)



Obrázok 4 – kampaň na čerpacích staniciach (Zdroj: Brožúry a letáky, 2022)



Obrázok 5 – obchodovanie s ľuďmi na Slovensku (Zdroj: Brožúry a letáky, 2022)