

# Návrh opatření pro zvyšování bezpečnosti vybrané kategorie měkkých cílů

Bc. Štěpán Vávra





Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2024/2025

## ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

|                      |                                                                                     |
|----------------------|-------------------------------------------------------------------------------------|
| Jméno a příjmení:    | Bc. Štěpán Vávra                                                                    |
| Osobní číslo:        | A23386                                                                              |
| Studijní program:    | N1032A020003 Bezpečnostní technologie, systémy a management                         |
| Specializace:        | Bezpečnostní management                                                             |
| Forma studia:        | Kombinovaná                                                                         |
| Téma práce:          | Návrh opatření pro zvyšování bezpečnosti vybrané kategorie měkkých cílů             |
| Téma práce anglicky: | Proposal of Measures to Enhance the Security of a Selected Category of Soft Targets |

### Zásady pro vypracování

1. Proveďte literární rešerši na dané téma.
2. Analyzujte právní rámec a metodiky analýzy rizik.
3. Identifikujte cílovou kategorii měkkých cílů.
4. Proveďte analýzu hrozeb a rizik.
5. Analyzujte stávající bezpečnostní stav.
6. Na základě provedených analýz, navrhnete vhodná konkrétní bezpečnostní opatření.

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

**Seznam doporučené literatury:**

1. ZEMAN, Petr, 2002. *Česká bezpečnostní terminologie*. Brno: Masarykova univerzita v Brně, Mezinárodní politologický ústav. ISBN 80-210-3037-2.
2. HESTERMAN, Jennifer L. *Soft target hardening: protecting people from attack*. 2. Edition. New York: Routledge. 2019. ISBN 9781138391109.
3. BAKER, Paul R. a Daniel J. BENNY. *The complete guide to physical security*. Boca Raton: CRC Press, 2013. ISBN 9781420099638.
4. DUFEK, Zdeněk; APELTAUER, Tomáš; HROMADA, Martin; MRÁZKOVÁ, Lucia; VANGELI, Benedikt et al., 2019. *Ochrana měkkých cílů*. Brno: Leges. ISBN 978-80-7502-427-5.
5. LUDĚK, Lukáš, 2017. *Teorie bezpečnosti*. I. Zlín: Radim Bačuvčík – VeRBuM. ISBN 978-80-87500-89-7.

Vedoucí diplomové práce: **prof. Ing. Martin Hromada, Ph.D.**  
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **29. listopadu 2024**

Termín odevzdání diplomové práce: **30. května 2025**

**doc. Ing. Jiří Vojtěšek, Ph.D. v.r.**  
děkan



**Ing. Milan Navrátil, Ph.D. v.r.**  
ředitel ústavu

Ve Zlíně dne 29. listopadu 2024

# PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

## **Beru na vědomí, že**

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- 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 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(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne 23.05.2025

Bc. Štěpán Vávra, v. r.  
podpis autora



## **ABSTRAKT**

Tato diplomová práce se zabývá návrhem opatření směřujícím ke zvýšení bezpečnosti úřadů s rozšířenou působností z hlediska měkkých cílů. V teoretické části je zahrnut terminologický, teoretický a právní rámec zkoumané problematiky. Shrnuty jsou zde jednotlivé metody analýzy rizik a metodická a koncepční podpora používána v České republice. Cílem praktické části této práce je navrhnout komplexně reálný přístup vedoucí ke zlepšení ochrany nejen samotného úřadu a jeho pracovníků, ale také občanů, kteří do této instituce přicházejí. Výstupem je analýza současného stavu bezpečnosti, identifikace zranitelných míst, ekonomická rozvaha a návrh konkrétních opatření vedoucích k minimalizaci rizika na přijatelnou úroveň a vytvoření bezpečnějšího prostředí pro výkon veřejné správy.

Klíčová slova: měkké cíle, bezpečnost, státní správa, analýza rizik, KARS, PNH, ochrana, úřad

## **ABSTRACT**

This thesis proposes measures to increase the security of authorities with extended competence in relation to soft targets. The theoretical section provides a terminological, theoretical and legal framework for the subject under study. It summarises the various risk analysis methods and the methodological and conceptual support used in the Czech Republic. The practical part of the thesis aims to propose a realistic, comprehensive approach to improving the protection of the authority itself, its staff and the citizens who visit this institution. The outcome is an analysis of the current security situation, identification of vulnerabilities, an economic analysis, and a proposal for specific measures to minimise risk and create a safer environment for public administration.

Keywords: soft targets, security, public administration, risk analysis, KARS, PNH, protection, authority

Tímto bych rád poděkoval vedoucímu mé diplomové práce, prof. Ing. Martinu Hromadovi Ph.D., za odborné vedení, rady, ochotu a vstřícnost při zpracování této práce. Velké díky také patří vedoucímu odboru zkoumaného úřadu, který byl velice přívětivý a umožnil mi zrealizovat prohlídku objektu a byl mi nápomocen i v průběhu psaní práce. Poděkovat chci také i své rodině, partnerce a všem blízkým za velkou trpělivost a podporu během celého studia.

# OBSAH

|                                                                                                         |           |
|---------------------------------------------------------------------------------------------------------|-----------|
| <b>ÚVOD.....</b>                                                                                        | <b>11</b> |
| <b>I TEORETICKÁ ČÁST .....</b>                                                                          | <b>12</b> |
| <b>1 TERMINOLOGICKÝ A TEORETICKÝ RÁMEC PROBLEMATIKY.....</b>                                            | <b>13</b> |
| 1.1 TERMINOLOGIE .....                                                                                  | 13        |
| 1.2 TEORETICKÝ RÁMEC .....                                                                              | 15        |
| 1.3 KATEGORIE MĚKKÝCH CÍLŮ .....                                                                        | 16        |
| 1.3.1 Rozdělení měkkých cílů.....                                                                       | 16        |
| 1.3.2 Vybraná kategorie měkkých cílů .....                                                              | 18        |
| <b>2 PRÁVNÍ RÁMEC PŘEDMĚTNÉ PROBLEMATIKY .....</b>                                                      | <b>20</b> |
| 2.1 ÚSTAVNÍ ZÁKON A LISTINA ZÁKLADNÍCH PRÁV A SVOBOD.....                                               | 20        |
| 2.2 ZÁKON O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ A NAŘÍZENÍ EVROPSKÉHO<br>PARLAMENTU A RADY EU.....                | 20        |
| 2.3 ZÁKON O KYBERNETICKÉ BEZPEČNOSTI A ZÁKON O INFORMAČNÍCH<br>SYSTÉMECH VEŘEJNÉ SPRÁVY .....           | 21        |
| 2.4 BEZPEČNOSTNÍ POLITIKA A STRATEGIE .....                                                             | 22        |
| <b>3 ANALÝZA RIZIK .....</b>                                                                            | <b>24</b> |
| 3.1 OBECNÉ METODY ANALÝZY RIZIK .....                                                                   | 25        |
| 3.2 VYBRANÉ SPECIFICKÉ METODY ANALÝZY RIZIK.....                                                        | 29        |
| 3.2.1 Teoretický rámec posuzování nebezpečí a hodnocení rizik (PNH).....                                | 30        |
| 3.2.2 Teoretický rámec metody kvalitativní analýza rizik s využitím jejich<br>souvztažnosti (KARS)..... | 32        |
| <b>4 METODICKÁ A KONCEPČNÍ PODPORA OCHRANY MĚKKÝCH<br/>    CÍLŮ.....</b>                                | <b>37</b> |
| 4.1 KONCEPCE OCHRANY MĚKKÝCH CÍLŮ PRO ROKY 2017–2020.....                                               | 37        |
| 4.2 METODIKA ZÁKLADY OCHRANY MĚKKÝCH CÍLŮ .....                                                         | 40        |
| 4.3 BEZPEČNOSTNÍ PLÁN MĚKKÉHO CÍLE ANEB CO BY NEMĚLO BÝT OPOMENUTO<br>PŘI JEHO ZPRACOVÁNÍ .....         | 43        |
| <b>II PRAKTICKÁ ČÁST.....</b>                                                                           | <b>48</b> |
| <b>5 CHARAKTERISTIKA MĚKKÉHO CÍLE.....</b>                                                              | <b>49</b> |
| 5.1 VEŘEJNĚ PŘÍSTUPNÉ ÚDAJE .....                                                                       | 50        |
| <b>6 ANALÝZA RIZIK .....</b>                                                                            | <b>53</b> |
| 6.1 IDENTIFIKACE AKTIV ZÁJMOVÉHO OBJEKTU .....                                                          | 53        |
| 6.2 KATALOG HROZEB.....                                                                                 | 55        |
| 6.3 APLIKACE METODY PNH .....                                                                           | 59        |
| 6.4 APLIKACE METODY KARS.....                                                                           | 62        |
| <b>7 AKTUÁLNÍ BEZPEČNOSTNÍ STAV .....</b>                                                               | <b>67</b> |

|                                                 |                                                            |            |
|-------------------------------------------------|------------------------------------------------------------|------------|
| 7.1                                             | ANALÝZA AKTUÁLNÍHO STAVU ZABEZPEČENÍ .....                 | 67         |
| 7.2                                             | VYHODNOCENÍ AKTUÁLNÍHO STAVU ZABEZPEČENÍ .....             | 91         |
| <b>8</b>                                        | <b>NÁVRH BEZPEČNOSTNÍCH OPATŘENÍ .....</b>                 | <b>95</b>  |
| 8.1                                             | DOPORUČENÝ NÁVRH KE ZLEPŠENÍ BEZPEČNOSTNÍCH PODMÍNEK ..... | 95         |
| 8.2                                             | EKONOMICKÁ ROZVAHA.....                                    | 98         |
| <b>ZÁVĚR.....</b>                               |                                                            | <b>102</b> |
| <b>SEZNAM POUŽITÉ LITERATURY .....</b>          |                                                            | <b>105</b> |
| <b>SEZNAM OBRÁZKŮ .....</b>                     |                                                            | <b>111</b> |
| <b>SEZNAM TABULEK.....</b>                      |                                                            | <b>113</b> |
| <b>SEZNAM ROVNIC .....</b>                      |                                                            | <b>114</b> |
| <b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK .....</b> |                                                            | <b>115</b> |
| <b>SEZNAM PŘÍLOH.....</b>                       |                                                            | <b>116</b> |

## ÚVOD

Bezpečnost měkkých cílů představuje v současnosti jedno z klíčových témat v oblasti ochrany veřejného prostoru, a to zejména s ohledem na rostoucí počet incidentů a agresivního chování vůči institucím veřejné správy. Měkké cíle, mezi něž patří úřady, školy, nemocnice či kulturní zařízení, se vyznačují svou otevřeností, vysokou koncentrací osob a často nedostatečnými bezpečnostními opatřeními. Tyto skutečnosti je činí zranitelnými vůči širokému spektru hrozeb, ať už se jedná o fyzické útoky, žhářství nebo psychologický tlak na zaměstnance. V této diplomové práci se budu věnovat návrhu opatření ke zvýšení bezpečnosti vybrané kategorie měkkých cílů, konkrétně na příkladu modelové veřejné instituce ve státní správě. Mým cílem bude identifikovat nejzávažnější bezpečnostní rizika, zhodnotit aktuální úroveň zabezpečení a navrhnout účinná a prakticky realizovatelná opatření, která mohou být přínosem i pro další obdobné objekty veřejné správy.

Teoretická část práce nejprve poskytne nezbytný rámec pro porozumění problematice ochrany měkkých cílů, a to prostřednictvím terminologického, teoretického a právního vymezení. Budou zde představeny obecné metody analýzy rizik doplněné o specifické přístupy metod PNH a KARS. Zmíněny budou také metodické a koncepční dokumenty vydané Ministerstvem vnitra České republiky, které se touto oblastí zabývají. Praktická část bude zaměřena na analýzu konkrétní veřejné instituce ve státní správě. Nejprve bude popsána charakteristika objektu a jeho okolí na základě veřejně dostupných informací, následně budou aplikovány zvolené metody analýzy rizik, konkrétně metody PNH a KARS. Po jejich vyhodnocení bude provedena analýza aktuálního stavu zabezpečení včetně fyzické prohlídky objektu. Na základě zjištěných a vyhodnocených údajů budou navržena konkrétní bezpečnostní opatření doplněná o ekonomickou rozvahu.

## **I    TEORETICKÁ ČÁST**

## 1 TERMINOLOGICKÝ A TEORETICKÝ RÁMEC PROBLEMATIKY

Začátek diplomové práce je věnován terminologii, jenž bude využita a používána v této práci a taktéž teoretickému rámci problematiky zaměřené na měkké cíle. Druhá podkapitola je zaměřena na právní problematiku charakterizující bezpečnost.

### 1.1 Terminologie

V rámci této podkapitoly jsou rozpracovány jednotlivé pojmy vztahující se k tématu diplomové práce. Termíny jsou rozděleny následovně:

**Měkké cíle** (dále jen „MC“) nemají v žádném právním předpise jednoznačně ukotvenou definici. V odborném prostředí se tedy pojmem MC rozumí místa s velkou koncentrací lidí a minimální ochranou před násilnými útoky. Pro bližší určení lze tento pojem definovat jako budovy, místa a události, kde se pravidelně shromažďuje větší množství lidí, avšak nemají žádnou nebo minimální ochranu proti cíleným násilným útokům. Útoky mohou probíhat závisle či nezávisle na sobě. Protikladem MC jsou takzvané (dále jen „tzv.“) **tvrdé cíle**. Ty představují dobře zabezpečené a hlídané objekty, které jsou chráněny před možnými útoky jako například (dále jen „např.“) některé vládní budovy, sídla bezpečnostních složek, vojenské areály nebo vysoce zabezpečené soukromé a komerční objekty. [1], [2]

**Násilný útok** značí reálné nebo na základě vyhrožování předpokládané použití zbraně, fyzické síly nebo moci vůči sobě, jiné osobě, skupině či společnosti, které vede nebo s vysokou pravděpodobností povede ke smrti, zranění, psychické újmě, špatnému vývoji či deprivaci neboli nedostatečné uspokojení důležité psychické či fyzické potřeby jednotlivce. [2], [3]

**Referenční objekt** představuje systém, u kterého se řeší prevence narušení a udržování bezpečnosti. Jeho podoba může být fyzická, neboli materiální, a nehmotná, čili nemateriální. Obecně lze říct, že referenční objekt se zakládá na společenské významnosti, jelikož představuje určitou sociální důležitost. Objektem se ve většině případů rozumí samostatně stojící funkční budova s pevnými základy, uzavřený obvodovými stěnami a zastřešením, ale toto nemusí být pravidlem. V některých případech se objektem v nemateriální podobě se objektem rozumí lidská práva, osobní údaje, čest, psychika či utajované informace. [2], [4], [5].

**Hrozba** je škodící jev, který svým působením na celek působí negativně. Na referenčním objektu může při dlouho trvající hrozbě vzniknout újma neboli negativní dopad. Hrozba ovšem nutně neznamená, že došlo k narušení bezpečnosti. Jedná se o vnější faktor, který může ohrozit nebo úmyslně narušit určitou hodnotu, avšak aby tak mohla učinit musí existovat možnost výskytu takové hrozby. Taková šance ohrožení bezpečnosti je vyjádřena jako riziko. **Riziko** je obvykle chápáno jako faktor, který představuje možnost vystavení hrozbě a rozsah jejího škodlivého dopadu na daný objekt. Jeho úroveň lze vyjádřit jak číselně, tak i popisem. Číselné vyjádření rizika je uváděno jako bezrozměrná veličina či ve vhodně zvolených jednotkách. Kvalitativní vyjádření se zaměřuje na slovní opis závažnosti dopadu velikosti rizika. [4], [5], [6]

**Negativní dopad** zahrnuje jakoukoliv materiální, ale i nemateriální újmu nebo nežádoucí jev, který postihne referenční objekt. Pokud by proti negativnímu dopadu nebyla přijata opatření, mohl by výrazně omezit jeho funkčnost daného objektu nebo vést až k jeho zániku. Potom by pro takový objekt byl negativní dopad nevhodný z existenčních důvodů. Druhy bezpečnosti a jejich opatření jsou zaváděny právě za účelem systematického předcházení těmto dopadům. Samotný pojem, negativní dopad, neurčuje jeho přesný rozměr, k jejímu konkrétnějšímu vyjádření se používá termín újma. **Újma** je obvykle zakotvena v právních předpisech a její rozsah lze často vyčíslit. Může být vyjádřena v konkrétních jednotkách, např. peněžních částkách, ale také bezrozměrně v závislosti na povaze dané velikosti újmy. [4]

S těmito pojmy souvisí **odolnost**, kterou lze definovat jako schopnost referenčního objektu čelit vnějším i vnitřním hrozbám, odolávat jejím účinkům, zmírňovat jejich dopady a obnovovat svou funkčnost. Tato schopnost zahrnuje jak prevenci, tedy předcházení vzniku újmy, tak i obnovu poškozených struktur a funkcí v případě, že došlo k jejímu poškození. Klíčový aspektem odolnosti je udržení základních funkcí a struktur objektu včasným a účinným způsobem, přičemž obnova musí být umožněna alespoň do přijatelné úrovně, aby nedošlo k úplnému zničení či zániku objektu. [2], [4]

Schopnost odolávat do jisté míry určuje **zranitelnost** objektu, která představuje vnitřní vlastnost jeho systému, jenž určují jeho citlivost na zdroje rizik a zvyšují pravděpodobnost vzniku škody nebo narušení bezpečnosti. Zranitelnost se projevuje přítomností slabých míst, která mohou být snadno překonána, což vede k nežádoucím dopadům. Identifikace těchto slabých míst je klíčová pro posílení odolnosti objektu, jelikož umožňuje přijmout opatření ke snížení nebo odstranění jeho zranitelnosti. [2], [4]

**Režimová opatření** jsou soubor organizačních a administrativních opatření zaměřených na přípravu a zavedení postupů, které tvoří základ pro efektivní fungování systému ochrany a zvýšení bezpečnosti daného objektu. **Bezpečnost** představuje stav, kdy systém dokáže odolávat známým a očekávaným vnějším i vnitřním hrozbám, které by mohly negativně narušit jeho jednotlivé prvky nebo celkovou funkčnost. Zároveň si udržuje svou strukturu, stabilitu, spolehlivost a cílené fungování. Tento stav tedy vyjadřuje úroveň stability systému a jeho schopnost primárního a sekundárního přizpůsobení se. [2]

## 1.2 Teoretický rámec

Z důvodu nedostatečných dat, která by se přímo týkala úřadů s rozšířenou působností, byla statistická data čerpána z Úřadu práce České republiky, a to konkrétně z let 2018 až 2024.

V posledních letech dochází k nárůstu incidentů, při nichž jsou státní zaměstnanci pracující na úřadech v České republice vystaveni stále frekventovanější agresi ze strany klientů. Nejvíce jsou ohroženy ženy, neboť ty tvoří většinu pracovníků úřadu. Incidenty zahrnují jak verbální, tak i fyzické útoky, přičemž jejich počet každoročně roste. Již v roce 2018 bylo zřejmé, že dochází k eskalaci těchto situací, neboť tehdy bylo evidováno 560 incidentů za celý rok. Za období roku 2022 až 2023 došlo téměř k 30% nárůstu incidentů za rok 2023 bylo zaznamenáno 794 incidentů. V roce 2024 došlo již během prvních deseti měsíců k 689 útokům v říjnu téhož roku bylo zaznamenáno 92 případů, což znamenalo meziroční nárůst o 84 %. [7], [8]

Mezi nejčastější formy útoků patří verbální agresivita, výhrůžky fyzickým napadením či zabitím, v některých případech i sexuální obtěžování. Významnou část incidentů však tvoří fyzická agrese, při níž dochází k úderům, kopání nebo tahání za vlasy. Závažné případy zahrnují i útoky vedoucí ke zranění zaměstnanců a jejich následné dočasné pracovní neschopnosti. Důvody napadení mohou být různé a převážně se týkají rozhodnutí úřadu, se kterým útočníci nesouhlasí. [7], [8]

Např. v říjnu 2024 došlo v Jihomoravském kraji k napadení pracovnice, která byla fyzicky atakována klientkou. Ta ji opakovaně udeřila hlavou o zeď. Jiný případ, jenž se stal tentýž měsíc, ale v Moravskoslezském kraji představoval situaci, kdy klient hrozil zastřelením pracovnice a následně vykřikoval, že vystřelí všechny přítomné. Podobné incidenty byly zaznamenány již ve sledovaném roce 2018, kdy útočnice způsobila zaměstnankyni vážná zranění na základě čehož byla obviněna následně odsouzena k podmíněnému trestu. Právní rámec poskytuje ochranu úředním zaměstnancům

prostřednictvím § 325 trestního zákoníku, který stanoví tresty za násilí proti úřední osobě. [7], [8], [9]

Na základě výše uvedeného bylo vyhodnoceno, že veřejným institucím, konkrétně úřadům, chybí zabezpečení poboček a zaměstnanců. Celkově tedy lze konstatovat, že útoky na státní zaměstnance představují rostoucí bezpečnostní problém, který vyžaduje zvýšení požadovaných opatření, které by přispěly ke snížení hrozeb. Preventivním opatřením může být modernizace bezpečnostního systému, ale i zefektivnění spolupráce s policií, čímž může dojít ke zmírnění rizik. Nutno podotknout, že není jisté, zdali zavedení větších bezpečnostních opatření bude z dlouhodobého hlediska dostačující, nebo bude nutné zavést další legislativní a vnitřní opatření na ochranu zaměstnanců.

### 1.3 Kategorie měkkých cílů

Jak již bylo uvedeno výše, samotnou definici MC nelze nelézt v žádném právním předpise. Nelze se tedy přímo opírat o právní ukotvení MC, ale je možné vycházet z odborných publikací, které je zpracovávají. MC představují lokality s vysokým počtem osob a nedostatečnými bezpečnostními opatřeními proti násilným útokům. [1], [2] Z důvodu chybějícího zabezpečení může být potencionálním útočníkem i terorista, osoba s duševním onemocněním, jedinec prožívající frustraci nebo pachatel jednající v afektu. [10]

#### 1.3.1 Rozdělení měkkých cílů

Existuje mnoho typů MC, a proto je zde uveden výčet těch nejpravděpodobnějších:

- *„školy, koleje, menzy, knihovny,*
- *památky a církevní prostory,*
- *nákupní, zábavní centra a sportovní centra,*
- *veřejná shromáždění,*
- *turisticky exponovaná místa,*
- *komunitní prostory,*
- *dopravní a logistické uzly,*
- *dopravní prostředky,*
- *nemocnice a zdravotnická zařízení.“* [10]

Některé z těchto objektů jsou níže rozepsány pro bližší pochopení kontextu:

Útoky ve **školách** jsou považovány za jedny z nejzávažnějších, a to kvůli přítomnosti dětí a jejich vysoké zranitelnosti. Historické i současné případy ukazují, že hrozbou ve školách mohou být teroristé, samotní žáci či nahodilý útočníci. Z tohoto důvodu je nutné zvolit pro školy specifická bezpečnostní opatření. [11]

**Památky a církevní prostory** představují zvláštní skupinu MC, spadají sem nejen konkrétní náboženské objekty, ale i místa bohoslužeb. Tato místa často čelí útokům ze strany islamistických extremistů i radikálních pravicových skupin. [11]

**Veřejné shromáždění** může být v podobě kulturní a společenské akce, nebo se může jednat hromadnou akci. První varianta představuje unikátní, předem organizovanou akci s přesně určeným místem a časem konání. Je zaměřená na prezentaci duchovních i materiálních hodnot lidské tvorby. [12] Hromadné akce jsou události, které při bezpečnostním plánování vyžadují rozsáhlejší spolupráci. Tyto akce se obvykle vyznačují alespoň jednou nebo více z následujících vlastností. Jedná se o publicitu, to znamená (dále jen „tzn.“) velkou až mezinárodní mediální přitažlivost, popularitu, spočívající v jejím historickém, politickém či kulturním významu a velkou účastí, která může zahrnovat mezinárodní návštěvy, VIP osobnosti či potenciálně rizikové osoby. [13]

Další z významných měkkých cílů jsou **dopravní prostředky a dopravní uzly**, jenž spolu úzce souvisí, neboť útoky na tuto kategorii MC můžou postihnout velké množství osob. Zároveň tak může dojít k narušení celé dopravní infrastruktury, čímž se dopad vůči společnosti znásobuje. [11]

**Nemocnice a zdravotnická zařízení**, jsou z důvodu nezbytného nepřetržitého provozu snadnými MC. To bylo možné vidět u tragické události ve Fakultní nemocnici Ostrava, při níž 42letý útočník v roce 2019 zastřelil sedm osob a dvě další vážně zranil. Z tohoto je patrné, že nemocnice a zdravotnická zařízení definitivně spadají do oblasti MC a zároveň tímto incidentem bylo poukázáno na zranitelnost těchto objektů. Taková místa vyžadují zvláštní ochranu, i přestože rychlý zásah zdravotnického personálu pomohl zachránit životy zraněných, ukázalo se, že preventivní bezpečnostní opatření nebyla dostatečná. Tato událost vyvolala diskusi o potřebě preventivních strategií, školení personálu a využití moderních technologií k ochraně pacientů a zdravotníků. Ochrana zdravotnických zařízení by jednoznačně měla být součástí komplexní bezpečnostní strategie, která zahrnuje nejen

fyzické opatření, ale i psychickou připravenost personálu a návštěvníků nemocnic na krizové situace. [14]

Existuje několik faktorů, které mohou přispět k minimalizaci dopadů útoků na MC. Především se jedná o efektivní reakci kolemdoucích, ta může výrazně přispět k prevenci a zmírnění následků krizových situací. Je klíčové, aby zúčastněné osoby věděly, jak správně reagovat. Zároveň může vhodné urbanistické plánování a bezpečnostní opatření vytvořit fyzickou bariéru mezi potenciálními útočníky a přihlížejícími, čímž se minimalizuje riziko útoku. Využití vzdálenosti, pohyblivých prvků a ochranných zábran se tak stává důležitým aspektem bezpečnostní strategie. Mezi a nejúčinnější opatření patří zabezpečené dveře a okna, která mohou výrazně snížit pravděpodobnost neoprávněného vniknutí. V praxi však tato zabezpečení často vykazují nedostatky, které mohou omezit jejich efektivitu. Současně je nutné věnovat pozornost místům, kde se shromažďují velké skupiny lidí, např. před vstupy do budov či areálů. Davy čekající na vstup se totiž mohou snadno stát cílem útoku, což vyžaduje pečlivé plánování preventivních opatření. Kromě technických a architektonických řešení je nezbytné zaměřit se také na zlepšení organizačních a operačních postupů spojených s řízením krizových situací. Současné systémy velení a reakce na incidenty často narážejí na řadu problémů, které mohou negativně ovlivnit jejich efektivitu. Pro dosažení vyšší úrovně bezpečnosti je proto nutné kombinovat fyzická opatření s dobře nastavenými bezpečnostními postupy a koordinací mezi jednotlivými složkami krizového řízení. [15]

### 1.3.2 Vybraná kategorie měkkých cílů

Pro účely této práce byla, vybrána veřejně dostupná státní instituce, konkrétně odbor dopravních a správních agend. Jedná se o úřad, který se nachází v obci s rozšířenou působností (dále jen „ORP“). [16], [17]

Zákonnou oporou pro ORP je z velké části zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů. Ten je známý jako tzv. „krizový zákon“, který upravuje působnost a pravomoc státních orgánů–a též orgánů územních samosprávných celků při přípravě na krizové situace a jejich řešení. Krizové situace mohou vzniknout působením útočníků na zmíněné úřady. Zvláštní roli zde mají ORP, neboť ty mají klíčové postavení v systému krizového řízení na územní úrovni. Rozdílné role mají podle zákona starostové ORP a obecní úřady ORP. [18]

Rolí starosty je především zajišťovat připravenost správního obvodu na řešení krizových situací. Dále řídit a kontrolovat přípravná opatření a činnosti k řešení krizových

situací prováděné územními správními úřady, orgány obcí, právníckými a fyzickými osobami ve správním obvodu. Taktéž zřizovat a řídit bezpečnostní radu ORP jako poradní orgán pro přípravu na krizové situace, organizovat přípravu správního obvodu na krizové situace a podílet se na jejich řešení. Nadále schvalovat krizový plán OPR po jeho projednání v bezpečnostní radě, zřizovat a řídit krizový štáb pro řešení krizových situací. V neposlední řadě musí starosta plnit úkoly stanovené hejtmánem a orgány krizového řízení při přípravě na krizové situace a jejich řešení. Posledním úkolem starosty, který mu ukládá tento zákon je, že odpovídá za využívání informačních a komunikačních prostředků krizového řízení určených Ministerstvem vnitra ČR (dále jen „MV ČR“). Jak je uvedeno, zákon taktéž ukládá úkoly obecním úřadům v oblasti zajištění připravenosti správního obvodu ORP na zvládání krizových situací. Spadá sem poskytování součinnosti hasičskému záchrannému sboru kraje při zpracování krizového plánu kraje a ORP, a následně i plnění úkolů podle krizového plánu ORP. Tyto povinnosti taktéž zahrnují vedení evidencí údajů o přechodných změnách pobytu osob, které je předáváno hasičskému záchrannému sboru kraje. Obecní úřad musí dále vést přehled možných zdrojů rizik a v rámci prevence odstraňovat nedostatky, jenž by mohly vést ke vzniku krizové situace. Na závěr je zákonem stanoveno, že pro účely plnění krizových opatření jednotlivé obecní úřady ORP zřizují pracoviště krizového řízení. [18]

Výše uvedené podmínky zákona č. 240/2000 Sb., zdůrazňují významnou roli ORP v systému krizového řízení, přičemž jejich úkoly a pravomoci jsou klíčové pro zajištění bezpečnosti a ochrany obyvatelstva, včetně ochrany MC na jejich území.

První kapitola se zaměřovala na základní pojmy a teoretických východisek týkajících se MC. Ty představují místa s vysokou koncentrací lidí a minimálním zabezpečením proti násilným útokům, přičemž jejich opakem jsou tzv. tvrdé cíle. Popsány jsou i související pojmy jako násilný útok, referenční objekt, hrozba, riziko, újma, odolnost, zranitelnost či bezpečnostní opatření. Teoretický rámec doplňují statistiky útoků na zaměstnance úřadu České republiky. Ty ukazují rostoucí agresi klientů vůči úředníkům a poukazují na nedostatečné zabezpečení těchto institucí. Pro podrobnější rozpracování byla proto zvolena veřejná státní instituce, konkrétně odbor dopravních a správních agend v ORP. Jejich role v krizovém řízení je podpořena zákonem č. 240/2000 Sb. Součástí této kapitoly je také rozdělení MC do různých kategorií, jako jsou školy, památky, dopravní uzly či nemocnice, a upozornění na potřebu kombinace technických, organizačních i legislativních opatření k minimalizaci jejich zranitelnosti a zvýšení odolnosti.

## 2 PRÁVNÍ RÁMEC PŘEDMĚTNÉ PROBLEMATIKY

Tato kapitola zahrnuje souhrn právních norem, předpisů a metodik, jež jsou spjaté se zpracovávaným tématem. Jedná se pouze o výčet dostupných dokumentů, který je následující:

- ústavní zákon a listina základních práv a svobod,
- zákon o zpracování osobních údajů a nařízení Evropského parlamentu a Rady EU,
- zákon o kybernetické bezpečnosti a zákon o informačních systémech veřejné správy,
- bezpečnostní politika a strategie,
- metodiky a koncepce zaměřené na ochranu měkkých cílů.

### 2.1 Ústavní zákon a listina základních práv a svobod

Ústavním zákonem České republiky je Ústava České republiky, tedy zákon č. 1/1993 Sb., která byla schválena 16. prosince 1992, avšak její účinnost se vztahuje k 1. lednu 1993, tedy k datu vzniku samostatné České republiky. Skládá se z preambule, osmi hlav a celkem 113 článků. Ústava České republiky byla již několikrát novelizována a doplňována, naposledy v roce 2024. Tento zákon je nejvyšším právním předpisem, který má vždy prioritu před ostatními zákony a stanovuje základní práva a povinnosti občanů, popisuje charakter státu, vymezuje strukturu nejvyšších státních orgánů a mimo jiné obsahuje státní symboly. [19]

Jak uvádí článek 3 Ústavy České republiky nedílnou součástí ústavního pořádku České republiky je i-Listina základních práv a svobod. Byla schválena Českou národní radou dne 16. prosince 1992, ale účinnosti nabyla, stejně jako Ústava České republiky, až vznikem Českého státu, tedy 1. ledna 1993. Skládá se z šesti hlav a 44 článků. Je zaměřena na ochranu a nedotknutelnost osoby, ale i jejího soukromí. Z pohledu bezpečnosti stanovuje, že nikdo nesmí být svévolně připraven o život. Také stanovuje právo na vzdělání a povinnou školní docházku. Z pohledu bezpečnosti sem spadá také ochrana majetku, jakožto i právo na jeho vlastnění, ochrana před neoprávněnými zásahy ostatních osob i státu. [20]

### 2.2 Zákon o zpracování osobních údajů a nařízení Evropského parlamentu a Rady EU

Zákon č. 110/2019 Sb., o zpracování osobních údajů ve znění pozdějších předpisů, jenž nabyl účinnosti dne 24. dubna 2019, doplňuje Obecné nařízení o ochraně osobních údajů

(dále jen „GDPR“), přičemž upravuje jeho použití v rámci národního prostředí. Ukládá práva a povinnosti při zpracování osobních údajů na území České republiky a doplňuje odchylky GDPR v oblastech, kde má stát prostor pro vlastní úpravu. Tím je myšleno zachování obranných a bezpečnostních zájmů České republiky. Kontrolním orgánem pro GDPR je Úřad pro ochranu osobních údajů. Práce s osobními údaji souvisí z pohledu úřadů s plněním zákonných povinností, veřejným zájmem či výkonem veřejné moci. [21], [22] Z hlediska bezpečnosti mají výše uvedené legislativní dokumenty potřebný účel, neboť v případě vzniku násilného útoku na úřad je možné využít nainstalovaných dohledových videosystémů (dále jen „VSS“), které mohou pomoci k identifikaci osob, jež násilný útok vůči objektu provedli. To je možné právě jen díky existující legislativě. Nutno podotknout, že VSS zpravidla naleznou využití až po daném incidentu, avšak může nastat situace, takzvaná barikádová, kdy bude systém za pomoci vzdáleného přístupu využit k vyhodnocení aktuální situace, čímž může dopomoci k lepšímu provedení zákroku. Tyto systémy také mohou poskytnout podklad k budoucímu taktickému cvičení. Mohou sloužit i jako preventivní prvek v ochraně majetku.

### **2.3 Zákon o kybernetické bezpečnosti a zákon o informačních systémech veřejné správy**

Nedílnou součástí digitalizace veřejné správy je zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, který zastřešuje kybernetickou bezpečnost v rámci České republiky. Tento zákon upravuje odpovědnost jednotlivců i subjektů a vymezuje kompetence a oprávnění orgánů veřejné správy v oblasti ochrany kybernetické bezpečnosti. Znění tohoto zákona je zaměřeno na posílení schopnosti odhalovat kybernetických bezpečnostních incidentů, zavedení povinnosti jejich hlášení a implementování systému opatření pro reakci na tyto hrozby. Další oblastí je definování základních standardů bezpečnostních opatření a regulace fungování dohledových center. [23] S nárůstem digitalizace veřejné správy a celkového využívání informačních systémů představuje provoz informačních systémů bezpečnostní riziko. K zajištění minimální úrovně ochrany v ekonomických, společenských či bezpečnostních organizacích, které splňují stanovená kritéria významnosti, byla vydána směrnice evropského parlamentu a rady neboli směrnice NIS 2. Jak uvádí příloha I této směrnice, do vysoce kritického odvětví spadá i veřejná správa. Patří zde centrální a místní subjekty veřejné správy vymezené členským státem, jenž jsou v souladu s vnitrostátními předpisy. Na základě vydání této směrnice vláda

České republiky dne 17. července 2024 přistoupila k novelizaci zákona o kybernetické bezpečnosti. [24], [25]

Z pohledu veřejné správy je důležitý i zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů, který upravuje podmínky pro provoz, správu a rozvoj informačních systémů veřejné správy v České republice. Předností tohoto zákona je odpovědnost orgánů veřejné správy za správu a provoz informačních systémů, zajištění bezpečnosti a ochranu dat v těchto systémech. Dále sem spadá definování jednotných pravidel a zabezpečení vzájemné kompatibility informačních systémů veřejné správy. Ministerstvu vnitra byla uložena role hlavního koordinátora digitalizace veřejné správy. Nakonec zákon definuje pravidla pro certifikaci a kontrolu informačních systémů veřejné správy. [26]

## 2.4 Bezpečnostní politika a strategie

Bezpečnostní politika je politickou koncepcí a představuje soubor klíčových cílů a prostředků státu k zajištění vnitřní a vnější bezpečnosti. Slouží k tomu, aby byla zajištěna ochrana státní svrchovanosti, územní integrity, demokratických principů, fungování demokratických institucí, ekonomický a sociální rozvoj. Také se zaměřuje na ochranu života a zdraví občanů, majetku, kulturního bohatství, životního prostředí a k plnění mezinárodních závazků v oblasti bezpečnosti. Nedílnou součástí bezpečnostní politiky je také bezpečnostní strategie. Ta byla přijata na základě usnesení č. 478 vlády ze dne 28. června 2023. Představuje klíčový dokument, ve kterém jsou uvedeny prostředky a způsoby, jak řešit definované bezpečnostní hrozby. Z tohoto tedy plyne, že bezpečnostní strategie vytváří podmínky i pro ostatní národní bezpečnostní postupy a koncepce. [27], [28], [6]

Bezpečnostní strategie České republiky tedy definuje klíčové hodnoty, postupy, prostředky a opatření, jejichž cílem je zajistit bezpečnost, obranu státu i jeho obyvatel. S ohledem na proměny bezpečnostního prostředí vláda neustále přizpůsobuje své přístupy k zajištění bezpečnosti České republiky a jejich občanů.-Tato nestálost s sebou přináší další a zcela nově hrozby nejen pro Českou republiku, neboť hlavním zdrojem rizika je proměnlivé mezinárodní prostředí. [27], [28] Na základě uvedených definicí, zákonů, hodnot bezpečnostní politiky a bezpečnostních strategií se následně stanovují jednotlivá bezpečnostní, ale i režimová opatření vedoucí ke zvyšování bezpečnosti měkkých cílů.

Tato kapitola se věnuje právnímu rámci souvisejícímu s ochranou měkkých cílů ve veřejné správě a zahrnuje přehled relevantních zákonů, nařízení a strategických dokumentů.

Úvodní část se soustřeďuje na Ústavu České republiky a Listinu základních práv a svobod, které tvoří základní právní pilíř ochrany života, zdraví, soukromí a majetku občanů. Následuje analýza zákona č. 110/2019 Sb. o zpracování osobních údajů, který spolu s evropským nařízením GDPR upravuje pravidla pro nakládání s osobními údaji včetně možností využití dohledových systémů jako nástroje prevence a reakce na násilné incidenty. Dále je rozebrán zákon č. 181/2014 Sb. o kybernetické bezpečnosti, který stanovuje povinnosti subjektů veřejné správy při ochraně před kybernetickými hrozbami, přičemž důraz je kladen na včasné hlášení incidentů, reakční opatření a dodržování bezpečnostních standardů. V návaznosti na evropskou směrnici NIS 2 vláda přistoupila k novelizaci tohoto zákona, čímž posílila ochranu informačních systémů veřejné správy. Doplněním je zákon č. 365/2000 Sb., který řeší provoz a správu informačních systémů státní správy, včetně jejich bezpečnosti, kompatibility a odpovědnosti jednotlivých orgánů. V závěru kapitoly je představena bezpečnostní politika a strategie České republiky vymezující cíle, nástroje a přístupy státu k ochraně vnitřní a vnější bezpečnosti. Bezpečnostní strategie z roku 2023 přitom reflektuje aktuální změny mezinárodního bezpečnostního prostředí a klade důraz na ochranu demokratických hodnot, veřejných institucí i obyvatelstva před novými typy hrozeb. Právní rámec tvoří nezbytný základ pro efektivní ochranu měkkých cílů včetně institucí veřejné správy.

### 3 ANALÝZA RIZIK

V této kapitole diplomové práce jsou uvedeny příklady jednotlivých analýz rizik, přičemž pro účely této práce byla vybrána specifická metoda, která představuje kvantitativní analýzu rizik s využitím jejich souvztažnosti. Tato metoda je podrobněji rozebrána ve zvláštní podkapitole.

Principem analýzy rizik je porozumění jejich povaze a vlastnostem, včetně jejich úrovně. Zahrnuje detailní posouzení nejistot, zdrojů rizik, jejich pravděpodobnosti, následků a nastiňuje možná opatření ke zvládnutí těchto rizik. Rizikové události mohou mít různé příčiny a následky a mohou zároveň ovlivnit více cílů současně. Úroveň podrobnosti a složitosti analýzy rizik závisí na jejím konkrétním účelu, dostupnosti a spolehlivosti informací i na dostupných zdrojích. Použité analytické metody mohou být kvalitativní, kvantitativní nebo jejich kombinací, přičemž volba konkrétní metody se odvíjí od charakteru analyzovaného rizika a účelu analýzy. Výsledek analýzy je ovlivněn řadou faktorů, jako jsou rozdílné názory zainteresovaných stran, podjatost, subjektivní vnímání rizik a vlastní úsudek. Dále hrají roli kvalita dostupných informací, technická omezení a použitá metoda analýzy rizik. Tyto aspekty by měly být zohledněny, zdokumentovány a sděleny rozhodovacím orgánům za účelem provedení kvalitní analýzy rizik. [29]

Analýza rizik by se měla zaměřovat zejména na následující faktory:

- „pravděpodobnost výskytu událostí a následků,
- povahu a závažnost následků,
- složitost a propojenost,
- časové faktory a míru kolísání hodnoty aktiv,
- efektivitu existujících opatření,
- úroveň citlivosti a spolehlivosti.“ [29]

Události, zejména ty s vážnými důsledky, mohou být obtížně kvantifikovatelné. V těchto případech poskytuje kombinace různých analytických technik komplexnější a přesnější pohled na danou problematiku. Analýza rizik následně slouží jako podklad pro rozhodování o tom, zda je nutné rizika ohodnotit, následně ošetřit, a jakým způsobem je třeba tak učinit. Výstupy poskytují přehled o přijatých rozhodnutích, alternativních přístupech a různých úrovních rizik. Díky tomu lze lépe pochopit dopady jednotlivých rozhodnutí a zajistit optimální opatření ke snížení či eliminaci identifikovaných rizik. [29]

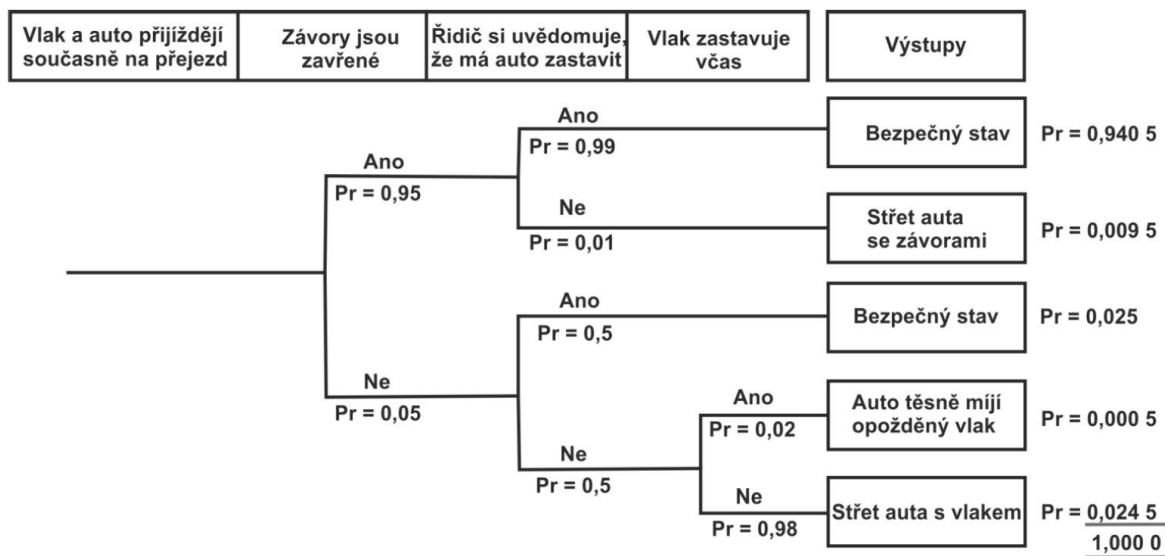
### 3.1 Obecné metody analýzy rizik

Tato podkapitola zahrnuje dílčí metody, které se používají pro analýzu rizik. Je třeba poznamenat, že se nejedná o úplný výčet metod. V tomto případě se jedná o strukturovanou techniku „co se stane, když“ (dále jen „SWIFT“) a o kontrolní seznam (dále také „checklist“). Mimo jiné existují i analytické metody, mezi které patří tzv. strom událostí (dále jen „ETA“) nebo strom poruchových stavů (dále jen „FTA“). [30], [31]

Metoda **SWIFT** je založena na principu tzv. strukturovaného brainstormingu. Ten představuje postup, jehož cílem je motivovat a inspirovat skupinu jednotlivců k vytváření a rozvíjení myšlenek spojených s jedním či více tématy bez ohledu na jejich charakter. Ke kvalitním výsledkům je zapotřebí mít k dispozici tým kvalifikovaných odborníků z dané oblasti. Během metody SWIFT je tento tým dobře obeznámen s analyzovaným procesem a systematicky zkoumá možné neočekávané události. Proces probíhá formou kladení a zodpovídání otázek směřujících k identifikaci potenciálních rizik a jejich dopadů. Tyto otázky začínají frázemi typu „co se stane, když...“, čímž se podporuje aktivní hledání možných scénářů a preventivních opatření. Cílem metody je rozpoznání potenciálně rizikových stavů a provozních situací a důkladné posouzení jejich možných dopadů. Na základě této analýzy jsou navržena adekvátní opatření s cílem minimalizovat rizika. Výsledkem je komplexní seznam rizik, v němž jsou jednotlivé hrozby klasifikovány dle úrovně rizika. Součástí výstupu jsou také specifické úkoly a opatření, které mohou sloužit jako podklad pro tvorbu plánu řízení a snižování rizik. [30], [32]

Možná nebezpečí jsou při použití metody **checklist** identifikována na základě předem připraveného seznamu. Ten obsahuje výčet typických nebezpečných látek a možných zdrojů nehod. Checklisty jsou obvykle velmi podrobné a navrženy tak, aby umožnily posoudit shodu stavu systému s platnými předpisy a normami. V případě posuzování rizik se využívají různými způsoby. Například k pochopení kontextu, identifikaci rizik a jejich seskupování, v rámci analýzy, při řízení rizik nebo pro vypracování zpráv či komunikaci o nich. V některých případech vycházejí negativních i pozitivních zkušeností z praxe. Také mohou být navrženy formálnější kategorizace a klasifikace, které slouží k rozdělení rizik na základě společných atributů. Výsledkem je efektivní a jednoduchý kontrolní seznam pro identifikaci nebezpečí, což umožňuje jeho aplikaci v kterékoliv fázi životního cyklu systému. Tento výstup rovněž zahrnuje pochopení nedostatků spojených s aplikací této metody, včetně případného vytvoření a seskupování seznamů rizik. [30], [33]

Metoda **ETA** je graficko-statická technika sloužící k modelování možných scénářů vývoje systému na základě iniciační události. Tento přístup umožňuje systematicky sledovat následné události, které se mohou v systému vyskytnout, přičemž každá událost je posuzována podle dvou variant, jako příznivého a nepříznivého průběhu. Výsledkem je rozvětvený graf, který přehledně zobrazuje interakce mezi jednotlivými prvky systému a identifikuje potenciální rizika. S narůstajícím počtem událostí se strom dále rozvětňuje, což umožňuje detailní hodnocení různých scénářů. Kvantifikace pravděpodobnosti výstupů se provádí na základě expertních posudků, historických dat nebo analýzy poruchových stavů. Tyto pravděpodobnosti jsou podmíněné a mohou se lišit v závislosti na reálných či ideálních provozních podmínkách. Výstup tak zahrnuje kvalitativní popis možných důsledků iniciačních událostí, kvantitativní odhady intenzity událostí nebo pravděpodobnost jejich výskytu, dále relativní význam různých sekvencí poruch a jiných přispívajících událostí. Součástí výstupu je také kvantitativní hodnocení účinnosti prvků řízení rizika. [30], [31], [34] Na následujícím obrázku (Obrázek 1) lze vidět výstup této metody, kdy pravděpodobnost iniciační události je zde předpokládána s hodnotou 1.

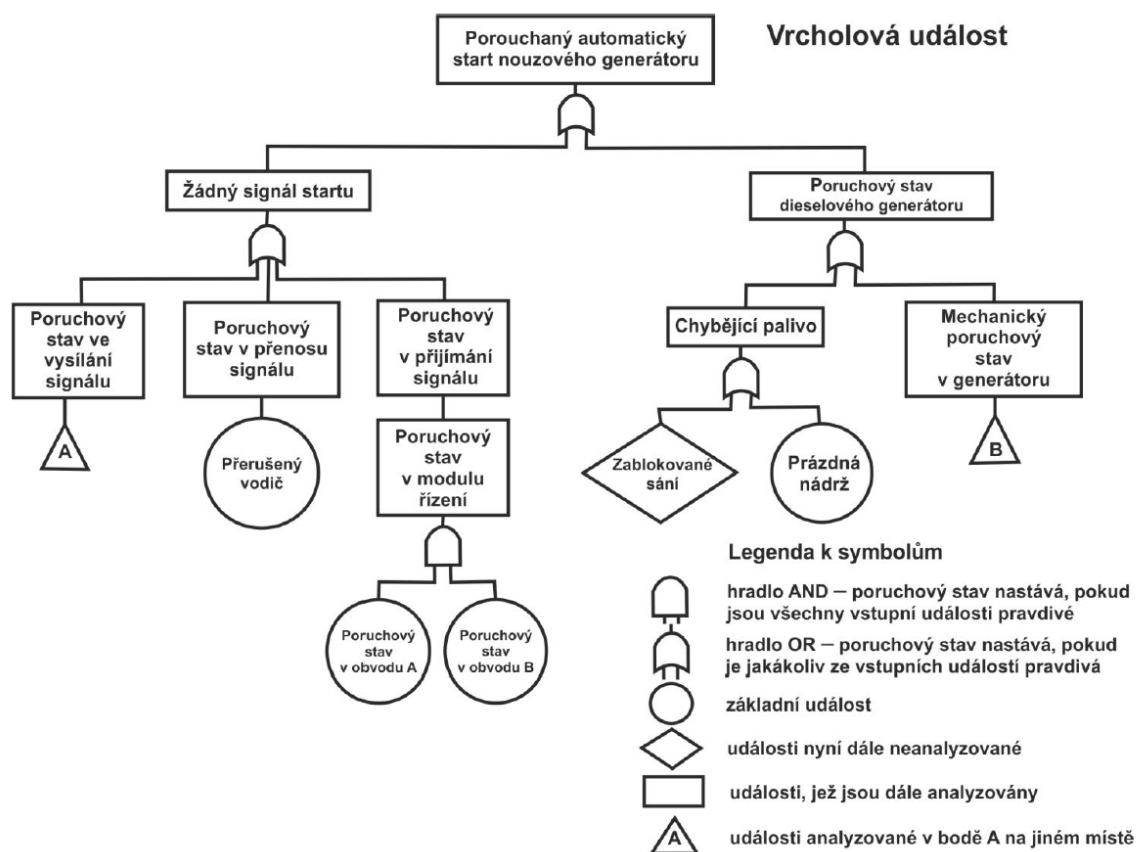


Obrázek 1 Výstup metody ETA

(zdroj: [30])

Graficko-analytická technika **FTA** je zaměřená na identifikaci a analýzu faktorů vedoucích k nežádoucí vrcholové události. Na rozdíl od předešlé metody, která sleduje směr dopředu, se FTA provádí zpětně a systematicky rozkládá události pomocí řetězce příčin, mezi něž patří hardwarové a softwarové poruchy, lidské chyby či další související faktory. Vztahy mezi těmito příčinami jsou vyjádřeny pomocí logických hradel „AND“ a „OR“. Celý

proces je pak vizualizován prostřednictvím stromového diagramu reprezentujícího Booleovu logiku. Cílem analýzy je stanovit pravděpodobnost výskytu vrcholové události pomocí analytických a statistických metod, což umožňuje identifikaci kritických faktorů a návrh opatření k minimalizaci rizik. Výstupem znázorněným na následujícím obrázku (Obrázek 2) je grafická reprezentace poukazující na možné scénáře vedoucí k výskytu vrcholové události. Zároveň zachycuje interakce mezi jednotlivými cestami, z nichž každá zahrnuje kombinaci dvou nebo více základních událostí. Součástí výsledků je také seznam minimálních kritických řezů, tedy jednotlivých cest k poruše, spolu s pravděpodobností jejich výskytu, pokud jsou dostupná relevantní data. V případě kvantitativní analýzy je klíčovým výstupem stanovení eventuálnosti vzniku vrcholové události a vyhodnocení relativní důležitosti jednotlivých základních událostí v rámci celkové analýzy rizik. [30], [31], [34]



Obrázek 2 Výstup metody FTA

(zdroj: [30])

Metody analýzy rizik využívají tzv. stupnice, které uvádějí úroveň rizika, hrozby či zranitelnosti, dále jejich hodnotu a popis. Jednotlivé stupnice jsou složeny ze tří sloupců

a čtyř řádků. Sloupce představují úroveň dopadu, a to od nízkého až po kritický. Hodnota značí pouze číselné vyjádření úrovně, zatímco popis poskytuje slovní charakteristiku dané úrovně. První tabulka (Tabulka 1) zobrazuje stupnici hodnocení rizik.

Tabulka 1 Stupnice hodnocení rizik

| Úroveň   | Popis rizika                                                                                                 |
|----------|--------------------------------------------------------------------------------------------------------------|
| Nízká    | Riziko je považováno za přijatelné.                                                                          |
| Střední  | Riziko lze snížit méně náročnými opatřeními, nebo pokud jsou opatření složitější, zůstává riziko přijatelné. |
| Vysoká   | Riziko je dlouhodobě neakceptovatelné a je nutné zahájit systematické kroky k jeho eliminaci.                |
| Kritická | Riziko je neakceptovatelné a je nutné okamžitě zahájit systematické kroky k jeho eliminaci.                  |

(zdroj: [35])

Druhá stupnice (Tabulka 2) vyjadřuje hodnocení hrozeb.

Tabulka 2 Stupnice hodnocení hrozeb

| Úroveň   | Hodnota | Popis hrozby                                                                                                             |
|----------|---------|--------------------------------------------------------------------------------------------------------------------------|
| Nízká    | 1       | Hrozba buď neexistuje, nebo je málo pravděpodobná. Realizace hrozby nenastane častěji než jednou za 5 let.               |
| Střední  | 2       | Hrozba se jeví jako málo pravděpodobná až pravděpodobná. Realizace hrozby se pohybuje v rozmezí od 1 do 5 let.           |
| Vysoká   | 3       | Hrozba se jeví jako pravděpodobná až vysoce pravděpodobná. Realizace hrozby se pohybuje v rozmezí od 1 měsíce do 1 roku. |
| Kritická | 4       | Hrozba je vysoce pravděpodobná až téměř nevyhnutelná. Realizace hrozby nastává častěji než jednou za měsíc               |

(zdroj: [35])

Poslední tabulka (Tabulka 3) představuje stupnici hodnocení zranitelnosti.

Tabulka 3 Stupnice hodnocení zranitelnosti

| Úroveň  | Hodnota | Popis zranitelnosti                                                                                                                                                                                                                                                                                                                             |
|---------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nízká   | 1       | Zranitelnost buď neexistuje, nebo její zneužití je málo pravděpodobné. Jsou implementována bezpečnostní opatření, která dokážou včas identifikovat potenciální zranitelnosti nebo pokusy o jejich zneužití.                                                                                                                                     |
| Střední | 2       | Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou implementována bezpečnostní opatření, jejichž účinnost je pravidelně vyhodnocována. Schopnost těchto opatření včas identifikovat potenciální zranitelnosti nebo pokusy o jejich obcházení je omezená. Neexistují úspěšné pokusy o překonání těchto bezpečnostních opatření. |

|          |   |                                                                                                                                                                                                                                                                                              |
|----------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Vysoká   | 3 | Zneužití zranitelnosti je pravděpodobné až vysoce pravděpodobné. Bezpečnostní opatření jsou zavedena, avšak jejich účinnost nezajišťuje pokrytí všech potřebných oblastí a není pravidelně monitorována. Existují úspěšné případy, kdy došlo k částečnému překonání bezpečnostních opatření. |
| Kritická | 4 | Zneužití zranitelnosti je vysoce pravděpodobné až téměř nevyhnutelné. Bezpečnostní opatření buď nejsou implementována, nebo jejich účinnost je výrazně omezená. Neprovádí se kontrola efektivity těchto opatření. Existují úspěšné případy, kdy došlo k překonání bezpečnostních opatření.   |

(zdroj: [35])

Z důvodu výpočtu a snadné interpretace výsledků analýzy rizik se používají právě výše uvedené varianty (Tabulka 1), (Tabulka 2) a (Tabulka 3). Díky nim lze chápat samotnou analýzu rizik a určit relevantní přístup k bezpečnosti a potenciálním rizikům

### 3.2 Vybrané specifické metody analýzy rizik

Pro efektivní analýzu rizik je klíčové správně porozumět hrozbám, které mohou ovlivnit bezpečnost zařízení. Identifikace hrozeb zahrnuje sběr informací, jako jsou typy protivníků, jejich taktiky, motivace a schopnosti. Tyto hrozby mohou mít jak lidský, tak přírodní původ. Informace o hrozbách lze získat z různých zdrojů, včetně zpravodajských služeb, studií kriminality, elektronických databází a odborné literatury. Tyto údaje lze analyzovat a strukturovat, což umožňuje identifikovat a upřednostňovat protivníky podle míry jejich riskantního potenciálu. Důležitou součástí hodnocení hrozeb je také vytváření lokálních sítí pro výměnu informací mezi bezpečnostními odborníky, což zvyšuje povědomí o rizicích a umožňuje zavádění preventivních opatření, mezi něž patří zvýšená ostražitost pracovníků vůči potenciálním hrozbám. Vzhledem k rozmanitosti a složitosti informací, které je třeba vyhodnotit, jsou v této části popsány tři specifické metody analýzy rizik – metoda CARVER, posuzování nebezpečí a hodnocení rizik (dále také „PNH“) a kvalitativní analýza rizik s využitím jejich souvztažnosti (dále také „KARS“). Tyto metody umožňují efektivní zhodnocení a interpretaci různorodých často nečíselných údajů, které jsou klíčové pro pochopení komplexních hrozeb, jež nelze jednoduše kvantifikovat. Díky těmto analýzám je možné subjektivně hodnotit rizika na základě odborných znalostí a zkušeností bezpečnostních profesionálů, kteří vyvozují závěry z různých faktorů, jako jsou bezpečnostní incidenty, chování protivníků nebo kontext dané oblasti. Tímto způsobem metody analýzy rizik umožňují flexibilní a komplexní přístup k hodnocení hrozeb, což je nezbytné pro účinnou prevenci a ochranu zařízení. [36], [37], [38]

Metoda **CARVER** představuje zkratku pro šest klíčových kritérií využívaných při posuzování toho, jak lákavým se může konkrétní cíl jevit pro potenciálního útočníka. Kritičnost (Criticality), přístupnost (Accessibility), obnovitelnost (Recuperability), zranitelnost (Vulnerability), dopad (Effect), rozpoznatelnost (Recognizability). Tato kritéria umožňují komplexní a systematické hodnocení rizik z pohledu potenciálního ohrožení. V některých případech se navíc zohledňuje sedmý prvek označovaný jako SHOCK. Ten představuje kombinované zdravotní, ekonomické a psychologické důsledky útoku na daný cíl. Tento rozšířený přístup poskytuje komplexnější pohled na možné dopady bezpečnostních incidentů a slouží jako doplněk ke klasickým hodnoticím kritériím. Jak již bylo uvedeno, při identifikaci zranitelnosti v rámci systému či infrastruktury je pro tuto metodu typický tzv. pohled potenciálního útočníka. Ten spočívá v simulaci myšlení útočníka s cílem určit nejatraktivnější cíle útoku. Výstupem této metody je buď matice nebo číselná hodnota. Výsledky umožňují zhodnotit slabá místa a možné důsledky potenciálních útoků, což usnadňuje návrh vhodných ochranných opatření. [38], [39], [40]

Na rozdíl od metody CARVER, která je založena na pohledu útočníka a pevně stanovených kritériích, metoda KARS lépe umožňuje práci s daty a zohlednit širší souvislosti. Díky tomu lépe odpovídá potřebám této práce, která se zaměřuje na rizika ve veřejných institucích jakožto měkkých cílech, kde je často nutné pracovat s různorodými a obtížně kvantifikovatelnými informacemi. Navíc metoda KARS podporuje tvorbu preventivních opatření nejen na základě výstupních hodnot, ale i hlubší interpretace kontextu, což je klíčové pro účinnou ochranu měkkých cílů. Lze tedy konstatovat, že metoda KARS byla navržena především k tomu, aby pomohla uživatelům určit, na která rizika by se měli zaměřit přednostně, protože představují nejvyšší hrozbu, a která mohou být řešena s jistým časovým odstupem. [41] Z těchto důvodů nebyla v rámci práce využita metoda CARVER, ale metoda KARS, která je blíže popsána níže.

### 3.2.1 Teoretický rámec posuzování nebezpečí a hodnocení rizik (PNH)

Metoda **PNH** patří mezi polo-kvantitativní metody. Umožňuje rychlé a přehledné vyhodnocení míry rizika v různých kontextech. Hodnocení rizika probíhá na základě tří hlavních složek, kterými jsou:

- P – pravděpodobnost vzniku rizika,
- N – možné následky rizika,
- H – dopad dle názoru hodnotitele. [42], [43]

Pravděpodobnost, že dojde ke vzniku a trvání nebezpečí, které může potenciálně nastat, se hodnotí pomocí vzestupné stupnice s hodnotami od 1 do 4. K tomuto se využije výše uvedená tabulka (Tabulka 2). [42]

Možné následky rizika, které mohou potenciálně nastat, jsou hodnoceny pomocí stupnice s hodnotami od 1 do 4, uspořádané vzestupně podle závažnosti. Stupnice je převzata z již uvedené tabulky (Tabulka 3). [42]

Hodnoty dopadu dle názoru hodnotitele jsou uvedeny v níže uvedené tabulce (Tabulka 4), přičemž i v tomto případě se jedná o vzestupnou stupnici s hodnotami od 1 do 4. [42]

Tabulka 4 Dopad dle názoru hodnotitele

| Úroveň       | Hodnota | Popis dopadu                                                |
|--------------|---------|-------------------------------------------------------------|
| Zanedbatelná | 1       | Téměř žádný dopad na úroveň rizika a ohrožení               |
| Malá         | 2       | Malý dopad na úroveň rizika a ohrožení                      |
| Střední      | 3       | Střední, pozorovatelný dopad na úroveň ohrožení a rizika    |
| Vysoká       | 4       | Vysoký, výrazný a zásadní dopad na úroveň ohrožení a rizika |

(zdroj:[42])

Tento polo-quantitativní přístup umožňuje zahrnout nejen objektivní vstupy, jako jsou pravděpodobnost a dopad, ale také subjektivní odborný názor hodnotitele. Tyto tři komponenty se následně kombinují do jednoduchého výpočtu ve formě součinu, který určuje výslednou míru rizika označenou jako „R“. Vzorec (1) slouží k vyjádření míry rizika a má následující podobu: [42]

$$R = P \times N \times H \quad (1)$$

K interpretaci výsledků je třeba využít níže uvedené škály. Škála je převzata a upravena z již uvedené tabulky (Tabulka 1). Upravená škála má tento tvar (Tabulka 5).

Tabulka 5 Stanovená škála míry rizika

| Úroveň   | Hodnota | Popis rizika                                                                                                 |
|----------|---------|--------------------------------------------------------------------------------------------------------------|
| Nízká    | 1–12    | Riziko je považováno za přijatelné.                                                                          |
| Střední  | 13–32   | Riziko lze snížit méně náročnými opatřeními, nebo pokud jsou opatření složitější, zůstává riziko přijatelné. |
| Vysoká   | 33–48   | Riziko je dlouhodobě neakceptovatelné a je nutné zahájit systematické kroky k jeho eliminaci.                |
| Kritická | 49–64   | Riziko je neakceptovatelné a je nutné okamžitě zahájit systematické kroky k jeho eliminaci.                  |

(zdroj:[42])

Hodnoty této škály určují, jak rychle je potřeba přijmout opatření ke snížení rizika a jakou důležitost má dané bezpečnostní opatření.

### 3.2.2 Teoretický rámec metody kvalitativní analýza rizik s využitím jejich souvztažnosti (KARS)

Z předchozího textu je patrné, že použití metody **KARS** není složité, neboť se jedná o kvalitativní analytickou metodu. Přesto je však nutné dodržet předem stanovený postup, který vede k určení míry rizika. Při použití této metody je zásadní dodržet následující kroky:

- „zpracování soupisu rizik,
- sestavení tabulky souvztažnosti rizik,
- vyplnění tabulky souvztažnosti rizik,
- vytvoření součtů souvztažnosti rizik,
- výpočet koeficientu aktivity a pasivity jednotlivých rizik,
- grafické vyhodnocení rizik,
- výpočet os koeficientu aktivity a pasivity,
- vyhodnocení analýzy KARS.“ [44]

Nejprve je nutné sestavit soupis rizik, který by měl být vypracován kvalifikovanými odborníky. Tento přehled by měl být co nejkomplexnější a nejpodrobnější, aby výsledná analýza poskytla relevantní a spolehlivé informace. [44] Druhým krokem je sestavení tabulky (Tabulka 6) souvztažnosti rizik. Lze předpokládat, že v daném systému se vyskytuje  $x$  rizik označených jako  $R_i$ , kde index  $i$  nabývá hodnot od 1 do  $x$ . Každá pozice v tabulce je pak specifikována jako  $R_{ij}$ , kde index  $i$  odpovídá číslu řádku a index  $j$  označuje příslušný sloupec. [41]

Tabulka 6 Výčet souvztažnosti rizik

|    | Riziko | 1. | 2. | 3. | 4. | 5. |
|----|--------|----|----|----|----|----|
| 1. |        |    |    |    |    |    |
| 2. |        |    |    |    |    |    |
| 3. |        |    |    |    |    |    |
| 4. |        |    |    |    |    |    |
| 5. |        |    |    |    |    |    |

(zdroj: [44])

Dalším bodem harmonogramu je vyplnění výše uvedené tabulky (Tabulka 6) souvztažnosti rizik za využití následující rovnice (2)

$$R_{ij} = 0 \text{ (pro } i = j \text{)} \quad (2)$$

Riziko  $R_i$  tedy nemůže způsobit samo sebe, tzn. že všechny hodnoty na hlavní diagonále budou rovny 0. Po aplikaci vznikne následující tabulka (Tabulka 7). [41], [44]

Tabulka 7 Vyplněná diagonála

|    | Riziko | 1. | 2. | 3. | 4. | 5. |
|----|--------|----|----|----|----|----|
| 1. |        | 0  |    |    |    |    |
| 2. |        |    | 0  |    |    |    |
| 3. |        |    |    | 0  |    |    |
| 4. |        |    |    |    | 0  |    |
| 5. |        |    |    |    |    | 0  |

(zdroj: [44])

Zbylé pozice ve výše uvedené tabulce (Tabulka 7) se vyplňují postupně po řádcích zleva doprava. Do pozic  $R_{ij}$  (pro  $i \neq j$ ), tedy hodnot mimo hlavní diagonálu, se použijí následující pravidla:

- hodnota 1 se zapíše, pokud existuje reálná možnost, že riziko  $R_i$  může způsobit riziko  $R_j$ ,
- hodnota 0 se zapíše v případě, že neexistuje reálná možnost, že riziko  $R_i$  může vést k výskytu rizika  $R_j$ . [41], [44]

Po dokončení vyplňování tabulky následuje vytvoření součtů souvztažnosti rizik. To se provede tak, že se k výše uvedené tabulce (Tabulka 7) přidá další řádek a sloupec. První buňka v těchto přidaných částí je označena jako  $\Sigma$  (suma). Následně se sečtou hodnoty v jednotlivých řádcích a sloupcích, čímž vznikne finální podoba tabulky souvztažnosti (Tabulka 8) souvztažnosti. [41], [44]

Tabulka 8 Konečný tvar tabulky

|    | Riziko | 1. | 2. | 3. | 4. | 5. | $\Sigma$ |
|----|--------|----|----|----|----|----|----------|
| 1. |        | 0  |    |    |    |    |          |
| 2. |        |    | 0  |    |    |    |          |
| 3. |        |    |    | 0  |    |    |          |
| 4. |        |    |    |    | 0  |    |          |

|          |  |  |  |  |  |   |   |
|----------|--|--|--|--|--|---|---|
| 5.       |  |  |  |  |  | 0 |   |
| $\Sigma$ |  |  |  |  |  |   | 0 |

(zdroj: [44])

Cílem tohoto kroku je převést výsledky do formátu vhodného pro matematickou a grafickou analýzu pomocí koeficientů aktivity a pasivity. Koeficient aktivity rizika (dále jen „ $K_{AR_i}$ “) vyjadřuje procentuální podíl rizik navázaných na riziko  $R_i$  která mohou nastat v případě jeho výskytu. Koeficient pasivity rizika (dále jen „ $K_{PR_i}$ “) představuje procentuální vyjádření celkového počtu rizik, která mohou způsobit výskyt  $R_i$ . Tento údaj umožňuje posoudit, jak výrazně je dané riziko ovlivněno ostatními identifikovanými riziky. [41]

$K_{AR_i}$  se vypočítá dle rovnice (3), kde  $\Sigma R_i$  je součet rizik v řádku  $i$  a  $x$  je celkový počet předpokládaných rizik. [41], [44]

$$K_{AR_i} = \left( \frac{\Sigma R_i}{x-1} \right) \cdot 100 \quad (3)$$

$K_{PR_i}$  se vypočítá dle rovnice (4), kde  $\Sigma R_j$  je součet rizik ve sloupci  $j$  a  $x$  je celkový počet předpokládaných rizik. [41], [44]

$$K_{PR_i} = \left( \frac{\Sigma R_j}{x-1} \right) \cdot 100 \quad (4)$$

Každé riziko  $R_i$  je tak definováno dvojicí koeficientů  $K_{AR_i}$  a  $K_{PR_i}$ . Pro přehledné zobrazení je vytvořena následující tabulka (Tabulka 9), která slouží jako podklad pro grafickou interpretaci. [41]

Tabulka 9 Koeficienty aktivity a pasivity

| Riziko         | 1. | 2. | 3. | 4. | 5. |
|----------------|----|----|----|----|----|
| $K_{AR_i}$ (%) |    |    |    |    |    |
| $K_{PR_i}$ (%) |    |    |    |    |    |

(zdroj: [44])

Předposledním krokem je výpočet os koeficientu aktivity a pasivity, jejichž cílem je určit míru nebezpečnosti jednotlivých rizik na základě vzájemných vazeb. Tento proces je realizován rozdělením grafu do čtyř základních oblastí pomocí os  $O_1$  a  $O_2$ , přičemž každá oblast vymezuje úroveň významnosti rizik, která se v ní nacházejí. Tyto oblasti se rozdělují následovně:

- **I. oblast** – primárně a sekundárně nebezpečná rizika,

- **II. oblast** – sekundárně nebezpečná rizika,
- **III. oblast** – primárně nebezpečná rizika,
- **IV. oblast** – relativně bezpečná. [44]

Graf je rozdělen na oblasti tak, aby do první oblasti spadalo 80 % všech analyzovaných rizik. Tato oblast, jak je uvedeno výše, je definována jako oblast primárních a sekundárních rizik na které je třeba se v nejbližší době co nejdříve zaměřit. [41]

Osa  $O_1$  představuje kolmici na osu x a osa  $O_2$  je kolmicí na osu y. Nejdříve je nutné si určit, jaký podíl rizik má být zahrnut do rozdělení pomocí odstavců. Jak je uvedeno v předešlém textu, v tomto případě se jedná o takové rozdělení, že do první oblasti spadá 80 % všech analyzovaných rizik. [44]

Na základě výše stanovených podmínek bude mít rovnice (5) pro výpočet osy  $O_1$  následující tvar:

$$O_1 = K_{A_{max}} - \frac{K_{A_{max}} - K_{A_{min}}}{100} \cdot 80 \quad (5)$$

a rovnice (6) pro výpočet osy  $O_2$  bude mít tento tvar:

$$O_2 = K_{P_{max}} - \frac{K_{P_{max}} - K_{P_{min}}}{100} \cdot 80 \quad (6)$$

Kde u rovnice (5)  $K_{A_{max}}$  značí maximální hodnotu k  $K_{AR_i}$ , zatímco  $K_{A_{min}}$  představuje minimální hodnotu k  $K_{AR_i}$ . V druhém případě, u rovnice (6)  $K_{P_{max}}$  značí maximální hodnotu k  $K_{PR_i}$ , zatímco  $K_{P_{min}}$  označuje minimální hodnotu k  $K_{PR_i}$ . [41], [44]

Posledním krokem je vyhodnocení analýzy KARS. Výstupem analýzy je graf znázorňující souvztažnosti rizik, který je sestaven na základě údajů z tabulky (Tabulka 9) a koeficientů  $K_{AR_i}$  a  $K_{PR_i}$ . Tento graf znázorňuje rozložení rizik a jejich vzájemné souvislosti, což přispívá k efektivnímu řízení bezpečnostních opatření. [44]

Třetí kapitola diplomové práce se zabývá metodami analýzy rizik se zaměřením na kvantitativní přístup využívající souvztažnost mezi jednotlivými riziky. Úvodem je popsán obecný princip analýzy rizik, která zahrnuje identifikaci, hodnocení a řízení rizik s přihlédnutím k jejich pravděpodobnosti, následkům a vzájemným vazbám. Jsou představeny tradiční metody jako SWIFT, checklist, ETA a FTA. Dále je vysvětleno použití hodnoticích stupnic pro rizika, hrozby a zranitelnosti. Následně jsou popsány specifické přístupy jako CARVER, který hodnotí atraktivitu cíle z pohledu útočníka, PNH, která patří

mezi polo-quantitativní metody a umožňuje rychlé a přehledné vyhodnocení míry rizika v různých kontextech. Dále také metoda KARS, jenž byla v této práci upřednostněna díky své flexibilitě a schopnosti pracovat s nečíselnými daty v kontextu ochrany státních institucí z pohledu měkkých cílů. Metoda KARS zahrnuje teoretický postup od identifikace rizik, přes tvorbu a vyplnění tabulky souvztažnosti, výpočet koeficientů až po grafické vyhodnocení, jehož výsledkem je vizuální rozdělení rizik podle jejich významnosti a určení prioritních opatření k jejich řešení.

## 4 METODICKÁ A KONCEPČNÍ PODPORA OCHRANY MĚKKÝCH CÍLŮ

V této kapitole jsou uvedeny jednotlivé metodiky a koncepce, které se svým obsahem zaměřují na ochranu a zvyšování bezpečnosti měkkých cílů. Zároveň byly vydány Ministerstvem vnitra ČR, tudíž mají kvalifikovaný odborný základ.

### 4.1 Koncepce ochrany měkkých cílů pro roky 2017–2020

Jeden z hlavních strategických dokumentů zaměřených na ochranu MC je Koncepce ochrany měkkých cílů z roku 2017–2020 (dále jen „Koncepce“), která byla na základě usnesení vlády č. 711 ze dne 27. července 2016 zadána k vypracování. Výstupem této Koncepce je komplexní podklad k problematice ochrany MC, který slouží jako základ pro vytvoření efektivního systému jejich ochrany. Důraz je kladen zejména na připravenost potenciálně ohrožených míst, aby v případě útoku byly možné škody co nejvíce minimalizovány a důsledky nebyly tak závažné jako v případě nepřipravenosti. Je důležité si uvědomit, že ochrana MC se primárně nezaměřuje na prevenci méně závažných trestných činů, jako jsou krádeže, požáry nebo havárie, ale cílem je zajištění bezpečnosti velkého počtu osob před teroristickými či jinými závažnými násilnými útoky. Prioritou v této oblasti není ochránění majetku, ale především ochrana života a zdraví osob. [45], [46]

Součástí Koncepce jsou i priority a návrhy ve formě konkrétních úkolů:

- „vytvoření stálého poradního sboru Ministerstva vnitra pro ochranu měkkých cílů,
- vytvoření série vzdělávacích kurzů a materiálů k ochraně měkkých cílů a jejich poskytování veřejnosti,
- realizace informační kampaně,
- standardizace formátu bezpečnostních plánů měkkých cílů,
- rozesílání varování vybraným zástupcům měkkých cílů.“ [45]

V rámci prvního úkolu je nezbytné sdílet informace o fungování bezpečnostního systému, zpracovávat připomínky k dokumentům a opatřením souvisejícím s realizací Koncepce a vytvořit odbornou konzultační platformu pro tuto oblast. Dále je kladen důraz na sdílení příkladů „dobré praxe“ z věrohodných zdrojů a pověření MV ČR koordinací aktivit, včetně zřízení poradního sboru složeného ze zástupců zainteresovaných subjektů. Poradní sbor se má pravidelně setkávat za účelem konzultace jednotlivých úkolů, dokumentů

a problémů při implementaci Koncepce. Cílem dalšího úkolu je vzdělávání odborníků ze složek bezpečnostního systému, majitelů, provozovatelů a vlastníků MC v oblasti jejich ochrany, přičemž součástí tohoto procesu je i vytvoření specifických metodik. Zahrnuje to zhotovení a realizaci komplexní série vzdělávacích kurzů zaměřených na ochranu MC a také vypracování a zveřejnění metodik, které zohledňují specifika různých typů MC, např. venkovních akcí. [45]

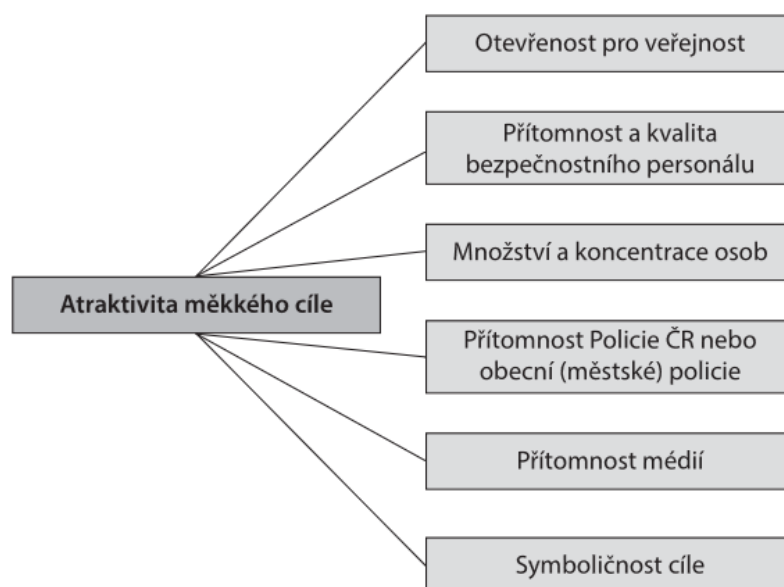
Realizace informační kampaně má za cíl zvýšit informovanost odborné i laické veřejnosti o chránění MC, a to prostřednictvím zveřejňování metodických podkladů, publikací, videí a dalších informačních materiálů. Informace publikované na webových a sociálních sítích MV ČR budou pravidelně aktualizovány. Dále budou šířeny prostřednictvím spolupracujících subjektů a dalších komunikačních kanálů, včetně médií. [45]

Standardizace formátu bezpečnostních plánů MC je zaměřena na sjednocení jejich podoby. Cílem je tvorba dokumentu, který stanoví jejich základní náležitosti. Tento dokument bude poté zveřejněn na stránkách MV ČR a distribuován dalšími komunikačními kanály. Posledním úkolem je zavedení systému varování pro vybrané měkké cíle a jejich zástupce prostřednictvím komunikační sítě. V případě potřeby budou důležité informace, např. o útoku na jiný měkký cíl, zasílány formou SMS na poskytnutá telefonní čísla. [45] Koncepce uvádí i příklady MC, které lze z obecného hlediska rozdělit takto:

- *„bary, kluby, diskotéky, restaurace a hotely,*
- *kina, divadla, koncertní sály, zábavní centra,*
- *komunitní centra,*
- *kulturní, sportovní, náboženské a další akce,*
- *náboženské památky a místa určená k uctívání,*
- *nákupní centra, tržiště a obchodní komplexy,*
- *nemocnice,*
- *parky a náměstí,*
- *politická shromáždění, průvody, demonstrace,*
- *sportovní haly a stadióny,*

- *školská zařízení, koleje, menzy, knihovny,*
- *turistické památky a zajímavosti, muzea, galerie,*
- *veřejné instituce,*
- *významné dopravní uzly, vlaková a autobusová nádraží, letištní terminály,*
- *jiná symbolicky významná místa či akce,*
- *a další.“ [45]*

Zásadním znakem je tzv. přitažlivost MC, která vyjadřuje, jak moc je daný cíl atraktivní pro útočníka, ať už z pohledu dopadu či způsobu útoku. Kritéria, která mohou ovlivnit atraktivitu objektu jsou znázorněna na následujícím obrázku (Obrázek 3):



Obrázek 3 Kritéria ovlivňující atraktivitu měkkého cíle

(zdroj: [46])

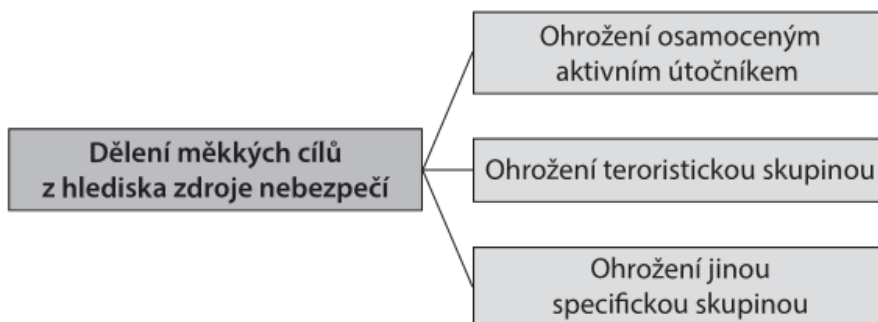
Dalším faktorem je časová působnost zdroje výskytu, tedy zda je místo působení trvalé či dočasné. Trvalé prostředí lze rozdělit následovně:

- vnitřní (např. divadla, nemocnice, obchodní centra),
- venkovní (např. trhy, stadiony a jiné sportovní areály). [45]

Dočasné prostředí je charakteristické proměnlivým časovým rozsahem, tzn. že výskyt tohoto zdroje na daném místě není stálý, ale závisí na okolních podmínkách. Mezi dočasné MC spadají např. shromáždění a venkovní akce, které mohou probíhat na veřejně přístupném, ale i soukromém pozemku. Dělí se na:

- akce bez vstupného (např. velikonoční a vánoční setkání, trhy, demonstrace)
- akce se vstupným (např. koncerty, festivaly). [45]

Posledním zmíněným kritériem dělení je zdroj nebezpečí, který může MC ohrožovat. Přehled tohoto rozdělení je uveden na následujícím obrázku (Obrázek 4):



Obrázek 4 Dělení měkkých cílů z hlediska zdroje nebezpečí

(zdroj: [46])

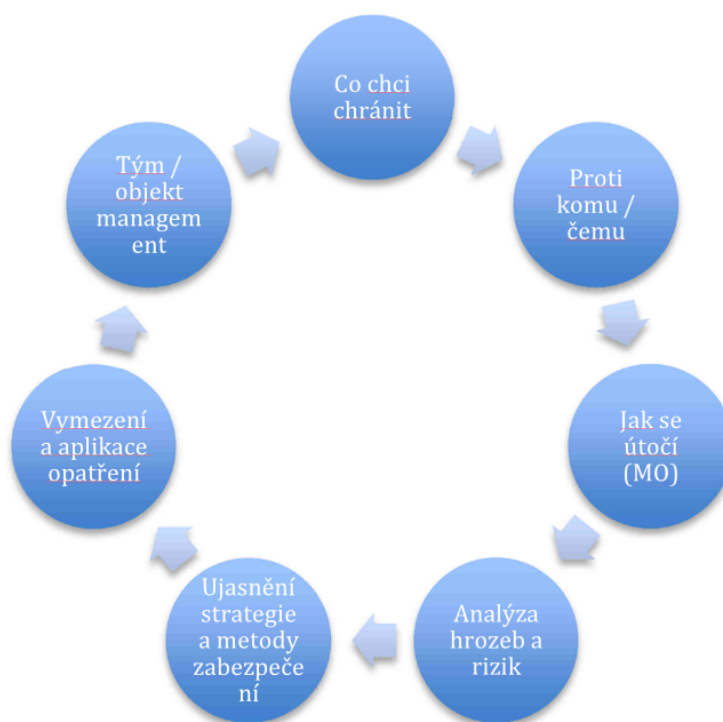
Z pohledu veřejných institucí se jedná především o různé úřady, ať už na centrální úrovni, nebo v rámci vyšších či nižších samosprávných celků, které jsou veřejnosti volně přístupné. V těchto místech se pravidelně shromažďuje větší počet lidí, zejména v předem stanovených časech úředních hodin. To potenciálním útočníkům usnadňuje odhadnutí nejvhodnějšího okamžiku k útoku na daný objekt. [45]

## 4.2 Metodika Základy ochrany měkkých cílů

Ministerstvo vnitra České republiky vydalo v červnu roku 2016 obecnou metodiku zaměřující se na ochranu MC. Ta se zaměřuje především na ochranu fyzických osob. Lze ji tedy spolehlivě využít nejen v případě potenciálních útoků ze strany teroristů, ale také z pohledu jednání extremistických jedinců či skupin. Mezi možné útočníky je možné zahrnout i osoby s kriminální motivací, osobními pohnutkami nebo duševními poruchami. Metodika je obecného charakteru, a proto ji lze aplikovat na jakýkoliv MC. [11]

Postupy na ochranu MC jsou zpravidla zaváděna dobrovolně jejich správci nebo vlastníky. Ačkoli tato doporučená opatření nejsou právně závazná, svou závažností a rozsahem mohou být natolik zásadní, že přesahují rámec běžných požadavků veřejného pořádku a bezpečnosti, a proto jsou i přes svou dobrovolnost často přijímána. Tato opatření nejsou určena k nahrazení stávajících bezpečnostních systémů, ale k jejich doplnění a posílení, a to v souladu s právními předpisy stanovenými státem. [11]

Vzhledem k široké a rozmanité škále objektů, které lze za měkké cíle považovat, je nezbytné stanovit principy zabezpečení určující obecný postup při vytváření efektivního bezpečnostního systému. Tento postup je rozdělen do sedmi kroků, jak znázorňuje obrázek níže (Obrázek 5):



Obrázek 5 Cyklus efektivního bezpečnostního systému

(zdroj: [11])

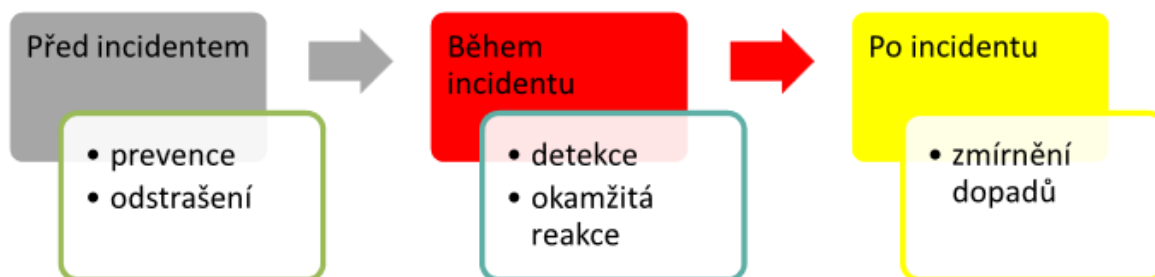
Při návrhu bezpečnostního systému je klíčové nejprve definovat chráněné zájmy. V úvodní fázi je třeba určit, co je nejcennější, co je třeba chránit, a jaké ztráty by byly nepřijatelné. Typicky jde o lidské životy a zdraví, majetek, informace, hodnoty či reputaci. Jak již bylo uvedeno výše, metodika se primárně zaměřuje na obranu před násilnými útoky, tedy zejména na zajištění bezpečnosti osob. Mnohá opatření však zároveň přispívají i k prevenci narušování veřejného pořádku, ochraně majetku nebo minimalizaci rizik spojených s technickými haváriemi. [11]

Dalším krokem je identifikace potenciálních zdrojů ohrožení a hrozeb vůči stanoveným zájmům. To zahrnuje analýzu možných útočníků nebo skupin s motivací zaútočit, s využitím informací o dosavadních incidentech i předvídání možných nebezpečí. Je nutné zohlednit specifika daného MC, jako je přítomnost významných osobností, mediální zájem, data konání, použití pyrotechniky či stavební odolnost objektu. [11]

Kvalitně definované zdroje ohrožení a konkrétní formy útoků tvoří základ bezpečnostního systému. Pokud nejsou podloženy důkladnou analýzou, hrozí neefektivita a plýtvání finančními i lidskými zdroji. Přístup vychází ze systematického zhodnocení hrozeb, na jehož základě jsou teprve navrhována adekvátní postupy. Identifikované hrozby jsou následně podrobeny analýze rizik, která pomáhá stanovit jejich prioritu. Existuje několik metod hodnocení, základní princip však spočívá v porovnání pravděpodobnosti realizace útoku s jeho možnými dopady. Výsledkem je efektivní rozdělení zdrojů tak, aby byly prioritně řešeny nejzávažnější hrozby, za předpokladu, že nelze opomíjet ani ty méně závažné. [11]

Na základě provedené analýzy jsou implementována konkrétní bezpečnostní opatření přizpůsobená danému objektu. Zahrnují technická řešení i bezpečnostní plány, které pokrývají preventivní opatření, standardní provozní postupy i krizové scénáře pro případ, že by se útoku nepodařilo zabránit. Cílem je minimalizace následků útoku a zabránění eskalaci krizové situace. Metodika se zaměřuje na násilné útoky, tedy úmyslné činy ohrožující život, zdraví, svobodu nebo lidskou důstojnost. Je však nutné počítat i s jejich sekundárními dopady, ať už materiálními, nebo finančními. [11]

K dalšímu klíčovému členění patří časová osa incidentu a souvisejících bezpečnostních kroků. Každý bezpečnostní incident je třeba řešit ve třech časových fázích, jak je možno vidět na následujícím obrázku (Obrázek 6). Je nezbytné zvážit opatření, která lze přijmout před jeho výskytem, a to tak, aby se snížila pravděpodobnost incidentu, minimalizace jeho následků nebo odvrácení útoku od cíle. Dále je nutné určit postupy v průběhu samotného incidentu a kroky pro zmírnění následků po jeho skončení. [11]



Obrázek 6 Časové fáze incidentu

(zdroj: [11])

První fází je tzv. fáze před incidentem. Jejím cílem je zavést preventivní opatření, která sníží pravděpodobnost útoku, zrychlí reakci a omezí následky. Součástí může být také

využití odstrašujících prvků, které útočníka odradí od výběru daného cíle, nebo asertivní komunikace zaměřená na uklidnění situace a deeskalaci konfliktu. [11]

V případě, že nelze útoku zabránit, je klíčová rychlá detekce podezřelého chování nebo narušení chráněného prostoru, a to ideálně ještě před samotným útokem. Následuje okamžitý zásah bezpečnostních složek nebo jiných odpovědných osob dle připraveného plánu. [11]

Po skončení incidentu nastupuje fáze řízení krizové situace v souladu se stanoveným koordinačním plánem a jeho prioritami. Závěrečnou částí je obnova provozu dané organizace v co nejkratším možném čase. [11]

### **4.3 Bezpečnostní plán měkkého cíle aneb co by nemělo být opomenuto při jeho zpracování**

Poslední zmíněnou metodikou v rámci této diplomové práce je bezpečnostní plán MC, respektive doporučení, které by při jeho zpracování neměla být opomenuta. Jak uvádí tato metodika, každý MC by měl mít zpracovaný tzv. bezpečnostní plán, jenž zahrnuje tři základní oblasti. Jsou jimi:

- identifikace MC,
- ochranné opatření,
- dění po incidentu. [47]

Do první oblasti spadají jednak identifikační údaje o zájmovém MC, ale také základní informace o objektu včetně jeho okolí. Identifikačními údaji se rozumí název, lokalita, povaha a struktura organizace, dále její provozní doba nebo celkový počet zaměstnanců, případně nejvyšší možný počet návštěvníků či alespoň průměrná návštěvnost. Základní informace představují charakteristiku a typické vlastnosti objektu, jeho plán a sousední objekty či místa mající vliv na bezpečnost zájmového MC. Spadají sem i podmínky vstupu do objektu. Ty lze kategorizovat na volný přístup bez omezení, kontrolovaný vstup (např. skrze vstupenku) a vstup s kontrolou zakázaných předmětů. [47]

Druhou oblastí jsou ochranná opatření, která metodika dělí na dvě následující oblasti:

- fyzická bezpečnost,
- technická opatření. [47]

Fyzickou bezpečnost je třeba chápat jako přítomnost pracovníků zaměřených na zajištění bezpečnostního dohledu v zájmovém MC a sem spadá i jejich školení. Zajištění dohledu lze rozdělit následovně:

- pouze běžný personál bez specializace na bezpečnost,
- interní bezpečnostní tým zahrnující bezpečnostního manažera nebo jiných odpovědných osob (včetně jejich počtu),
- ochranu zajišťuje externí bezpečnostní agentura (s uvedením počtu pracovníků),
- dobrovolnická bezpečnostní nebo poradatelská služba (včetně počtu členů),
- přítomnost bezpečnostních složek (např. policie) a podmínky jejich nasazení v rámci spolupráce,
- žádné bezpečnostní zajištění, není zde přítomen bezpečnostní personál. [47]

Nedílnou součástí fyzické bezpečnosti je i plán školení bezpečnostních pracovníků, ostatního personálu a managementu. Tento plán by měl brát zřetel na všechny klíčové aktéry a obsahovat tematický plán školení zaměřený na bezpečnostní postupy. Frekvence školení závisí na rozhodnutí a kapacitách odpovědných osob MC, obecně se však doporučuje pravidelné školení. V případě vzniku bezpečnostního incidentu je vhodné svolat poradu a vyhodnotit konkrétní kroky k řešení situace. Školení lze rozdělit na:

- školení procedur,
- školení na asertivní komunikaci
- školení zaměřená na bezpečnostní pohovory,
- školení na rozpoznávání podezřelých předmětů, osob, zásilek a vozidel,
- právní školení pro odborný personál,
- školení týkající se koordinačního plánu. [47]

Dalším druhem je pravidelné školení ostatního personálu MC. Je totiž zapotřebí klást důraz i na přípravu zbytku personálu na krizové situace. Dobře informovaný a koordinovaný tým může výrazně zmírnit následky mimořádné události. Toto školení může být zaměřeno na zlepšení povědomí o bezpečnosti, hlášení neobvyklých situací (např. neznámý předmět či osoba v budově), případně na základní bezpečnostní postupy (např. utíkej – schovej se – bojuj). [47]

Druhou oblast školení tvoří školení managementu, a to i nad rámec obecného školení o bezpečnosti. Sem spadá koordinační plán určený pro vedení MC, jenž obsahuje postupy pro zvládání různých fází po incidentu. Jeho cílem je minimalizovat následky potenciálního útoku, usnadnit rozhodování odpovědných osob, stanovit jasné kompetence a přispět k rychlému obnovení provozu MC. [47]

Technická opatření zahrnují nejen seznam použitých prvků, ale i jejich účel, způsob použití a osoby zodpovědné za jejich obsluhu. Stejně jako u předchozí oblasti je i zde nutné stanovit standardizované postupy a způsob hodnocení informací. Součástí technické ochrany jsou i školení zaměřená na technické systémy. Např. školení personálu pracujícího s VSS. [47], [48] Technické prostředky slouží k tomu, aby efektivně podporovaly uplatňování režimových opatření, zvyšovaly úroveň fyzické bezpečnosti a současně působily preventivně proti narušitelům tím, že jim komplikují přístup k chráněným hodnotám a prodlužují dobu potřebnou k jejich překonání. [49] Technická ochrana se dělí na elektronické, mechanické, kombinované a speciální prvky. Mezi elektronické prvky spadá ochrana založená na využití elektronických systémů a technických komponent sloužících k ochraně chráněného prostoru nebo objektu. Např. poplachové zabezpečovací a tísňové systémy (dále jen „PZTS“), VSS, elektronická kontrola vstupu (dále jen „EKV“), vnitřní rozhlas k evakuaci osob a další. Mechanické prvky spočívají v ochraně osob a majetku za použití fyzických bariér a konstrukčních prvků, které ztěžují nebo znemožňují neoprávněný přístup, jako jsou třeba. bezpečnostní dveře, okna, zátarasy k objektu, zdi, ploty a další. Kombinované prvky zahrnují elementy z uvedených předešlých skupin, tedy z oblasti elektronických a mechanických prvků. Speciální prvky ochrany se zaměřují na individuální technická opatření k zabezpečení kritické infrastruktury. Dále zahrnuje chemickou a fyzikální ochranu dokumentů a předmětů a také využívá obranně-technické zásahy. Klíčovou součástí jsou technické prohlídky objektů, jejichž cílem je odhalení a prevence proti instalaci nelegálních odposlechových, sledovacích či záznamových zařízení v budovách a zabezpečených prostorech. [47], [48], [49]

Poslední částí bezpečnostního plánu MC je tzv. dění po incidentu, tedy situace s postupy v případě bezpečnostního incidentu. Vzniklý incident je třeba řádně zaevidovat. Správné vyhodnocení a analýza incidentu mohou přispět ke zlepšení opatření a pomoci např. policii při odhalení pachatelů. Informace je vhodné sdílet nejen s policií, ale i s ostatními MC, protože se může jednat o součást rozsáhlejšího útoku. Evidence taktéž může pomoci policii při budoucí identifikaci pachatelů, nebo je díky ní je možné odhalit pracovníky, kteří

úmyslně vyvolávají tyto incidenty, čímž se může předejít dalším problémům. Doporučeno je taktéž sdílet informace o těchto bezpečnostních událostech i s ostatními MC v okolí, nikoliv pouze s policií. Na základě toho může dojít ke zjištění, že se incidenty staly i na jiných místech, což může být klíčová informace, která naznačuje např. sběr informací pro přípravu na závažný násilný, či teroristický útok. [47]

Evidenci se v případě výskytu bezpečnostního incidentu rozumí sepsání zprávy o události přítomným bezpečnostním pracovníkem. Následně se tato zpráva předá vedoucímu v úseku bezpečnosti, např. bezpečnostní manažer), který incident zanalyzuje a na základě vyhodnocení může upravit stávající postupy. Jak již bylo uvedeno výše, tak informace o incidentu by se měly dále sdílet s relevantními subjekty, mezi ně patří Policie České republiky (dále také „PČR“), další organizace v okolí nebo vedení daného MC. Součástí evidencí by měl tedy být i seznam kvalifikovaných kontaktních osob, kterým se oznámí výskyt bezpečnostního incidentu. Tyto osoby by měly být nápomocné k vyřešení bezpečnostních incidentů a následnému stanovení postupů ke zlepšení podmínek. [47]

Bezpečnostní plán MC představuje klíčový nástroj pro zajištění bezpečnosti osob i majetku. Měl by být komplexní, pravidelně aktualizovaný a obsahovat nejen preventivní opatření, ale i postupy pro zvládání incidentů. Mezi zásadní oblasti bezpečnostního plánu se řadí identifikace MC, ochranná opatření a dění po incidentu. Klíčový prvek vedoucí ke zlepšení zahrnuje důsledné školení všech aktérů, pravidelnou analýzu hrozeb a incidentů, spolupráci s dalšími subjekty a implementaci fyzických, ale i technických bezpečnostních opatření. Systematický přístup k bezpečnosti zajistí nejen ochranu návštěvníků a zaměstnanců, ale i efektivní reakci na případné hrozby.

Tato kapitola se zaměřila na metodiky a koncepce vydané MV ČR týkající se ochrany MC, tedy veřejně přístupných míst s koncentrací osob a nízkou úrovní zabezpečení. Klíčovým dokumentem je Koncepce ochrany měkkých cílů pro roky 2017–2020, jejímž cílem je vytvoření efektivního systému ochrany s důrazem především na prevenci a minimalizaci následků teroristických či jiných závažných násilných útoků. Stanovuje strategické priority, jako je zřízení poradního sboru, realizace vzdělávacích kurzů a informačních kampaní, standardizace bezpečnostních plánů a zavedení systému včasného varování. Koncepce rovněž kategorizuje MC dle typu, atraktivity pro útočníky, časové působnosti a dle zdrojů hrozeb. Na ni navazuje obecná metodika z roku 2016, která popisuje bezpečnostní cyklus v sedmi krocích zahrnující identifikaci chráněných zájmů, analýzu hrozeb a rizik, zavedení konkrétních preventivních i reaktivních opatření a řízení incidentů

ve všech jejich časových fázích. Závěrečná část kapitoly se věnuje tvorbě bezpečnostního plánu MC, jenž má být komplexní a zahrnovat identifikaci objektu, ochranná opatření, školení personálu, spolupráci s bezpečnostními složkami a scénáře postupu po incidentu. Cílem všech zmíněných přístupů je zvýšit připravenost a schopnost efektivně čelit bezpečnostním hrozbám.

Teoretická část diplomové práce poskytla komplexní základ pro pochopení problematiky ochrany MC ve veřejné správě, přičemž se zaměřila na vymezení vybraných pojmů, právní rámec, metody analýzy rizik a strategické přístupy k ochraně těchto objektů. Úvodní část definovala měkké cíle jako veřejně přístupná místa s vysokou koncentrací osob a nízkou úroveň ochrany proti násilným útokům a objasnila související pojmy jako riziko, hrozba, újma, zranitelnost, odolnost a bezpečnostní opatření. Statistiky útoků na zaměstnance jiné státní instituce potvrdily rostoucí míru agrese vůči pracovníkům veřejné správy, což podtrhuje aktuálnost a naléhavost této problematiky. Jako modelový měkký cíl byla zvolena konkrétní instituce, a to odbor dopravních a správních agend v ORP, jejíž činnost je nedílnou součástí krizového řízení a veřejné správy. Dále byla podrobně rozebrána právní opora ochrany měkkých cílů zahrnující ústavní záruky práv a svobod, zákony o ochraně osobních údajů, kybernetické bezpečnosti a správě informačních systémů veřejné správy doplněné o bezpečnostní strategii státu, která reflektuje proměnlivé mezinárodní bezpečnostní prostředí a vymezuje nástroje ochrany veřejných institucí. Třetí část se věnovala metodám analýzy rizik, kde byly použity metody PNH a KARS jako hlavní nástroj praktické části práce díky své schopnosti zohlednit souvztažnost rizik, pracovat s kvalitativními údaji a vizualizovat výsledky v podobě matice. Součástí teoretického rámce jsou rovněž strategické a metodické dokumenty Ministerstva vnitra ČR, zejména Koncepce ochrany měkkých cílů a navazující metodiky, které stanovují zásady plánování bezpečnosti, bezpečnostního cyklu v sedmi krocích a důraz na koordinaci, prevenci, školení i spolupráci s bezpečnostními složkami. Všechny uvedené aspekty dohromady tvoří pevný základ pro navazující praktickou část diplomové práce, jejímž cílem je provést konkrétní analýzu rizik v prostředí veřejné instituce.

## **II PRAKTICKÁ ČÁST**

## 5 CHARAKTERISTIKA MĚKKÉHO CÍLE

S ohledem na charakter diplomové práce, která se zaměřuje na problematiku ochrany měkkých cílů, a s přihlédnutím k citlivosti analyzovaného objektu, není z bezpečnostních důvodů v této práci možné uvést konkrétní název ani přesné umístění zkoumané instituce. Tato míra anonymizace je nezbytná nejen z důvodu ochrany samotného objektu, ale také kvůli ochraně bezpečnostních zájmů, informací a postupů, které by mohly být v rámci zveřejnění této práce zneužity. S ohledem na zásady bezpečnostního managementu nejsou identifikační údaje zmíněny, zatímco ostatní části analýzy si zachovávají věcný charakter, popisnou formu a jsou podloženy odbornými poznatky.

Obecně lze říct, že se jedná o veřejnou státní instituci, která vykonává činnost v působnosti okresní státní správy. Jejím primárním úkolem je poskytování veřejných služeb občanům, zejména v oblastech evidence, správního řízení a poradenství. Tato instituce má každodenní přímý kontakt s občany a zajišťuje klíčové agendy, které mají přímý dopad na běžné fungování jednotlivců i celých domácností. Typicky jde např. o činnosti spojené s evidencí motorových vozidel, vydáváním úředních dokumentů a průkazů, vedením správních řízení v oblasti dopravy a další administrativní úkony, které vyžadují osobní účast klienta a interakci s úředníkem.

Výše popsaný charakter provozu, tedy vysoká míra veřejné přístupnosti, každodenní provoz v úředních hodinách a zaměření na poskytování služeb široké veřejnosti, přispívá k tomu, že danou instituci lze z hlediska bezpečnostní terminologie považovat za tzv. měkký cíl. Měkké cíle, jak již bylo uvedeno v teoretické části této práce, jsou definovány jako objekty, které jsou snadno dosažitelné, zpravidla volně přístupné, bez výrazného fyzického zabezpečení a zároveň se v nich vyskytuje vyšší koncentrace osob. Typickým rysem těchto objektů je skutečnost, že nejsou chráněny na rozdíl od kritické infrastruktury nebo významná místa z hlediska obrany státu. Přesto mohou být potenciálním cílem násilných útoků, teroristických činů, nebo jiných krizových událostí s možnými závažnými dopady na lidské životy, zdraví ale i kontinuitu služeb.

I když tento konkrétní objekt formálně nespadá pod režim kritické infrastruktury podle krizového zákona, jeho faktické zasažení by mohlo mít značné škodlivé důsledky. Ty by se mohly projevit nejen narušením provozu samotné instituce, ale i ztrátou důvěry veřejnosti, dezorganizací státní správy na místní úrovni nebo v nejvíce závažném případě i ohrožení bezpečnosti klientů a zaměstnanců. Zkoumaná instituce tedy plní důležitou společenskou,

správní i legislativní roli. Její činnost je nedílnou součástí systému veřejné správy a představuje spojovací článek mezi státem a občany. Přesto však její zabezpečení zůstává na velmi základní úrovni, která neodpovídá současným bezpečnostním výzvám ani potenciálním rizikům spojeným s výskytem mimořádných událostí.

Při hlubší analýze je zřejmé, že celková zranitelnost objektu není způsobena pouze fyzickými nebo technickými nedostatky, ale je podmíněna také nízkou mírou bezpečnostního povědomí na straně zřizovatele instituce a taktéž je značně závislá na finančních prostředcích. Zřizovatelé často bezpečnostní hrozby podceňují, považují je za málo pravděpodobné nebo irelevantní, a proto nejsou přijímána žádná systematická preventivní opatření. Chybí pravidelné audity bezpečnosti, revize rizik nebo simulace krizových scénářů. Tento přístup však neodpovídá realitě současných bezpečnostních hrozeb, které se stále častěji zaměřují právě na veřejně přístupné a symbolicky významné cíle.

Vzhledem k tomu, že tato instituce zajišťuje každodenní kontakt s vyššími desítkami až stovkami osob a že její prostorová i provozní struktura vykazuje značnou otevřenost, existuje reálné riziko incidentu, ať už úmyslného (např. násilný útok, vandalismus), nebo neúmyslného (např. panika při falešném poplachu, technická havárie). Z pohledu zaměření této diplomové práce lze proto tento objekt považovat za vhodný a reprezentativní modelový příklad měkkého cíle v oblasti veřejné správy, jehož analýza přináší cenné poznatky pro návrh opatření směřujících ke zvýšení jeho bezpečnostní odolnosti.

## 5.1 Veřejně přístupné údaje

Při popisu vybrané instituce byly použity veřejně přístupné údaje o ní, dále o prostředí, ve kterém se zájmová instituce nachází a o protiprávních deliktech, jenž byly v této souvislosti spáchány. Jednotlivá data o charakteru prostředí a jeho případné závadnosti byla získána především z mapy kriminality.

Data z mapy kriminality byla získána za období přibližně šesti předchozích let, tedy z období, kdy vedoucí zkoumaného odboru zastával svou funkci. Konkrétně se jednalo o časové rozměnění od 1. 1. 2019 do 30. 4. 2025. Je nezbytné ještě zmínit, že následující údaje představují oblast v okolí samotného objektu v celé působnosti okresního města. Za uvedené období bylo v této části zaznamenáno celkem 679 protiprávních jednání. Z toho se 76 případů týkalo trestných činů v různých oblastech, jako jsou násilná trestná činnost, požáry a výbuchy, krádeže vloupáním, jiné krádeže, podvody, jiná majetková trestná činnost,

obecně nebezpečné trestné činy, dopravní nehody, toxikomanie, zbraně a extremismus. Z celkových 76 trestných činů se 7 skutků týkalo násilné trestné činnosti, v oblasti požárů a výbuchů nebyl zaznamenán žádný případ. V uvedeném období došlo ke 21 krádežím (včetně krádeží vloupáním), 8 podvodům a 18 dalším majetkovým trestným činům (např. trestné činy proti veřejnému zájmu). Celkem 6 trestných činů bylo zařazeno do kategorie obecně nebezpečných. Došlo také ke 2 dopravním nehodám a k 24 případům souvisejících s toxikomanií. Nebyl zde zaznamenán žádný trestný čin v oblasti zbraní (střelné, chladné či výbušniny). Evidován byl jeden případ extremismu, do kterého spadá i sprejersství. Většinu zdokumentovaných událostí představují přestupky, celkem 603 případů. Do této kategorie spadají přestupky proti majetku, proti veřejnému pořádku a občanskému soužití, přestupky na úseku ochrany před alkoholismem a toxikomanií, dále na úseku Bezpečnosti silničního provozu a silničního hospodářství. Patří sem i další přestupky, např. na úseku střeliva, používání výbušnin, obrany České republiky, zákona o pobytu cizinců a další. [50], [9]

Součástí veřejně přístupných údajů bylo také zjištění dalších informací o okolí zájmového objektu v případě vzniku krizové situace. Nejbližší sídlo Policie České republiky se nachází ve vzdálenosti přibližně 1,6 km, což odpovídá zhruba 4 minutám jízdy autem. Oproti tomu nejbližší sídlo městské policie (dále také „MP“) je vzdáleno méně než jeden kilometr, s orientační dojezdovou dobou přibližně 2 minuty. Výjezdové stanoviště zdravotnické záchranné služby spolu s nemocnicí se nachází necelých 200 metrů od zájmového objektu, což odpovídá přibližnému dojezdovému času 30 sekund. Hasičský záchranný sbor je rovněž situován poblíž, konkrétně ve vzdálenosti necelého jednoho kilometru a dojezdová doba činí asi 2 minuty. Nejdůležitější záchranné složky jsou tedy v blízkém okolí, což je ve prospěch sledovaného objektu. Je však nutné zdůraznit, že výše uvedené časy jsou pouze orientační a mohou se lišit v závislosti na okolnostech, jako je např. hustota provozu nebo momentální připravenost jednotlivých složek. Ve vzdálenosti zhruba 10 kilometrů se ve vedlejším městě nachází neveřejné mezinárodní letiště.

Tato zjištění hodnotím velmi pozitivně, neboť ukazují na strategické rozmístění složek integrovaného záchranného systému v daném ORP. Uvedené rozmístění a krátké dojezdové časy mohou působit odstrašujícím dojmem na potenciálního útočníka, neboť si může být vědom rychlého příjezdu zasahujících složek, což snižuje prostor pro napáchání závažnějších škod. Vlakové nádraží, jenž je považováno za rizikový faktor, se nachází ve vzdálenosti zhruba 600 metrů. Vozidlem lze odtud k zájmovému objektu dojet ve velmi krátkém čase, avšak větší riziko spatřuji v možnosti pěšího přesunu. Od nádraží se lze

k objektu dostat zhruba za 5 minut, a to přímou cestou přes železniční trať. Tato snadná dostupnost zvyšuje pravděpodobnost nepředvídaného a rychlého útoku.

Pátá kapitola se zabývá analýzou anonymizované veřejné instituce, která byla zvolena jako modelový příklad tzv. měkkého cíle. Instituce působí v rámci okresní státní správy a denně zajišťuje služby veřejnosti, přičemž charakter její činnosti, jako je vysoká návštěvnost, veřejná přístupnost a administrativní funkce, zvyšuje její zranitelnost vůči různým druhům bezpečnostních hrozeb. Přestože není klasifikována jako kritická infrastruktura, její narušení by mohlo mít závažné důsledky pro veřejnost i správní chod regionu. Veřejně dostupná data z mapy kriminality ukazují, že v bezprostředním okolí objektu došlo v posledních šesti letech ke 679 protiprávním jednáním, z nichž 76 představovalo trestné činy, včetně násilné trestné činnosti, krádeží, podvodů a případů toxikomanie. Převážnou část tvořily přestupky. Pozitivně byla hodnocena blízkost složek integrovaného záchranného systému, které mají velmi krátké dojezdové časy. To přispívá ke zvýšení bezpečnostní odolnosti objektu. Naopak za rizikový faktor byla označena blízkost vlakového nádraží, které umožňuje rychlý a nenápadný přístup k objektu. Celkově kapitola poukazuje na zranitelnost institucí tohoto typu a zdůrazňuje potřebu systematického a promyšleného přístupu k jejich ochraně v rámci moderního bezpečnostního managementu.

## 6 ANALÝZA RIZIK

Předposlední kapitola představuje jeden z klíčových pilířů celé diplomové práce, jelikož obsahuje podrobnou analýzu hrozeb a rizik vztahujících se ke konkrétní kategorii měkkých cílů. Měkké cíle, tedy objekty a místa s omezenou mírou zabezpečení a vysokou koncentrací osob, představují atraktivní potenciální cíle různých typů útoků, zejména v kontextu současných bezpečnostních hrozeb. Z tohoto důvodu je důkladné prozkoumání možných rizik a identifikace konkrétních hrozeb zásadní pro pochopení jejich zranitelnosti a pro návrh efektivních opatření na jejich ochranu. [51]

Analýza hrozeb a rizik je v této části práce zpracována v co nejširší možné míře a zahrnuje všechna rizika, která mohou danému objektu hrozit. Hlavní důraz je kladen na oblast měkkých cílů. Cílem je rovněž popsat jednotlivé typy hrozeb, které je mohou ohrozit. Zvláštní pozornost je věnována identifikaci vnitřních i vnějších faktorů, které mohou ovlivnit úroveň rizika, a také dynamice, s jakou se tyto faktory mohou v čase měnit.

Pro samotné zpracování analýzy byla zvolena kvalitativní metoda hodnocení rizik, která umožňuje pracovat s daty i v případě, že nejsou k dispozici přesné číselné hodnoty. V rámci této metodiky byla konkrétně využita metoda KARS, zaměřená nejen na identifikaci a hodnocení rizik, ale i na vzájemné souvislosti mezi jednotlivými hrozbami a jejich možnými dopady. Tato metoda poskytuje ucelený a systematický přístup k hodnocení rizik, jenž zohledňuje komplexnost problematiky měkkých cílů a umožňuje navrhnout adekvátní opatření ke snížení zjištěných rizik.

Měkké cíle jsou obecně charakterizovány nízkou úrovní zabezpečení, otevřeností vůči veřejnosti a vysokou koncentrací osob. Dopravní úřad tyto charakteristiky zcela naplňuje, a proto je nezbytné identifikovat potenciální hrozby a rizika, která by mohla ohrozit jeho fungování, bezpečnost zaměstnanců, klientů, majetku i dat.

### 6.1 Identifikace aktiv zájmového objektu

Pro efektivní vyhodnocení rizik a zajištění bezpečnosti je nezbytné definovat aktiva, která jsou pro chod vybrané státní instituce zásadní. Tato aktiva představují hodnoty, jejichž ohrožení by mohlo vést k omezení činnosti úřadu, poškození zdraví osob, úniku citlivých informací či narušení důvěry veřejnosti. Aktiva lze členit do následujících kategorií:

**Lidská aktiva** jsou ta nejdůležitější. Sem patří samotní zaměstnanci úřadu, včetně referentů a vedoucích pracovníků. Dále se jedná o klíčové osoby, jako jsou vedoucí odboru,

správci informačních systémů nebo hlavní metodici, jejichž nepřítomnost by mohla ohrozit plynulý chod agend. Významná je také odborná znalostní báze, dovednosti a kompetence personálu, které určují jejich schopnost reagovat na mimořádné situace. V této kategorii je třeba zohlednit rovněž psychickou odolnost pracovníků a kvalitu mezilidských vztahů a sociálního klimatu na pracovišti.

**Fyzická aktiva** představují hmotné prostředky nezbytné pro výkon agend úřadu. Zahrnují především budovu a jednotlivá pracoviště. Nedílnou součástí je kancelářské vybavení, jako jsou stoly, židle, regály či skříně, dále pak technické vybavení, například počítače, tiskárny, skenery a výtah. Významná jsou také pokladní místa, přepážky, sklep, vstupní prostory a další zázemí určené pro veřejnost. Specifickými prvky jsou archivy, spisovny a další fyzická úložiště důležitých dokumentů. Do této skupiny spadají rovněž ochranné pracovní prostředky sloužící k zajištění bezpečnosti personálu i klientů.

**Informační aktiva** zahrnují systémy a informace, které úřad spravuje nebo vytváří. Patří sem zejména informační systémy sloužící k vedení registru řidičů, vozidel, evidence obyvatel a dalších agend. Dále sem spadají veškeré elektronické a listinné dokumentace, databáze obsahující osobní údaje občanů, přístupové údaje, hesla a oprávnění k těmto systémům. Z hlediska provozní bezpečnosti mají význam i zálohovací systémy a fyzická datová úložiště. V neposlední řadě je nutno zohlednit interní předpisy, směrnice a bezpečnostní protokoly, které upravují nakládání s informacemi.

**Technologická a infrastrukturní aktiva** jsou nezbytná pro chod úřadu. Zahrnují elektrické rozvody a napájení budov, telekomunikační infrastrukturu, telefonní a internetové připojení, serverové jednotky a síťové prvky. Významná jsou rovněž zařízení pro regulaci vnitřního prostředí, jako jsou klimatizační, vytápěcí a ventilační systémy. V případě krizových situací nabývá na významu dostupnost záložního napájení. Dále sem patří přístupové systémy včetně zámků a elektronických čipů.

**Organizační a procesní aktiva** tvoří soubor pravidel a postupů, které určují chod jednotlivých agend. Mezi ně patří pracovní a rozhodovací postupy, standardizované procesy, evakuační plány a krizové scénáře. Významné jsou také komunikační kanály pro vnitřní i vnější komunikaci, včetně možnosti rychlého předávání informací během mimořádných událostí. Dále se jedná o spolupráci s externími partnery, například dodavateli IT služeb, úklidových služeb nebo bezpečnostních agentur. V rámci této kategorie lze zahrnout také dohody o zajištění kontinuity provozu, jako jsou záložní pracoviště nebo smluvní ujednání o externí podpoře.

**Právní a reputační aktiva** se vztahují k právní odpovědnosti úřadu a jeho postavení na veřejnosti. Zahrnují zejména právní závazky vyplývající z platné legislativy, např. zákona o ochraně osobních údajů. Významné je také postavení úřadu jako veřejné instituce a důvěra, kterou mu občané přisuzují. Mezi klíčové prvky této kategorie patří schopnost úřadu komunikovat s veřejností, zachovat transparentnost a zvládnout krizové situace tak, aby nedošlo k poškození jeho reputace.

## 6.2 Katalog hrozeb

Identifikace rizik představuje klíčový krok v procesu řízení rizik, jehož cílem je systematicky rozpoznat potenciální hrozby, které by mohly negativně ovlivnit aktiva zájmového objektu či omezit jeho projekty, organizační strukturu nebo kontinuitu provozu. V této fázi je důležité nejen zaznamenat existující hrozby, ale také odhalit možná skrytá nebo nepředvídatelná rizika, která by se mohla v budoucnu projevit. Pro účely této práce byly hrozby rozděleny do následujících skupin, přičemž v každé skupině jsou uvedena i konkrétní rizika.

### **Fyzické hrozby:**

- fyzický útok jednotlivce nebo skupiny – úmyslné násilí páchané osobou/osobami z řad veřejnosti,
- ozbrojený útok – aktivní útočník s palnou zbraní nebo jiným nebezpečným nástrojem,
- teroristický útok – koordinovaný útok s cílem vyvolat paniku nebo způsobit škody na zdraví či majetku,
- krádež vybavení nebo dokumentů – krádež počítače, úředních tiskopisů, registračních značek,
- sabotáž – úmyslné narušení provozu ze strany vnitřní nebo vnější osoby,
- žhářství – úmyslné založení požáru v objektu úřadu,
- vandalismus – poškození majetku (rozbití oken, sprejerství nebo ničení nábytku).

### **Hrozby provozní, organizační a sociální nedostatky:**

- přetížení kapacity – vysoký počet klientů vede k zahlcení prostor, ztrátě přehledu a zvýšeným bezpečnostním rizikům,

- zastaralé nebo nefunkční bezpečnostní vybavení – např. nefunkční kamery, zamykací systémy, detektory,
- nezvládnutá evakuace – chyby v průběhu evakuace (zablokované únikové východy, absence koordinace),
- nejasná kompetenční struktura při krizích – chybějící určení rolí a odpovědnosti při mimořádné situaci,
- nedostatečně vyškolený personál – zaměstnanci nejsou připraveni na krizové situace a neznají své úlohy,
- chybná evidence přístupů a návštěv,
- selhání bezpečnostních protokolů – neexistence nebo nefunkčnost vnitřních postupů při krizových situacích, neschopnost reagovat,
- vniknutí nepovolané osoby – neoprávněný přístup do neveřejných zón úřadu.
- nedostatek personálu – způsobený nemocí, odchodem nebo nedostatečnými kapacitami,
- nedostatečné materiální nebo technické zázemí – chybějící osobní ochranné pracovní prostředky, IT technika,
- chybná krizová komunikace – neschopnost podat jasné a srozumitelné informace veřejnosti během mimořádné situace.

**Hrozby informační a kybernetická:**

- kybernetický útok (malware, ransomware) – napadení systému s cílem ohromit provoz úřadu nebo získat citlivá data (hesla, neoprávněný přístup),
- nezabezpečená síťová infrastruktura – možnost průniku do systému kvůli technickým slabínám (neaktualizovaný software, Wi-Fi),
- nelegální připojení k interním sítím (USB, Wi-Fi) – obcházení zabezpečení zevnitř,
- ztráta nebo poškození dat – hardwarová nebo softwarová chyba bez zálohování datových uložišť.
- zneužití pracovního zařízení k osobním účelům – nelegální stahování dat nebo porušení politiky bezpečnosti.

**Hrozby vnějšího prostředí a přirozených jevů:**

- požár technického původu – např. zkrat v elektroinstalaci, porucha elektrospotřebiče,
- výpadek elektrické energie – omezení provozu a funkčnosti IT systémů,
- znečištění vody nebo zdroje vody v objektu – poruchy hygienických zařízení, zdravotní rizika,
- dlouhodobé stavební práce v okolí – vibrace, hluk, omezení přístupnosti nebo evakuace,
- výpadek dodavatelských služeb – selhání externích dodavatelů (např. IT správy, úklidu, bezpečnostní agentury).

**Hrozby sociální a psychologická:**

- panika klientů – hromadný spontánní útěk vyvolaný ohrožením nebo falešným poplachem,
- psychický nátlak nebo vyhoření personálu – chronický stres pracovníků, práce s obtížnými klienty, syndrom vyhoření,
- sebepoškození klienta v prostorách úřadu – demonstrativní čin s vážným psychologickým dopadem na okolí,
- neoprávněné natáčení či šíření dezinformací – šíření videí s citlivým obsahem z úřadu bez souhlasu nebo zkreslování informací.

**Hrozby legislativní a reputační:**

- ztráta důvěry veřejnosti – následek špatného zvládnutí krize, úniku informací nebo medializace incidentu,
- chyby v řízeních vedoucí k právním sporům – administrativní pochybení s dopadem na prezentaci úřadu,
- neetické chování zaměstnanců (korupce, střet zájmů) – ztráta důvěry a možný právní postih,
- neúspěšné veřejné vystoupení představitele úřadu – neprofesionální komunikace, která může zhoršit vnímání instituce,

- únik osobních údajů – nedbalost nebo úmyslné zveřejnění citlivých informací, např. evidence vozidel, špatné zabezpečení databáze.

#### **Živelní pohromy a přírodní jevy:**

- vichřice nebo tornádo – poškození střechy, fasády nebo oken budovy, ohrožení osob vně i uvnitř,
- výskyt škůdců v objektu (hlodavci, hmyz) – ohrožení hygieny a technické infrastruktury,
- sopečný popel – dopad na dopravu, kvalitu ovzduší,
- povodně nebo přívalové deště – zatopení objektu úřadu, omezení dostupnosti, poškození dokumentace nebo archivu,
- extrémní mrazy nebo námraza – neprůchodnost přístupových cest, zvýšené riziko úrazů,
- extrémní vedra a sucha – přetížení techniky, snížení pracovní výkonnosti, riziko požáru,
- dlouhodobý déšť a blesky – riziko úderu blesku do objektu, výpadky napájení a IT systémů,
- sesuvy půdy, propady, zemětřesení – ohrožení statiky budovy v případě nestabilního terénu, drobné otřesy, které mohou poškodit konstrukci nebo IT zařízení,
- znečištění ovzduší (inverze, prach) – např. inverze nebo prach, který má vliv na zdraví klientů a pracovníků, zhoršené mikroklima.

#### **Epidemiologické a biologické hrozby:**

- epidemie nebo pandemie – omezení provozu, uzavření úřadu, práce na dálku, personální výpadky,
- biologická kontaminace prostor – např. při přenosu infekcí kontaktem s dokumenty, předměty nebo osobami.
- nákaza škůdci – nemoc přenášená hmyzem.

**Průmyslové a dopravní havárie v okolí:**

- dopravní havárie s únikem toxických látek – ohrožení personálu a klientů chemickými látkami (např. havárie cisterny),
- zácpa nebo omezení přístupu k úřadu kvůli dopravnímu omezení – omezení docházky personálu a dostupnosti služeb,
- výbuch v blízkosti úřadu – např. v průmyslové zóně, trafostanici (tlaková vlna, poranění, panika),
- hromadná dopravní nehoda – způsobující blokaci přístupových cest k úřadu (zásahy IZS, evakuace),
- pád letadla – poškození/zničení budovy, omezení provozu úřadu.

**Technická selhání a infrastruktura:**

- destrukce stavebních prvků – úmyslné či nahodilé poškození stavebních prvků např. kolaps stropní konstrukce, pád regálů s dokumentací,
- výpadek telekomunikačních spojení – nefunkční telefon, datové připojení, nemožnost komunikace s veřejností,
- zničení důležitých dokumentů kvůli špatnému uskladnění – např. vlhkost, plísň v archivu,
- mechanické poškození zařízení – způsobené opotřebením nebo chybou obsluhy.

Posledním rozdělením jsou **hrozby vyšší moci a globálních vlivů** k nimž např. patří:

- politické změny – ovlivnění financování nebo legislativních rámců fungování úřadu,
- migrační vlna – zvýšený počet žadatelů, jazykové a bezpečnostní bariéry,
- náhlý výpadek klíčových osob – ovlivnění chodu agend kvůli odchodu nebo nepřítomnosti vedoucí osoby či IT správce.

### **6.3 Aplikace metody PNH**

K aplikaci metody PNH byl využit výše uvedený katalog hrozeb a tabulky (Tabulka 2), (Tabulka 3) a (Tabulka 4), které jsou uvedené v teoretické části práce. Souhrnný přehled aplikace této metody je uveden v následující tabulce (Tabulka 10).

Tabulka 10 Aplikovaná metoda PNH

|    | Hrozba                                              | PNH |   |   | R  |
|----|-----------------------------------------------------|-----|---|---|----|
|    |                                                     | P   | N | H |    |
| 1  | fyzický útok jednotlivce nebo skupiny               | 3   | 3 | 2 | 18 |
| 2  | ozbrojený útok                                      | 2   | 3 | 3 | 18 |
| 3  | teroristický útok                                   | 1   | 4 | 4 | 16 |
| 4  | krádež vybavení nebo dokumentů                      | 3   | 3 | 2 | 18 |
| 5  | sabotáž                                             | 2   | 3 | 3 | 18 |
| 6  | žhářství                                            | 1   | 4 | 4 | 16 |
| 7  | vandalismus                                         | 2   | 3 | 3 | 18 |
| 8  | přetížení kapacity                                  | 4   | 2 | 2 | 16 |
| 9  | zastaralé nebo nefunkční bezpečnostní vybavení      | 2   | 2 | 3 | 12 |
| 10 | nezvládnutá evakuace                                | 3   | 2 | 3 | 18 |
| 11 | nejasná kompetenční struktura při krizích           | 1   | 2 | 4 | 8  |
| 12 | nedostatečně vyškolený personál                     | 2   | 3 | 3 | 18 |
| 13 | chybná evidence přístupů a návštěv                  | 2   | 3 | 2 | 12 |
| 14 | selhání bezpečnostních protokolů                    | 2   | 3 | 4 | 24 |
| 15 | vniknutí nepovolané osoby                           | 3   | 4 | 3 | 36 |
| 16 | nedostatek personálu                                | 1   | 4 | 4 | 16 |
| 17 | nedostatečné materiální nebo technické zázemí       | 3   | 3 | 2 | 18 |
| 18 | chybná krizová komunikace                           | 2   | 3 | 3 | 18 |
| 19 | kybernetický útok (malware, ransomware)             | 1   | 4 | 4 | 16 |
| 20 | nezabezpečená síťová infrastruktura                 | 1   | 4 | 4 | 16 |
| 21 | nelegální připojení k interním sítím (USB, Wi-Fi)   | 4   | 1 | 3 | 12 |
| 22 | ztráta nebo poškození dat                           | 2   | 2 | 4 | 16 |
| 23 | zneužití pracovního zařízení k osobním účelům       | 4   | 3 | 1 | 12 |
| 24 | požár technického původu                            | 1   | 4 | 4 | 16 |
| 25 | výpadek elektrické energie                          | 3   | 2 | 3 | 18 |
| 26 | znečištění vody nebo zdroje vody v objektu          | 1   | 3 | 4 | 12 |
| 27 | dlouhodobé stavební práce v okolí                   | 3   | 1 | 1 | 3  |
| 28 | výpadek dodavatelských služeb                       | 3   | 2 | 3 | 18 |
| 29 | panika klientů                                      | 2   | 3 | 3 | 18 |
| 30 | psychický nátlak nebo vyhoření personálu            | 2   | 2 | 4 | 16 |
| 31 | sebepoškození klienta v prostorách úřadu            | 1   | 3 | 2 | 6  |
| 32 | neoprávněné natáčení či šíření dezinformací         | 2   | 4 | 3 | 24 |
| 33 | ztráta důvěry veřejnosti                            | 1   | 4 | 4 | 16 |
| 34 | chyby v řízeních vedoucí k právním sporům           | 2   | 3 | 2 | 12 |
| 35 | neetické chování zaměstnanců (korupce, střet zájmů) | 1   | 3 | 3 | 9  |
| 36 | neúspěšné veřejné vystoupení představitele úřadu    | 2   | 2 | 2 | 8  |
| 37 | únik osobních údajů                                 | 2   | 3 | 3 | 0  |
| 38 | vichřice nebo tornádo                               | 1   | 4 | 4 | 0  |
| 39 | výskyt škůdců v objektu (hlodavci, hmyz)            | 1   | 1 | 1 | 1  |
| 40 | sopečný popel                                       | 1   | 3 | 3 | 9  |
| 41 | povodně nebo přívalové deště                        | 2   | 2 | 4 | 16 |

|    |                                                              |   |   |   |    |
|----|--------------------------------------------------------------|---|---|---|----|
| 42 | extrémní mrazy nebo námraza                                  | 2 | 2 | 4 | 16 |
| 43 | extrémní vedra a sucha                                       | 2 | 2 | 4 | 16 |
| 44 | dlouhodobý déšť a blesky                                     | 2 | 2 | 4 | 16 |
| 45 | sesuvy půdy, propady, zemětřesení                            | 2 | 2 | 4 | 16 |
| 46 | znečištění ovzduší (inverze, prach)                          | 3 | 2 | 4 | 24 |
| 47 | epidemie nebo pandemie                                       | 2 | 2 | 4 | 16 |
| 48 | biologická kontaminace prostor                               | 2 | 2 | 4 | 16 |
| 49 | nákaza škůdci                                                | 1 | 2 | 1 | 2  |
| 50 | dopravní havárie s únikem toxických látek                    | 1 | 4 | 4 | 16 |
| 51 | zácpa nebo omezení přístupu k úřadu kvůli dopravnímu omezení | 3 | 1 | 1 | 3  |
| 52 | výbuch v blízkosti úřadu                                     | 1 | 4 | 4 | 16 |
| 53 | hromadná dopravní nehoda                                     | 3 | 3 | 2 | 18 |
| 54 | pád letadla                                                  | 1 | 3 | 4 | 12 |
| 55 | destrukce stavebních prvků                                   | 1 | 4 | 4 | 16 |
| 56 | výpadek telekomunikačních spojení                            | 2 | 3 | 4 | 24 |
| 57 | zničení důležitých dokumentů kvůli špatnému uskladnění       | 1 | 3 | 3 | 9  |
| 58 | mechanické poškození zařízení                                | 2 | 3 | 3 | 18 |
| 59 | politické změny                                              | 2 | 2 | 4 | 16 |
| 60 | migrační vlna                                                | 2 | 3 | 3 | 18 |
| 61 | náhlý výpadek klíčových osob                                 | 3 | 3 | 2 | 18 |

(zdroj: vlastní)

K vyhodnocení výše uvedené tabulky byla použita poupravená tabulka (Tabulka 5), která vypadá následovně (Tabulka 11).

Tabulka 11 Poupravená škála míry rizika

| Úroveň   | Hodnota | Popis rizika                                                                                                 |
|----------|---------|--------------------------------------------------------------------------------------------------------------|
| Nízká    | 1–12    | Riziko je považováno za přijatelné.                                                                          |
| Střední  | 13–23   | Riziko lze snížit méně náročnými opatřeními, nebo pokud jsou opatření složitější, zůstává riziko přijatelné. |
| Vysoká   | 24–48   | Riziko je dlouhodobě neakceptovatelné a je nutné zahájit systematické kroky k jeho eliminaci.                |
| Kritická | 49–64   | Riziko je neakceptovatelné a je nutné okamžitě zahájit systematické kroky k jeho eliminaci.                  |

(zdroj: vlastní)

Po vyhodnocení aplikované metody PNH (Tabulka 10) byla pro další účely práce vybrána rizika spadající do úrovně **střední**, **vysoká** a **kritická**. Důvodem, proč nebyla zvolena rizika v úrovni **nízká** je skutečnost, že jejich hodnota se nachází na přijatelné úrovni. Vybraná rizika budou následně využita v rámci metody KARS, tedy v následující kapitole práce.

## 6.4 Aplikace metody KARS

Metoda KARS je založena na identifikaci hrozeb, které jsou následně klasifikovány, kvantifikovány a posuzovány pomocí párového porovnávání. Dále je popsán jednotlivý postup aplikace této metody.

Dalším krokem je vytvoření součtů souvztažnosti rizik. Pro lepší přehlednost je tento součet zpracován do dvou tabulek, které jsou uvedeny v příloze této práce a označeny jako příloha P I a P II. Jednotlivá rizika jsou uvedena ve sloupci i v řádku a všechna jsou očíslována od 1 do 48. Jak je již bylo zmíněno, z důvodu čitelnosti výsledků jsou tabulky rozděleny na dvě části a jsou očíslovány od 1–24 a 25–48.

Následně se pro jednotlivá rizika vypočítává koeficient aktivity, tedy  $K_{AR_i}$  a pasivity  $K_{PR_i}$ , podle rovnice (3) a (4). Níže je uveden příklad výpočtu těchto koeficientů pro konkrétní riziko, a to teroristický útok. Nejdříve je uvedený koeficient aktivity:

$$K_{AR_i} = \left( \frac{\sum R_i}{x - 1} \right) \cdot 100$$

$$K_{AR_i} = \left( \frac{34}{44 - 1} \right) \cdot 100$$

$$K_{AR_i} = \left( \frac{34}{43} \right) \cdot 100$$

$$K_{AR_i} = 79,07 \%$$

Následně koeficient pasivity:

$$K_{PR_i} = \left( \frac{\sum R_j}{x - 1} \right) \cdot 100$$

$$K_{PR_i} = \left( \frac{35}{44 - 1} \right) \cdot 100$$

$$K_{PR_i} = \left( \frac{35}{43} \right) \cdot 100$$

$$K_{PR_i} = 81,40 \%$$

Pro zápis výsledků se použije tabulka (Tabulka 9), která má po aplikaci výše uvedených vzorců následující podobu. Z důvodu přehlednosti jsou rizika rozdělena do čtyř tabulek.

První tabulka (Tabulka 12) určuje  $K_{AR_i}$  a  $K_{PR_i}$  pro rizika 1–11.

Tabulka 12 Koeficient aktivity a pasivity pro rizika 1–11

| Riziko        | 1     | 2     | 3     | 4     | 5     | 6     | 7     | 8     | 9     | 10    | 11    |
|---------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| $K_{ARi}$ (%) | 41,86 | 60,47 | 79,07 | 30,23 | 62,79 | 39,53 | 18,60 | 27,91 | 23,26 | 34,88 | 53,49 |
| $K_{ARi}$ (%) | 20,93 | 16,28 | 13,95 | 30,23 | 53,49 | 18,60 | 25,58 | 46,51 | 65,12 | 27,91 | 79,07 |

(zdroj: vlastní)

Tato tabulka (Tabulka 13) je pro koeficienty rizik 12–22.

Tabulka 13 Koeficient aktivity a pasivity pro rizika 12–22

| Riziko        | 12    | 13    | 14    | 15    | 16    | 17    | 18    | 19    | 20    | 21    | 22    |
|---------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| $K_{ARi}$ (%) | 51,16 | 27,91 | 25,58 | 32,56 | 32,56 | 25,58 | 20,93 | 34,88 | 34,88 | 27,91 | 20,93 |
| $K_{ARi}$ (%) | 51,16 | 32,56 | 69,77 | 81,40 | 23,26 | 32,56 | 55,81 | 37,21 | 55,81 | 62,79 | 72,09 |

(zdroj: vlastní)

Předposlední tabulka (Tabulka 14) určuje koeficienty pro rizika 23–33

Tabulka 14 Koeficient aktivity a pasivity pro rizika 23–33

| Riziko        | 23    | 24    | 25    | 26    | 27    | 28    | 29    | 30    | 31    | 32    | 33    |
|---------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| $K_{ARi}$ (%) | 39,53 | 20,93 | 25,58 | 32,56 | 51,16 | 48,84 | 32,56 | 37,21 | 32,56 | 44,19 | 30,23 |
| $K_{ARi}$ (%) | 58,14 | 32,56 | 41,86 | 39,53 | 0,00  | 4,65  | 0,00  | 0,00  | 6,98  | 13,95 | 37,21 |

(zdroj: vlastní)

Poslední tabulka (Tabulka 15) je pro rizika 34–44

Tabulka 15 Koeficient aktivity a pasivity pro rizika 34–44

| Riziko        | 34    | 35    | 36    | 37    | 38    | 39    | 40    | 41    | 42    | 43    | 44    |
|---------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| $K_{ARi}$ (%) | 32,56 | 30,23 | 37,21 | 44,19 | 20,93 | 46,51 | 30,23 | 32,56 | 44,19 | 20,93 | 39,53 |
| $K_{ARi}$ (%) | 11,63 | 37,21 | 25,58 | 30,23 | 27,91 | 23,26 | 55,81 | 48,84 | 32,56 | 20,93 | 58,14 |

(zdroj: vlastní)

Po vyhotovení výpočtů koeficientů aktivity ( $K_{ARi}$ ) a pasivity ( $K_{PRi}$ ) následuje jejich grafické znázornění. Předtím je však třeba vypočítat hodnoty os, na jejichž základě se graf sestavuje. Graf je rozdělen do čtyř oblastí pomocí os  $O_1$  a  $O_2$ , přičemž jednotlivé oblasti určují významnost rizik:

- **I. oblast** – primárně a sekundárně nebezpečná rizika,
- **II. oblast** – sekundárně nebezpečná rizika,

- **III. oblast** – primárně nebezpečná,
- **IV. oblast** – relativně bezpečná.

Výsledky jsou rozděleny tak, aby do první oblasti spadalo 80 % všech analyzovaných rizik. K tomuto rozdělení se použije pro výpočet  $O_1$  rovnice (5):

$$O_1 = K_{A_{max}} - \frac{K_{A_{max}} - K_{A_{min}}}{100} \cdot 80$$

$$O_1 = 79,07 - \frac{79,07 - 16,28}{100} \cdot 80$$

$$O_1 = 79,07 - \frac{62,79}{100} \cdot 80$$

$$O_1 = 28,84$$

Pro výpočet osy  $O_2$  se použije rovnice (6):

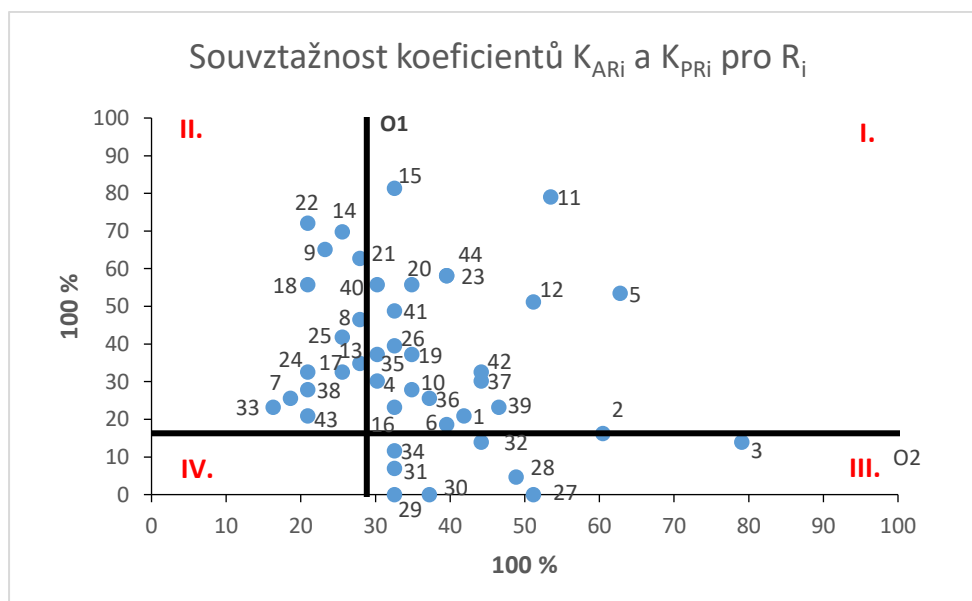
$$O_2 = K_{P_{max}} - \frac{K_{P_{max}} - K_{P_{min}}}{100} \cdot 80$$

$$O_2 = 81,40 - \frac{81,40 - 0}{100} \cdot 80$$

$$O_2 = 81,40 - \frac{81,40}{100} \cdot 80$$

$$O_2 = 16,28$$

Na základě těchto výpočtů byl sestaven graf. Ten je uveden níže (Obrázek 7)



Obrázek 7 Souvztažnost koeficientů  $K_{A_{Ri}}$  a  $K_{P_{Ri}}$  pro  $R_i$

(zdroj: vlastní)

Závěrečným krokem bylo zhodnocení analýzy rizik pomocí metody KARS. Výsledky ukazují, že analyzovaná rizika byla rozdělena pouze do tří oblastí, a to I., II. a III. Nejvíce rizik jich spadá do **I. oblasti**, která zahrnuje jak primárně, tak sekundárně nebezpečná rizika, konkrétně 22 případů. Do **II. oblasti**, odpovídající sekundárně nebezpečným rizikům, spadá 8 rizik. **III. oblast**, představující primárně nebezpečná rizika, obsahuje 14 rizik. Překvapivě nebylo žádné riziko zařazeno do **IV. oblasti**, tedy mezi relativně bezpečná.

**I. oblast** zahrnuje rizika označovaná jako primárně nebezpečná: fyzický útok jednotlivce/skupiny, ozbrojený útok, krádež vybavení nebo dokumentů, sabotáž, žhářství, nedostatečně vyškolený personál, selhání bezpečnostních protokolů, vniknutí nepovolané osoby, chybná krizová komunikace, kybernetický útok, požár technického původu, výpadek elektrické energie, psychický nátlak či vyhoření personálu, únik osobních údajů, biologická kontaminace prostor, dopravní havárie s únikem toxických látek, výbuch v blízkosti úřadu, destrukce stavebních prvků, výpadek telekomunikačních spojení, mechanické poškození zařízení, politické změny a náhlý výpadek klíčových osob.

**II. oblasti** zahrnuje rizika klasifikovaná jako sekundárně nebezpečná: teroristický útok, vichřice/tornádo, povodně/přívalové deště, extrémní mrazy/námraza, extrémní vedra a sucha, dlouhodobý déšť a blesky, sesuvy půdy, propady, zemětřesení, epidemie/pandemie.

**III. oblast** obsahuje primárně nebezpečná rizika jako: vandalismus, přetížení kapacity, nezvládnutá evakuace, nedostatek personálu, nedostatečné materiální nebo technické zázemí, nezabezpečená síťová infrastruktura, ztráta/poškození dat, výpadek dodavatelských služeb, panika klientů, neoprávněné natáčení nebo šíření dezinformací, ztráta důvěry veřejnosti, znečištění ovzduší, hromadná dopravní nehoda či migrační vlna.

Jak je již uvedeno výše, relativně bezpečná oblast, tedy **IV. oblast** neobsahuje žádné riziko.

Tato kapitola diplomové práce se zaměřuje na komplexní analýzu hrozeb a rizik, které se vztahují ke kategorii měkkých cílů, konkrétně k dopravnímu úřadu. Kapitola identifikuje tato místa jako potenciálně zranitelná z důvodu nízké úrovně zabezpečení, otevřenosti vůči veřejnosti a vysoké koncentrace osob. Cílem je určit míru ohrožení jednotlivých aktiv, která jsou klíčová pro chod úřadu. V rámci analýzy byla nejprve kategorizována aktiva úřadu, tedy lidská, fyzická, informační, technologická, organizační a reputační, a následně byl sestaven katalog potenciálních hrozeb, rozdělený do několika skupin podle jejich charakteru, například fyzické, provozní, kybernetické, přírodní, sociální, legislativní a další.

K hodnocení rizik byla použita metoda PNH, která pracuje s pravděpodobností výskytu, následky a schopností hrozbu detekovat. Výsledky byly rozděleny podle úrovně závažnosti do kategorií nízké, střední, vysoké a kritické. Pro další analýzu byla vybrána pouze rizika mimo nízkou kategorii. Následně byla využita metoda KARS, která pomocí párového porovnávání rizik stanovuje koeficient aktivity a pasivity jednotlivých hrozeb a zobrazuje je graficky ve čtyřech kvadrantech podle jejich významnosti. Výsledky ukazují, že většina rizik spadá do nejzávažnější oblasti, která zahrnuje jak primárně, tak sekundárně nebezpečné faktory. Mezi nejvýznamnější hrozby patří např. ozbrojený útok, žhářství, vniknutí nepovolané osoby, nedostatečně vyškolený personál, psychický nátlak na personál nebo biologická kontaminace. Z grafického rozdělení vyplývá, že žádné z analyzovaných rizik nebylo hodnoceno jako relativně bezpečné. Tato zjištění potvrzují nezbytnost důsledné bezpečnostní politiky a preventivních opatření na ochranu měkkých cílů ve veřejných institucích.

## 7 AKTUÁLNÍ BEZPEČNOSTNÍ STAV

Sedmá kapitola se zabývá shrnutím aktuálního bezpečnostního stavu zájmového objektu. Jeho analýza byla provedena formou rozboru veřejně přístupných údajů, dále prostřednictvím fyzické návštěvy objektu a získané podklady byly na závěr analyzovány použitím specifické metody analýzy rizik, kterou je metoda KARS.

### 7.1 Analýza aktuálního stavu zabezpečení

Analýza aktuálního bezpečnostního stavu zájmové instituce byla provedena formou fyzické obhlídky po předchozí dohodě s vedoucím odboru. Do objektu je možné vstoupit dvěma způsoby, a to buď skrze dvůr, kde se nachází parkoviště pro zaměstnance a návštěvníky, nebo hlavním vchodem. Je nutno uvést, že všechny níže uvedené fotografie jsou vlastní a byly pořízeny po předchozí dohodě s vedoucím odboru dané instituce.

Po vstupu ze dvora (Obrázek 8) se na pravé stěně nachází systém PZTS (Obrázek 9), který slouží k odkódování budovy, zejména při poplachu mimo pracovní dobu. V jeho blízkosti je také pohybové čidlo, jehož umístění není ideální, neboť snímač je nasměrován ke vstupním dveřím ze dvora. Toto umístění může být problematické kvůli vlivům počasí, které mohou způsobovat falešné poplachu. Naproti těmto dveřím se nachází další vstup, vedoucí do hlavní haly.



Obrázek 8 Vstup do objektu ze dvora

Jak již bylo uvedeno, v tomto prostoru (Obrázek 9) se nachází také PZTS od firmy Paradox.



a

Obrázek 9 PZTS u vstupu ze dvora

Na následujících obrázcích (Obrázek 10), (Obrázek 11) a (Obrázek 12) je zachyceno I. podlaží, tedy vstupní halu, do níž lze vstoupit jak hlavními vstupními dveřmi, tak ze dvora. Ve vstupní hale se nachází celkem 2 pohybové detektory, výtah a boční dveře do suterénu. Jedno z čidel je umístěno v prostoru hlavní haly a druhé se nachází hned za hlavními dveřmi (Obrázek 13) a (Obrázek 14). Na těchto snímcích je rovněž patrné schodiště vedoucí na II. podlaží a jeho chodbu



Obrázek 10 Vstupní hala z pohledu od dvora a schody do II. podlaží

Na obrázku (Obrázek 11) je zachycen panel, který určitým způsobem plní funkci EKV, avšak slouží pouze zaměstnancům k evidenci docházky.



Obrázek 11 Vstupní hala z pohledu od hlavních vstupních dveří

U dalšího obrázku (Obrázek 12) je možné vidět umístění výtahu ve vstupní hale. Dále jsou zde zachyceny boční dveře, které vedou do suterénu.



Obrázek 12 Výtah ve vstupní hale a dveře do suterénu

Jedno ze dvou pohybových čidel se nachází hned u dveří, které vedou k prostoru vstupu ze dvora (Obrázek 13). Tyto dveře jsou umístěny přímo naproti hlavnímu vchodu.



Obrázek 13 Dveře k prostoru ke vstupu od dvora a pohybové čidlo

Jak již bylo zmíněno, následující obrázek (Obrázek 14) zobrazuje pohybové čidlo nacházející se na I. podlaží v prostoru za hlavními dveřmi. Snímač tohoto čidla nesměřuje směrem ke dveřím, což nemůže vyvolat falešné poplachy vlivem působení venkovních podmínek.



Obrázek 14 Pohybové čidlo u hlavního vchodu

Na obrázcích (Obrázek 15), (Obrázek 16) a (Obrázek 17) je zachycena chodba ve II. podlaží u čekárny registru silnicích vozidel. Zde se nachází také výtah, jediné neuzamykatelné toalety pro veřejnost a schodiště do suterénu a vyšších pater.



Obrázek 15 Chodba II. podlaží

Na následujícím obrázku (Obrázek 16) je možné vidět výtah ve II. podlaží a hlavní schodiště zájmové budovy, které vede do vyšších podlaží nebo do suterénu. Stejně jako v ostatních podlažích je možné, že pachatel využije výtahu k rychlejšímu přesunu po budově. Případně jej zablokuje, aby jej zaměstnanci v případě útoku nemohli použít k úniku.



Obrázek 16 Výťah a hlavní schodiště na II. podlaží

Další obrázek (Obrázek 17) zachycuje jediné veřejné toalety v objektu, které nejsou uzamykatelné, ale pouze uzavřené. Z tohoto hlediska mohou toalety představovat riziko v podobě místa, kde se potenciální útočník může nachystat a nikdo jej nespátří.



Obrázek 17 Veřejné toalety na II. podlaží

Další tři obrázky (Obrázek 18), (Obrázek 19) a (Obrázek 20) zobrazují hlavní místnost II. podlaží objektu. Nachází se zde registr silničních vozidel, který slouží pro přihlašování, odhlašování, změny nebo schvalování technické způsobilosti vozidel. Na obrázcích je také zachycena čekárna a jediný pohybový senzor v této místnosti.



Obrázek 18 Vstupní dveře do čekárny registru silničních vozidel

Příštím obrázkem (Obrázek 19) zobrazuje část čekárny nacházející se na II. podlaží registru silničních vozidel. Je možné zde vidět i kameru, která je následně zobrazena na budoucím obrázku (Obrázek 21).



Obrázek 19 Čekárna registru silničních vozidel 1

Na dalším obrázku (Obrázek 20) je možné vidět druhou část čekárny a zároveň jediné pohybové čidlo nacházející se v této místnosti. Pozitivní je existence pohybového čidla, avšak by bylo lepší jej přemístit z důvodu možných falešných poplachů od trubek topení.



Obrázek 20 Čekárna registru silničních vozidel 2

Na dalším obrázku (Obrázek 21) je zaznamenána kamera značky Dahua, která je umístěna v této čekárně. Slouží výhradně pouze pro zaměstnance jako informační zdroj, kolik se nachází v čekárně lidí. Kamera má takové rozlišení, aby nebylo nutné zpracovávat osobní údaje.



Obrázek 21 Kamera v čekárně II. podlaží

Vstup do suterénu, kde se nachází technické místnosti, archiv a výtah, je přes hlavní schodiště z II. podlaží (Obrázek 22) není mechanicky nijak chráněn. Přístupu brání pouze plastový řetěz, který lze snadno překonat.



Obrázek 22 Vstup do suterénu zájmového objektu skrze hlavní schodiště

Alternativní vstup do suterénu je možný i bočními dveřmi z I. podlaží (Obrázek 23), které dle vyjádření vedoucího odboru nebývají zamykány a jsou pouze uzavřené.



Obrázek 23 Vstup do suterénu bočními dveřmi z I. podlaží

Obrázky (Obrázek 24), (Obrázek 25) a (Obrázek 26) zobrazují prostory samotného suterénu zájmového MC. Zde se nachází technické místnosti, archiv a výtah.



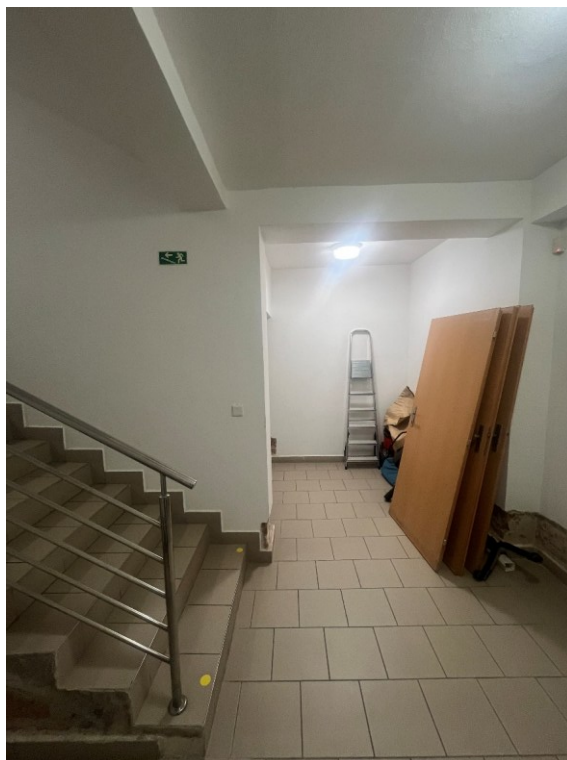
Obrázek 24 Sklep zájmového objektu 1

Následující obrázek (Obrázek 25) je pohled ze suterénu směrem na schody a technickou místnost.



Obrázek 25 Sklep zájmového objektu 2

Na obrázku (Obrázek 26) je zachycen prostor za schodištěm, kde není instalováno žádné pohybové čidlo. Tento prostor lze z hlediska bezpečnosti považovat za rizikový, neboť by zde potenciální útočník mohl setrvat nepovšimnut.



Obrázek 26 Sklep zájmového objektu 3

Na III. podlaží se nachází agenda evidence řidičských oprávnění konkrétně zkušební komisaři, registr řidičů a provozování autoškol. To je zachyceno na následujících fotografiích (Obrázek 27), (Obrázek 28) a (Obrázek 29).



Obrázek 27 Dveře ke zkušební místnosti, zkušebnímu komisaři a provozování autoškol

Následuje obrázek (Obrázek 28), kde je vyobrazena čekárna za těmito dveřmi, kde bývá v průběhu pracovních dní větší pohyb návštěvníků objektu.



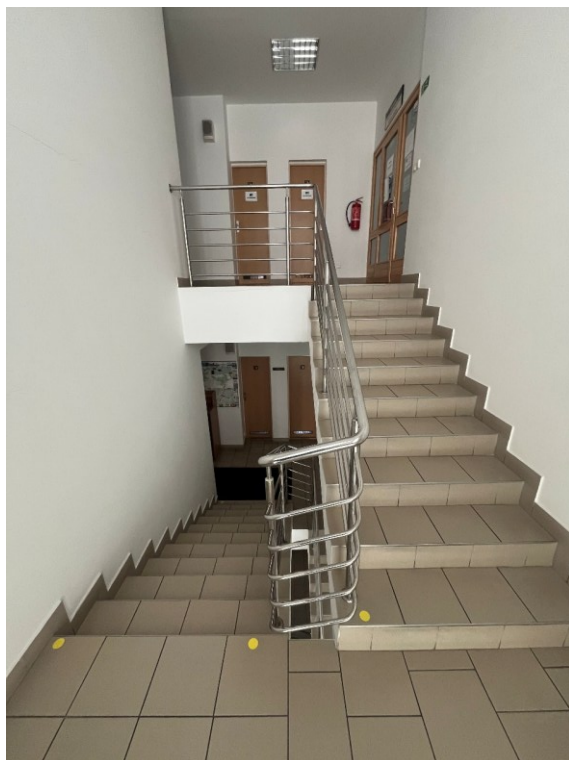
Obrázek 28 Chodba ke zkušební místnosti, zkušebnímu komisaři a provozování autoškol

Na posledním obrázku (Obrázek 29) z III. podlaží je čekárna registru řidičů. Ta se nachází na opačné straně od dveří ke zkušební místnosti, zkušebnímu komisaři a provozování autoškol.



Obrázek 29 Čekárna registru řidičů na III. podlaží

Z chodby z III. podlaží, kde se nachází i výtah se lze po schodech (Obrázek 30) dostat i do posledního podlaží, tedy IV.



Obrázek 30 Schodiště vedoucí z III. do IV. podlaží

V nejvyšším, tedy ve IV. podlaží se nachází odbor dopravních a správních agend, kde spadá projednávání dopravních přestupků, ale také je na tomto podlaží i vedoucí odboru. Následující obrázky (Obrázek 31) a (Obrázek 32) zobrazují společnou chodbu IV. podlaží. Zde se nachází, stejně jako ve III. podlaží, toalety určené pouze pro zaměstnance, výtah a 2 hasičské přístroje. Stejně jako ve všech předešlých patrech, i zde se nachází interní rozhlasové zařízení v případě nutné evakuace.



Obrázek 31 Chodba IV podlaží. a zaměstnanecké toalety

Na dalším obrázku (Obrázek 32), jak je již výše uvedeno, lze vidět umístění výtahu v tomto podlaží, kdy stejně jako i v ostatních podlažích výtah může představovat riziko.



Obrázek 32 Umístění výtahu na IV. podlaží

Z chodby na IV. podlaží je poté možné se dostat skrze dveře k čekárně na chodbě příslušící vedení odboru (Obrázek 33) nebo do prostor odboru dopravních a správních agend, kde se nachází jednotlivé kanceláře k šetření dopravních přestupků.



Obrázek 33 Čekárna vedení odboru

Nyní budou následovat obrázky (Obrázek 34), (Obrázek 35), na nichž vyobrazena místnost zástupce vedoucího odboru.



Obrázek 34 Místnost zástupce vedoucího odboru 1

Další obrázek (Obrázek 35) ukazuje jiný úhel pohledu dané místnosti s tím, že se jedná o místnost zástupce vedoucího odboru.



Obrázek 35 Místnost zástupce vedoucího odboru 2

Další obrázky (Obrázek 36), (Obrázek 37), (Obrázek 38) a (Obrázek 39) zobrazují přestupkové místnosti. Nutno zmínit, že se nejedná o všechny místnosti, neboť ty byly typově stejné a nemělo by význam je zde uvádět. Rozdíl byl pouze v tom, že se jednalo o zrcadlově obrácené místnosti.



Obrázek 36 Přestupková místnost č. 1

Ve dvou případech se v zájmovém objektu nacházela místnost, kde mají místo pracoviště dva pracovníci zároveň. Jednalo se o rohové místnosti a jednu z těchto místností lze vidět na následujících obrázcích (Obrázek 37) a (Obrázek 38).



Obrázek 37 Rohová místnost se dvěma pracovišti 1



Obrázek 38 Rohová místnost se dvěma pracovišti 2

Poslední přestupkovou místností z odboru dopravních a správních agend je možné vidět na následujícím obrázku (Obrázek 39).



Obrázek 39 Přestupková místnost č. 2

Na předposledním obrázku (Obrázek 40) je zachyceno tísňové tlačítko napojené na operační středisko městské policie dané ORP. Po stisknutí se tedy pošle signál na toto pracoviště, následně dojde k telefonickému ověření, zdali se nejedná o nedbalostní zmáčknutí či jde skutečně o stav nouze. Z důvodu zamezení možného útoku v případě nepotvrzení nouze ze strany objektu toto středisko vyšle k prověření dostupnou hlídku městské policie. Toto tlačítko je instalováno u vedoucího odboru a jeho zástupce i ve všech přestupkových místnostech.



Obrázek 40 Tísňové tlačítko

Poslední fotografie (Obrázek 41) zachycuje PZTS značky Jablotron, která je umístěna v kanceláři vedoucího odboru v zájmovém objektu sloužící k zakódování kanceláře.



Obrázek 41 PZTS v kanceláři vedoucího odboru

## 7.2 Vyhodnocení aktuálního stavu zabezpečení

Po fyzické obhlídce objektu byly zjištěny následující slabiny:

- volný přístup bez registrace nebo kontroly osob a volný pohyb návštěvníků po objektu,
- nízká míra technické ochrany,
- nedostatečná kontrola vstupních bodů,
- chybějící bezpečnostní dozor uvnitř objektu,
- nedostatečné školení zaměstnanců,
- výrazná provozní vytíženost.

Vstup do budovy je možný bez jakékoli kontroly. Během úředních hodin je provoz plně otevřen veřejnosti a přístup k jednotlivým kancelářím bývá minimálně kontrolován, zpravidla pouze namátkově zaměstnanci úřadu. V objektu chybí systematická forma ochrany, jako je recepce s ověřováním totožnosti, detekční brány či jiná aktivní opatření zaměřená na prevenci vnášení nebezpečných předmětů. Přístup je volný, bez nutnosti registrace nebo kontroly osob, a umožňuje volný pohyb po celém objektu. Návštěvníci tak mohou vstoupit do prostor bez předchozí identifikace a bez jakéhokoli omezení pohybu v rámci objektu. Tento stav výrazně zvyšuje riziko neoprávněného vniknutí, krádeže majetku nebo jiných bezpečnostních incidentů, zejména při vyšší koncentraci osob na jednom místě. Vzhledem k povaze objektu je tento přístup sice částečně pochopitelný a do určité míry akceptovatelný, avšak existují možnosti, jak volný pohyb návštěvníků efektivně omezit.

Technická ochrana je omezena pouze na pasivní prvky, jako jsou uzamykatelné kanceláře a mechanické zábrany (např. mříže). Chybí moderní bezpečnostní systémy, mezi něž patří elektronická kontrola přístupu nebo monitorování pohybu osob v objektu. Takový přístup výrazně omezuje schopnost efektivní detekce a reakce na případné incidenty v reálném čase. Ani prostory samotné, ani lidský faktor nejsou připraveny na potenciální krizové situace.

Kontrola vstupních bodů je rovněž nedostatečná. Objekt disponuje dvěma samostatnými přístupovými cestami, které nejsou trvale monitorovány ani obsluhou, ani elektronickými systémy. Ačkoli jsou tyto vstupy vybaveny základními technickými prvky, jako jsou pohybová čidla, jejich efekt je omezený. Tato čidla se aktivují až po zakódování celého objektu a pouze od určité doby. Výhodou je napojení poplachového systému na příslušné pracoviště Městské policie ORP. V objektu se trvale nenachází žádný bezpečnostní

dozor v podobě pracovníka ostrahy, ať už jde o zaměstnance přímo zřizovatele instituce, nebo zajištěného formou služby externí bezpečnostní agenty. Při mimořádné situaci, incidentu nebo narušení pořádku nelze zajistit okamžitou reakci odpovědné osoby s odpovídajícím výcvikem, čímž dochází ke zpoždění reakce.

Nedostatečné školení zaměstnanců představuje další významný bezpečnostní deficit. Zaměstnanci jsou pravidelně proškoleni pouze na základní mimořádné události, jako je např. evakuace při požáru. Chybí však školení pro závažnější mimořádné situace, čímž může být útok aktivního střelce, vyjednávání s agresorem nebo zvládnutí paniky. Rovněž chybí vypracovaná krizová komunikace, jak interní, tak směrem k veřejnosti a neexistují detailní scénáře či návody pro reakci na různé typy incidentů.

Výrazná provozní vytíženost objektu je patrná zejména v určitých částech dne. V těchto obdobích dochází k vysoké frekvenci pohybu osob, což výrazně komplikuje jakýkoli pokus o selektivní či cílenou kontrolu. Denně se jedná o desítky až stovky osob. Vysoký počet lidí v budově snižuje přehlednost a zvyšuje pravděpodobnost nepozorovaného pohybu osob, které se v objektu nacházejí neoprávněně.

Suterén byl vyhodnocen jako nejvíce nebezpečné místo. Jednotlivé dveře v něm jsou sice uzavřené a uzamčené, což nelze považovat za dostatečné zabezpečení. Za těmito jednotlivými dveřmi jsou buď uloženy archívy či technické místnosti. V suterénu je taktéž výtah, kterým je taktéž možné se dostat do každého patra celé budovy. Pozitivním zjištěním bylo, že ve sklepech bylo umístěno jedno pohybové čidlo, které by mohlo zabránit možnému skrytí útočníka do dalšího dne. Avšak čidlo směřuje pouze ke schodišti a bylo by tak možné jej obejít. Třeba v případě, kdy by se útočník dostal do suterénu výtahem v době úředních hodin a následně by zde vyčkal přes noc do dalšího dne, tak by jej čidlo nezachytilo. Kladným poznatkem bylo i to, že na všech oknech patřících k suterénu budovy jsou zvenčí nainstalovány mechanické zábranné systémy, a to v podobě mříží.

Tyto faktory v souhrnu znamenají, že instituce může být snadno zneužita jako cíl útoku, za účelem narušení provozu nebo jiného krizového scénáře, a to jak ze strany jednotlivce, tak i organizované skupiny.

Bezpečnostní analýza zájmové instituce byla provedena na základě veřejně dostupných údajů a fyzické obhlídky objektu. V rámci šetření byly zmapovány všechny přístupové cesty, vnitřní uspořádání budovy i stávající technické zabezpečení. Bylo zjištěno, že objekt umožňuje volný vstup bez nutnosti registrace či identifikace návštěvníků, což znamená, že

se osoby mohou volně pohybovat po budově bez jakéhokoliv dohledu. Tato skutečnost zásadně snižuje bezpečnostní úroveň objektu a výrazně zvyšuje riziko neoprávněného vniknutí nebo ohrožení osob. Technická ochrana budovy byla vyhodnocena jako nedostatečná. Chybí moderní bezpečnostní systémy, jako je elektronická kontrola přístupu nebo kamerový systém. Stávající pohybová čidla jsou aktivována až po uzamčení objektu a jejich rozmístění není strategicky účelné. Některé části budovy, zejména v suterénu, zůstávají zcela mimo jejich dosah. V budově rovněž chybí fyzická přítomnost bezpečnostního personálu a zaměstnanci nejsou dostatečně proškoleni pro zvládání mimořádných situací, jimiž může být násilný útok, evakuace nebo panika. Významným poznatkem bylo zjištění, že suterén budovy představuje z hlediska bezpečnosti nejzranitelnější místo. Přestože jsou jednotlivé dveře v suterénu zpravidla uzamčené a za nimi se nacházejí technické místnosti nebo archivy, existují zde vážná rizika. Suterén je přímo propojen s výtahem, kterým lze bez omezení cestovat mezi patry, což představuje možné slabé místo v zabezpečení. V suterénu bylo umístěno alespoň jedno pohybové čidlo, jehož směr je naneštěstí orientován pouze ke schodišti. Na druhou stranu bylo pozitivně vyhodnoceno, že všechna okna suterénu jsou zabezpečena mechanickými zábranami v podobě venkovních mříží, které snižují riziko neoprávněného vstupu z vnějšího prostoru. Dalším problémem je vysoká provozní vytíženost objektu, která ztěžuje kontrolu pohybu osob a znemožňuje efektivní reakci na nestandardní situace. Z celkového pohledu lze tedy konstatovat, že úroveň zabezpečení objektu je nedostačující. Objekt je zranitelný vůči širokému spektru fyzických, organizačních, informačních i sociálních hrozeb. Pro zajištění vyšší míry bezpečnosti je nezbytné implementovat technická, organizační i personální opatření, která povedou k celkovému zvýšení odolnosti objektu vůči krizovým scénářům.

## 8 NÁVRH BEZPEČNOSTNÍCH OPATŘENÍ

Závěrečná část diplomové práce je věnována návrhu bezpečnostních opatření, jejichž cílem je zvýšení úrovně bezpečnosti a minimalizace rizik na co nejnížší možnou úroveň v dané instituci. Na základě analýzy rizik a po konzultaci s vedoucím odboru byla vybrána pouze nejzásadnější rizika z první oblasti. Konkrétně se jedná o fyzický útok jednotlivce nebo skupiny, ozbrojený útok, žhárství, nedostatečně proškolený personál, neoprávněné vniknutí do objektu, požár technického původu, psychický nátlak či vyhoření personálu a biologickou kontaminaci prostor. Tento výběr byl učiněn s ohledem na praktickou využitelnost navržených bezpečnostních opatření.

### 8.1 Doporučený návrh ke zlepšení bezpečnostních podmínek

Výstupem tohoto doporučení není návrh komplexní ochrany, neboť tato varianta není reálná ani z pohledu zřizovatele, ani s ohledem na charakter zájmového objektu. Cílem je vytvořit rovnováhu mezi dostupností služeb pro občany a zajištění alespoň základní úrovně bezpečnosti pro zaměstnance i návštěvníky.

Tato podkapitola je rozdělena do dvou fází. První fáze vychází z analýzy rizik, druhá je založena na výsledcích fyzické obhlídky zájmového objektu. Nejprve jsou uvedena doporučení ke zlepšení bezpečnostních podmínek vycházející z první fáze.

Jedním z významných rizik je **fyzický útok jednotlivce nebo skupiny** z řad veřejnosti, jehož cílem je úmyslné násilí vůči zaměstnancům nebo klientům. Prevencí těchto incidentů je zejména instalace kamerového systému ve veřejně přístupných částech budovy a přítomnost kvalifikované ostrahy, která monitoruje pohyb osob a dokáže včas reagovat. Doporučuje se také školení zaměstnanců zaměřené na včasné rozpoznání a zvládání konfliktního chování.

V případě **ozbrojeného útoku**, tedy výskytu aktivního útočníka s palnou zbraní nebo jiným nebezpečným nástrojem, je nezbytné zavést krizový postup typu „Utíkej, skryj se, boj“ (anglicky „Run, Hide, Fight“) a pravidelně jej procvičovat. Mezi další doporučená opatření patří možnost okamžitého uzamčení místností, vytvoření úkrytových prostor a propojení kamerového systému s policií za účelem rychlého přenosu informací. Klíčová je také existence aktuálních evakuačních plánů a proškolení všech pracovníků v jejich používání, včetně praktického nácviku.

**Vniknutí nepovolané osoby** do neveřejných částí úřadu představuje reálnou hrozbu jak z hlediska bezpečnosti osob, tak z pohledu ochrany citlivých dat. Pro minimalizaci tohoto rizika je vhodné zavést elektronický přístupový systém s čipovými kartami, zajistit přítomnost recepční služby s evidencí návštěv a viditelně označit neveřejné prostory. Vzhledem k tomu, že se jedná o veřejně přístupný objekt, není možné uplatnit tento systém na návštěvníky. Tam, kde je to proveditelné, se doporučuje instalace mechanických zábranných prvků, například bezpečnostních dveří nebo turniketů. Tato opatření se týkají i přístupu do suterénu a provozu výtahu. Ke vstupu do suterénu by měly být instalovány mříže a výtah by měl být funkční do této části budovy pouze po ověření oprávnění zaměstnance prostřednictvím čipu nebo karty.

Další závažnou hrozbou je úmyslné založení požáru, tedy **žhářství**. Zásadní je technická prevence, zejména instalace detektorů kouře a požárních hlásičů. Rizikové prostory jako například suterén by měly být nepřístupné veřejnosti a pravidelně kontrolovány pracovníky úřadu nebo bezpečnostní službou. Důležitá je také spolupráce s Hasičským záchranným sborem a začlenění jeho doporučení do vnitřních směrnic, které je třeba šířit mezi zaměstnance. Nedostatek únikových cest z vyšších pater představuje riziko. Proto se doporučuje vybudování alternativní únikové cesty nebo vybavení budovy evakuačním lanem nebo nafukovací záchrannou matrací. **Technickému požáru**, např. v důsledku zkratu nebo poruchy elektrospotřebiče, je třeba předcházet pravidelnými revizemi a používáním výhradně certifikovaných zařízení. Zaměstnanci by měli být proškoleni v bezpečném zacházení s technikou a měli by mít k dispozici jasné pokyny pro postup v případě technického selhání. I zde platí, že je třeba zajistit více únikových cest z vyšších pater budovy.

Podceňovaným rizikem je i **nedostatečně vyškolený personál**. Zaměstnanci, kteří nejsou připraveni na krizové situace, mohou situaci svou nejistotou zhoršit. Doporučuje se proto systematické školení všech pracovníků v oblastech evakuace, první pomoci, zvládání stresu, znalosti konkrétních postupů a v rozpoznání a deeskalaci konfliktního chování. Vhodné je také zřízení krizového týmu s jasně definovanými kompetencemi, přičemž alespoň jeden člen tohoto týmu by měl být vždy v budově přítomen.

**Psychická zátěž zaměstnanců**, zejména dlouhodobý stres, práce s konfliktními klienty a syndrom vyhoření, může vést ke snížení výkonnosti, zdravotním komplikacím nebo dokonce ke vzniku bezpečnostních hrozeb. Úřad by měl podporovat duševní pohodu zaměstnanců prostřednictvím supervizí, umožnění přístupu k psychologické pomoci

a možností rotace pracovních pozic. Důležité je také sledovat pracovní podmínky a pravidelně vyhodnocovat míru pracovní spokojenosti.

Riziko **biologické kontaminace** prostor, ke kterému může dojít přenosem infekcí kontaktem s kontaminovanými dokumenty, povrchy nebo osobami, lze snížit zajištěním dostatečné hygieny na pracovišti, dostupností dezinfekčních prostředků a školením zaměstnanců o zásadách hygieny. V okolnostech podezření na výskyt infekčního onemocnění by měl být nastaven jasný postup včetně izolace, dekontaminace a možnosti přechodu na práci z domova, pokud to charakter práce umožňuje.

Bezpečnostní návrhy druhé fáze vycházejí z fyzické obhlídky zájmové instituce. Prioritním opatřením je instalace kamerového systému s možností vzdáleného online připojení. Tento systém by měl být přístupný operačnímu středisku Policie České republiky nebo Městské policie dané obce s rozšířenou působností. Dále se doporučuje realizace cvičení ve spolupráci s policií na situaci s aktivním útočníkem, tzv. scénář AMOK. U tohoto cvičení je třeba zvážit možný negativní dopad na zaměstnance, a proto je nezbytné nejprve zjistit, zda je takové cvičení vůbec možné ze strany policie a zda o něj mají zaměstnanci zájem. Cvičení by mělo být dopředu naplánované a zaměstnanci o něm musí být informováni, aby nebyli vystaveni nepřiměřenému stresu. Pokud by cvičení nemohlo proběhnout přímo na úřadě, je vhodné zajistit účast pracovníků na externím školení, kde by se mohli s touto problematikou seznámit.

Dalším doporučením je zavedení pracovníka ostrahy, a to buď z řad zřizovatele, nebo ve spolupráci s externí bezpečnostní agenturou. Pokud tato spolupráce není možná, je nezbytné alespoň vybavit budovu kamerovým systémem s online přístupem pro městskou policii. Ta by mohla na základě sledovaného přenosu vyslat na místo hlídku.

Zaměstnanci, kteří pracují s přestupkovou agendou, by mohli být vybaveni osobními ochrannými prostředky, například teleskopickým obuškem, taktickým perem, kubotanem nebo pepřovým sprejem v ne-aerosolové formě. K používání těchto prostředků by byli proškoleni příslušníky městské policie. Kdyby někteří zaměstnanci neměli zájem o tyto pomůcky, mohli by absolvovat školení sebeobrany. Tato forma podpory by mohla zvýšit jejich sebedůvěru v krizových situacích. V rámci školení požární ochrany by zaměstnanci také měli mít možnost praktického nácviku s hasicím přístrojem.

Suterén byl vyhodnocen jako nejrizikovější část objektu, protože zde může útočník nenápadně vyčkat na vhodnou příležitost. Přístup po schodišti není nijak zabezpečen, proto

je třeba prostor zabezpečit například instalací mříží. Boční dveře, které vedou ze suterénu na hlavní chodbu, by měly být trvale uzavřeny a z vnitřní strany opatřeny koulí, aby nešly otevřít. Výtah též umožňuje přístup do suterénu, a proto by měl být jeho provoz omezen čipovým nebo kartovým ověřením.

Efektivním řešením je zavedení elektronické kontroly vstupu a regulace pohybu osob v budově. Všechny kanceláře by měly být zvenčí opatřeny koulí a vstupy by měly být zabezpečeny elektronickým přístupem. Při příchodu by zaměstnanci přiložili čipovou kartu a zadali svůj osobní kód, čímž by došlo k aktivaci jejich přístupových práv. Při odchodu by celý proces opakovali a přístup by se deaktivoval. Pokud by byl pracovník posledním v kanceláři, provedlo by se současně zakódování místnosti. Při případném odcizení nebo pokusu o zneužití karty by se neoprávněná osoba bez znalosti kódu do místnosti nedostala.

Předvolané osoby by při vstupu do budovy zadaly na rezervačním panelu číslo jednací. Panel by následně zobrazil číslo podlaží a příslušnou telefonní linku. V daném patře by byly vstupní dveře opatřeny koulí a čtečkou. Návštěvník by kontaktoval pracovníka a vyčkal na jeho příchod. Ten by tak mohl předem zhodnotit, zda osoba nevykazuje známky agresivního nebo podezřelého chování. Tímto opatřením by byl znemožněn volný pohyb osob po budově a případný útočník by čelil další překážce.

Nadstandardní zabezpečení může zahrnovat bezpečnostní rámy pro detekci podezřelých předmětů nebo rentgenové zařízení pro kontrolu zavazadel. Tato řešení jsou však z finančního hlediska velmi náročná a jejich zavedení je z pohledu zřizovatele nepravděpodobné. Totéž platí i pro bezpečnostní propustné dveře.

## 8.2 Ekonomická rozvaha

Poslední část diplomové práce je věnována ekonomickému odhadu nákladů spojených s navrhovanými bezpečnostními opatřeními. Rozvaha vychází ze snahy najít rovnováhu mezi nutností posílení ochrany zaměstnanců a návštěvníků a ekonomickou udržitelností celého souboru řešení. Vzhledem k tomu, že zavedení komplexní ochrany není z pohledu provozních ani investičních možností zřizovatele reálné. Ekonomická rozvaha pracuje s orientačními tržními cenami a předpokládá průměrné veřejné zadání. U každého opatření jsou uvedeny předpokládané pořizovací náklady, a u některých rovněž náklady provozní, které je nutné zohlednit při rozhodování o jejich implementaci. Tabulky opatření jsou uvedeny níže (Tabulka 16), (Tabulka 17), (Tabulka 18), (Tabulka 19) a (Tabulka 20).

Tabulka 16 Technická opatření

| Opatření                                                                     | Odhad nákladů (Kč bez DPH) |
|------------------------------------------------------------------------------|----------------------------|
| Kamerový systém (8–12 kamer, záznamové zařízení, napojení na PČR)            | 200 000 – 450 000          |
| Propojení systému s PČR / Městskou policií (licence, IT práce, připojení)    | 30 000 – 120 000           |
| Elektronický přístupový systém (čtečky, software, čipové karty, 10–20 dveří) | 150 000 – 500 000          |
| Vstupní panel pro veřejnost (rezervační systém, propojení s IS)              | 50 000 – 150 000           |
| Mechanické zabezpečení (mříže, bezpečnostní dveře, koule na dveře)           | 60 000 – 250 000           |
| <b>Celkem (Kč bez DPH)</b>                                                   | <b>490 000 – 1 470 000</b> |

(zdroj: vlastní)

Tabulka 17 Fyzická bezpečnost a školení

| Opatření                                                                     | Odhad nákladů (Kč bez DPH)                        |
|------------------------------------------------------------------------------|---------------------------------------------------|
| Přítomnost ostrahy (externí agentura, 1 pozice, 8 hod./den, ročně)           | 250 000 – 650 000 ročně                           |
| Alternativa: interní pracovník (mzda, odvody, vybavení)                      | 225 000 – 500 000 ročně                           |
| Školení zaměstnanců (konfliktní situace, sebeobrana, deeskalace)             | 30 000 – 60 000                                   |
| Ochranné pomůcky pro rizikové pozice (např. pepřový sprej, kubotan, školení) | 3 000 – 5 000/osoba                               |
| Cvičení scénáře AMOK s PČR / externí školení                                 | 30 000 – 100 000                                  |
| <b>Celkem (Kč bez DPH)</b>                                                   | <b>508 000 – 1 215 000 + opakující se náklady</b> |

(zdroj: vlastní)

Tabulka 18 Protipožární a krizová opatření

| Opatření                                                              | Odhad nákladů (Kč bez DPH) |
|-----------------------------------------------------------------------|----------------------------|
| Instalace detektorů kouře a hlásičů (15–20 ks + centrální jednotka)   | 50 000 – 180 000           |
| Vybudování alternativní únikové cesty (pokud je fyzicky proveditelná) | 300 000 – 1 500 000        |
| Evakuační vybavení (lana, nafukovací matrace)                         | 5 000 – 100 000            |
| Praktické školení hašení požárů                                       | 10 000 – 30 000            |
| Spolupráce a HZS a aktualizace směrnic                                | 10 000 – 20 000            |
| <b>Celkem (Kč bez DPH)</b>                                            | <b>375 000 – 1 830 000</b> |

(zdroj: vlastní)

Tabulka 19 Školení, duševní zdraví a hygienická opatření

| Opatření                                                                   | Odhad nákladů (Kč bez DPH)                      |
|----------------------------------------------------------------------------|-------------------------------------------------|
| Školení první pomoci, evakuace, zvládán stresu                             | 30 000 – 70 000                                 |
| Zřízení krizového týmu (školení, metodika, komunikace)                     | 20 000 – 50 000                                 |
| Podpora duševního zdraví (supervize, přístup k psychologovi, rotace pozic) | 80 000 – 250 000 ročně                          |
| Zajištění dezinfekce, školení o hygieně, protiepidemická opatření          | 15 000 – 40 000 ročně                           |
| <b>Celkem (Kč bez DPH)</b>                                                 | <b>145 000 – 410 000 + opakující se náklady</b> |

(zdroj: vlastní)

Tabulka 20 Celkový odhad nákladů

| Opatření                                      | Odhad nákladů (Kč bez DPH)                         |
|-----------------------------------------------|----------------------------------------------------|
| Technická opatření                            | 490 000 – 1 470 000                                |
| Fyzická bezpečnost a školení                  | 508 000 – 1 215 000                                |
| Protipožární a krizová bezpečnost             | 375 000 – 1 830 000                                |
| Školení, duševní zdraví a hygienická opatření | 145 000 – 410 000                                  |
| <b>Celkem (Kč bez DPH)</b>                    | <b>1 518 000 – 4 925 000+ opakující se náklady</b> |

(zdroj: vlastní)

Nejefektivnější poměr cena/přínos má kamerový systém, elektronický přístup a školení personálu. Fyzická ostraha a zabezpečení suterénu jsou důležité z hlediska nejrizikovějších situací. Nadstandardní technologie (např. rentgen, bezpečnostní rámy) nejsou ekonomicky obhájitelné.

Závěrečná část diplomové práce se zaměřuje na návrh bezpečnostních opatření s cílem zvýšit úroveň ochrany a minimalizovat rizika v prostředí veřejné instituce. Na základě analýzy rizik a konzultací s odborníky byla identifikována hlavní ohrožení, jako jsou fyzické a ozbrojené útoky, zhářství, technické požáry, neoprávněné vniknutí, psychická zátěž zaměstnanců, nedostatečné školení a biologická kontaminace. Součástí návrhu je také ekonomický odhad nákladů, který se snaží nalézt rovnováhu mezi nutností zvýšení bezpečnosti a finančními možnostmi instituce. Navržená opatření vycházejí z orientačních tržních cen. Celkové náklady na realizaci bezpečnostních opatření se pohybují v rozmezí 1 518 000 až 4 925 000 Kč bez DPH, přičemž některé položky zahrnují i opakující se provozní výdaje. Nejefektivnější poměr mezi cenou a přínosem mají kamerový systém,

elektronický přístup a školení personálu, zatímco nákladné technologie, jako jsou rentgeny nebo bezpečnostní rámy, nejsou v aktuálním kontextu ekonomicky přijatelné.

Praktická část diplomové práce prokázala vysokou míru zranitelnosti veřejné instituce, která slouží jako modelový příklad měkkého cíle v prostředí okresní státní správy. Bezpečnostní analýza, provedená na základě fyzické prohlídky a veřejně dostupných údajů, odhalila řadu nedostatků v technickém i organizačním zabezpečení objektu. Nejzávažnějšími problémy jsou absence moderních bezpečnostních systémů, volný pohyb návštěvníků bez identifikace, nedostatečné krizové plánování a chybějící školení zaměstnanců. Za zvláště rizikové bylo označeno podzemní podlaží objektu, které je snadno přístupné a nedostatečně monitorované, což umožňuje potenciální skrytý pohyb osob a ohrožení zevnitř. Na základě kategorizace aktiv a identifikace hrozeb byla pomocí metod PNH a KARS vyhodnocena nejzávažnější bezpečnostní rizika, včetně ozbrojeného útoku, žhářství, vniknutí nepovolané osoby, nedostatečně vyškoleného personálu, psychického nátlaku na personál nebo biologické kontaminace. Výsledky ukázaly, že žádné z hodnocených rizik nelze považovat za nízké, což dokládá vysokou míru ohrožení měkkých cílů tohoto typu. Získané poznatky byly dále využity k návrhu konkrétních bezpečnostních opatření, která reflektují jak aktuální potřeby objektu, tak ekonomické možnosti instituce. Doporučená opatření zahrnují technické zabezpečení (kamerový systém, elektronická kontrola přístupu), personální zajištění (ostraha, školení), krizový management a zajištění hygienických a psychosociálních podmínek. Tato opatření a jejich realizace by měla významně přispět ke zvýšení odolnosti objektu vůči reálným hrozbám. Celkově praktická část podtrhuje význam systematického přístupu k ochraně měkkých cílů a potřebu zavedení komplexní bezpečnostní politiky ve veřejných institucích, které sice nepatří mezi prvky kritické infrastruktury, avšak jejich narušení by mohlo mít zásadní dopady na veřejnost i chod veřejné správy.

## ZÁVĚR

Ve své diplomové práci jsem se zabýval tématem návrhu opatření pro zvyšování bezpečnosti vybrané kategorie měkkých cílů. Teoretická část diplomové práce představuje základní rámec pro pochopení problematiky ochrany měkkých cílů ve veřejné správě. Nejprve jsou zde vymezeny klíčové pojmy, jako jsou měkký cíl, hrozba, riziko, újma, odolnost či bezpečnostní opatření. Měkké cíle jsou charakterizovány jako veřejně přístupná místa s vysokou koncentrací osob a nízkou úrovní ochrany. Uvedené pojmy jsou doplněny statistickými daty, která potvrzují narůstající agresi vůči zaměstnancům veřejné správy a poukazují na potřebu systematické ochrany těchto institucí. Dále se práce věnuje právnímu rámci, který vychází z Ústavy ČR a Listiny základních práv a svobod a zahrnuje také zákony o ochraně osobních údajů, kybernetické bezpečnosti a správě informačních systémů. Samostatná kapitola je zaměřena na strategické dokumenty Ministerstva vnitra ČR, mimo jiné na Koncepti ochrany měkkých cílů a související metodiky, jenž zdůrazňují důležitost prevence, plánování, vzdělávání a spolupráce s bezpečnostními složkami. V závěru teoretické části jsou představeny metody analýzy rizik, mezi nimiž jsou upřednostněny metody PNH a KARS. Metoda KARS pracuje s daty, které lze následně přehledně vizualizovat, což je vhodné pro zhodnocení zranitelnosti veřejných institucí, a proto bude stěžejní pro následnou praktickou část.

Praktická část diplomové práce je zaměřena na analýzu anonymizované veřejné instituce, která slouží jako modelový příklad měkkého cíle ve státní správě. Vzhledem k veřejné přístupnosti, vysoké návštěvnosti a administrativní činnosti je objekt zranitelný vůči různým bezpečnostním hrozbám, i přestože nepatří mezi prvky kritické infrastruktury. Analýza vycházela z veřejně dostupných dat, fyzické prohlídky objektu a zhodnocení aktuálního zabezpečení. Zjištěny byly zásadní nedostatky spočívající zejména ve volném pohybu osob, nízké míře technické ochrany, chybějícím dozoru uvnitř objektu, nedostatečném školení zaměstnanců a výrazné provozní vytíženosti. Rizikovým místem se ukázal být zejména suterén objektu. K vyhodnocení hrozeb byly použity metody PNH a KARS, které identifikovaly nejzávažnější rizika, jimiž jsou ozbrojený útok, žhářství, psychická zátěž personálu či biologická kontaminace prostor. Na základě těchto zjištění byla navržena konkrétní bezpečnostní opatření včetně možných úprav, organizačních změn a školení. V rámci těchto opatření byla vytvořena i ekonomická rozvaha. V ní jsou uvedeny i orientační ceny, neboť vzhledem k veřejné povaze této instituce by výběr konkrétního dodavatele probíhal formou veřejných zakázek. Práce potvrdila, že účinná ochrana měkkých

cílů vyžaduje systematický přístup založený na důsledné prevenci, pravidelném hodnocení rizik a spolupráci ostatních státních subjektů. Navržená řešení mohou přispět ke zvýšení bezpečnosti nejen analyzované instituce, ale i dalších podobných objektů státní správy.



## SEZNAM POUŽITÉ LITERATURY

- [1] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, 2025. *Ochrana měkkých cílů*. Online. In: Ministerstvo vnitra České republiky. Dostupné z: <https://mv.gov.cz/clanek/ochrana-mekkych-cilu.aspx> [cit. 2025-01-18].
- [2] HROMADA, Martin, FRÖHLICH, Tomáš, 2021. *Metodika zvyšování ochrany a odolnosti vybraných kategorií měkkých cílů*. Zlín: Univerzita Tomáše Bati ve Zlíně. [cit. 2025-01-18]
- [3] World Health Organization. WHO, 2022. *Violence Prevention Unit: Approach, Objectives and Activities, 2022-2026*. Dostupné z: <https://www.who.int/publications/m/item/who-violence-prevention-unit--approach--objectives-and-activities--2022-2026> [cit. 2025-01-18].
- [4] LUDĚK, Lukáš, 2017. *Teorie bezpečnosti. I*. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-89-7.
- [5] HESTERMAN, Jennifer L., 2019. *Soft target hardening: protecting people from attack*. 2. Edition. New York: Routledge. ISBN 9781138391109.
- [6] ZEMAN, Petr, 2002. *Česká bezpečnostní terminologie: výklad základních pojmů*. Online. Brno: Masarykova univerzita v Brně, Mezinárodní politologický ústav. ISBN 80-210-3037-2. Dostupné také z: <https://ndk.cz/uuid/uuid:7ae54b60-e10d-11e5-984e-005056827e52> [cit. 2025-01-18]
- [7] ÚŘAD PRÁCE ČESKÉ REPUBLIKY, 2025. *Za napadení úředníka může útočníkům hrozit i vězení*. Online. In: Úřad práce ČR. 2018. Dostupné z: <https://www.uradprace.cz/za-napadeni-urednika-muze-utocnikum-hrozit-i-vezeni>. [cit. 2025-03-01].
- [8] ÚŘAD PRÁCE ČESKÉ REPUBLIKY, 2025. *Útoky na zaměstnance Úřadu práce přibývají. Úřad posiluje zabezpečení svých poboček a zaměstnanců*. Online. In: Úřad práce ČR. 2024. Dostupné z: <https://www.uradprace.cz/utoky-na-zamestnance-uradu-prace-pribyvaji-urad-posiluje-zabezpeceni-svych-pobocek-a-zamestnancu>. [cit. 2025-03-01].
- [9] ČESKO. *Zákon č. 40/2009 Sb. Trestní zákoník*. Online. In: Elektronická Sbírka zákonů a mezinárodních smluv. Dostupné z: <https://www.e-sbirka.cz/sb/2009/40> [cit. 2025-03-25].

- [10] DRDLA, Miloš a kol., 2021. *Bezpečnost měkkých cílů*. Online. In: Univerzita Palackého v Olomouci. Dostupné z: [https://www.klus.upol.cz/wp-content/uploads/2021/02/mekke\\_cile\\_Drdla-2.pdf](https://www.klus.upol.cz/wp-content/uploads/2021/02/mekke_cile_Drdla-2.pdf). [cit. 2025-03-20].
- [11] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Dokumenty a odkazy – Dokumenty k měkkým cílům: *Metodika ochrany měkkých cílů*. Online. In: Ministerstvo vnitra České republiky. Dostupné z: <https://mv.gov.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx>. [cit. 2025-02-10].
- [12] KOTKOVÁ, Dora et al., 2021. *Hromadné společenské a kulturní akce a jejich ochrana*. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. ISBN 978-80-7678-058-3.
- [13] UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE. *The European House of Major Events* Online. In: UNICRI, 2021 Dostupné z: [https://unicri.org/sites/default/files/2021-06/Full\\_Text\\_%20the\\_European\\_house\\_of\\_major\\_events.pdf](https://unicri.org/sites/default/files/2021-06/Full_Text_%20the_European_house_of_major_events.pdf). [cit. 2025-03-20].
- [14] POLICIE ČESKÉ REPUBLIKY. *Odložení případu*. Online 2020. Dostupné z: <https://policie.gov.cz/clanek/krajske-reditelstvi-severomoravskeho-kraje-zpravodajstvi-odlozeni-pripadu.aspx>. [cit. 30. 3. 2025].
- [15] HOLLYWOOD, John S.; GIERLACK, Keith; MOORE, Pauline; GOODE, Thomas; WILLIS, et al. *Keeping Soft Targets and Crowded Places Safe from Mass-Casualty Attacks: Insights from a Landscape Assessment* Online. Santa Monica: RAND Corporation, Dostupné z: [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RRA2200/RRA2260-2/RAND\\_RRA2260-2.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2200/RRA2260-2/RAND_RRA2260-2.pdf). [cit. 2025-03-23].
- [16] ČESKO. *Zákon č. 51/2020 Sb. O územně správním členění státu a o změně souvisejících zákonů (zákon o územně správním členění státu), ve znění pozdějších předpisů*. Online. In: Elektronická Sbírka zákonů a mezinárodních smluv. Dostupné z: <https://www.e-sbirka.cz/sb/2020/51> [cit. 2025-03-25].
- [17] MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR, 2020. *Územní rozvoj: Strategie – Územní rozvoj*. Online. In: Integrovaný regionální operační program 2014–2020. Dostupné z: <https://irop.gov.cz/cs/irop-2014-2020/temata/uzemni-rozvoj> [cit. 2025-03-25].

- [18] ČESKO. *Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů*. Online. In: Elektronická Sbírka zákonů a mezinárodních smluv. Dostupné z: <https://www.e-sbirka.cz/sb/2000/240>. [cit. 2025-03-29].
- [19] ČESKO. *Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších ústavních zákonů*. Online. In: Poslanecká sněmovna parlamentu České republiky. Dostupné z: <https://www.psp.cz/docs/laws/constitution.html>. [cit. 2025-01-19].
- [20] ČESKO. *Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších ústavních zákonů*. Online. In: Poslanecká sněmovna parlamentu České republiky. Dostupné z: <https://www.psp.cz/docs/laws/listina.html>. [cit. 2025-01-19].
- [21] ČESKO. *Zákon č. 110/2019 Sb. o zpracování osobních údajů, ve znění pozdějších předpisů*. Online. In: Elektronická Sbírka zákonů a mezinárodních smluv. Dostupné z: <https://www.e-sbirka.cz/sb/2019/110>. [cit. 2025-01-22].
- [22] EVROPSKÝ PARLAMENT A RADA EU. *Nařízení - 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), ve znění pozdějších předpisů*. Online. In: Evropská Unie, EUR-Lex. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32016R0679>. [cit. 2025-01-22].
- [23] ČESKO. *Zákon č. 181/2014 Sb. o kybernetické bezpečnosti, ve znění pozdějších předpisů*. Online. In: Elektronická Sbírka zákonů a mezinárodních smluv. Dostupné z: <https://www.e-sbirka.cz/sb/2014/181>. [cit. 2025-01-26].
- [24] PORTÁL NÚKIB. *Nový zákon o kybernetické bezpečnosti*. Online. In: Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: <https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti>. [cit. 2025-01-26].
- [25] EVROPSKÝ PARLAMENT A RADA EU. *Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*. Online. In: Evropská Unie, EUR-Lex. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32022L2555&qid=1738341297850>. [cit. 2025-01-26].

- [26] ČESKO. *Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů*. Online. In: Elektronická Sbírka zákonů a mezinárodních smluv. Dostupné z: <https://www.e-sbirka.cz/sb/2000/365>. [cit. 2025-01-26].
- [27] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČESKÉ REPUBLIKY. *Bezpečnostní politika*. Online. In: Ministerstvo zahraničních věcí České republiky. Dostupné z: [https://mzv.gov.cz/jnp/cz/zahranicni\\_vztahy/bezpecnostni\\_politika/](https://mzv.gov.cz/jnp/cz/zahranicni_vztahy/bezpecnostni_politika/). [cit. 2025-01-18].
- [28] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČESKÉ REPUBLIKY, 2023. *Bezpečnostní strategie České republiky 2023*. Online. In: Ministerstvo zahraničních věcí České republiky. Dostupné z: [https://mzv.gov.cz/jnp/cz/zahranicni\\_vztahy/bezpecnostni\\_politika/bezpecnostni\\_strategie/](https://mzv.gov.cz/jnp/cz/zahranicni_vztahy/bezpecnostni_politika/bezpecnostni_strategie/). [cit. 2025-01-18].
- [29] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ, 2018. *ČSN ISO 31000:2018, Management rizik – Směrnice*. Česká agentura pro standardizaci.
- [30] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ, 2020. *ČSN EN IEC 31010 ED. 2, Management rizik – Techniky posuzování rizik*. Česká agentura pro standardizaci.
- [31] CRDR SPOL. S R.O. *Metody a způsoby hodnocení rizik na pracovišti*. Online. In: DokumentaceBOZP.cz. 2018. Dostupné z: [https://www.dokumentacebozp.cz/aktuality/metody-hodnoceni-rizik-bozp/#kap\\_5](https://www.dokumentacebozp.cz/aktuality/metody-hodnoceni-rizik-bozp/#kap_5). [cit. 2025-03-05].
- [32] GUARD7, V. O. S. *Metoda „What – If“ (Co se stane, když..)*. Online. In: Guard7 safety solutions. 2022. Dostupné z: <https://www.guard7.cz/metoda-what-if-co-se-stane-kdyz/>. [cit. 2025-03-05].
- [33] GUARD7, V. O. S. *Kontrolní seznam (Checklist)*. Online. In: Guard7 safety solutions. 2022. Dostupné z: <https://www.guard7.cz/kontrolni-seznam-checklist/>. [cit. 2025-03-05].
- [34] VÝZKUMNÝ ÚSTAV BEZPEČNOSTI PRÁCE, V. V. I. *Rizika a nebezpečí: Metody hodnocení rizik*. Online. In: Znalostní systém prevence rizik v BOZP. Dostupné z: <https://zsbozp.vubp.cz/metody-hodnoceni-rizik>. [cit. 2025-03-05].

- [35] ČESKO. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). Online. In: Elektronická Sbírka zákonů a mezinárodních smluv. Dostupné z: <https://www.e-sbirka.cz/sb/2018/82> [cit. 20. 3. 2025].
- [36] BAKER, Paul R. a Daniel J. BENNY, 2013. *The complete guide to physical security*. Boca Raton: CRC Press. ISBN 9781420099638.
- [37] PACINDA, Štefan, 2010. *Síťová analýza a metoda KARS*. The Science for Population Protection. Online. ISSN 1803-635X. Dostupné z: <http://www.population-protection.eu/prilohy/casopis/8/56.pdf> [cit. 2025-03-10].
- [38] Willis, H. H. a LaTourrette, T, 2014. *Vulnerability Assessment Method Pocket Guide: A Tool for Center of Gravity Analysis*. Online. In: Santa Monica (CA): RAND Corporation, Dostupné z: <https://www.rand.org/pubs/tools/TL129.html>. ISBN 978-0-8330-8689-1
- [39] FDA, *CARVER + SHOCK PRIMER AN OVERVIEW OF THE CARVER PLUS SHOCK METHOD FOR FOOD SECOTR VULNERABILITY ASSESSMENTS*
- [40] SECURITY MANAGEMENT INTERNATIONAL, LLC, 2025. *What is the CARVER Method?* Online. In: SMI. Dostupné z: <https://www.smiconsultancy.com/what-is-carver> [cit. 2025-04-18]
- [41] BREHOVSKÁ, Lenka a Libor LÍBAL, 2014. *Identifikace rizik u sociálních zařízení pro případ výpadku elektrické energie jako prevence během mimořádných událostí*. Online. In: Trilobit. Dostupné z: <https://trilobit.fai.utb.cz/identifikace-rizik-u-socialnich-zarizeni-pro-pripad-vypadku-elektricke-energie-jako-prevence-behem-mimoradnych-udalosti> [cit. 2025-03-10].
- [42] RYŠAVÝ, J., (2018). *Strategický plán obce Rudná a jeho vliv na bezpečnost sídla. Regionální rozvoj mezi teorií a praxí*, no. 4, pp. 45-61. ISSN 1805-3246.
- [43] KMOSEK.COM. *PNH metoda*. Online. Dostupné z: <https://www.kmosek.com/slovník/pojem/pnh-metoda/> [cit. 2025-04-30].
- [44] JELŠOVSKÁ, K., PETERKOVÁ, A, 2013. *Řešení krizových situací – metody a jejich aplikace*. Online. In: Slezská univerzita v Opavě. Dostupné z: [www.slu.cz/file/cul/67f86af0-d484-45dc-87cf-52b7d488c52a](http://www.slu.cz/file/cul/67f86af0-d484-45dc-87cf-52b7d488c52a) [cit. 2025-03-10].

- [45] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Dokumenty a odkazy – Dokumenty k měkkým cílům: *Koncepce ochrany měkkých cílů pro roky 2017-2020*. Online. In: Ministerstvo vnitra České republiky. Dostupné z: <https://mv.gov.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx>. [cit. 2025-02-04].
- [46] DUFEK, Zdeněk; APELTAUER, Tomáš; HROMADA, Martin; MRÁZKOVÁ, Lucia; VANGELI, Benedikt, et al., 2019 *Ochrana měkkých cílů*. Brno: Leges. ISBN 978-80-7502-427-5 Dostupné z: <https://profesis.ckait.cz/wp-content/uploads/2020/10/r8-1.pdf>. [cit. 2025-02-05].
- [47] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Dokumenty a odkazy – Dokumenty k měkkým cílům: *Bezpečnostní plán měkkého cíle*. Online. In: Ministerstvo vnitra České republiky. Dostupné z: <https://mv.gov.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx>. [cit. 2025-02-15].
- [48] LUKÁŠ, Luděk a kolektiv, 2013. *Bezpečnostní technologie, systémy a management III*. Zlín: VeRBuM.. ISBN 978-80-87500-35-4
- [49] LUKÁŠ, Luděk a kolektiv, 2011. *Bezpečnostní technologie, systémy a management I*. Zlín: VeRBuM.. ISBN 978-80-87500-05-7
- [50] POLICIE ČESKÉ REPUBLIKY, *Mapa kriminality*, Online. Dostupné z: <https://kriminalita.policie.gov.cz/> [cit. 2025-04-30]
- [51] EUROPEAN COMMISSION. *Action Plan to Support the Protection of Public Spaces*. Online. In: EUR-Lex – Přístup k právu Evropské unie. Brusel: Evropská komise, 2017. Dostupné z: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0612> [cit. 2025-04-29]

## SEZNAM OBRÁZKŮ

|                                                                                      |    |
|--------------------------------------------------------------------------------------|----|
| Obrázek 1 Výstup metody ETA.....                                                     | 26 |
| Obrázek 2 Výstup metody FTA.....                                                     | 27 |
| Obrázek 3 Kritéria ovlivňující atraktivitu měkkého cíle .....                        | 39 |
| Obrázek 4 Dělení měkkých cílů z hlediska zdroje nebezpečí .....                      | 40 |
| Obrázek 5 Cyklus efektivního bezpečnostního systému .....                            | 41 |
| Obrázek 6 Časové fáze incidentu.....                                                 | 42 |
| Obrázek 7 Souvztažnost koeficientů $K_{ARI}$ a $K_{PRI}$ pro $R_i$ .....             | 64 |
| Obrázek 8 Vstup do objektu ze dvora.....                                             | 68 |
| Obrázek 9 PZTS u vstupu ze dvora .....                                               | 68 |
| Obrázek 10 Vstupní hala z pohledu od dvora a schody do II. podlaží .....             | 69 |
| Obrázek 11 Vstupní hala z pohledu od hlavních vstupních dveří .....                  | 70 |
| Obrázek 12 Výťah ve vstupní hale a dveře do suterénu.....                            | 70 |
| Obrázek 13 Dveře k prostoru ke vstupu od dvora a pohybové čidlo.....                 | 71 |
| Obrázek 14 Pohybové čidlo u hlavního vchodu .....                                    | 72 |
| Obrázek 15 Chodba II. podlaží .....                                                  | 73 |
| Obrázek 16 Výťah a hlavní schodiště na II. podlaží .....                             | 74 |
| Obrázek 17 Veřejné toalety na II. podlaží .....                                      | 75 |
| Obrázek 18 Vstupní dveře do čekárny registru silničních vozidel .....                | 76 |
| Obrázek 19 Čekárna registru silničních vozidel 1 .....                               | 76 |
| Obrázek 20 Čekárna registru silničních vozidel 2 .....                               | 77 |
| Obrázek 21 Kamera v čekárně II. podlaží .....                                        | 77 |
| Obrázek 22 Vstup do suterénu zájmového objektu skrze hlavní schodiště .....          | 78 |
| Obrázek 23 Vstup do suterénu bočními dveřmi z I. podlaží .....                       | 79 |
| Obrázek 24 Sklep zájmového objektu 1 .....                                           | 79 |
| Obrázek 25 Sklep zájmového objektu 2 .....                                           | 80 |
| Obrázek 26 Sklep zájmového objektu 3 .....                                           | 81 |
| Obrázek 27 Dveře ke zkušební místnosti, zkušebnímu komisaři a provozování autoškol.. | 82 |
| Obrázek 28 Chodba ke zkušební místnosti, zkušebnímu komisaři a provozování autoškol  | 82 |
| Obrázek 29 Čekárna registru řidičů na III. podlaží .....                             | 83 |
| Obrázek 30 Schodiště vedoucí z III. do IV. podlaží .....                             | 84 |
| Obrázek 31 Chodba IV podlaží. a zaměstnanecké toalety.....                           | 85 |
| Obrázek 32 Umístění výťahu na IV. podlaží.....                                       | 85 |
| Obrázek 33 Čekárna vedení odboru.....                                                | 86 |
| Obrázek 34 Místnost zástupce vedoucího odboru 1 .....                                | 87 |

|                                                        |    |
|--------------------------------------------------------|----|
| Obrázek 35 Místnost zástupce vedoucího odboru 2 .....  | 87 |
| Obrázek 36 Přestupková místnost č. 1 .....             | 88 |
| Obrázek 37 Rohová místnost se dvěma pracovišti 1 ..... | 89 |
| Obrázek 38 Rohová místnost se dvěma pracovišti 2 ..... | 89 |
| Obrázek 39 Přestupková místnost č. 2 .....             | 90 |
| Obrázek 40 Tísňové tlačítko .....                      | 91 |
| Obrázek 41 PZTS v kanceláři vedoucího odboru .....     | 91 |

**SEZNAM TABULEK**

|                                                                  |     |
|------------------------------------------------------------------|-----|
| Tabulka 1 Stupnice hodnocení rizik .....                         | 28  |
| Tabulka 2 Stupnice hodnocení hrozeb .....                        | 28  |
| Tabulka 3 Stupnice hodnocení zranitelnosti .....                 | 28  |
| Tabulka 4 Dopad dle názoru hodnotitele .....                     | 31  |
| Tabulka 5 Stanovená škála míry rizika .....                      | 31  |
| Tabulka 6 Výčet souvztažnosti rizik .....                        | 32  |
| Tabulka 7 Vyplněná diagonála .....                               | 33  |
| Tabulka 8 Konečný tvar tabulky .....                             | 33  |
| Tabulka 9 Koeficienty aktivity a pasivity .....                  | 34  |
| Tabulka 10 Aplikovaná metoda PNH .....                           | 60  |
| Tabulka 11 Poupravená škála míry rizika .....                    | 61  |
| Tabulka 12 Koeficient aktivity a pasivity pro rizika 1–11 .....  | 63  |
| Tabulka 13 Koeficient aktivity a pasivity pro rizika 12–22 ..... | 63  |
| Tabulka 14 Koeficient aktivity a pasivity pro rizika 23–33 ..... | 63  |
| Tabulka 15 Koeficient aktivity a pasivity pro rizika 34–44 ..... | 63  |
| Tabulka 16 Technická opatření .....                              | 99  |
| Tabulka 17 Fyzická bezpečnost a školení .....                    | 99  |
| Tabulka 18 Protipožární a krizová opatření .....                 | 99  |
| Tabulka 19 Školení, duševní zdraví a hygienická opatření .....   | 100 |
| Tabulka 20 Celkový odhad nákladů .....                           | 100 |

**SEZNAM ROVNIC**

|                                                                      |    |
|----------------------------------------------------------------------|----|
| Rovnice 1 Výpočet metody Posuzování nebezpečí a hodnocení rizik..... | 31 |
| Rovnice 2 Vyplnění tabulky souvztažnosti.....                        | 33 |
| Rovnice 3 Koeficient aktivity rizik.....                             | 34 |
| Rovnice 4 Koeficient pasivity rizik .....                            | 34 |
| Rovnice 5 Výpočet osy $O_1$ .....                                    | 35 |
| Rovnice 6 Výpočet osy $O_2$ .....                                    | 35 |

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

|            |                                                |
|------------|------------------------------------------------|
| EKV        | Elektronická kontrola vstupu                   |
| ETA        | Analýza stromu událostí                        |
| FTA        | Analýza stromu poruchových stavů               |
| GDPR       | Obecné nařízení o ochraně osobních údajů       |
| checklist  | Kontrolní seznam                               |
| KARS       | Kritická analýza rizikových scénářů            |
| $K_{AR_i}$ | Koeficient aktivity rizika                     |
| Koncepce   | Koncepce ochrany měkkých cílů z roku 2017–2020 |
| $K_{PR_i}$ | Koeficient pasivity rizika                     |
| MC         | Měkké cíle                                     |
| MP         | Městská policie                                |
| MV         | Ministerstvo vnitra                            |
| např.      | Například                                      |
| ORP        | Obec s rozšířenou působností                   |
| PČR        | Policie České republiky                        |
| PZTS       | Poplachové zabezpečovací a tísňové systémy     |
| SWIFT      | Strukturovaná technika co se stane, když       |
| tzn.       | To znamená                                     |
| tzv.       | Takzvaný                                       |
| VSS        | Dohledové videosystémy                         |

**SEZNAM PŘÍLOH**

Příloha P I: Vyplněná tabulka souvztažnosti rizik (část A)

Příloha P II: Vyplněná tabulka souvztažnosti rizik (část B)



|    |                                               |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|----|-----------------------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | Nedostatečné materiální nebo technické zázemí | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 15 | Chybná krizová komunikace                     | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 16 | Kybernetický útok                             | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| 17 | Nezabezpečená síťová infrastruktura           | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| 18 | Ztráta nebo poškození dat                     | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 19 | Požár technického původu                      | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| 20 | Výpadek elektrické energie                    | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 |
| 21 | Výpadek dodavatelských služeb                 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| 22 | Panika klientů                                | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 23 | Psychický nátlak nebo vyhoření personálu      | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 24 | Neoprávněné natáčení či šíření dezinformací   | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| 25 | Ztráta důvěry veřejnosti                      | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 26 | Únik osobních údajů                           | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |
| 27 | Vichřice nebo tornádo                         | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| 28 | Povodně nebo přívalové deště                  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |

|    |                                           |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|----|-------------------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 29 | Extrémní mrazy/námraza                    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| 30 | Extrémní vedra a sucha                    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| 31 | Dlouhodobý déšť a blesky                  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |   |
| 32 | Sesuvy půdy, propady, zemětřesení         | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 |
| 33 | Znečištění ovzduší                        | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 34 | Epidemie nebo pandemie                    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 35 | Biologická kontaminace prostor            | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 36 | Dopravní havárie s únikem toxických látek | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 |
| 37 | Výbuch v blízkosti úřadu                  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| 38 | Hromadná dopravní nehoda                  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 39 | Destrukce stavebních prvků                | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| 40 | Výpadek telekomunikačních spojení         | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 41 | Mechanické poškození zařízení             | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| 42 | Politické změny                           | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 43 | Migrační vlna                             | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |

|    |                              |   |   |   |    |    |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|------------------------------|---|---|---|----|----|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 44 | Náhlý výpadek klíčových osob | 0 | 0 | 0 | 0  | 1  | 0 | 0  | 1  | 1  | 1  | 1  | 0  | 1  | 1  | 1  | 0  | 1  | 1  | 0  | 0  | 1  | 1  | 1  | 0  |
| Σ  |                              | 9 | 7 | 6 | 13 | 23 | 8 | 11 | 20 | 28 | 12 | 34 | 22 | 14 | 30 | 35 | 10 | 14 | 24 | 16 | 24 | 27 | 31 | 25 | 14 |

## ŘÍLOHA P II: VYPLNĚNÁ TABULKA SOUVZTAŽNOSTI RIZIK (ČÁST B)

|    | Riziko                                | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | Σ  |
|----|---------------------------------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1  | Fyzický útok jednotlivce nebo skupiny | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 18 |
| 2  | Ozbrojený útok                        | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 26 |
| 3  | Teroristický útok                     | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 34 |
| 4  | Krádež vybavení nebo dokumentů        | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 13 |
| 5  | Sabotáž                               | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 1  | 27 |
| 6  | Žhářství                              | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 0  | 1  | 1  | 1  | 1  | 0  | 0  | 17 |
| 7  | Vandalismus                           | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 8  |
| 8  | Přetížení kapacity                    | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 12 |
| 9  | Nezvládnutá evakuace                  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 10 |
| 10 | Nedostatečně vyškolený personál       | 1  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 15 |
| 11 | Selhání bezpečnostních protokolů      | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 1  | 1  | 0  | 0  | 0  | 23 |
| 12 | Vniknutí nepovolané osoby             | 0  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 1  | 0  | 0  | 0  | 22 |
| 13 | Nedostatek personálu                  | 1  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 0  | 1  | 0  | 0  | 0  | 1  | 12 |

|    |                                               |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |    |
|----|-----------------------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|
| 14 | Nedostatečné materiální nebo technické zázemí | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 11 |
| 15 | Chybná krizová komunikace                     | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 14 |
| 16 | Kybernetický útok                             | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 14 |
| 17 | Nezabezpečená síťová infrastruktura           | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 11 |
| 18 | Ztráta/poškození dat                          | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 9  |
| 19 | Požár technického původu                      | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 15 |
| 20 | Výpadek elektrické energie                    | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 15 |
| 21 | Výpadek dodavatelských služeb                 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 12 |
| 22 | Panika klientů                                | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 9  |
| 23 | Psychický nátlak/vyhoření personálu           | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 17 |
| 24 | Neoprávněné natáčení či šíření dezinformací   | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 9  |
| 25 | Ztráta důvěry veřejnosti                      | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 11 |
| 26 | Únik osobních údajů                           | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 14 |
| 27 | Vichřice/tornádo                              | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 22 |
| 28 | Povodně/přívalové deště                       | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 21 |

|    |                                           |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |    |
|----|-------------------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|
| 29 | Extrémní mrazy/námraza                    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 14 |
| 30 | Extrémní vedra a sucha                    | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 16 |
| 31 | Dlouhodobý déšť a blesky                  | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 14 |
| 32 | Sesuvy půdy, propady, zemětřesení         | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 19 |
| 33 | Znečištění ovzduší                        | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 7  |
| 34 | Epidemie/pandemie                         | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 14 |
| 35 | Biologická kontaminace prostor            | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 13 |
| 36 | Dopravní havárie s únikem toxických látek | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 16 |
| 37 | Výbuch v blízkosti úřadu                  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 19 |
| 38 | Hromadná dopravní nehoda                  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 9  |
| 39 | Destrukce stavebních prvků                | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 20 |
| 40 | Výpadek telekomunikačních spojení         | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 13 |
| 41 | Mechanické poškození zařízení             | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 14 |
| 42 | Politické změny                           | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 19 |
| 43 | Migrační vlna                             | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 9  |

|    |                              |    |    |   |   |   |   |   |   |    |   |    |    |    |    |    |    |    |    |   |    |    |
|----|------------------------------|----|----|---|---|---|---|---|---|----|---|----|----|----|----|----|----|----|----|---|----|----|
| 44 | Náhlý výpadek klíčových osob | 1  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0  | 0 | 0  | 0  | 0  | 0  | 0  | 1  | 1  | 1  | 0 | 0  | 17 |
| Σ  |                              | 18 | 17 | 0 | 2 | 0 | 0 | 3 | 6 | 10 | 5 | 16 | 11 | 13 | 12 | 10 | 24 | 21 | 14 | 9 | 25 |    |