

# Bezpečnostní prostředí v kontextu ochrany měk- kých cílů

Dominik Vávra

---

Bakalářská práce  
2020



Univerzita Tomáše Bati ve Zlíně  
Fakulta logistiky a krizového řízení

---

# Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav ochrany obyvatelstva

Akademický rok: 2019/2020

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE (projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: **Dominik Vávra**  
Osobní číslo: **L17422**  
Studijní program: **B2825 Ochrana obyvatelstva**  
Studijní obor: **Ochrana obyvatelstva**  
Forma studia: **Prezenční**  
Téma práce: **Bezpečnostní prostředí v kontextu ochrany měkkých cílů**

### Zásady pro vypracování

1. Seznamte se s teoretickými základy problematiky měkkých cílů a jejich ochrany.
2. Zvolte konkrétní objekt představující měkký cíl.
3. Realizujte analýzu rizik zvoleného měkkého cíle se zaměřením na zvolené násilné útoky.
4. Vyhodnoťte současný stav zabezpečení před násilnými útoky a navrhněte případná opatření ke zvýšení bezpečnosti.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam doporučené literatury:

1. KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti České republiky, 2014, 390 s. ISBN 9788026071150.
2. VALOUCH, Jan. *Projektování integrovaných systémů*. Vydání druhé. Zlín: Univerzita Tomáše Bati ve Zlíně, 2015, 1 online zdroj (169 stran). ISBN 9788074545573.
3. HESTERMAN, Jennifer L. *Soft target hardening: protecting people from attack*. Second Edition. London: Routledge, Taylor & Francis Group, 2019, xxvi, 460 s. ISBN 9781138391109.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce:

**Ing. Jakub Rak, Ph.D.**  
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: 1. listopadu 2019  
Termín odevzdání bakalářské práce: 15. května 2020

L.S.

---

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

---

**prof. Ing. Dušan Vičar, CSc.**  
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2019

## PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užit své dílo – bakalářskou 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 bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považuji 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 15. 5. 2020

Jméno a příjmení studenta: Dominik Vávra

.....  
podpis studenta

## **ABSTRAKT**

Tato bakalářská práce je zaměřena na problematiku zabezpečení měkkých cílů. V teoretické části práce jsou uvedeny základní informace o měkkých cílech, bezpečnostních systémech a základní pojmy. V praktické části se nachází popsaný objekt Academic School v Uherském Hradišti a dále metody a analýzy na něj aplikované jako SWOT a KARS. Praktická část je zakončena kapitolou věnující se možným opatřením, které představují zlepšení systému zabezpečení tohoto objektu.

Klíčová slova: měkké cíle, SWOT, analýza, zabezpečení, KARS

## **ABSTRACT**

This bachelor thesis is focused on the issue of the soft targets security. The theoretical part of the thesis contains basic informations about soft targets, security systems and basic concepts. In the practical part there is described object Academic school in Uherské Hradiště and methods and analyzes applied to this object including SWOT and KARS. The practical part is ended with a chapter of possible measurements that can improve the security systém of this object.

Klíčová slova: soft targets, SWOT, analysis, security, KARS

Mé poděkování patří vedoucímu mé bakalářské práce panu Ing. Jakubu Rakovi, Ph.D., jehož cenné rady byly vždy obrovským přínosem. Velký dík patří také mé rodině, přítelkyni a přátelům za jejich trpělivost, cenné rady a podporu po celou dobu mého studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

# OBSAH

<b>ÚVOD</b> .....	<b>9</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>10</b>
<b>1 MĚKKÉ CÍLE</b> .....	<b>11</b>
1.1 PRÁVNÍ PŘEDPISY A DOKUMENTY SOUVISEJÍCÍ S PROBLEMATIKOU OCHRANY MĚKKÝCH CÍLŮ V ČESKÉ REPUBLICE .....	13
1.1.1 Základy ochrany měkkých cílů – metodika (1. verze).....	13
1.1.2 Koncepce ochrany měkkých cílů .....	13
1.1.3 Norma ČSN 73 4400 Prevence kriminality – řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení.....	14
<b>2 BEZPEČNOSTNÍ SYSTÉMY</b> .....	<b>15</b>
2.1 MECHANICKÉ ZÁBRANNÉ SYSTÉMY .....	15
2.2 ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE .....	17
2.2.1 Hlásiče požáru .....	18
2.2.2 Hlásiče kouře ionizační .....	19
2.2.3 Hlásiče kouře optické .....	19
2.2.4 Hlásiče teplot.....	20
2.2.5 Hlásiče plamene .....	21
2.2.6 Ústředny elektrické požární signalizace.....	21
2.3 POPLACHOVÉ ZABEZPEČOVACÍ A TÍŠŇOVÉ SYSTÉMY.....	22
2.3.1 Prvky používané v poplachových zabezpečovacích a tísňových systémech .....	23
2.4 CCTV SYSTÉMY.....	24
2.4.1 Norma ČSN EN 50132.....	26
2.4.2 ČSN EN 50132 – 1 – Systémové požadavky .....	26
2.4.3 ČSN EN 50132 – 5 – Přenos videosignálu .....	27
2.4.4 ČSN EN 50132 – 7 – Pokyny pro aplikaci .....	28
<b>3 ZÁKLADNÍ POJMY</b> .....	<b>30</b>
<b>II PRAKTICKÁ ČÁST</b> .....	<b>32</b>
<b>4 CÍLE A METODY PRÁCE</b> .....	<b>33</b>
<b>5 ZABEZPEČENÍ MĚKKÝCH CÍLŮ</b> .....	<b>34</b>
5.1 ACADEMIC SCHOOL, MATEŘSKÁ A ZÁKLADNÍ ŠKOLA, S.R.O. ....	34
5.2 STÁVAJÍCÍ ZABEZPEČENÍ ŠKOLSKÉHO ZAŘÍZENÍ .....	36
5.2.1 Vyhodnocení stávajícího zabezpečení prostor Academic School, Mateřské a základní školy, s.r.o. v Uherském Hradišti.....	45
<b>6 ANALÝZA RIZIK</b> .....	<b>46</b>
6.1 KVALITATIVNÍ ANALÝZA RIZIK S VYUŽITÍM JEJICH SOUVZTAŽNOSTI (KARS) .....	46
6.2 METODA SWOT ANALÝZY .....	52
<b>7 NÁVRH MOŽNÝCH OPATŘENÍ</b> .....	<b>57</b>
<b>ZÁVĚR</b> .....	<b>60</b>

<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>61</b>
<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>64</b>
<b>SEZNAM OBRÁZKŮ .....</b>	<b>65</b>
<b>SEZNAM TABULEK.....</b>	<b>66</b>
<b>SEZNAM PŘÍLOH.....</b>	<b>67</b>



## ÚVOD

V posledních letech je problematika zabezpečení měkkých cílů velmi diskutovaným tématem. Jejich ochrana je obtížná z mnoha důvodů, mezi které patří především vysoká koncentrace osob a nízká míra jejich kontroly. Potenciální útočníci jsou s tímto faktem dobře seznámeni a vybírají si proto často za cíl svého útoku právě měkký cíl.

Tato bakalářská práce se zabývá právě zabezpečením měkkých cílů, mezi které se řadí například školská zařízení, kina, divadla, obchodní centra nebo demonstrace. Každý z měkkých cílů by měl mít alespoň nějakou míru zabezpečení a základními prvky, kterými se často tato bezpečnost zajišťuje jsou například fyzická ostraha, elektrická požární signalizace, mechanické zábranné systémy, uzavřené kamerové okruhy, poplachové zabezpečovací a tísňové systémy.

Útoky na měkké cíle přichází neočekávaně a jejich následky jsou většinou právě díky vysoké koncentraci osob kritické. Vlastníci či provozovatelé měkkých cílů by tedy měli věnovat prioritní pozornost jejich zabezpečení, a tedy bezpečnosti osob uvnitř měkkého cíle. V případě vyskytnutí útoku by všichni zúčastnění měli vědět, jakým způsobem se zachovat, aby byly v největší možné míře odvráceny negativní důsledky tohoto útoku.

Cílem bakalářské práce je seznámení se s teoretickými základy ochrany měkkých cílů a zabezpečovacích systémů, zvolení a konkretizace vybraného měkkého cíle, analýza rizik pro tento měkký cíl s prioritním zaměřením na násilné útoky a následné navržení možných opatření ke zvýšení míry jeho bezpečnosti.

## I. TEORETICKÁ ČÁST

## 1 MĚKKÉ CÍLE

Pro název měkké cíle (anglicky Soft Targets) prozatím neexistuje přesná a jednohlasně přijímaná definice, avšak obecně se termín měkký cíl dá popsat jako místo, které se vyznačuje vysokou koncentrací osob a zároveň disponuje nízkou mírou zabezpečení proti násilným útokům. Tyto místa jsou pro útočníky při výběru terče útoku lákavé a výhodné z mnoha důvodů. Jedním z hlavních důvodů je to, že není očekáván odpor ze strany civilistů a v případě úspěšného provedení je také zaručena vysoká míra obětí. Měkké cíle konkrétně mohou být například:

- tržišť, obchodní komplexy, nákupní centra,
- školská zařízení,
- divadla, kina, koncertní sály,
- restaurace, hotely, bary,
- nemocnice
- sportovní haly a stadiony,
- průvody, demonstrace atd.

Přímým protějškem měkkých cílů jsou místa, která nazýváme tvrdé cíle (anglicky Hard Targets). Tyto místa oproti měkkým cílům disponují vysokou mírou zabezpečení proti útokům a tím jsou pro útočníky méně atraktivní. Mezi tvrdé cíle můžeme řadit například vojenské objekty, některé státní objekty, objekty dalších bezpečnostních složek atd. [1, 5, 8]

Měkké cíle můžeme rozdělovat na:

- trvalé,
- dočasné.

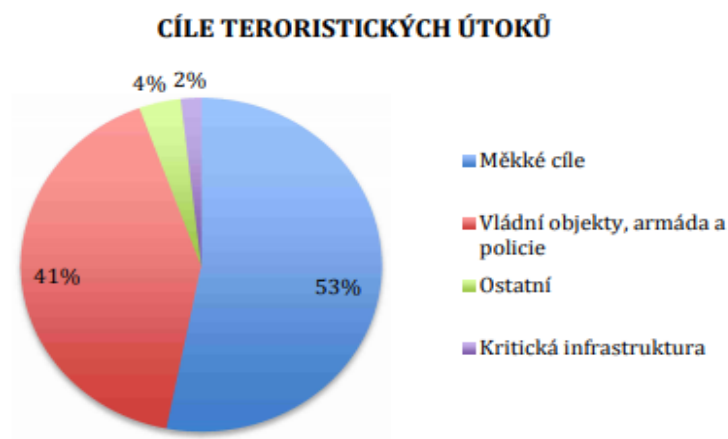
Trvalé měkké cíle můžeme dále dělat na:

- vnitřní (např. divadla, nákupní centra, nemocnice),
- venkovní (např. tržišť, stadiony a další sportoviště).

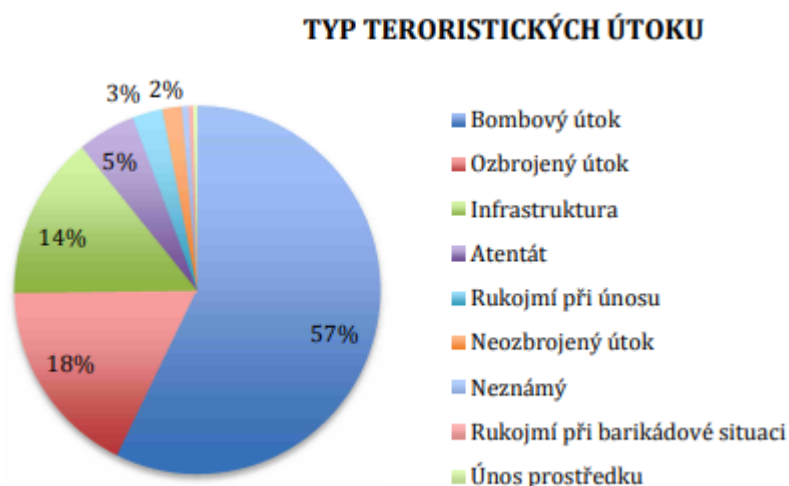
Za dočasné měkké cíle můžeme považovat shromáždění, které se mohou konat jak na soukromém, tak na veřejném pozemku. Lze je dále dělit na:

- dočasné akce s volným vstupem (např. trhy, maratony, demonstrace),
- dočasné placené akce (např. koncerty, festivaly). [6]

Nejen díky rozmachu terorismu ve světě z posledních let, se do popředí právem dostala i problematika ochrany měkkých cílů. Velké ohrožení měkkých cílů především terorismem dokazuje analýza teroristických útoků. Data pro analýzu se sbírala 16 let od roku 1998 v rámci evropského kontinentu a zahrnuje 5297 údajů. Data z analýzy jsou znázorněna na níže uvedených obrázcích (viz Obrázek 1-2) v podobě cílů a typů provedení teroristických útoků a z obrázku je patrné, že nejohroženější skupinou teroristickými útoky jsou měkké cíle a je nutné klást důraz na jejich ochranu. Z obrázků můžeme také vyvodit, proti jakým typům provedení útoku je nutné tuto ochranu přednostně směřovat. [5, 7]



Obrázek 1 - Cíle teroristických útoků [5]



Obrázek 2 - Typy teroristických útoků [5]

## **1.1 Právní předpisy a dokumenty související s problematikou ochrany měkkých cílů v České republice**

Jelikož v České republice zatím neexistuje žádný samostatný zákon, který by se věnoval primárně problematice ochrany měkkých cílů, je potřeba při jejich ochraně vycházet z metodik, strategií, koncepcí a norem. Mezi nejzákladnější dokumenty, které řeší problematiku ať už ochrany měkkých cílů nebo s ní úzce spjatým terorismem, patří:

- Základy ochrany měkkých cílů – metodika (1. verze),
- Koncepce ochrany měkkých cílů,
- Norma ČSN 73 4400 Prevence kriminality – řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení,
- Bezpečnostní strategie České republiky,
- Strategie České republiky pro boj proti terorismu. [3]

### **1.1.1 Základy ochrany měkkých cílů – metodika (1. verze)**

Tato metodika je založena prioritně na násilné činy s velkou mírou závažnosti a ochranu proti nim. Je možné tuto metodiku použít pro teroristické útoky i pro násilné útoky, které nejsou považovány za teroristické, jako například útoky extremistů nebo osobní útoky (narušený žák atd.). Tento dokument se zaměřuje na zmírnění dopadů takových činů, ale i na prevenci proti nim. Obsahem metodiky je také charakteristika a definice termínu „měkké cíle“, principy jejich zabezpečení, druhy bezpečnostních opatření, základní kategorie bezpečnostních prvků a doporučení pro zvýšení odolnosti měkkých cílů. Dokument je dostupný veřejnosti na internetových stránkách ministerstva vnitra a byl zpracován Institutem ochrany měkkých cílů, který byl založen roku 2015 v Praze. Jedná se o první soukromou společnost, která se zabývá problematikou měkkých cílů v České republice. [3, 8, 10]

### **1.1.2 Koncepce ochrany měkkých cílů**

Tento dokument schválila vláda v roce 2016 a jeho platnost je pro roky 2017-2020. Cílem Koncepce ochrany měkkých cílů je vytvoření fungujícího národního systému ochrany měkkých cílů, s jehož pomocí bude možné rychle, komplexně a pružně reagovat na hrozbu tero-

ristických či násilných útoků. Dále je cílem co nejvíce měkkých cílů v České republice připravit tak, aby při útoku byly škody mnohonásobně nižší, než kdyby je útok postihl nepřipravené. Obsahem dokumentu je charakteristika měkkých cílů, principy a právní prostředí jejich ochrany, současný stav ochrany měkkých cílů v České republice, příklady útoků na měkké cíle, pilíře systému jejich ochrany a návrhy opatření k jejich ochraně. [3, 6, 10]

### **1.1.3 Norma ČSN 73 4400 Prevence kriminality – řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení**

Tato norma z oblasti prevence kriminality se věnuje problematice ochrany konkrétního měkkého cíle a tím jsou školská zařízení. Cílem této normy je posouzení rizik kriminálního a antisociálního chování a posouzení bezpečnostních opatření. Jejím obsahem jsou pomůcky pro správné koncepční řešení bezpečnosti školských zařízení při jejich stavbách nebo rekonstrukcích. Normu ČSN 73 4400 je možné využít pro všechny druhy škol, jako jsou soukromé školy, veřejné školy či jiné státní instituce. Na stavby vysokých škol se norma nevztahuje, je však možné ji využít jako návod k řízení rizik a prevenci kriminality. Tuto normu zpracovala Technická normalizační komise 148 v roce 2016. [3, 17, 23]

## 2 BEZPEČNOSTNÍ SYSTÉMY

Již od počátků lidské společnosti bylo jedním ze základních potřeb lidstva zajištění bezpečnosti ať už osob, nebo majetku. Postupem času se tyto bezpečnostní systémy vyvíjely ruku v ruce s vývojem technologií, ale i nových hrozeb, jako je dnes například terorismus. Snaha zajistit bezpečí životů a majetku je tedy i dnes pro většinu lidstva prioritou. K dosažení tohoto cíle lidstvu slouží bezpečnostní systémy, které dnes můžeme dělit do několika skupin.

Mezi nejpoužívanější bezpečnostní systémy dnešní doby patří:

- MZS (Mechanické zábranné systémy),
- EPS (Elektrická požární signalizace),
- PZTS (Poplachový zabezpečovací a tísňový systém),
- CCTV systémy (Uzavřený televizní okruh – Closed Circuit Television). [12]

### 2.1 Mechanické zábranné systémy

Mechanické zábranné systémy jsou jedním z nejstarších a nyní jedním z nejdůležitějších bezpečnostních systémů vůbec, obzvláště pro zabezpečení objektů. Z dávných dob můžeme tyto systémy znát jako ohrady z větví pro dobytek, palisádová opevnění, ploty nebo zajištění vchodů do obydlí. Dnes je pro nás setkávání se s těmito systémy každodenní rutinou, lze tedy říci, že mechanické zábranné systémy tvoří základní prvek ochrany bytových ale i nebytových prostor. Podstatou mechanických zábranných systému je to, že doba, kterou pachatel stráví jejich překonáváním je mnohdy pro pachatele neúnosná, proto pokus o prolomení vzdá.

Úkolem mechanických zábranných systémů je tedy ztížení, zpomalení nebo úplné zabránění násilnému vniknutí nepovolané osoby do chráněného prostoru či manipulace s chráněným předmětem. [15]

Dělení MZS:

- obvodová ochrana – zde patří visací zámky, ploty, zdi a jejich průchody,
- objektová ochrana (plášťová) – dveře, okna,
- individuální ochrana (předmětová) – mříže, zámky, trezory,
- speciální ochrana – chemická ochrana: (prášky, laky), ostatní ochrana: (pečetě, plomby).

Prolomit lze každý zábranný systém a úkolem mechanických zábranných systémů je dobu tohoto prolomení posunout do pásma bezpečnosti. Hodnotu prolomení mechanických zábranných systémů ovlivňují tyto faktory:

- kvalita mechanických zábranných systémů,
- využití energetických zdrojů,
- znalost konstrukce překonávaného mechanického zábranného systému,
- poloha mechanického zábranného systému,
- kvalita a druh techniky použité k prolomení.

Násilnému vniknutí do objektu lze těžko zabránit výhradně díky tomu, že nelze určit přesný čas, kdy k němu dojde. Je tedy nutné toto riziko minimalizovat na únosnou úroveň, k tomu nám mohou sloužit jednoduché preventivní úkony, např.:

- být informován o kriminalitě v okolí bydliště,
- osvětlení chodeb v objektu, zamykání vstupních dveří do objektu,
- v případě potřeby (odcizení klíčů, ztráta klíčů, nastěhování) vždy vyměnit zámkovou vložku,
- pojištění majetku,
- osoby v objektu seznamovat s tímto nebezpečím a nabádat je k obezřetnosti,
- velkou pozornost věnovat oknům, bytovým dveřím, lodžii, balkonům. [15]

K chápání důležitosti a nezbytnosti MZS k ochraně osob a majetku nám slouží následující tabulka zahrnující metody prolomení vstupních dveří a ochranu proti nim:

Tabulka 1 – Metody překonání vstupních dveří a ochrana proti nim [15]

Metoda	Ochrana
<b>Rozlomení vložky zámku</b>	Protizlomová vložka nebo bezpečnostní kování
<b>Odvrtání vložky zámku</b>	Kování s ocelovou krytkou vložky
<b>Otevření planžetou</b>	Bezpečnostní vložka s překrytým profilem nebo s klíčem s důlky
<b>Roztažení dveřního rámu</b>	Vyplnění prostoru rámu betonem



<b>Prokopnutí dveří</b>	Oplechování vnitřní strany dveří
<b>Vysazení dveří</b>	Zábrany vysazení závěsů (pantů)
<b>Vyháčkování dvoukřídlých dveří</b>	Zajištění západek neotvíraného křídla šrouby, kolíky, vzpěrou
<b>Nasazení páčidla</b>	Obití rámu dveří z vnější strany kovovým profilem k zakrytí škvíry mezi rámem a dveřmi
<b>Vyražení dveří</b>	Zpevnění zárubně ocelovým pásem podél celého obvodu dveří

## 2.2 Elektrická požární signalizace

System elektrické požární signalizace je jedním z nejdůležitějších prvků budovy v oblasti bezpečnosti staveb. Jeho důležitost nám dokazují i čísla, která nám říkají, že v ČR každoročně požár zahubí okolo 100 osob a další stovky zraní. Přímé materiální škody poté dosahují řádu miliard korun. Největší přínos systému EPS spočívá v jeho schopnosti požár detekovat většinou rychleji než člověk a také ve schopnosti rychle předat informace složkám zajišťujícím zásah. Zkrácením této doby mezi začátkem požáru a upozorněním na něho tedy může evakuace osob z budovy stejně jako zásah jednotek integrovaného záchranného systému začít mnohem dříve a tím i minimalizovat škody jak na životech, tak na majetku. [11, 14]

Konfiguraci systému EPS tvoří:

- hlásiče požáru,
- ústředna EPS,
- signalizační a doplňující zařízení.

Pro splnění základních funkcí systému EPS jsou potřebné hlásiče požáru a ústředna EPS, jejichž spojení se nazývá požární smyčka nebo také hlásicí linka. Požadavky na systémy EPS specifikuje norma ČSN EN 54, ve které se dále probírají postupy zkoušení a technické požadavky.

Systémy EPS můžeme dělit do dvou skupin, a to dle schopnosti identifikace místa požáru. Jsou to systémy:

- s kolektivní adresací,
- s individuální adresací.

Základním rozdílem mezi těmito skupinami je schopnost přesné identifikace místa požáru. Systémy EPS s kolektivní adresací, které jsou schopny rozlišit pouze signál požár, už nedokáží dále určit, ze kterého hlásiče tento signál přišel, je tedy nemožné určit přesné místo požáru. Tento systém se již v dnešní době považuje za nedostatečný.

Systémy EPS s individuální adresací se pyšní systémem, který dokáže rozlišit hlásiče na hlásicí lince a tím, na rozdíl od systémů EPS s kolektivní adresací, určit přesné místo vzniklého požáru. Dnešní EPS využívají obzvláště systém založený na datové komunikaci mezi ústřednou EPS a hlásiči požáru, přičemž požární smyčka zde má úlohu jako datová sběrnice, která tuto komunikaci umožňuje. [4, 14]

### 2.2.1 Hlásiče požáru

Hlásiče požáru jsou určeny k lokalizaci a identifikaci požáru ve stádiu jeho vzniku a jeho rozvoje. Základním rozdělením můžeme tyto hlásiče dělit do dvou typů, tj. hlásiče tlačítkové a hlásiče samočinné. Tlačítkové hlásiče a jejich funkce jsou založeny na jejich aktivaci zúčastněnou osobou, která sama požár vyhodnotí. Tyto hlásiče můžeme opět rozdělit do dvou typů a to:

- Hlásiče s nepřímou obsluhou, jejichž aktivace spočívá v rozbití skla nebo posunutí ochranného prvku hlásiče a dále zmáčknutí funkčního tlačítka hlásiče příslušnou osobou.
- Hlásiče s přímou obsluhou, jejichž aktivace spočívá na rozdíl od hlásičů s nepřímou obsluhou pouze v rozbití skla nebo posunutí ochranného prvku hlásiče.

Hlásiče samočinné na rozdíl od hlásičů tlačítkových vykonávají stejnou činnost, ovšem bez potřeby lidského činitele při aktivaci. Vyhodnocování vzniklých požárů je zde prováděno hlásiči samostatně pomocí zjištěného výskytu nebo změny fyzikálních jevů, které mají souvislost se vznikem požáru v místě instalace těchto hlásičů. Existují různé druhy těchto hlásičů a nejúčinnější metoda jejich rozdělení je právě dle těchto fyzikálních jevů. Samočinné požární hlásiče můžeme tedy rozdělit následovně: [14]

- hlásiče plynu,
- hlásiče teplot,
- hlásiče plamene,

- hlásiče multisenzorové,
- hlásiče kouře:
  - ionizační,
  - optické.

### 2.2.2 Hlásiče kouře ionizační

Plyny jsou za normálních okolností z velké části nevodivé, jsou tedy skvělé izolanty. Plyny se stávají při jejich malém množství iontů vodivé jen a okolností, které souvisí s nabýváním a udržováním těchto iontů, neboli ionizací plynu. K této ionizaci je tedy třeba neustálého vytváření a iontů, kterého lze docílit například:

- vysokou teplotou,
- radioaktivním zářením,
- elektrickým polem,
- elektromagnetickým zářením.

Hlásiče kouře ionizační jsou tedy pomocí tohoto principu založeny na vyhodnocování změny vodivosti plynů v detekční komůrce v důsledku přítomnosti neoxidovaných pevných částic kouře v komůrce. Tyto hlásiče je vhodné používat pro detekování požárů, které provádí vývin viditelných i neviditelných zplodin hoření. Uspokojivě reaguje i na zplodiny vytvářené žhnutím. Je nepoužitelný v případě výskytu kouře za běžných podmínek, v prostředí s výpary některých chemikálií, v prašném prostředí nebo v prostředí silně agresivním. [4, 14]

### 2.2.3 Hlásiče kouře optické

Pevné částice kouře uvolňované v průběhu požáru ovlivňují šíření světelného paprsku emitovaného skrz vrstvu vzduchu kontaminovaného kouřem. Na tomto principu jsou založeny optické hlásiče kouře a lze je využít k detekci požáru těmito způsoby:

- vyhodnocení pohlcování optického paprsku,
- vyhodnocení rozptylu optického paprsku.

Metoda vyhodnocení pomocí pohlcování optického paprsku je nejčastěji využívána u hlásičů kouře lineárních. Tyto hlásiče fungují na principu vyhodnocování změn intenzity záření vedeného zdrojem k přijímači v důsledku jeho pohlcením kouřem při průchodu kontrolovaným prostorem.

Hlásiče, které pro detekci požáru využívají metodu vyhodnocování rozptylu optického paprsku, bývají nejčastěji hlásiče bodové. Tyto hlásiče k detekci používají princip, při kterém dochází k rozptýlení paprsku v důsledku interakce pevných částic kouře a optického záření. Hlásič se skládá z detekční komůrky, ve které se nachází optický přijímač a zdroj optického záření. Tato komůrka je obehnaná lamelami, které zabraňují vpádu okolního světla do komůrky, avšak ponechávají možnost vniknutí kouře. Barva těchto lamel musí být z vnitřní části matně černá, kvůli schopnosti optického záření se v detekční komůrce odrážet a tím spouštět planý poplach. Optickým zdrojem v detekční komůrce je nejčastěji LED dioda konající v infračervené oblasti. Optický přijímač tvoří infračervený detektor. [4, 14]

#### 2.2.4 Hlásiče teplot

V souvislosti s vývojem prvků, které se užívají pro detekci požáru v systému elektrické požární signalizace, jsou nejstaršími prvky hlásiče teplot. Cely systém detekce je založený na principu sledování změn teplot na místě instalace, které jsou vyvolávány v důsledku uvolňování tepla při exotermickém charakteru reakce hoření. Tyto hlásiče lze rozdělit do dvou skupin:

- lineární hlásiče teplot,
- bodové hlásiče teplot.

U lineárních hlásičů teplot funguje systém detekce na bázi vyhodnocování modulační frekvence IR paprsku, který prochází z vysílače do přijímače, skrz kontrolovaný prostor. Dále lze tyto hlásiče dělit na lineární hlásiče teplot a na lineární hlásiče teplot liniového typu.

Lineární hlásiče teplot liniového typu můžeme dále dělit dle použitého teplocitlivého detekčního prvku následovně:

- hlásiče s optickým detekčním kabelem,
- hlásiče pneumatické,
- hlásiče s metalickým detekčním kabelem.

Hlásiče s metalickým detekčním kabelem můžeme dále rozdělit na digitální a analogové.

- Digitální lineární hlásiče fungují na principu vyhodnocování skokové změny odporu detekčního metalického kabelu díky zkratu vodičů detekčního kabelu.
- Analogové lineární hlásiče jsou, stejně jako digitální lineární hlásiče, tvořeny dvoužilovým vodičem. Zde se využívá situace, kdy použitá izolace žil ztrácí svou izolační

schopnost v důsledku zvýšení teplot. Zvýšení teploty detekčního kabelu způsobené požárem se dále projevuje nedokonalým zkratem mezi žilami vodiče. Po poklesu teploty se parametry detektoru většinou vrací do původních hodnot, tento jev je totiž do určité teploty reverzibilní. [14]

### 2.2.5 Hlásiče plamene

Tyto hlásiče lze s ohledem na jejich správnou instalaci a nastavení považovat za hlásiče s nejkratší dobou reakce na vzniklý požár ve smyslu rychlosti detekce. Dle konfigurace jsou to hlásiče bodového typu. Detekce požáru je u těchto hlásičů založena na principu vyhodnocování vlastností radiace plamene. Mezi vlastnosti, pomocí kterých probíhá detekce požáru, patří:

- spektrální charakter vyzařování,
- intenzita vyzařování,
- jejich časová proměnlivost.

Hlásiče plamene se mohou lišit v zaměření na konkrétní oblast vlnových délek elektromagnetického spektra. Dle tohoto zaměření je můžeme dělit na:

- infračervené (IR) hlásiče plamene,
- ultrafialové (UV) hlásiče plamene,
- kombinované (UV/IR) hlásiče plamene. [4, 14]

### 2.2.6 Ústředny elektrické požární signalizace

Ústřednu EPS lze považovat za nejdůležitější součást systému EPS. Ke správnému fungování všech prvků systému je třeba její nepřetržitá a bezchybná funkce. Aby byla tato podmínka splněna, musí ústředna EPS plnit tyto základní funkce:

- Kontrola provozuschopnosti systému – zde je třeba zabezpečovat tuto funkci:
  - automaticky – kontrola signalizačních, hlásicích linek a dalších komponentů systému,
  - manuálně – v testovacím režimu,
  - samočinně – za běžného provozu.
- Vyhodnocování a přijímání signálů z připojených hlásičů – provádění této funkce se odvíjí od druhu používaného systému, tj. zda se jedná o systém s individuální adresací nebo kolektivní adresací.

- Systém s kolektivní adresací – u tohoto systému se pro vyhodnocení a přenos signálu obvykle používá metoda vyhodnocení proudových změn v požární smyčce, nebo metoda vyhodnocení napěťových změn v požární smyčce.
- Systém s individuální adresací – zde je pro vyhodnocení a přenos signálu používáno datové komunikace mezi jednotlivými komponenty systému a ústřednou, vyhodnocování proudových impulzů generovaných hlásičem při komunikaci s ústřednou, nebo systém paralelní individuální adresace.
- Ovládání zařízení spojených se systémem EPS – u systémů s individuální adresací lze ovládání provádět pomocí ovládacích jednotek, které jsou zapojeny hlásičí linky, nebo lze využít jak v případě systémů s individuální, tak s kolektivní adresací potenciálové a bezpotenciálové výstupy ústředny.
- Neustálé napájení součástí systému EPS elektrickou energií – zde je využíváno hlavního, náhradního a záložního zdroje napájení.
- Indikace funkčních stavů systému optická i akustická – zde je minimální požadavek pro bezchybné fungování ústředny EPS schopnost akusticky a opticky indikovat tyto funkční stavy:
  - stav KLID,
  - stav PORUCHA,
  - stav POŽÁRNÍ POPLACH,
  - stav TEST,
  - stav VYPNUTO. [4, 14]

### 2.3 Poplachové zabezpečovací a tísňové systémy

Poplachové zabezpečovací a tísňové systémy (anglicky Intruder and Hold-up Alarm System – IaHAS) slouží k signalizaci nebezpečí v určeném objektu. PZTS slouží převážně k informaci o vniknutí do objektu, může ale sloužit i k signalizaci široké škály jiných nebezpečí, jako je například: [4, 11, 16]

- únik plynu,
- přepadení,
- zdravotní potíže,
- požární nebezpečí,
- zaplavení,

- jiné nebezpečí.

### 2.3.1 Prvky používané v poplachových zabezpečovacích a tísňových systémech

Jednotlivé prvky používané v poplachových zabezpečovacích a tísňových systémech můžeme dělit na:

- Prvky plášťové ochrany – určeny k monitorování destrukce či otevření plášťových prostorů budovy (např. dveře, okna).
  - Čidla na ochranu skleněných ploch,
  - mechanické kontakty,
  - čidla vibrační,
  - magnetické kontakty,
  - poplachové tapety a fólie,
  - rozpěrné tyče,
  - čidla drátová.
- Prvky prostorové ochrany – určeny k identifikaci nežádoucího pohybu narušitele ve střeženém prostoru.
  - Pasivní IR čidla,
  - aktivní IR čidla,
  - čidla mikrovlnná,
  - čidla ultrazvuková,
  - kombinovaná duální čidla.
- Prvky předmětové ochrany – slouží k identifikaci nežádoucího nakládání se střeženým předmětem.
  - Čidla na ochranu závěsných předmětů,
  - čidla otřesová,
  - kapacitní čidla.
- Speciální čidla.
  - Nášlapné koberce,
  - tlaková čidla.
- Prvky tísňové ochrany – tyto prvky slouží k provedení hlášení do místa, odkud může být poskytnuta pomoc v případě přímého ohrožení zaměstnanců či veřejnosti. [4, 11, 16]
  - Skryté tísňové hlásiče,

- veřejné tísňové hlásiče,
  - osobní tísňové hlásiče.
- Prvky venkovní obvodové (perimetrické) ochrany – tyto prvky jsou určeny k signalizaci narušení vnějších částí, především u rozlehlých objektů.
  - Zemní tlakové hadice,
  - štěrbinové kabely a mikrovlnné bariéry,
  - mikrofonicke kabely a IR závory a bariéry,
  - perimetrická pasivní infračervená čidla.
- Ovládací zařízení – tyto prvky jsou určeny primárně k uvádění systému do stavu klidu či střežení.
  - Propouštěcí a spínací zámky,
  - blokovací zámky,
  - ovládací a indikační díly,
  - kódové klávesnice.
- Přenosová zařízení – slouží ke zprostředkování informace o narušení objektu či o stavu systému.
  - Automatické telefonní voliče a hlásiče,
  - bezdrátová přenosová zařízení.
- Výstražná zařízení – prvky určeny k upozornění na poplachový stav.
  - Sirény,
  - zábleskový maják.
- Poplachové ústředny – centrální části poplachových systémů.
  - Ústředny s přímou adresací,
  - klasické smyčkové ústředny,
  - ústředny s bezdrátovým přenosem signálu od čidel,
  - ústředny smíšeného typu. [4,11,16]

## 2.4 CCTV systémy

CCTV systémy (Closed Circuit Television – uzavřený televizní okruh) můžeme v dnešní době potkávat stále častěji a častěji. Instalují se v rodinných domech, na úřadech, složitých křižovatkách, obchodních domech atd. V dnešní době jsou kamerové systémy využívány jako nástroj prevence kriminality, technické prvky ochrany majetku a osob nebo pro podporu logistických procesů a průmyslových společností. [9, 15]



Tyto systémy nám konkrétně slouží k monitoringu a střežení vybraných prostor a následně k přenesení obrazu na monitor. Aby byl celý CCTV systém funkční, jsou k tomu třeba tyto komponenty:

- kamery,
- hardwarové prvky:
  - přenosové prvky,
  - zobrazovací prvky.
- software pro činnost systému
- doplňující prvky:
  - záznamový prostor,
  - mikrofony,
  - reproduktory.

V dnešní době se velmi dbá na soukromí a ochranu osobních údajů. Jelikož kamerové systémy jsou úzce spojeny se soukromím občanů, je potřeba zavést určitá pravidla jejich používání a tím i chránit osobní údaje občanů. Za tímto účelem byla vydána metodika nazývající se „*Provozování kamerových systémů*“, která pojednává o základních povinnostech při provozování kamerových systémů a ochraně osobních údajů. Tuto metodiku vydal Úřad pro ochranu osobních údajů v roce 2012.

Při provozování kamerových systémů je za zpracovávání osobních údajů považováno, pokud je kromě kamerového sledování:

- prováděn záznam (zvukový nebo obrazový),
- účelem pořizování záznamu je identifikace osoby v souvislosti s jejím jednáním.

Provozovat kamerový systém, který disponuje záznamovým zařízením (tím zpracovává osobní údaje) je možné za několika okolností a to:

- pokud je to nezbytné pro ochranu právem chráněných zájmů a práv správce nebo jiného subjektu – hlavně pro ochranu majetku,
- pokud je zpracování potřebné k dodržení právní povinnosti správce,
- na základě souhlasu subjektů údajů – pouze v případě, že lze vymezit okruh monitorovaných osob (např. bytové domy). [4, 9, 15]

### 2.4.1 Norma ČSN EN 50132

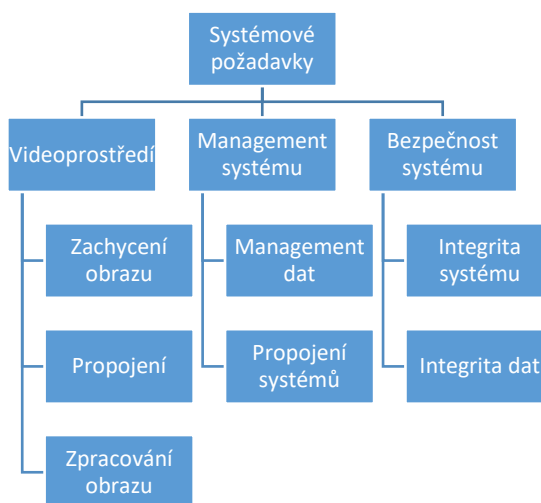
Tato česká technická norma byla vydána v roce 1999 Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví, zkráceně ÚNMZ. Každá z jejích sedmi částí řeší jinou problematiku oblasti kamerových systémů. Překlad evropské normy ji však zredukoval pouze na 3 části a to:

- ČSN EN 50132 – 1 – Systémové požadavky,
- ČSN EN 50132 – 5 – Přenos videosignálu,
- ČSN EN 50132 – 7 – Pokyny pro aplikaci.

Česká republika verzi této normy přijala v dubnu roku 2013. [15]

### 2.4.2 ČSN EN 50132 – 1 – Systémové požadavky

V této části, která se zabývá systémovými požadavky na provoz kamerových systémů, se definují prvky kamerového systému. Dělí se do 3 oddílů, kde každý z nich řeší téma návrhu kamerových systému z jiného úhlu pohledu:



Obrázek 3 – Systémové požadavky [15]

Jelikož mohou být kamerové systémy ovlivňovány vlivy okolního prostředí, řeší dále norma rozdělení prostředí podle okolních fyzikálních jevů, které na kamerový systém působí. Pro prostředí rozdělujeme do čtyř kategorií, kdy je největší důraz kladen na vlhkost, teplotu a technické specifikace budovy:

Tabulka 2 – Kategorie prostředí [15]

Třída	Název prostředí	Teploty	Příklady
<b>I</b>	Vnitřní	+5 až +40	Obchodní projekty, obytné místnosti
<b>II</b>	Vnitřní všeobecné	-10 až +40	Nestálá teplota, haly, chodby, schodiště
<b>III</b>	Venkovní chráněné	-25 až +50	Vně budovy, komponenty nejsou plně vystaveny environmentálním vlivům, přístřešky, terasy
<b>IV</b>	Venkovní všeobecné	-25 až +60	Vně budovy, komponenty jsou plně vystaveny environmentálním vlivům prostředí

K dalším kritériím pro rozdělení kamerových systémů patří zabezpečení. K tomuto účelu nám slouží čtyři stupně zabezpečení, založené na bezpečnostních požadavcích v jednotlivých stupních zabezpečení a kritériích provozu:

- Stupeň 1 – nulová ochrana proti narušení a není požadován monitoring základních funkcí. Určeno k dohledu nad událostmi s nízkým rizikem.
- Stupeň 2 – jednoduchá ochrana proti narušení a není požadován monitoring základních funkcí. Určeno k dohledu nad událostmi s nízkým až středním rizikem.
- Stupeň 3 – střední ochrana proti narušení a je požadován jednoduchý monitoring základních funkcí. Určeno k dohledu nad událostmi se středním až vysokým rizikem.
- Stupeň 4 – vysoká ochrana proti narušení a je požadován stálý monitoring základních funkcí. Určeno k dohledu nad událostmi s vysokým rizikem. [13, 15]

#### 2.4.3 ČSN EN 50132 – 5 – Přenos videosignálu

Tato část normy stanovuje základní specifikace technických parametrů na přenosové systémy využívané v kamerových systémech, zahrnující vysílací zařízení, přijímací zařízení a přenosový kanál. Dále část normy stanovuje metody ověření splnění parametrů, zavádí IP protokoly přenosu obrazu pro zařízení v bezpečnostních aplikacích a dále zavádí obecné požadavky na přenos signálu. Požadavky se týkají zabezpečení, shody se základním IP pojetím a výkonu.

Dle normy ČSN EN 50132 – 5 jsou tyto požadavky rozděleny na:

- ČSN EN 50132 – 5 – 1: Videopřenosy – obecné provozní požadavky,
- ČSN EN 50132 – 5 – 2: IP videopřenosové protokoly,
- ČSN EN 50132 – 5 – 3: Videopřenosy – analogový a digitální videopřenos.

Norma ČSN EN 50132 – 5 také zavádí různé výkonnostní kategorie dle požadavku na funkčnost daného zařízení pro přenos. Zde jsou uvedeny prvky, které mohou nejvíce ovlivnit efektivnost kamerového systému: [15]

- provozní požadavky,
- technická infrastruktura,
- provozní procesy a postupy.

#### 2.4.4 ČSN EN 50132 – 7 – Pokyny pro aplikaci

Tato norma obsahuje požadavky a doporučení pro výběr, přejímku, instalaci, plánování, zkoušení a údržbu kamerových systémů. Pracovní rámec, který má tato norma za cíl poskytnout, umožňuje zákazníkům stanovit jejich požadavky při výběru zařízení.

Při návrhu kamerového systému je nutné provést analýzu rizik, díky které identifikujeme nebezpečí a hrozby pro objekty. Dále se posoudí jejich dopad a odhadne se pravděpodobnost vzniku mimořádné události. Základním důvodem návrhu kamerového systému je zmenšení rizika, které z analýzy vyplynulo. Různé objekty s sebou nesou také různé hrozby a rizika, proto není možné navrhnout jednotný model řešení, ale je třeba brát u jednotlivých objektů v potaz: [14,15]

- lokalita (lokalita objektu, zabezpečení objektu, klimatické podmínky),
- náklady ztrát (materiální, intelektuální a finanční hodnoty v objektu),
- historie krádeží a hrozeb (lidský faktor a environmentální vlivy)

Výsledek lze použít při rozhodování o účelu kamerového systému a také při jeho realizaci a instalaci. Norma ČSN EN 50132 – 7 nám udává takový doporučený postup projektování a realizace kamerového systému:

1. **Vypracování funkčních požadavků** (přesné potřeby a požadavky zákazníka na funkčnost a účel kamerového systému – analýza potřeb zákazníka)
2. **Návrh systému** (vypracování nabídky a funkčních požadavků s konkrétním řešením)

3. **Odsouhlasení specifikace** (vypracování technické dokumentace, zpracování změn a ověření úplnosti)
4. **Instalace a ověření funkčnosti systému** (plán instalace, značení a trasování kabeláže, montáž a konfigurace, revize, start systému, funkční zkouška a zahájení zkušebního provozu)
5. **Předání systému zákazníkovi** (školení, předání dokumentace a manuálů k obsluze)
6. **Údržba** (prováděna dle plánu údržby vždy pouze zaškoleným a kvalifikovaným personálem, výsledky zachovávat)

Pro specifikaci účelu kamerového systému se musí vymezit a definovat, jaký prostor bude monitorován a jak využít informaci z kamerového systému. Norma ČSN EN 50132 – 7 zde nabízí detailní popis snímané scény vůči výšce osoby v závislosti na rozlišení snímacího zařízení. Tento popis nese název Stupeň identifikace osoby. Zde je nutné, aby byla shodná nastavení rozlišení zobrazovacího a snímacího zařízení, aby nedošlo ke zkreslení informací v důsledku disproporce zařízení a následné změně množství detailů. Zde se navrhuje řešení v rámci rozmístění kamer a volby objektivů. Následující tabulka znázorňuje procentuální přepočty úrovně rozpoznání osob pro různá rozlišení: [13, 14, 15]

Tabulka 3 – Procentuální přepočty úrovně rozpoznání osob [15]

Kategorie	PAL	1080p	720p	WSVGA 4CIF	VGA	2CIF CIF	QCIF
<b>Monitoring</b>	400	150	250	300	350	600	1200
<b>Detekce</b>	100	40	60	70	85	150	300
<b>Observace</b>	50	20	30	35	45	70	150
<b>Rekognoskace</b>	25	10	15	20	25	35	70
<b>Identifikace</b>	10	10	10	10	10	15	30
<b>Inspekce</b>	5	5	5	5	5	10	15

### 3 ZÁKLADNÍ POJMY

V této kapitole jsou definovány základní pojmy týkající se ochrany měkkých cílů:

- Aktivní střelec – Nebezpečná osoba, která se záměrem dosažení vlastních cílů užije zbraň proti jiné osobě či osobám. Jeho záměrem bývá zranit nebo zabít co největší množství osob. [21]
- Bezpečnost – Bezpečnost je definována jako stav, kdy jsou hrozby pro objekt a jeho zájmy eliminovány na efektivní míru, přičemž je tento objekt k omezení těchto hrozeb vybaven a ochoten při něm spolupracovat. [19]
- Evakuace – souhrn opatření, který zajišťuje přemístění osob, zvířat nebo věcí z místa ohroženého mimořádnou událostí na místo, kde nebezpečí mimořádné události nehrozí. [21]
- Hrozba – skutečnost, která má potenciální schopnost poškodit chráněné hodnoty a zájmy.
- Integrovaný záchranný systém – koordinovaný postup jeho složek při provádění záchranných a likvidačních prací a při přípravě na mimořádné události.
- Krizová situace – jedná se o mimořádnou událost, narušení kritické infrastruktury či jiné nebezpečí, v jehož důsledku je vyhlášen stav nebezpečí, nouzový stav či stav ohrožení státu. [21]
- Měkký cíl – místo či objekt, který disponuje vysokou koncentrací osob a nízkou úrovní zabezpečení vůči násilným útokům. [5]
- Mimořádná událost – škodlivé působení sil a jevů vyvolaných přírodními vlivy nebo činností člověka, ale také havárie, které ohrožují život, majetek, zdraví nebo životní prostředí a následně vyžadují provedení záchranných a likvidačních prací.
- Ochrana obyvatelstva – soubor úkolů a činností odpovědných orgánů veřejné správy, podnikajících fyzických a právnických osob a občanů, s účelem zabezpečení ochrany života, životního prostředí, zdraví a majetku, v souladu s platnými právními předpisy. [6]
- Prevence – jedná se o soubor opatření s účelem snížení nebo úplné eliminace rizika vzniku mimořádné události.
- Riziko – pravděpodobnost, že vznikne událost, která je z bezpečnostního hlediska považována za nežádoucí. [21]

- Terorismus – organizované zastrašování pomocí hrozby či násilí, často proti nezúčastněným osobám, se záměrem dosažení politických, náboženských nebo ideologických cílů. [19]
- Tvrdé cíle – objekt, který disponuje vysokým stupněm zabezpečení vůči násilným útokům a napadení.

## **II. PRAKTICKÁ ČÁST**



## 4 CÍLE A METODY PRÁCE

V této kapitole jsou definovány hlavní a dílčí cíle bakalářské práce a použité metody nacházející se v praktické části práce.

Hlavní cíl práce:

- navrhnout opatření k zabezpečení zvoleného měkkého cíle proti násilným útokům.

Dílčí cíle práce:

- popis zvoleného měkkého cíle,
- analýza rizik pro zvolený měkký cíl,
- analýza stávajícího zabezpečení měkkého cíle,
- návrh zdokonaleného zabezpečení.

Použité metody:

- Analýza – metoda analýzy patří k základním a nejpoužívanějším vědeckým metodám. Jde o proces reálného či myšlenkového rozkládání zkoumaného objektu na části, které jsou poté předmětem dalšího zkoumání. V praktické části bakalářské práce je analýza užívána pro realizaci návrhu zdokonalených opatření v zabezpečení měkkého cíle. Analyzována byla různá rizika, která mohou narušit bezpečnost měkkého cíle a následně byla navržena opatření pro jejich eliminaci.
  - Metoda SWOT – metoda SWOT se používá k identifikaci slabých a silných stránek a také k identifikaci hrozeb i příležitostí. Výstup metody SWOT pomáhá si určit, kde je potřeba vylepšení a na co je zapotřebí se zaměřit.
  - Metoda KARS – tato metoda slouží k identifikaci rizik, které jsou nejnebezpečnější pro zkoumaný systém, a proto je nutné se těmito riziky zabývat prioritně.
- Dotazování – metodu dotazování můžeme dělit do několika typů (ústní, elektronické, písemné). V případě této bakalářské práce je zvolen typ ústního dotazování, kde byl využit ke zjištění bezpečnostních prvků v prostorách zkoumaného objektu.
- Modelování – touto metodou se rozumí aplikování různých typů modelů pro řešení vybrané problematiky. Jedná se o náhradu objektu reálného právě objektem modelovým, přičemž je nutné respektovat klíčové vlastnosti objektu. [22]

Z důvodu velkého množství společností ve vybraném objektu, je tato práce omezena pouze na prostory školského zařízení.

## 5 ZABEZPEČENÍ MĚKKÝCH CÍLŮ

Zabezpečení měkkých cílů je v posledních letech, obzvláště v důsledku hrozby terorismu, velmi diskutovaným tématem. Obrovská obtížnost zabezpečení měkkých cílů tkví převážně ve vysoké koncentraci osob a často v nedostatečných kontrolách těchto osob. Dalším problémem v zabezpečení měkkých cílů může mnohdy být také neochota soukromých společností, organizací či zařízení zabezpečit měkký cíl ve svém vlastnictví. Často se tak děje z finančních důvodů, jelikož soukromé společnosti jsou většinou založeny kvůli ziskům a dostatečné zabezpečení může být nákladné. Bezpečí osob v objektu by ale mělo být vždy prioritou. [5, 19]

V důsledku často nedostatečného zabezpečení je pro potenciálního útočníka jednoduché dostat se například do prostor školských zařízení. Konkrétně pro tuto bakalářskou práci byly vybrány prostory Mateřské a základní školy Academic School v Uherském Hradišti. Tyto prostory byly v rámci aktuálnosti problematiky vybrány v důsledku častých útoků na školská zařízení na území ČR v nedávné době.

### 5.1 Academic School, Mateřská a základní škola, s.r.o.

Mateřská a základní škola Academic School se nachází v Uherském Hradišti v kampusu Fakulty logistiky a krizového řízení univerzity Tomáše Bati ve Zlíně. V prostorách školy se v době vyučování běžně nachází přibližně 150 dětí a 35 zaměstnanců.



Obrázek 4 – Academic School [vlastní]

Prostory školského zařízení se nachází ve čtyřpatrové budově, přičemž samotné mateřské a základní škole jsou vyčleněny prostory druhého a třetího nadzemního podlaží a menší prostor recepce ve vstupní hale budovy v přízemním podlaží. Ostatní prostory jsou užívány jako kanceláře či sídla jiných společností. Čtvrté patro se využívá jako sklad, je tedy nejméně používané. Mimo základní školy se v budově nachází také:

- MISS Centrum s. r. o. + M.I.S.S., s.r.o.,
- Fakulta veřejnoprávních a ekonomických studií v Uherském Hradišti,
- Knihovna Bedřicha Beneše Buchlovana, p. o.,
- Mgr. Ludmila Bednaříková – speciální pedagog,
- Maltéžská pomoc, o.p.s.,
- Park Rochus, o.p.s.,
- Smart Venture, s.r.o.,
- Václav Hrabec s.r.o.,
- Mgr. Yvona Gregorová – výuka cizích jazyků a překladatelství,
- Akademie krizového řízení a managementu s.r.o.,
- Autoškola Driver,
- Mgr. Helena Březinová – Příprava do školy,
- Kristýna Koběrská a Petr Koběrský – Kooperativa a.s.,
- Počítačová služba s.r.o.,
- M-Centrum, konzultační, rekvalifikační a školící středisko, z.s.,
- NIO s.r.o.,
- Centrum svaté Sary – sociálně aktivizační služba pro rodiny s dětmi,
- Krajská hospodářská komora Zlínského kraje,
- Czech point – Okresní středisko Uherské Hradiště,
- Brunnbauer – Moravia, s.r.o.

Mimo zmíněné společnosti se v budově nachází také ubytovací zařízení pro kantory z Fakulty logistiky a krizového řízení UTB. Ovšem prostory ubytovacího zařízení a školského zařízení jsou, na rozdíl od výše zmíněných společností, odděleny.

## 5.2 Stávající zabezpečení školského zařízení

V přízemním podlaží objektu se při vstupu nachází recepce, kde sídlí zaměstnanec školského zařízení, který kontroluje vstup do budovy pomocí ID karet. Tyto karty má k dispozici každý zaměstnanec školského zařízení či firmy sídlící v budově a veřejnost se po vstupu do budovy musí hlásit na recepci a uvést důvod a místo návštěvy.

V prvním patře u schodiště se také nachází mechanický zábranný systém v podobě zábrany, která při jejím uzavření zamezí průchodu do vyšších pater budovy a tím i do školních prostor. Tato zábrana (viz Obrázek 5) se uzavírá manuálně pomocí klíče, který má k dispozici pouze vedení školy.



Obrázek 5 – Zábrana [vlastní]

V případě nebezpečí je možné použít rozhlasové zařízení (viz Obrázek 6), které se nachází v každém patře používaném školským zařízením a varovat tak osoby nacházející se v prostorech budovy.



Obrázek 6 – Rozhlasové zařízení [vlastní]

V souvislosti zabezpečení prostor před požáry se v každém patře nachází práškový hasicí přístroj (viz Obrázek 7), který je v případě nebezpečí možné použít. Žádnou jinou ochranou před požáry ovšem prostory školského zařízení nedisponují.



Obrázek 7 – Hasicí přístroj [vlastní]

V prostorách mateřské a základní školy jsou dále nainstalována pasivní infračervená čidla, které patří mezi poplachové zabezpečovací a tísňové systémy. Konkrétně se jedná o typ PARADOX PIR PRO Plus (476), který slouží k detekci pohybu v interiéru školského zařízení. Tento typ PIR dále disponuje: [18]

Tabulka 4 – PARADOX PIR PRO Plus (476) [18]

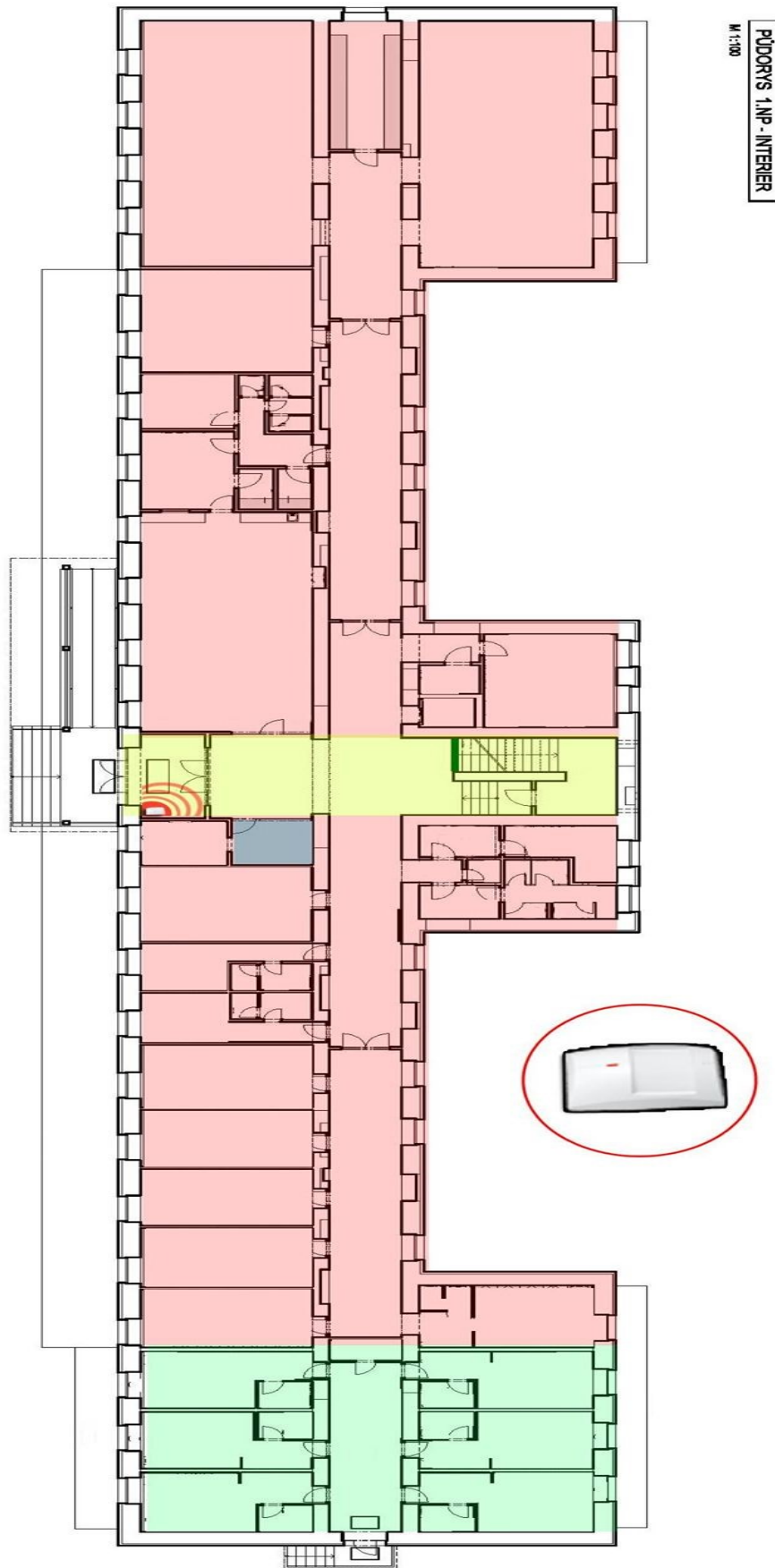
Typ detektoru	Analogový
Senzor	Duální
Citlivost	Dvě nastavitelné úrovně
Napájení	9 - 16 VDC
Proudový odběr	Min. 15 mA, max. 27 mA
Montážní výška	2 – 2,7 m
Dosah	11 m, 110° (standardní čočka WA-1)
Detekční rychlost	0,2 až 7 m/s
Optická indikace	Zelená LED dioda
Barva krytu	Bílá
Rozměry (šířka x výška x hloubka)	70 mm x 95 mm x 60 mm
Provozní podmínky	-10 °C až 50 °C, maximální vlhkost 95 %

V celém prostoru školského zařízení je nainstalováno 13 detektorů pohybu PARADOX PIR PRO Plus (476). V době jejich aktivace tedy zajišťují dostatečnou ochranu před násilným vniknutím do budovy.



Obrázek 8 – PARADOX PIR PRO Plus (476) [vlastní]

Nainstalovány jsou se základní čočkou WA-1 s dosahem 11 m a záběrem 110°. V případě potřeby je možná výměna čočky na základě prostoru, ve kterém je PIR instalován. Pro větší dosah, ale menší záběr ve stupních, je k mání například čočka LR-4, která disponuje dosahem až 30,4 m, hodící se spíše do chodeb objektů. Naopak pro větší stupňový záběr je možné nainstalovat například čočku WA-2, která disponuje dosahem 14 m a záběrem 140°. Kompatibilní se zařízením PARADOX PIR PRO Plus (476) jsou dále čočky LR-1, LR-2, LR-3 a WA-3, přičemž každá disponuje jiným dosahem, záběrem ve stupních a hustotou záběru. [2, 18]

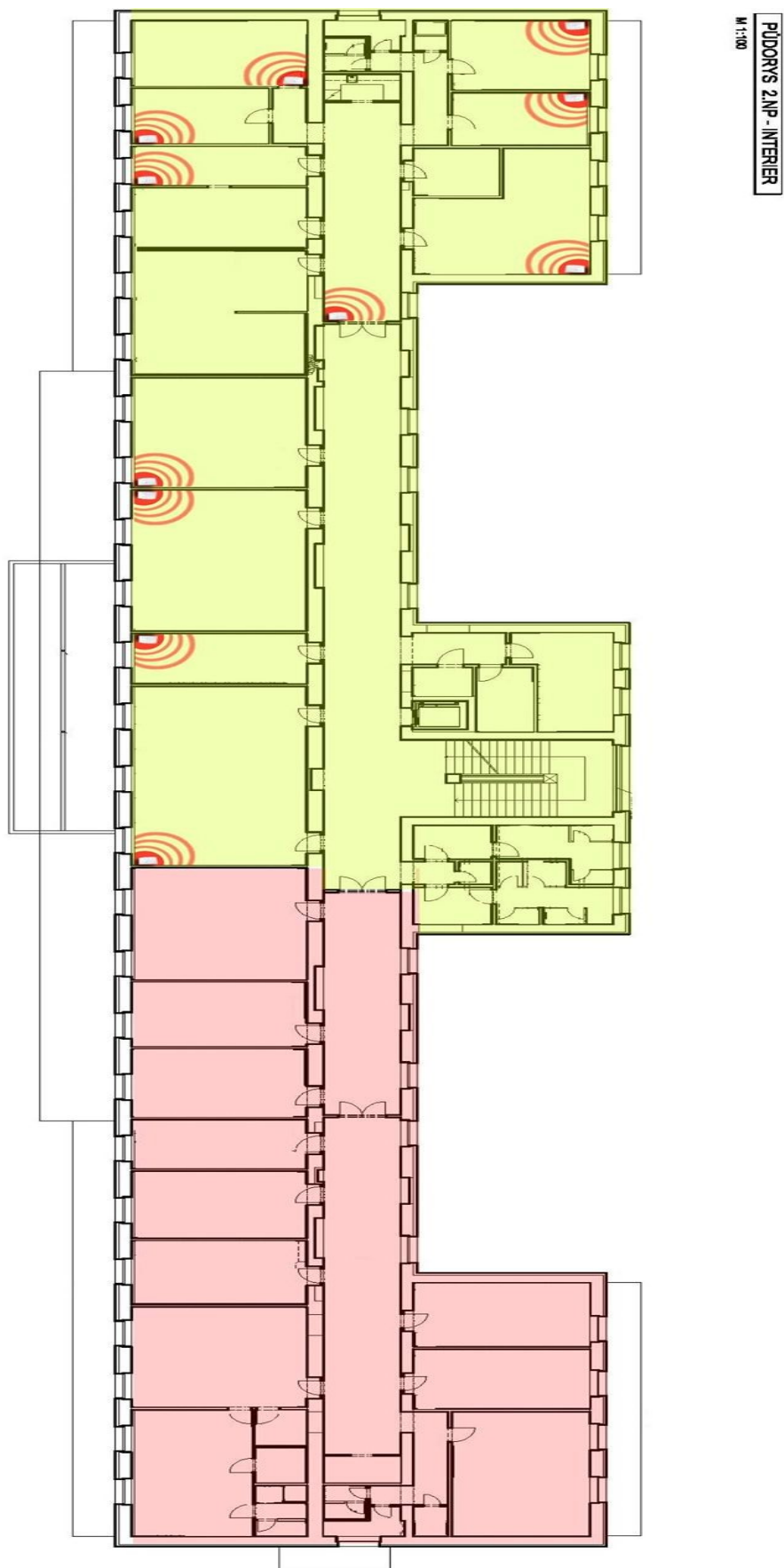


Obrázek 9 – Plán přízemního patra [vlastní]



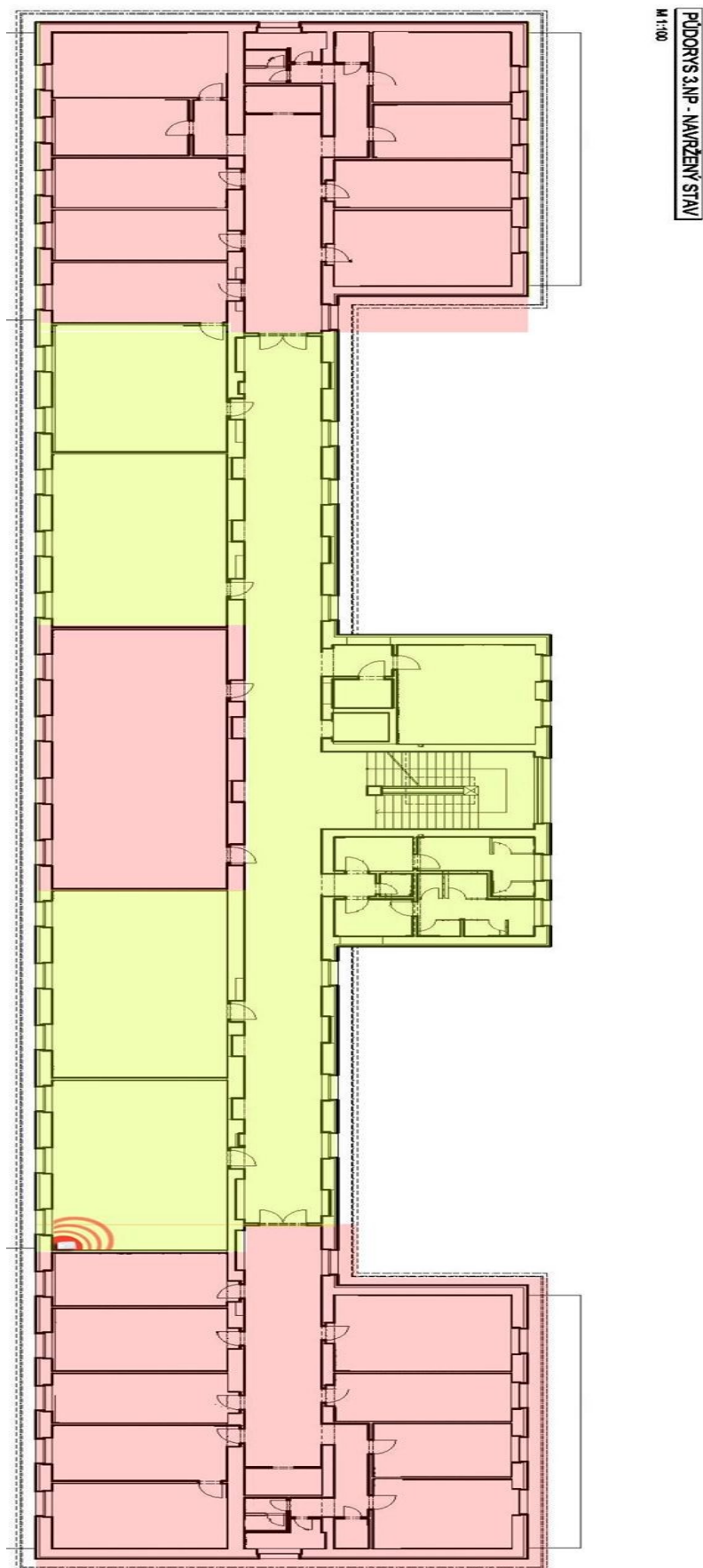
Na výše uvedeném obrázku (viz Obrázek 9), se nachází plán rozložení přízemního patra budovy v měřítku 1:100. Žlutou barvou je naznačen prostor, kterým se vchází do budovy a školského zařízení a který tedy lze považovat za prostor využívaný mateřskou a základní školou. Červenou barvou jsou dále naznačeny prostory, které ke škole nepatří včetně barvy světle zelené, kterou jsou označeny oddělené kantorské ubytovny. Šedě je naznačena výše zmíněná recepce, kde probíhá kontrola osob zaměstnancem školského zařízení při vstupu do budovy. Dále je zde rudou barvou označeno pasivní infračervené čidlo, které se nachází za vstupními dveřmi do budovy. Na plášti budovy se také nachází dvě kamery, ke kterým ale školní zařízení nemá přístup, nejsou proto do plánu zahrnuty. Tmavě zelenou barvou je dále zvýrazněna výše zmíněná zábrana, která v případě aktivace slouží k zamezení vstupu na schodiště.

Na níže uvedeném obrázku (viz Obrázek 10) je naznačen plán rozložení druhého patra, taktéž v měřítku 1:100. Na tomto patře v prostorách školského zařízení se nachází 11 různě rozmístěných PIR detektorů pohybu. Značení prostorů a bezpečnostních prvků je provedeno totožně jako na plánu přízemního patra (viz Obrázek 9). V těchto prostorách se nachází především třídy, ve kterých probíhá vyučování, menší kuchyňka a kabinety kantorů mateřské a základní školy. Také se zde nachází toalety jak pro žáky, tak pro personál školy.



Obrázek 10 – Plán 2. patra [vlastní]

Třetí patro budovy je naznačeno na obrázku níže (viz Obrázek 11). V tomto patře se nachází jediný PIR detektor, který je v jedné ze tříd. Menší množství PIR detektorů je ve třetím patře pochopitelné z důvodu menší pravděpodobnosti vniknutí do budovy okny, které by v tomto patře bylo velice obtížné. Způsob značení prostor a bezpečnostních prvků je totožný s předchozími plány (viz Obrázek 9-10).



Obrázek 11 – Plán 3. patra [vlastní]

### 5.2.1 Vyhodnocení stávajícího zabezpečení prostor Academic School, Mateřské a základní školy, s.r.o. v Uherském Hradišti

Velkou slabinou v zabezpečení školského zařízení je úplná absence EPS. V prostorách se nachází hasicí přístroje, ale ty jsou v případě většího požáru nedostatečné. Žhářský útok mířený například na schodiště budovy by navíc zamezil útěku osob z vyšších pater, protože z budovy vede pouze jediný východ a skok z okna v takové výšce nepřipadá v úvahu. Stejný problém by nadešel například i při útoku aktivního střelce. V tomto případě se v přízemním patře sice nachází výše zmíněná zábrana (viz Obrázek 5), ale je velmi pravděpodobné, že aktivace této zábrany by nebyla včasná a v přítomnosti aktivního střelce neuskutečnitelná, jelikož se aktivace provádí manuálně pomocí klíče na místě zábrany. Další velkou slabinou je tedy i absence dalších východů z budovy.

Slabou stránkou školského zařízení je také sdílení prostor s dalšími společnostmi a nedostatečná kontrola osob vcházejících do budovy. Zaměstnanci společností sídlících v budově se sice prokazují ID kartami a veřejnost hlásí na recepci místo a důvod návštěvy, ale jejich další kontrola neprobíhá. Pro potenciálního útočníka se tak stává lehčí projít do budovy a vnést si s sebou například chladnou zbraň.

V prostorách školského zařízení dále chybí CCTV systémy. Tyto systémy většinou slouží až ke zpětné identifikaci pachatele, ale jejich přítomnost v prostorách školy by mohla sloužit jako zastrašení pro potenciálního útočníka, nebo k určení polohy útočníka při držení rukojmích v prostorách školy.

V rámci připravenosti osob na možné mimořádné události je součástí výuky ve školském zařízení také téma bezpečnosti. Konají se zde přednášky členů složek IZS, jedenkrát ročně se pořádá cvičný požární poplach a přibližně 20 hodin ročně se kantoři s žáky věnují různým tématům bezpečnosti. Chybí ale podrobnější cvičení s tématem násilného útoku, jako je například útok aktivního střelce.

PIR detektory zajišťují bezpečnost školských prostor v nočních hodinách. Jejich rozmístění a počet je k tomuto účelu dostatečný.

## 6 ANALÝZA RIZIK

Tato kapitola se věnuje možným násilným útokům a dalším hrozbám, jejichž negativní působení v prostorách Academic School, Mateřské a základní školy, s.r.o. by mohlo narušit její chod a způsobit škody na životech, zdraví a majetku. Hrozby a s nimi spojená rizika jsou vyhledávána a hodnocena pomocí vybraných metod a analýz. Pro tyto účely byla konkrétně vybrána Kvalitativní analýza rizik s využitím jejich souvztažnosti (KARS), pomocí které můžeme najít rizika, na které se primárně zaměřit při navrhování opatření. Dále v této kapitole bude využita metoda SWOT analýzy, za účelem nalezení správné strategie ke zlepšení stávajícího stavu bezpečnosti v prostorách školského zařízení.

### 6.1 Kvalitativní analýza rizik s využitím jejich souvztažnosti (KARS)

Pomocí metody KARS je možné odhalit největší a nejpravděpodobnější rizika a následně je rozdělit do skupin dle jejich nebezpečnosti. Prvním krokem pro správnou aplikaci analýzy KARS je vytvoření seznamu rizik, které by mohly ohrozit daný objekt a jejich následné vložení do tabulky. Pro prostory školského zařízení Academic School v Uherském hradišti byly vybrány tyto rizika: [4]

1. Žhářství
2. Násilné vniknutí
3. Aktivní střelec
4. Zranění osob
5. Agresor s chladnou zbraní
6. Bombový útok
7. Panika
8. Chemický útok
9. Rukojmí
10. Vandalismus

Tabulka 5 – Tabulka rizik [vlastní]

Riziko	1	2	3	4	5	6	7	8	9	10	Součet
1. Žhářství											
2. Násilné vniknutí											
3. Aktivní střelec											
4. Zranění osob											
5. Agresor s chladnou zbraní											
6. Bombový útok											
7. Panika											
8. Chemický útok											
9. Rukojmí											
10. Vandalismus											
<b>Součet</b>											

Metoda KARS je postavena na vzájemném působení a souvztažnosti rizik. Její princip spočívá v postupném ověřování jednotlivých rizik pomocí otázky, zda může riziko zapříčinit vznik rizika druhého. Do tabulky jsou dle odpovědi na tuto otázku doplňovány hodnoty 0 či 1. Hodnota 0 je zapsána v případě, že odpověď zní ne, tedy riziko nemůže vyvolat riziko druhé. Hodnotu 1 zapisujeme v případě, že odpověď je ano, tedy riziko může vyvolat riziko druhé. Pro účely metody KARS se předpokládá, že rizika nejsou schopna vyvolat sama sebe. Z tohoto důvodu jsou dané buňky v tabulce označeny šedou barvou, a nikoliv číselnou hodnotou.

Tabulka 6 – Vyplněná tabulka rizik [vlastní]

Riziko	1	2	3	4	5	6	7	8	9	10	Součet
1. Žhářství		1	1	1	1	0	1	0	1	0	6
2. Násilné vniknutí	1		1	1	1	1	1	1	1	0	8
3. Aktivní střelec	1	1		1	1	0	1	0	1	0	6
4. Zranění osob	0	0	0		0	0	1	0	0	0	1
5. Agresor s chladnou zbraní	0	0	0	1		0	1	0	1	0	3
6. Bombový útok	0	1	0	1	0		1	0	1	0	4
7. Panika	0	0	0	1	0	0		0	0	1	2
8. Chemický útok	0	1	0	1	0	0	1		1	0	4
9. Rukojmí	0	0	0	1	0	0	1	0		0	2
10. Vandalismus	1	1	0	1	1	0	1	0	0		5
<b>Součet</b>	<b>3</b>	<b>5</b>	<b>2</b>	<b>9</b>	<b>4</b>	<b>1</b>	<b>9</b>	<b>1</b>	<b>5</b>	<b>1</b>	

Po vyplnění tabulky je nutné použití koeficientů aktivity a pasivity, pomocí kterých je tabulka přeformulována do matematického znázornění a které jsou nutné pro správnou kvalifikaci rizik. Tyto koeficienty jsou:

- $K_{ARi}$  (koeficient aktivity) – v případě, že nastane riziko označené  $R_i$ , je možné, že toto riziko vyvolá další rizika. Koeficient aktivity procentuálně značí počet těchto potenciálně vyvolaných rizik.
- $K_{PRi}$  (koeficient pasivity) – tento koeficient naopak procentuálně značí, kolik rizik má schopnost vyvolat riziko označené  $R_i$ .



Jedním z předpokladů pro vyjádření koeficientu aktivity a pasivity je sestavení počtu kombinací. Jak již bylo řečeno výše, pro účely metody KARS se předpokládá, že riziko nemůže vyvolat samo sebe. Je ale možné, že vyvolá rizika jiná, nebo že bude jinými riziky vyvoláno. V tomto případě se tedy počet rizik rovná  $x - 1$ . [4]

#### Výpočet koeficientu aktivity $K_{ARi}$ pro jednotlivá rizika $R_i$ :

$$K_{ARi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%]$$

1.  $K_{ARi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%] = \frac{6}{10-1} \cdot 100 = \frac{6}{9} \cdot 100 = 66,66\%$
2.  $K_{ARi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%] = \frac{8}{10-1} \cdot 100 = \frac{8}{9} \cdot 100 = 88,88\%$
3.  $K_{ARi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%] = \frac{6}{10-1} \cdot 100 = \frac{6}{9} \cdot 100 = 66,66\%$
4.  $K_{ARi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%] = \frac{1}{10-1} \cdot 100 = \frac{1}{9} \cdot 100 = 11,11\%$
5.  $K_{ARi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%] = \frac{3}{10-1} \cdot 100 = \frac{3}{9} \cdot 100 = 33,33\%$
6.  $K_{ARi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%] = \frac{4}{10-1} \cdot 100 = \frac{4}{9} \cdot 100 = 44,44\%$
7.  $K_{ARi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%] = \frac{2}{10-1} \cdot 100 = \frac{2}{9} \cdot 100 = 22,22\%$
8.  $K_{ARi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%] = \frac{4}{10-1} \cdot 100 = \frac{4}{9} \cdot 100 = 44,44\%$
9.  $K_{ARi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%] = \frac{2}{10-1} \cdot 100 = \frac{2}{9} \cdot 100 = 22,22\%$
10.  $K_{ARi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%] = \frac{5}{10-1} \cdot 100 = \frac{5}{9} \cdot 100 = 55,55\%$

#### Výpočet koeficientu pasivity $K_{PRi}$ pro jednotlivá rizika $R_i$ :

$$K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%]$$

1.  $K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%] = \frac{3}{10-1} \cdot 100 = \frac{3}{9} \cdot 100 = 33,33\%$
2.  $K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%] = \frac{5}{10-1} \cdot 100 = \frac{5}{9} \cdot 100 = 55,55\%$
3.  $K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%] = \frac{2}{10-1} \cdot 100 = \frac{2}{9} \cdot 100 = 22,22\%$
4.  $K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%] = \frac{9}{10-1} \cdot 100 = \frac{9}{9} \cdot 100 = 99,99\%$
5.  $K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100 [\%] = \frac{4}{10-1} \cdot 100 = \frac{4}{9} \cdot 100 = 44,44\%$

$$6. K_{PRi} = \frac{\sum Ri}{x-1} \cdot 100 [\%] = \frac{1}{10-1} \cdot 100 = \frac{1}{9} \cdot 100 = 11,11\%$$

$$7. K_{PRi} = \frac{\sum Ri}{x-1} \cdot 100 [\%] = \frac{9}{10-1} \cdot 100 = \frac{9}{9} \cdot 100 = 99,99\%$$

$$8. K_{PRi} = \frac{\sum Ri}{x-1} \cdot 100 [\%] = \frac{1}{10-1} \cdot 100 = \frac{1}{9} \cdot 100 = 11,11\%$$

$$9. K_{PRi} = \frac{\sum Ri}{x-1} \cdot 100 [\%] = \frac{5}{10-1} \cdot 100 = \frac{5}{9} \cdot 100 = 55,55\%$$

$$10. K_{PRi} = \frac{\sum Ri}{x-1} \cdot 100 [\%] = \frac{1}{10-1} \cdot 100 = \frac{1}{9} \cdot 100 = 11,11\%$$

**Tabulka koeficientů aktivity a pasivity:**

Tabulka 7 – Tabulka koeficientů aktivity a pasivity [vlastní]

Riziko Ri	1	2	3	4	5	6	7	8	9	10
$K_{ARi} [\%]$	66,66	88,88	66,66	11,11	33,33	44,44	22,22	44,44	22,22	55,55
$K_{PRi} [\%]$	33,33	55,55	22,22	99,99	44,44	11,11	99,99	11,11	55,55	11,11

Po sestavení tabulky koeficientů aktivity a pasivity je posledním krokem ke správnému provedení metody KARS vytvoření a následné vyhodnocení grafického znázornění.

**Výsledný graf souvztažnosti:**

Ke stanovení souvztažnosti rizik v systému a jejich významnosti slouží graf souvztažnosti.

Tento graf dělí dvě osy označené jako  $O_1$  a  $O_2$  do čtyř různých kategorií:

- I. Primárně a sekundárně nebezpečná rizika
- II. Sekundárně nebezpečná rizika
- III. Primárně nebezpečná rizika
- IV. Oblast relativně bezpečná

V grafu souvztažnosti bývá oblast číslo I. pokryta 80% z celkové oblasti grafického znázornění. Pro osu  $O_1$  tedy platí:

$$K_{Amax} - K_{Amin} = 100 \%$$

V případě stavby osy  $O_1$  za splnění 80% podmínky to bude rovnoběžka s osou y ve vzdálenosti:

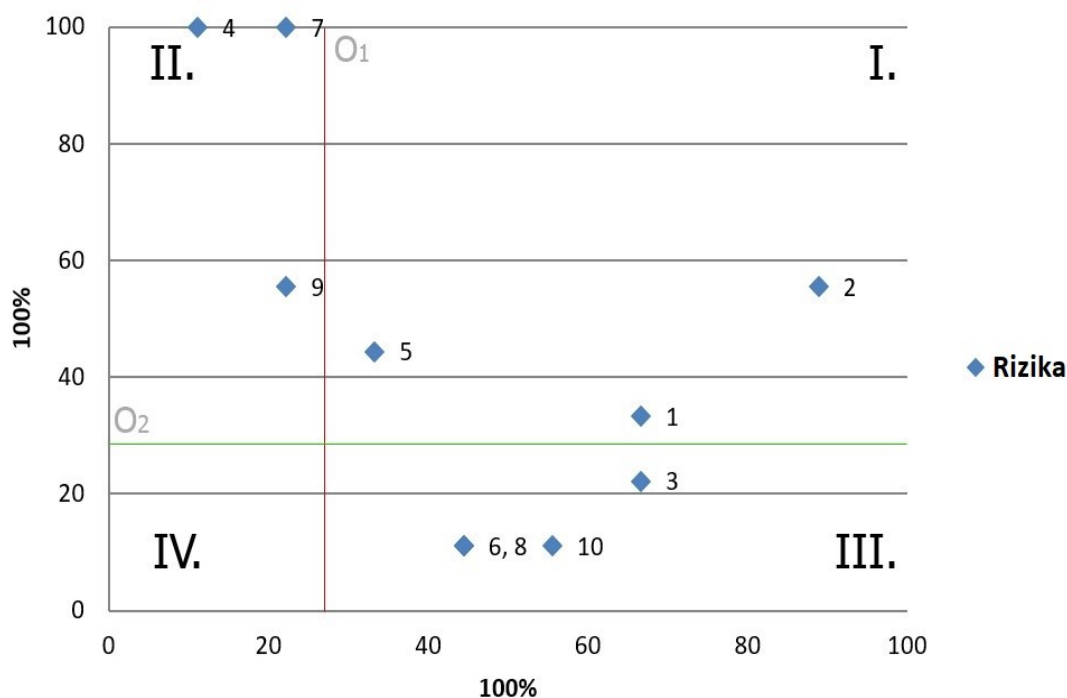
$$O_1 = K_{Amax} - \frac{K_{Amax} - K_{Amin}}{100} \cdot 80$$

$$O_1 = 88,88 - \frac{88,88 - 11,11}{100} \cdot 80 = 88,88 - 62,22 \doteq 26,70\%$$

Pro osu  $O_2$  je rovnoběžka s osou x ve vzdálenosti:

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

$$O_2 = 99,99 - \frac{99,99 - 11,11}{100} \cdot 80 = 99,99 - 71,10 \doteq 28,90\%$$



Obrázek 12 – Graf souvztažnosti [vlastní]

#### Vyhodnocení pomocí grafu souvztažnosti:

- Oblast I. primárně a sekundárně nebezpečných rizik – žhářství, násilné vniknutí, agresor s chladnou zbraní.
- Oblast II. sekundárně nebezpečných rizik – zranění osob, panika, rukojmí.
- Oblast III. primárně nebezpečných rizik – aktivní střelec, bombový útok, chemický útok, vandalizmus.
- Oblast IV. relativně bezpečná – neobsahuje žádné riziko (není podmínkou, aby zde bylo jakékoliv riziko).

Dle výsledků metody KARS je zřejmé, že největší a nejpravděpodobnější rizika pro Academic School, Materskou a základní školu, s.r.o. v Uherském Hradišti jsou:

- žhářství,
- agresor s chladnou zbraní,

- násilné vniknutí.

Na tyto rizika je tedy nutné se primárně zaměřit při návrhu zabezpečení prostor školského zařízení.

## 6.2 Metoda SWOT analýzy

Metoda SWOT byla využita pro specifitější analýzu. Jde o komplexní metodu, která napomáhá ke kvalitativnímu hodnocení veškerých stránek fungování. Anglická zkratka SWOT znamená: Strengths (silné stránky), Weaknesses (slabé stránky), Opportunities (příležitosti), Threats (Hrozby). Do těchto čtyř skupin se následně budou rozdělovat jednotlivé faktory, které se poté budou bodově ohodnocovat. Prvním krokem SWOT analýzy je tedy nalezení silných a slabých stránek, příležitostí ke zlepšení stávajícího stavu bezpečnosti a zvolení hrozeb, které by se mohly pro školské zařízení negativně projevit.

Dalším krokem SWOT analýzy je bodové hodnocení těchto faktorů dle jejich důležitosti. Pro silné stránky a příležitosti jsou využity známky od 1 do 5, přičemž známka 5 znamená nejvyšší spokojenost a známka 1 naopak nejnižší. Pro slabé stránky a hrozby je využita totožná stupnice, ale v záporných hodnotách. Bodování pro slabé stránky a hrozby tedy probíhá následovně: Znamky od -1 do -5, kde známka -5 znamená nejvyšší nespokojenost, -1 naopak nejnižší nespokojenost. Další krok je druhé bodové hodnocení, které spočívá v hodnocení jednotlivých složek SWOT analýzy pomocí čísel, podmínkou je však, aby byl součet těchto čísel v každé ze čtyř skupin roven 1. Platí zde, že čím větší číslo, tím větší důležitost položce přiřazujeme v dané kategorii.

Finálním krokem je grafové znázornění, které je výsledkem předešlých výpočtů. Z tohoto grafu vyplynou jednotlivé strategie, které napomáhají ke zvolení postupu ke zlepšení nynějšího stavu. Tyto strategie mohou být:

- Strategie SO – využití silných stránek k zužitkování příležitostí.
- Strategie ST – využití silných stránek k čelení hrozbám.
- Strategie WO – překonává slabiny s využitím příležitostí.
- Strategie WT – Strategie řeší kumulaci nepříznivých předpokladů a zaměřuje se na minimalizaci negativních jevů. [20]

Pro potřeby analýzy SWOT na prostory Academic School, Mateřské a základní školy, s.r.o. v Uherském Hradišti byly zvoleny silné stránky, slabé stránky, příležitosti a hrozby následovně:

- Silné stránky:
  - **Zaměstnanci** – v prostoru školského zařízení se pravidelně v průběhu vyučování a tím pádem největší zranitelnosti nachází 35 zaměstnanců. V poměru se 150-ti dětmi je toto číslo poměrně vysoké, zaměstnanci byli tedy zvoleni mezi silné stránky.
  - **Lokalita** – v okolí místa, kde sídlí školské zařízení se nepřetržitě pohybuje poměrně vysoké množství osob, a to i v noci. Pro útočníka, který nechce být při útoku spatřen, se proto lokalita může zdát neatraktivní.
  - **ID karty** – každá zaměstnanec, jak již bylo zmíněno v kapitole 5.2, se musí při vstupu prokazovat svou ID kartou, tím pádem se do jisté míry zamezuje přístupu veřejnosti do budovy. Tyto ID karty mají k dispozici všichni zaměstnanci budovy, tedy nejen školského zařízení, ale i společností sídlících v budově. Z těchto důvodů se ID karty řadí mezi silné stránky.
- Slabé stránky:
  - **Evakuace** – budova disponuje únikovým východem, tento únikový východ je ovšem zároveň jediným vchodem i východem z budovy. V případě násilného útoku či jiného nebezpečí spojeného s blokadou schodiště a jediného východu z budovy mohou být škody ohromné.
  - **Nedostatečné zabezpečení objektu** – jelikož se v prostoru školského zařízení nachází pouze 13 pasivních infračervených čidel, které jsou aktivní pouze v časech, kdy školní prostory nikdo neobývá, je zde velký prostor pro zlepšení stávajícího zabezpečení.
  - **Společnosti sídlící v objektu** – školské zařízení sdílí prostory s dalšími dvaceti společnostmi. Tyto společnosti mohou pro školské zařízení znamenat hrozbu v podobě pohybující se veřejnosti v budově a tím pádem větší pravděpodobnosti proniknutí útočníka do budovy a školních prostor.
- Příležitosti:
  - **Vybudování dalšího východu z budovy** – z důvodu jediného vstupu a výstupu budovy by bylo vybudování jiného únikového východu velkým zlepšením stávajícího zabezpečení budovy.

- **Rozšířené školení žáků a učitelů v oblasti bezpečnosti** – v oblasti bezpečnosti je nutné se zaměřit nejen na technickou stránku zabezpečení školského zařízení, ale také na připravenost žáků a učitelů na případné násilné útoky. Je nutné, aby každý věděl, jak se v případě útoku chovat, aby se v co největší míře minimalizovaly negativní následky tohoto útoku.
- **Instalace dalších bezpečnostních prvků** – z důvodu malého množství bezpečnostních zařízení ve školních prostorech by byla jejich další instalace také velkým zlepšením pro bezpečnost školy.
- **Hrozby** – v evropském měřítku převládají dle výzkumu uvedeném v dokumentu Základy ochrany měkkých cílů – metodika bombové útoky (viz Obrázek 2). Tento typ teroristických útoků a útoků na měkké cíle obecně se ovšem České republice zatím vyhýbá. Z tohoto důvodu a s ohledem na skutečnost, že z výše uvedené metody KARS (viz Obrázek 12) vyšly jako jedny z největších a nejpravděpodobnějších hrozeb žhář a agresor s chladnou zbraní, byly ke SWOT analýze vybrány tyto hrozby:
  - **aktivní střelec,**
  - **žhář,**
  - **agresor s chladnou zbraní.**

Tabulka 8 – SWOT analýza [vlastní]

Silné stránky (S)	Slabé stránky (W)
Zaměstnanci	Evakuace
Lokalita	Nedostatečné zabezpečení objektu
ID karty	Společnosti sídlící v objektu
Příležitosti (O)	Hrozby (T)
Vybudování dalšího východu z budovy	Aktivní střelec
Rozšířené školení žáků a učitelů v oblasti bezpečnosti	Žhář
Instalace dalších bezpečnostních prvků	Agresor s chladnou zbraní

Následně byla každá z těchto silných stránek, slabých stránek, příležitostí a hrozeb bodově ohodnocena s ohledem na jejich váhu a důležitost. Dalším krokem je součin těchto hodnot a následné sečtení výsledných hodnot v každé z kategorií.

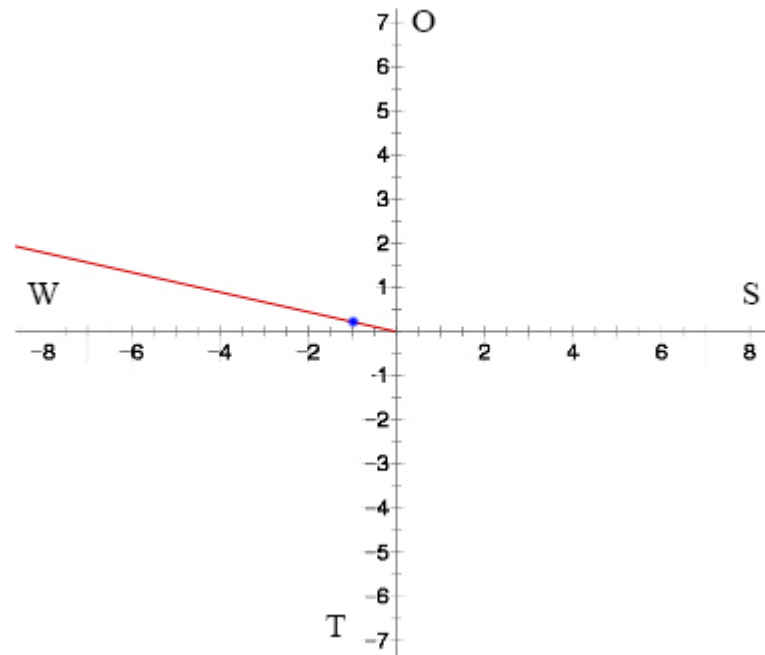
Tabulka 9 – Hodnocení jednotlivých kategorií SWOT analýzy [vlastní]

Silné stránky (S)	Váha	Hodnocení	Součin	Slabé stránky (W)	Váha	Hodnocení	Součin
Zaměstnanci	0,5	3	1,5	Evakuace	0,3	-4	-1,2
Lokalita	0,2	3	0,6	Nedostatečné zabezpečení objektu	0,4	-4	-1,6
ID karty	0,3	2	0,6	Společnosti sídlící v objektu	0,3	-3	-0,9
<b>Součet</b>	1	8	<b>2,7</b>	<b>Součet</b>	1	-11	<b>-3,7</b>
Příležitosti (O)	Váha	Hodnocení	Součin	Hrozby (T)	Váha	Hodnocení	Součin
Vybudování dalšího východu z budovy	0,3	4	1,2	Aktivní střelec	0,3	-3	-0,9
Rozšířené školení žáků a učitelů v oblasti bezpečnosti	0,3	3	0,9	Žhář	0,3	-3	-0,9
Instalace dalších bezpečnostních prvků	0,4	4	1,6	Agresor s chladnou zbraní	0,4	-4	-1,6
<b>Součet</b>	1	11	<b>3,7</b>	<b>Součet</b>	1	-10	<b>-3,4</b>

Dalším krokem je provedení součtu výsledných hodnot mezi jednotlivými kategoriemi, a to takto: součet silné a slabé stránky (interní) a součet příležitostí a hrozeb (externí).

- Silné stránky (S) a slabé stránky (W):  $2,7 + (-3,7) = -1$
- Příležitosti (O) a hrozby (T):  $3,7 + (-3,4) = 0,3$

Posledním krokem je rozdíl interních a externích kategorií, interní s hodnotou -1 a externí s hodnotou 0,3. Výsledná hodnota je tedy -1,3. Interní a externí hodnoty jsou dále zapsány do grafického znázornění, jehož výsledkem je jedna ze strategií, kterou by měla mateřská a základní škola využít ke zlepšení bezpečnosti. [20]



Obrázek 13 – Grafické znázornění SWOT analýzy [vlastní]

Po zapsání výsledků analýzy do grafu je patrné, že se jedná o strategii WO. Tato strategie se zaměřuje na překonání svých slabých stránek s využitím naskytnutých příležitostí. Znamená to, že v zabezpečení školy se nachází nedostatky, které je třeba vylepšit nebo úplně eliminovat.



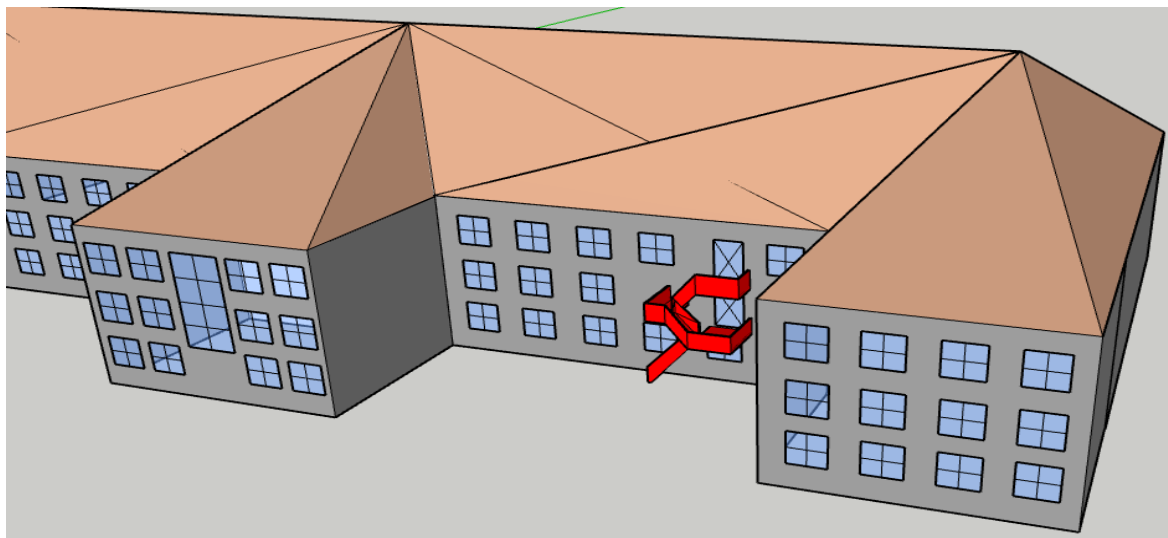
## 7 NÁVRH MOŽNÝCH OPATŘENÍ

Cílem této kapitoly je návrh opatření, kterými by se zvýšila bezpečnost vybraného měkkého cíle (Academic School, Mateřská a základní škola, s.r.o. v Uherském Hradišti), především vůči násilným útokům.

Jeden z největších přínosů, díky kterému by se zvýšila bezpečnost v prostorách školského zařízení, je vybudování dalších východů z budovy. Jak již bylo řečeno výše (viz kapitola 5.2.1), téměř jakýkoliv násilný útok, především útok aktivního střelce nebo žhářský útok mířený na schodiště budovy by mohl mít obrovské negativní následky. Z tohoto důvodu bylo navrženo vybudování východu z budovy. Vzhledem ke struktuře budovy a pozici školského zařízení v objektu je pro východ nejvhodnějším místem chodba ve třetím patře budovy. Z této chodby by bylo vyvedeno schodiště až k zemi s mezipatrem ve druhém patře objektu.

Tento krok by vyžadoval zrušení třech oken, přičemž místo dvou z nich (3. a 2. patro) by byly namontovány právě výstupní dveře. Výstupní dveře by bylo možné nainstalovat i v přízemním patře budovy, ale jelikož se na tomto místě nenachází prostory školského zařízení a žáci školy se zde nepohybují, nebyla tato možnost do návrhu zahrnuta. Dalším důvodem, proč nebyly v návrhu vytvořeny výstupní dveře i v přízemním patře objektu, je možnost úniku osob okny, které se nachází nízko nad zemí a nehrozí zde poranění.

V časech, kdy objekt není využíván, by schodiště a dveře mohly představovat riziko vniknutí osob, byly proto v návrhu zabezpečení ke každým z těchto dveří přidány PIR detektory (viz Obrázek 20-21). Vybudování tohoto východu z objektu chrání osoby nejen před útoky násilnými, ale také nenásilnými, jako je například vznik požáru. Model stávající podoby objektu a návrh schodiště je nastíněn níže (viz Obrázek 14) a v přílohách (viz Obrázek 15-18).



Obrázek 14 – Model návrhu východu z budovy [vlastní]

Další velkou slabinou objektu je absence EPS. Při provozu školského zařízení může dojít k požáru například vinou zhářského útoku, lidského selhání nebo při selhání elektroniky, která se nachází téměř v každé místnosti školského zařízení. Z tohoto důvodu bylo do návrhů opatření přidáno 21 detektorů EPS. Patnáct z těchto detektorů se nachází v druhém patře, kde bylo dvanáct z nich rozmístěno do tříd a kabinetů. Zbylé detektory byly umístěny do dvou menších chodeb před toaletami pro žáky a do kuchyňky pro kantory.

Ve třetím patře bylo navrženo rozmístění šesti detektorů EPS. Přidány byly do každé ze tříd a také do chodby před toaletami pro žáky. Takové rozmístění EPS by zaručilo bezpečnost před zhářskými útoky i před požáry způsobenými například selháním elektroniky. Plán návrhu zabezpečení EPS je znázorněn na obrázcích v přílohách (viz Obrázek 20-21), kde jsou detektory EPS označeny oranžovou barvou.

Dalším přínosem pro zlepšení bezpečnosti v objektu by byla instalace CCTV systémů. Hlavní přínos CCTV v kontextu ochrany před násilnými útoky je především v působení na psychiku útočníka, který by při zjištění přítomnosti těchto systémů mohl činu zanechat. Stejný účinek by mohla mít i mnohem levnější kamerová atrapa, ovšem ve školském zařízení je vhodné mít prostředky ke zpětnému vypátrání pachatele například při krádežích. Z těchto důvodů bylo do návrhů možných opatření ke zlepšení bezpečnosti objektu přidáno 6 kamerových zařízení.

První kamera byla umístěna za vchodové dveře v přízemí budovy, kde působí na psychiku útočníka okamžitě při příchodu do objektu a zároveň snímá dění u vstupu. Dvě kamery byly

umístěny do druhého patra. Jedna z nich snímá schodiště a druhá je umístěna tak, aby zachycovala prostor chodby, po které se může pohybovat veřejnost při návštěvách ostatních společností v objektu. Tato kamera monitoruje také navržený východ z budovy (viz Obrázek 14). Poslední tři kamerová zařízení byla nainstalována do třetího patra budovy. Jedna opět umístěna pro monitoring schodiště a další dvě na konce chodbových prostor školského zařízení, aby bylo znovu možné monitorovat veřejnost nepatřící ke škole a další navržený východ z budovy (viz Obrázek 14). Umístění kamerových zařízení v objektu je znázorněno na plánech zabezpečení školského zařízení v přílohách (viz Obrázek 19-21).

V rámci připravenosti osob ve školském zařízení na násilný útok by také bylo zlepšení v podobě cvičení. Nejvhodnějším k tomuto účelu se jeví cvičení ochrany proti aktivnímu střelci. Kantoři s žáky by zkoušeli svoje znalosti a dovednosti v kontextu ochrany proti tomuto útoku pomocí hesla utíkej/schovej se/bojuj (evakuace, barikády dveří atd.). Dle svého uvážení by v průběhu cvičení zkusili tyto varianty potřebné k přežití s vyhodnocením výsledků na konci cvičení a doporučením správného postupu v jednotlivých situacích. K tomuto účelu a také v kontextu vzdělávání žáků ohledně bezpečnosti může být nápomocna Fakulta logistiky a krizového řízení UTB ve Zlíně v rámci smlouvy o spolupráci.

## ZÁVĚR

Bakalářská práce byla zaměřena na problematiku ochrany měkkých cílů. Práce se dělí do dvou částí, a to část teoretickou a část praktickou.

Část teoretická je složena ze tří kapitol, přičemž první z nich se věnuje charakteristice měkkých cílů, jejich členění a problémům jejich ochrany. Další z kapitol se zabývá teoretickými základy zabezpečovacích systémů, jejich dělením a možnostem jejich použití. Třetí kapitolou práce je výběr základních pojmů, které se dotýkají problematiky ochrany měkkých cílů a jejich následná definice.

Část praktická je složena ze čtyř kapitol. Čtvrtá kapitola definuje cíle bakalářské práce a popisuje metody a analýzy, které byly v práci použity. Obsahem páté kapitoly je představení vybraného měkkého cíle, jeho popis a vyznačení jeho bezpečnostních prvků. Kapitola šestá je zaměřena na analýzu rizik, k čemuž byly zvoleny dvě metody. První z nich je metoda KARS, pomocí které byly zjištěny ty nejmenší, a naopak i největší rizika pro zvolený měkký cíl. Jedny z největších rizik byly poté použity pro další metodu, kterou je metoda SWOT analýzy. Pomocí této metody byla vytyčena strategie, kterou by se měl ubírat další rozvoj zvoleného měkkého cíle v kontextu se zabezpečením proti násilným útokům. Sedmá kapitola obsahuje návrhy inovací stávajícího zabezpečení zvoleného měkkého cíle.

Cíle práce byly definovány jako seznámení se s teoretickými základy měkkých cílů a jejich ochrany, zvolení konkrétního měkkého cíle, realizace analýzy rizik pro zvolený objekt s prioritním zaměřením na násilné útoky, vyhodnocení současného stavu zabezpečení objektu a navržení opatření pro jeho zlepšení.

Z analýz a výsledků vyplynulo, že objekt je sice způsobilý k provozu, avšak v jeho zabezpečení se nachází mezery, které by v případě násilného útoku mohly mít fatální následky.

**SEZNAM POUŽITÉ LITERATURY**

- [1] Bezpečnostní politika: Ochrana měkkých cílů. Ministerstvo vnitra České republiky [online]. Praha: MVČR, 2019 [cit. 2020-07-28]. Dostupné z: <https://www.mvcr.cz/clanek/ochrana-mekkych-cilu.aspx>
- [2] Čočky pro detektory. *Varnet* [online]. Praha: Varnet, c2020 [cit. 2020-07-28]. Dostupné z: <https://www.varnet.cz/zbozi/0701-103-cocky-pro-detektory-lr-4>
- [3] DVOŘÁČEK, Robin. *Prevence a ochrana měkkých cílů proti terorismu*. Ostrava, 2019. Magisterská práce. Vysoká škola báňská - Technická univerzita Ostrava. Vedoucí práce Prof. PhDr. Hana Vykopalová CSc.
- [4] DŽERMANSKÝ, Martin. *Zabezpečení společenských akcí*. Uherské Hradiště, 2019. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení. Vedoucí práce Ing. Jakub Rak, Ph.D.
- [5] HESTERMAN, Jennifer L. *Soft target hardening: protecting people from attack*. Boca Raton: CRC Press, Taylor & Francis Group, [2015]. ISBN 978-1-4822-4421-2.
- [6] CHOVANEC, Milan. *Koncepce ochrany měkkých cílů pro roky 2017-2020*. Praha: Ministerstvo vnitra, 2017.
- [7] JANOŠEC, Josef. *O terorismu: pro pracovníky bezpečnostního systému*. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2010. SPBI Spektrum. Červená řada. ISBN 978-80-7385-097-5.
- [8] KALVACH, Zdeněk. *ZÁKLADY OCHRANY MĚKKÝCH CÍLŮ METODIKA*. Praha: Ministerstvo vnitra, 2016.
- [9] KRUEGLE, Herman. *CCTV Surveillance: Video Practices and Technology 2nd Edition*. 2. Amsterdam: Butterworth-Heinemann, 2007. ISBN 978-0750677684.
- [10] KRÍŽEK, Tomáš. *Strategie ochrany měkkých cílů*. Brno, 2019. Magisterská práce. MASARYKOVA UNIVERZITA. Vedoucí práce PhDr. Martin Bugala, Ph.D.

- [11] KINDL, Jiří, 2004. Projektování bezpečnostních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 80-731-8165-7.
- [12] LUKÁŠ, Luděk, 2011. Bezpečnostní technologie, systémy a management. I. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-35-4.
- [13] LUKÁŠ, Luděk, 2012. Bezpečnostní technologie, systémy a management. II. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-19-4.
- [14] LUKÁŠ, Luděk, 2013. Bezpečnostní technologie, systémy a management. III. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-35-4.
- [15] LUKÁŠ, Luděk, 2014. Bezpečnostní technologie, systémy a management. IV. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-57-6.
- [16] LUKÁŠ, Luděk, 2015. Bezpečnostní technologie, systémy a management. V. Zlín: Radim Bačuvčík – VeRBuM. ISBN 978-80-87500-67-5.
- [17] Metodika pro aplikaci nové technické normy ČSN 73 4400. *Ministerstvo vnitra* [online]. Praha: Ministerstvo vnitra, 2017 [cit. 2020-07-28]. Dostupné z: <https://www.mvcr.cz/clanek/metodika-pro-aplikaci-nove-technicke-normy-csn-73-4400.aspx>
- [18] PARADOX PIR PRO plus. *Elnika* [online]. Praha: Elnika, c2020 [cit. 2020-07-28]. Dostupné z: [https://www.elnika.cz/cz/e-shop/zabezpecovaci-systemy-ezs/paradox-system-ezs/detektory-ezs/pir-pro-plus476-analogovy-pir-detektor-pohybu.html?fbclid=IwAR2EDssPR-NoqAaLwCg52VVvNzGgjkZ\\_TZzkF\\_1T9Se13geSqajrpJbssUxk](https://www.elnika.cz/cz/e-shop/zabezpecovaci-systemy-ezs/paradox-system-ezs/detektory-ezs/pir-pro-plus476-analogovy-pir-detektor-pohybu.html?fbclid=IwAR2EDssPR-NoqAaLwCg52VVvNzGgjkZ_TZzkF_1T9Se13geSqajrpJbssUxk)
- [19] PURPURA, Philip P. *Security: an introduction*. Boca Raton: CRC Press, c2011. ISBN 9781420092837.
- [20] SWOT analýza. *Cevelova* [online]. Praha, c2020 [cit. 2020-07-28]. Dostupné z: <https://www.cevelova.cz/proc-swot-analyza/>
- [21] *TERMINOLOGICKÝ SLOVNÍK POJMŮ Z OBLASTI KRIZOVÉHO ŘÍZENÍ, OCHRANY OBYVATELSTVA, ENVIRONMENTÁLNÍ BEZPEČNOSTI A PLÁNOVÁNÍ OBRANY STÁTU*. Praha: Ministerstvo vnitra, 2016.

- [22] Závěrečná práce - metodika. *Lorenc* [online]. Praha: Ministerstvo vnitra, 2013 [cit. 2020-07-28]. Dostupné z: <https://lorenc.info/zaverecne-prace/metodika.htm>
- [23] Zveřejnění české technické normy ČSN 73 4400 „Prevence kriminality – řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení“. *Ministerstvo vnitra* [online]. Praha: Ministerstvo vnitra, 2016 [cit. 2020-07-28]. Dostupné z: <https://www.mvcr.cz/clanek/zverejneni-ceske-technicke-normy-csn-73-4400-prevence-kriminality-rizeni-bezpecnosti-pri-planovani-realizaci-a-uzivani-skol-a-skolskych-zarizeni.aspx>

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

MZS	Mechanické zábranné systémy.
EPS	Elektrická požární signalizace.
PZTS	Poplachový zabezpečovací a tísňový systém.
CCTV	Closed Circuit Television (Uzavřený televizní okruh).
IR	Infračervené.
UV	Ultrafialové.
KARS	Kvalitativní analýza rizik s využitím jejich souvztažnosti.
SWOT	Analytická metoda srovnávající slabé a silné stránky, hrozby a příležitosti.
UTB	Univerzita Tomáše Bati.
PIR	Pasivní infračervené čidlo.
ČR	Česká republika.
ČSN	Česká technická norma.
LED	Elektroluminiscenční dioda.
IZS	Integrovaný záchranný systém.



**SEZNAM OBRÁZKŮ**

Obrázek 1 - Cíle teroristických útoků [5] .....	12
Obrázek 2 - Typy teroristických útoků [5] .....	12
Obrázek 3 – Systémové požadavky [15] .....	26
Obrázek 4 – Academic School [vlastní] .....	34
Obrázek 5 – Zábrana [vlastní] .....	36
Obrázek 6 – Rozhlasové zařízení [vlastní] .....	37
Obrázek 7 – Hasicí přístroj [vlastní] .....	37
Obrázek 8 – PARADOX PIR PRO Plus (476) [vlastní] .....	39
Obrázek 9 – Plán přízemního patra [vlastní] .....	40
Obrázek 10 – Plán 2. patra [vlastní] .....	42
Obrázek 11 – Plán 3. patra [vlastní] .....	44
Obrázek 12 – Graf souvztažnosti [vlastní] .....	51
Obrázek 13 – Grafické znázornění SWOT analýzy [vlastní] .....	56
Obrázek 14 – Model návrhu východu z budovy [vlastní] .....	58
Obrázek 15 – Model stávající podoby objektu [vlastní] .....	68
Obrázek 16 – Model návrhu schodiště [vlastní] .....	68
Obrázek 17 – Model návrhu schodiště (pohled z vrchu) [vlastní] .....	69
Obrázek 18 – Model návrhu schodiště 2 [vlastní] .....	69
Obrázek 19 – Návrh zabezpečení 1. patra [vlastní] .....	70
Obrázek 20 – Návrh zabezpečení 2. patra [vlastní] .....	71
Obrázek 21 – Návrh zabezpečení 3. patra [vlastní] .....	72

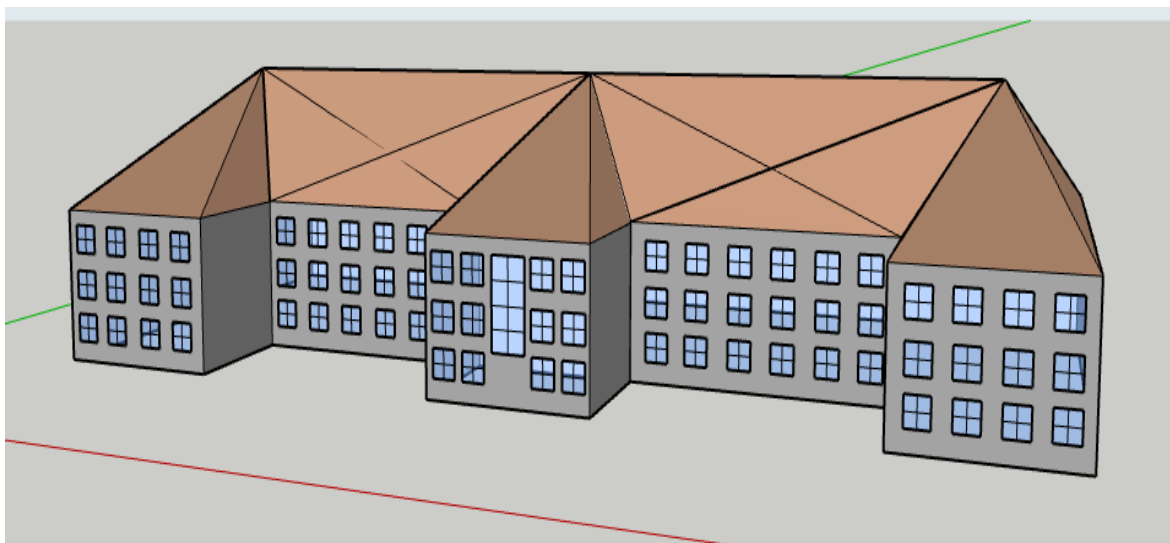
**SEZNAM TABULEK**

Tabulka 1 – Metody překonání vstupních dveří a ochrana proti nim [15] .....	16
Tabulka 2 – Kategorie prostředí [15].....	27
Tabulka 3 – Procentuální přepočítání úrovně rozpoznání osob [15] .....	29
Tabulka 4 – PARADOX PIR PRO Plus (476) [18].....	38
Tabulka 5 – Tabulka rizik [vlastní].....	47
Tabulka 6 – Vyplněná tabulka rizik [vlastní] .....	48
Tabulka 7 – Tabulka koeficientů aktivity a pasivity [vlastní] .....	50
Tabulka 8 – SWOT analýza [vlastní] .....	54
Tabulka 9 – Hodnocení jednotlivých kategorií SWOT analýzy [vlastní] .....	55

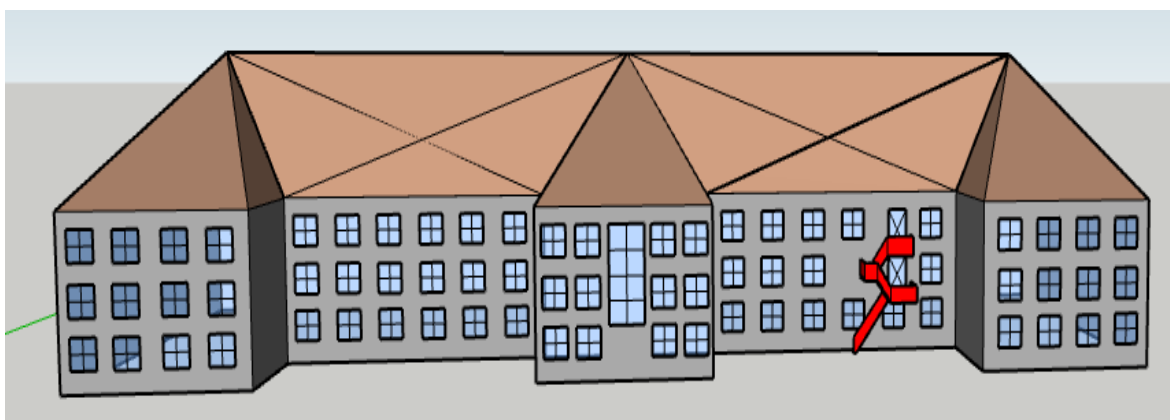
## SEZNAM PŘÍLOH

Příloha P I – Návrh zabezpečení prostor školy

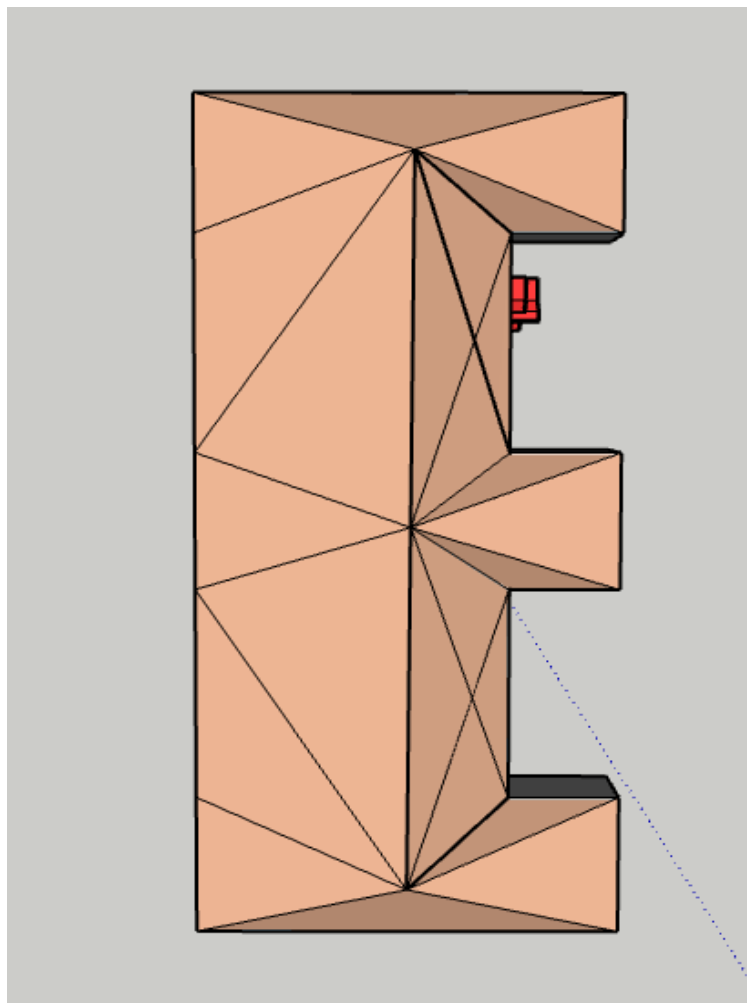
## PŘÍLOHA P I: NÁVRH ZABEZPEČENÍ PROSTOR ŠKOLY



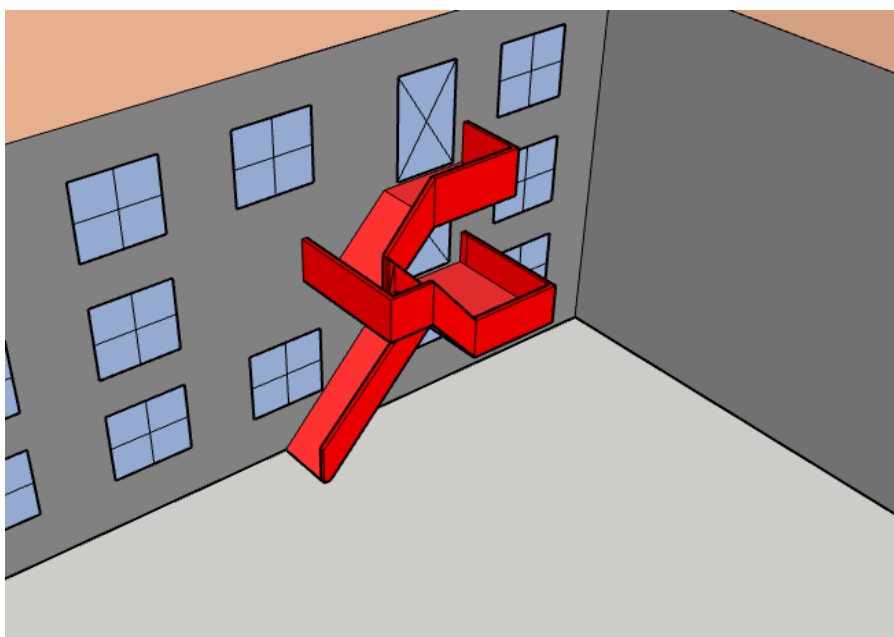
Obrázek 15 – Model stávající podoby objektu [vlastní]



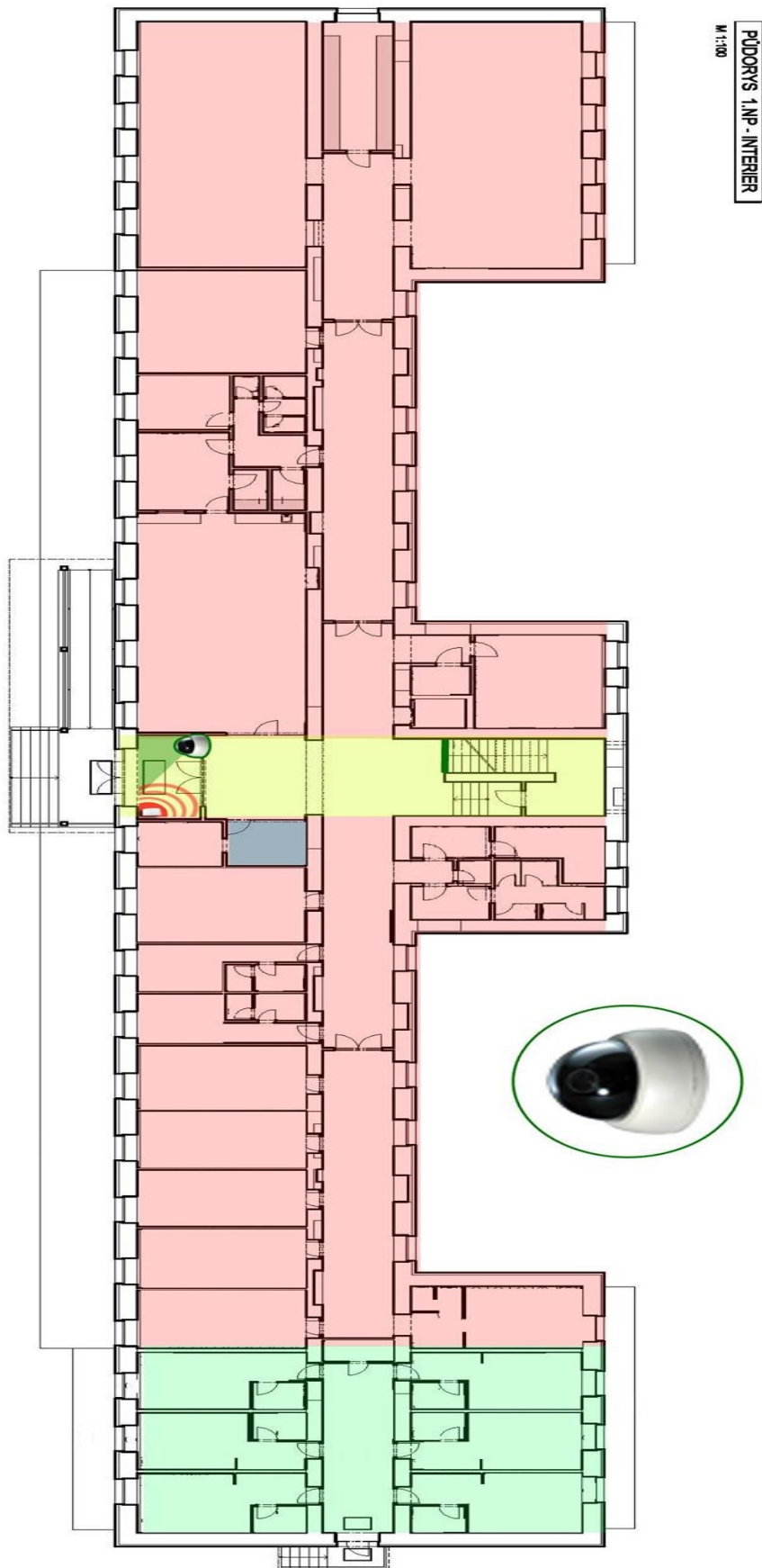
Obrázek 16 – Model návrhu schodiště [vlastní]



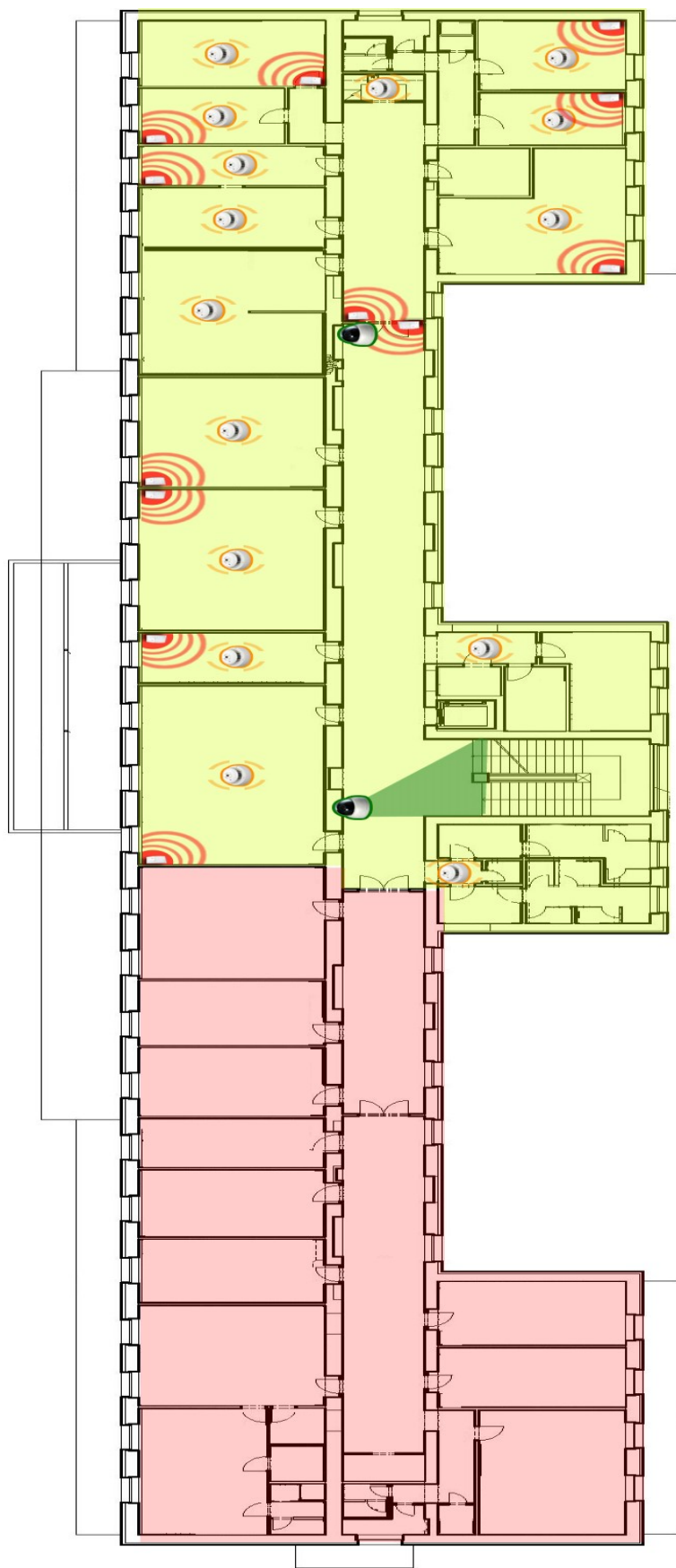
Obrázek 17 – Model návrhu schodiště (pohled z vrchu) [vlastní]



Obrázek 18 – Model návrhu schodiště 2 [vlastní]



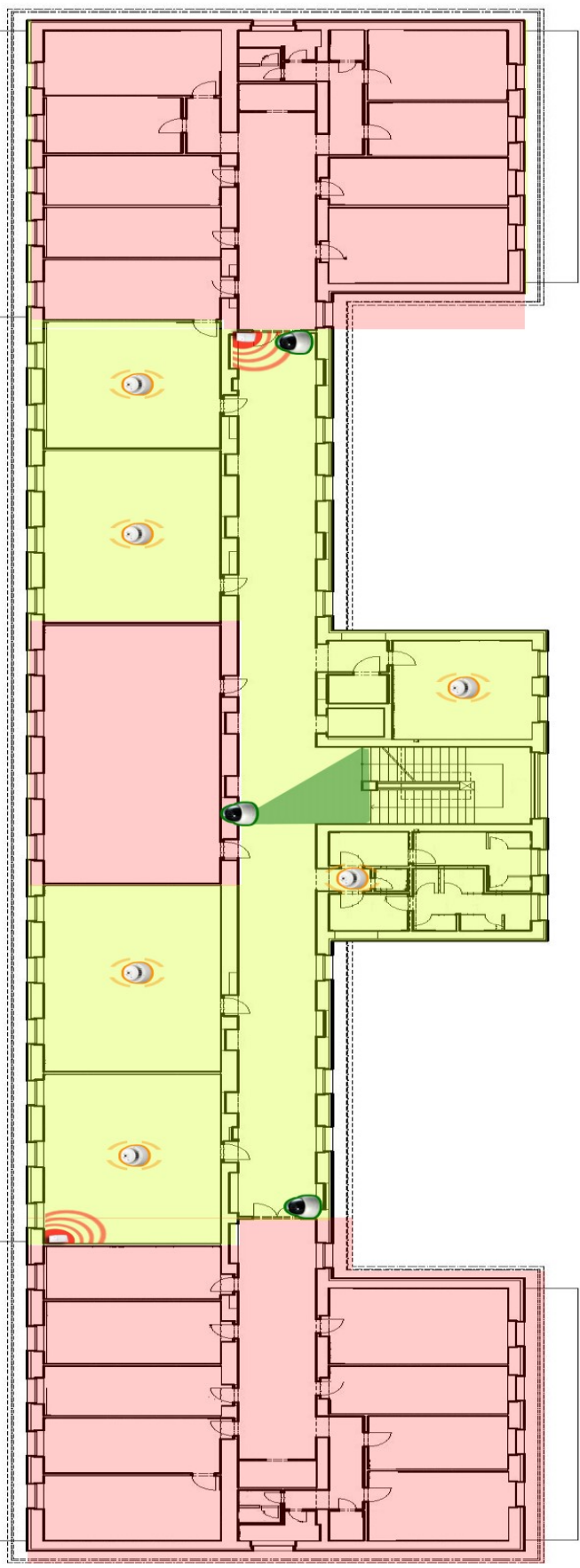
Obrázek 19 – Návrh zabezpečení 1. patro [vlastní]



PLANOVS 2.NP - INTERIER  
M 1:100

Obrázek 20 – Návrh zabezpečení 2. patro [vlastní]

PŮDORYS 3.NP - NAVRŽENÝ STAV  
M 1:100



Obrázek 21 – Návrh zabezpečení 3. patro [vlastní]