

Analýza a návrh opatření pro zvýšení bezpečnosti vybraného objektu

Bc. Klára Burdová

Diplomová práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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. Klára Burdová
Osobní číslo:	A23759
Studijní program:	N1032A020003 Bezpečnostní technologie, systémy a management
Specializace:	Bezpečnostní management
Forma studia:	Kombinovaná
Téma práce:	Analýza a návrh opatření pro zvýšení bezpečnosti vybraného objektu
Téma práce anglicky:	Analysis and Proposal of Measures to Increase the Security of a Selected Object

Zásady pro vypracování

- Seznamte se s teoretickými základy předmětné problematiky.
- Analytujte příslušné právní normy.
- Diskutujte o vybraných aspektech analýzy rizik a bezpečnostních opatřeních.
- Realizujte analýzu rizik a analýzu aktuálního stavu zabezpečení vybraného objektu.
- Popište stávající stav zabezpečení vybraného objektu.
- Navrhněte konkrétní opatření ke zvýšení bezpečnosti.

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

Seznam doporučené literatury:

1. BAKER, Paul R. a Daniel J. BENNY. The Complete Guide to Physical Security. Boca Raton: CRC Press, 2013. xxi, 339 s. ISBN 978-1-4200-9963-8.
2. IVANKA, J. Mechanické zábranné systémy. 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 978-80-7318-910-5.
3. KYNCL, Jaromír. Bezpečnost objektu ve světle moderních technologií. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.
4. LOVEČEK, Tomáš. Bezpečnostné systémy: poplachové systémy. Žilina: Edis, 2015. ISBN 978-80-5541-144-6.
5. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. 1. vydání. Ostrava: Key Publishing, 2011. ISBN 978-80-87500-05-7.
6. POPOV, Georgi, Bruce K. LYON a Bruce HOLLCROFT, eds. Risk Assessment: A Practical Guide to Assessing Operational Risks. Hoboken: Wiley, 2016. xxv, 451 s. ISBN 978-1-118-91104-4.

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 24.05.2025

Bc. Klára Burdová, v.r.
podpis autora

ABSTRAKT

Tato diplomová práce se zabývá problematikou zajištění bezpečnosti školských zařízení, konkrétně základní školy speciální, která je považována za vysoce zranitelný měkký cíl. Práce je rozdělena na teoretickou a praktickou část. Teoretická část se zaměřuje na vymezení základních pojmů, právního rámce, zásad bezpečnosti a metod řízení rizik s důrazem na využití vybraných metod. Praktická část zahrnuje charakteristiku vybraného objektu, identifikaci aktiv a hrozeb, aplikaci zvolených metod a experimentální ověření připravenosti zaměstnanců školy na mimořádnou událost. Výsledkem je návrh bezpečnostních opatření doplněný o ekonomický rámec, která směřují ke zvýšení celkové úrovně ochrany.

Klíčová slova: bezpečnost, hrozba, měkký cíl, ochrana, analýza rizik, bezpečnostní opatření

ABSTRACT

This thesis deals with the issue of ensuring the security of educational facilities, specifically a special elementary school, which is considered a highly vulnerable soft target. The thesis is divided into theoretical and practical parts. The theoretical part focuses on defining basic terms, the legal framework, security principles, and risk management methods, with an emphasis on the use of selected approaches. The practical part includes the characterization of the selected facility, identification of assets and threats, application of the chosen methods, and experimental verification of the school staff's preparedness for an emergency situation. The result is a proposal of security measures, supplemented by an economic framework, aimed at increasing the overall level of protection.

Keywords: Security, Threat, Soft Target, Protection, Risk Analysis, Security Measures

Ráda bych tímto poděkovala panu prof. Ing. Martinu Hromadovi, Ph.D., za jeho odborné vedení, cenné rady a podnětné připomínky, které mi během zpracování diplomové práce velmi pomohly. Velké poděkování patří také mému příteli za podporu a trpělivost, kterou mi věnoval po celou dobu mého studia.

OBSAH

ÚVOD.....	13
I TEORETICKÁ ČÁST.....	14
1.1 ZÁKONNÁ ÚPRAVA.....	15
1.2 PROVÁDĚCÍ PŘEDPISY	17
1.3 TECHNICKÉ NORMY A STANDARDY	18
1.4 METODICKÉ DOKUMENTY	19
1.5 TERMINOLOGICKÝ RÁMEC.....	21
2 BEZPEČNOSTNÍ HROZBA A RIZIKO	23
2.1 BEZPEČNOSTNÍ HROZBA	23
2.1.1 Klasifikace bezpečnostních hrozeb	23
2.2 BEZPEČNOSTNÍ RIZIKO	24
2.3 TEORETICKÝ RÁMEC MANAGEMENTU RIZIK	25
2.4 ŘÍZENÍ RIZIK.....	27
2.4.1 Identifikace rizik	27
2.4.2 Analýza rizik	28
2.4.3 Hodnocení rizik.....	30
2.4.4 Zmírnění rizik.....	31
2.4.5 Zvládání rizik	31
2.4.6 Ověření připravenosti v praxi.....	32
2.5 TYPY ANALÝZY RIZIK.....	33
2.5.1 Vybrané metody analýzy rizik	34
3 OBECNÁ VÝCHODISKA BEZPEČNOSTI.....	38
3.1 DĚLENÍ BEZPEČNOSTI.....	39
3.1.1 Security vs. Safety.....	39
3.1.2 Vnitřní a vnější bezpečnost	39
3.2 FYZICKÁ BEZPEČNOST	39
3.2.1 Struktura fyzické bezpečnosti dle prostorové charakteristiky	40
3.3 SOUČASNÉ TRENDY V OBLASTI BEZPEČNOSTI.....	41
3.3.1 Chytré kamerové systémy	42
3.3.2 Pokročilé systémy kontroly přístupu.....	43
3.3.3 IoT a chytré senzory	44
4 OCHRANA MĚKKÝCH CÍLŮ.....	47
4.1 ZÁKLADY OCHRANY MĚKKÝCH CÍLŮ.....	47
4.2 PRINCIPY OCHRANY MĚKKÝCH CÍLŮ.....	49
4.3 SPECIFIKA ŠKOL JAKO MĚKKÝCH CÍLŮ	50
4.3.1 Atraktivita cíle z pohledu útočníka	50

4.3.2	Reálné možnosti zabezpečení cíle	51
4.4	ZÁSADY OCHRANY ŠKOL	52
4.5	VYBRANÉ METODIKY	54
5	ZÁVĚR TEORETICKÉ ČÁSTI	59
II	PRAKTICKÁ ČÁST	60
6	CHARAKTERISTIKA VYBRANÉHO OBJEKTU	61
6.1	OBEZNÉ INFORMACE	61
6.2	UMÍSTĚNÍ OBJEKTU	62
6.3	IDENTIFIKACE AKTIV	64
6.4	IDENTIFIKACE HROZEB	65
7	ANALÝZA RIZIK.....	67
7.1	METODA CARVER.....	67
7.1.1	Aplikace metody CARVER	70
7.1.2	Vyhodnocení metody CARVER	72
7.2	METODA PNH	74
7.2.1	Aplikace metody PNH.....	75
7.2.2	Vyhodnocení metody PNH	75
7.2.3	Zjištěné skutečnosti na základě analýzy rizik	77
7.3	EXPERIMENT.....	78
7.3.1	Hypotéza.....	78
7.3.2	Použitá metoda	79
7.3.3	Popis scénáře experimentu	79
7.3.4	Subjekty experimentu.....	80
7.3.5	Výsledky experimentu.....	80
7.3.6	Závěr a hodnocení zjištěných skutečností	81
7.3.7	Zjištěné skutečnosti v rámci experimentu	81
7.4	DÍLČÍ EXPERIMENT	82
8	POPIS AKTUÁLNÍHO STAVU ZABEZPEČENÍ A DISPOZIČNÍHO USPOŘÁDÁNÍ VYBRANÉHO OBJEKTU	84
8.1.1	Perimetrická ochrana	84
8.1.2	Plášťová ochrana	86
8.1.3	Prostorová ochrana	87
9.1	NÁVRH PŘIPRAVENOSTI A VZDĚLÁVÁNÍ	103
9.2	NÁVRHY PRO ZVÝŠENÍ FYZICKÉ BEZPEČNOSTI.....	107
9.3	ORGANIZAČNÍ A REŽIMOVÉ OPATŘENÍ.....	111
9.4	PODPORA ZE STRANY ZŘIZOVATELE A MÍSTNÍ SAMOSPRÁVY	111
9.5	EKONOMICKÝ RÁMEC NÁVRHŮ BEZPEČNOSTNÍCH OPATŘENÍ	112
	ZÁVĚR.....	117
	SEZNAM POUŽITÉ LITERATURY	119

SEZNAM OBRÁZKŮ	128
SEZNAM TABULEK.....	129
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	130
SEZNAM PŘÍLOH	132

ÚVOD

Zajištění bezpečnosti objektů patří mezi zásadní témata současnosti, zvláště pokud se jedná o školní zařízení. Školy jsou totiž řazeny mezi tzv. měkké cíle a představují z pohledu krizového řízení a bezpečnostního plánování vysoce zranitelné prostředí. Ochrana škol by proto měla být prioritou, a to nejen kvůli zajištění bezpečí žáků a zaměstnanců, ale také jako prevence rizik spojených s neoprávněným vstupem, kriminalitou, požáry či dalšími mimořádnými událostmi. Tato diplomová práce se zaměřuje na problematiku bezpečnosti konkrétní základní školy speciální.

Cílem je provést analýzu rizik daného objektu, identifikovat aktiva a hrozby a následně navrhnout vhodná opatření vedoucí ke zvýšení úrovně ochrany.

Teoretická část práce se věnuje právnímu, metodickému a terminologickému rámci, metodám analýzy rizik, specifikům ochrany měkkých cílů a zásadám fyzické bezpečnosti. Popsány jsou rovněž mezinárodně uznávané přístupy k řízení rizik, zejména dle normy ČSN ISO 31000, a detailně rozpracovány dvě konkrétní metody, jedná se o metodu CARVER a PNH.

Praktická část se soustředí na obecnou charakteristiku školy, která je z důvodu ochrany citlivých údajů anonymizována. Následuje identifikace aktiv a hrozeb, aplikace metod CARVER a PNH a experimentální ověření připravenosti zaměstnanců a žáků na krizovou situaci. Výsledkem je komplexní návrh bezpečnostních opatření, která zároveň reflektují zjištěné nedostatky. Návrh je doplněn také o ekonomický rámec, jenž poskytuje vedení školy přehled o finanční náročnosti realizace doporučených kroků.

I TEORETICKÁ ČÁST

1 PRÁVNÍ, METODICKÝ A TERMINOLOGICKÝ RÁMEC PROBLEMATIKY

Tato kapitola vychází z rešerše relevantních právních předpisů, metodických dokumentů a odborných materiálů dostupných v České republice. Zdroje zahrnují platné zákony, vyhlášky, metodiky a doporučení vydané státními institucemi, zejména Ministerstvem vnitra, Ministerstvem školství mládeže a tělovýchovy, Českou agenturou pro standardizaci aj.

Rešerše probíhala prostřednictvím veřejně dostupných databází právních předpisů a oficiálních webových portálů státních institucí, jako jsou např. zakonyprolidi.cz, mvr.cz, msmt.cz, nbu.cz, pcr.cz nebo edu.gov.cz.

1.1 Zákonná úprava

Bezpečnost základních škol není v českém právním řádu upravena jednotně jedním zákonem. Ochrana života a zdraví, osob a to i např. v prostředí škol je však zakotvena v celé řadě právních předpisů. Jsou jimi např. základní ústavní dokumenty, speciální zákony upravující školství, práci, bezpečnost a ochranu zdraví, až po zákony související s požární ochranou či ochranou osobních údajů.

Níže jsou uvedeny relevantní příklady zákonů České republiky včetně konkrétních ustanovení, která se týkají bezpečnosti ve školním prostředí.

Ústava České republiky

Ústava České republiky (zákon č. 1/1993 Sb.) je základní zákon státu, který vymezuje jeho základní principy, strukturu státní moci a klíčové hodnoty. Byla přijata Českou národní radou dne 16. prosince 1992, vyhlášena ve Sbírce zákonů pod číslem 1/1993 Sb. a nabyla účinnosti 1. ledna 1993, tedy v den vzniku samostatné České republiky. [1]

Tvoří základ ústavního pořádku a spolu s Listinou základních práv a svobod zajišťuje ochranu základních práv a svobod jednotlivce. Přestože přímo neřeší otázku bezpečnosti ve školách, tvoří základní rámec, do kterého je nutno ochranu měkkých cílů zařadit.

Školský zákon

Školský zákon (zákon č. 561/2004 Sb.) je základní právní předpis upravující vzdělávání v České republice. Stanovuje práva a povinnosti škol, žáků, pedagogických pracovníků i zřizovatelů.

Ve vztahu k bezpečnosti jsou důležité zejména tyto paragrafy [2] [3]:

- **§ 22** – Žáci mají povinnost dodržovat pravidla školy a chránit své zdraví i zdraví ostatních.
- **§ 22a** – Práva pedagogických pracovníků na zajištění bezpečnosti a ochrany zdraví při práci, na ochranu před násilím, šikanou a jinými formami psychického nátlaku.
- **§ 22b** – Povinnosti pedagogů chránit bezpečnost a zdraví dětí, žáků a studentů, předcházet všem formám rizikového chování.
- **§ 29** – Povinnost školy zajišťovat bezpečnost a ochranu zdraví žáků při vzdělávání a s ním přímo souvisejících činnostech a při poskytování školských služeb.
- **§ 30** – Součástí školního řádu musí být také ustanovení, která stanoví pravidla pro zajištění bezpečnosti a ochrany zdraví žáků, stejně jako opatření zaměřená na prevenci sociálně patologických jevů. Jedná se o diskriminaci, násilné chování či jiné projevy nepřátelství.
- **§ 31** – Ochrana zdraví žáků při poskytování školních služeb.
- **§ 164 odst. 1 písm. h)** – Ředitel školy odpovídá za zajištění dohledu nad dětmi a nezletilými žáky ve škole a školském zařízení.

Zákon o požární ochraně

Zákon o požární ochraně (zákon č. 133/1985 Sb.) stanovuje povinnosti právnických i fyzických osob v oblasti požární ochrany. Pro školy z něj vyplývá povinnost přijímat opatření k ochraně žáků a zaměstnanců v případě požáru nebo jiných mimořádných událostí. Jedná se o následující paragrafy [4]:

- **§ 5 odst. 1 písm. b)** – Povinnost právnických osob (tedy i škol) zajišťovat požární bezpečnost provozovaných činností.
- **§ 15 odst. 1** – Povinnost vypracovat požární evakuační plán.
- **§ 16** – Povinnost provádět pravidelná školení zaměstnanců a cvičné evakuace.

Zákon o integrovaném záchranném systému

Zákon o integrovaném záchranném systému (zákon č. 239/2000 Sb.) upravuje činnost a organizaci složek integrovaného záchranného systému („dále jen IZS“), jejich vzájemnou součinnost a spolupráci s dalšími subjekty, včetně škol, při řešení mimořádných událostí.

Pro školy je důležité znát své postavení v systému krizového řízení a musí být připraveny na spolupráci s IZS. Spolupráce a součinnost je zmíněná v následujících paragrafech [5]:

- **§ 2 odst. 3** – IZS tvoří základní složky, které chrání život a zdraví. IZS může spolupracovat i s dalšími orgány a subjekty, např. školami.
- **§ 4** – Zásady přípravy na mimořádné události, povinnost škol spolupracovat s IZS.
- **§ 10** – Povinnost obcí a dalších subjektů (včetně škol) podílet se na ochraně života a zdraví.
- **§ 21 odst. 3** – Povinnost právnických osob spolupracovat s IZS při cvičeních a plnění opatření.

1.2 Prováděcí předpisy

Bezpečnost škol a školských zařízení se neřídí pouze zákony, ale i spoustou prováděcích předpisů. Tyto předpisy specifikují technické, organizační a režimové požadavky, které školy musí aplikovat zejména v oblastech požární ochrany, fyzického zabezpečení, hygieny či stavebního řešení budov. V praxi školám pomáhají převést zákonné povinnosti do konkrétních pravidel a postupů. Jsou také základem pro vytváření školních bezpečnostních plánů a dokumentací, které zařízení používá každý den.

Níže jsou uvedeny některé prováděcí předpisy vztahující se k bezpečnosti škol:

Vyhláška o technických podmínkách požární ochrany staveb

Vyhláška č. 23/2008 Sb., o technických podmínkách požární ochrany staveb stanovuje požadavky na požární bezpečnost staveb včetně školních budov. Řeší mimo jiné konstrukční požadavky na únikové cesty, vybavení požárně bezpečnostními zařízeními, rozmístění hasicích přístrojů nebo nouzové osvětlení. [6]

Vyhláška o fyzické bezpečnosti a certifikaci technických prostředků

Tato vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků stanovuje pravidla pro certifikaci a používání technických prostředků fyzické ochrany. Školy se podle ní mohou řídit při nastavování bezpečnostních opatření, např. výběru zámků, kamerových systémů nebo zabezpečených vstupů. [7]

Vyhláška o podmínkách požární bezpečnosti a výkonu státního požárního dozoru

Vyhláška č. 246/2001 Sb., o podmínkách požární bezpečnosti a výkonu státního požárního dozoru upravuje povinnosti právnických osob, včetně škol, v oblasti požární prevence. Ukládá zpracování konkrétních dokumentů a pravidelná školení zaměstnanců. [8]

1.3 Technické normy a standardy

Technické normy a standardy sice nejsou přímo závazné jako zákony, ale hrají důležitou roli při zajišťování bezpečí ve školách. Fungují jako osvědčené postupy a doporučení, podle kterých se dá řídit např. vstup do školy, technické vybavení nebo zajištění bezpečného provozu. Pomáhají školám dělat věci správně, předejít problémům a zároveň splnit zákonné požadavky na bezpečnost a ochranu zdraví.

Níže jsou uvedeny příklady technických norem, které lze využít k řízení bezpečnosti škol:

ČSN 73 4400 – Prevence kriminality

ČSN 73 4400 je česká technická norma zaměřená na prevenci kriminality a řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení. Byla zavedena 1. srpna 2016 a nabyla účinnosti 1. září 2016. Norma byla vypracována Technickou normalizační komisí TNK 148 „Prevence kriminality a ochrana obyvatel“ ve spolupráci s Ministerstvem vnitra ČR a dalšími odborníky. [9]

ČSN ISO 31000 – Management rizik

ČSN ISO 31000 je česká technická norma zaměřená na řízení rizik ve všech typech organizací. Poskytuje zásady a doporučení, jak systematicky identifikovat, hodnotit a zvládat rizika s cílem podpořit dosažení cílů organizace a zvýšit její odolnost. Norma byla zavedena 1. ledna 2019 a je vhodná pro jakýkoli obor i velikost organizace. [10] Více o této normě bude popsáno v podkapitole 2.3 Teoretický rámec managementu rizik.

Další normy v oblasti bezpečnosti

Zajištění bezpečnosti v základních školách, nelze chápat pouze jako otázku organizačních a režimových opatření či krizového plánování. Nedílnou součástí komplexní ochrany školního prostředí je i využití technických prostředků a systémů, jejichž kvalitu, funkčnost a bezpečnostní úroveň upravují příslušné technické normy.

Níže jsou uvedeny některé z nich a jsou rozděleny do tematických oblastí podle typu použité technologie či zabezpečovacího systému [11] [12] [13]:

a) mechanické zábranné systémy

- ČSN EN 1300 – Norma definuje kritéria pro zámky s vysokou úrovní zabezpečení, včetně jejich odolnosti vůči neoprávněnému vniknutí a manipulaci, a zároveň stanovuje metody jejich zkoušení.
- ČSN EN 1627 – Norma stanovuje podmínky a klasifikační systém pro hodnocení odolnosti proti vloupání u konstrukčních prvků, jako jsou dveře, okna, lehké obvodové pláště, mříže a okenice.

b) poplachové, zabezpečovací a tísňové systémy

- ČSN EN 50131-2-6 – Norma definuje technické a provozní požadavky na detektory otevření, tedy magnetické kontakty, které jsou součástí poplachových zabezpečovacích a tísňových systémů instalovaných ve vnitřních prostorech budov.
- ČSN EN 50134-1 – Norma stanovuje technické a funkční požadavky na systémy přivolání pomoci

c) kamerové systémy

- ČSN EN 62676-1-1 – Norma stanovuje minimální technické požadavky a poskytuje doporučení pro dohledové videosystémy (VSS), dříve označované jako CCTV, které jsou využívány pro účely zajištění bezpečnosti.
- ČSN EN 62676-4 – Norma stanovuje požadavky a doporučení pro výběr, projektování, instalaci, uvedení do provozu, údržbu a testování dohledových videosystémů (VSS). Tyto systémy zahrnují kamery, propojení a zařízení pro zpracování obrazu a jsou určeny k použití v bezpečnostních aplikacích.

1.4 Metodické dokumenty

Metodické dokumenty představují podpůrný nástroj pro školy a jejich zřizovatele při zavádění a udržování bezpečnostních opatření v praxi. Nejedná se o právně závazné předpisy, ale o doporučení a návody vycházející z aktuálních hrozeb, osvědčených postupů a zkušeností z praxe. Jejich cílem je poskytnout školám konkrétní pomoc při nastavování systémových i organizačních kroků k ochraně žáků, zaměstnanců a dalších osob v areálu školy.

Níže uvedené dokumenty představují příklady metodických materiálů, které se zaměřují na různé aspekty bezpečnosti ve školním prostředí:

Metodické doporučení v oblasti bezpečnosti a ochrany škol a školských zařízení jako měkkých cílů

Tento dokument se zaměřuje na problematiku ochrany škol a školských zařízení jako tzv. měkkých cílů, tedy míst, která jsou veřejně přístupná a snadno napadnutelná, např. v případě teroristických útoků nebo útoků žáků. Cílem je pomoci vedení škol lépe se orientovat v bezpečnostní problematice, pochopit základní terminologii a získat přehled o opatřeních, která mohou zvýšit bezpečnost školy. Metodika nabízí teoretický rámec (včetně přehledu legislativy) i praktické postupy, jak přizpůsobit bezpečnostní opatření specifickým podmínkám každé školy. [14]

Minimální standard bezpečnosti v regionálním školství

Materiál zpracovaný Ministerstvem školství, mládeže a tělovýchovy ve spolupráci s bezpečnostními složkami přináší ucelený soubor doporučení zaměřený na posílení fyzické bezpečnosti osob pohybujících se ve školním prostředí a během vzdělávacích aktivit. Dokument nahrazuje předchozí standardy a obsahuje hlavní dokument a 11 příloh, které detailně rozpracovávají jednotlivé oblasti bezpečnosti, například vstupní režim do školy, krizové situace nebo spolupráci s policií a hasiči. Doporučení je určeno pro všechny typy škol a má sloužit jako základní rámec pro nastavení bezpečnostních opatření. [15]

Škola a neštěstí: Jsme připraveni!

Tento dokument reaguje na skutečnost, že školy mohou zasáhnout různé nepříznivé události např. od úmrtí, šikany, pandemie, války až po přírodní katastrofy. Metodické doporučení poskytuje školám návod, jak na tyto situace adekvátně reagovat a jak se na ně připravit. Jedná se o aktualizovanou a rozšířenou verzi starší příručky a je kladen důraz nejen na zvládání samotných krizových situací, ale i na následnou podporu žáků, zaměstnanců a celé školní komunity. [16] Dokument bude podrobněji rozpracován v samostatné kapitole věnované ochraně měkkých cílů.

Manuál bezpečné školy

Manuál bezpečné školy vychází z české technické normy ČSN 73 4400 a shrnuje zásady a doporučení pro snižování rizika kriminality a antisociálního chování ve školách. Obsahuje návrhy bezpečnostních opatření, postupy pro krizové situace, doporučení pro

technické zabezpečení školy, režimová opatření i vzdělávání personálu. Manuál je určen ředitelům, pedagogům i zřizovatelům a pomáhá jim aplikovat normu v praxi, včetně upozornění na možná úskalí a časté chyby při zavádění bezpečnostních opatření. Dokument bude podrobněji rozpracován v samostatné kapitole věnované ochraně měkkých cílů. [10]

1.5 Terminologický rámec

Aktivum = osoba, objekt, zařízení, proces, informace nebo jiná hodnota, kterou je nutné chránit před hrozbami. [17]

Objekt = fyzická lokalita, budova, areál nebo zařízení, které je předmětem ochrany a správy podle bezpečnostních a provozních pravidel. [17]

Měkký cíl = objekt, prostor nebo skupina osob s nízkou úrovní fyzického zabezpečení a omezenými možnostmi obrany, často veřejně přístupný a snadno zranitelný vůči útokům. [18]

Tvrdý cíl = objekt nebo místo s vysokou úrovní zabezpečení, chráněný fyzickými bariérami, technickými prostředky a bezpečnostním personálem, obtížně přístupný a odolný vůči útokům. [18]

Bezpečnost = stav, kdy jsou osoby, objekty nebo informace chráněny před hrozbami, riziky a škodlivými vlivy, a existují účinné mechanismy prevence a reakce na ohrožení. [17]

Hrozba = potenciální příčina nežádoucí události, která může způsobit škodu nebo ztrátu na zdraví, majetku, informacích nebo provozu. [17]

Riziko = možnost, že dojde k události s negativním dopadem, přičemž se zvažuje pravděpodobnost výskytu a závažnost následků. [17]

Zranitelnost = míra náchylnosti objektu, systému nebo procesu k účinkům určité hrozby, často způsobená slabiny v ochraně, technologiích nebo organizaci. [17]

Prevence = soubor opatření a aktivit směřujících k zabránění vzniku rizikové nebo krizové situace, zahrnující plánování, vzdělávání, osvětu i technická opatření. [17]

Ochranná opatření = preventivní nebo reaktivní nástroje a postupy sloužící ke zvýšení bezpečnosti a minimalizaci dopadů hrozeb, zahrnující fyzické, technické i organizační prvky. [17]

Protiopatření (bezpečnostní opatření) = konkrétní kroky, systémy nebo postupy zavedené za účelem minimalizace rizik a posílení ochrany osob, majetku nebo informací. [17]

Bezpečnostní audit = odborné a systematické posouzení úrovně bezpečnosti v organizaci, jehož cílem je identifikace slabých míst a návrh opatření ke zlepšení. [17]

Krizové řízení = soubor procesů a nástrojů používaných k přípravě na mimořádné události, jejich zvládnutí a následné obnově běžného provozu organizace nebo společnosti. [17]

Evakuační plán = dokument obsahující jasné definované postupy pro bezpečné a organizované opuštění objektu nebo prostoru při ohrožení nebo mimořádné situaci. [17]

Incident = jakákoli událost, která narušuje běžný provoz, bezpečnost nebo integritu systému, a vyžaduje reakci k obnovení normálního stavu. [17]

Reakce na incident = soubor okamžitých a koordinovaných kroků přijatých ke zvládnutí neočekávané události ohrožující bezpečnost osob, majetku nebo provozu. [17]

Shrnutí kapitoly

První kapitola obsahuje přehled právních předpisů, technických norem a metodických dokumentů, které v České republice upravují oblast bezpečnosti školských zařízení. Uvádí rovněž konkrétní prováděcí vyhlášky, jež stanovují požadavky na požární bezpečnost, fyzické zabezpečení a krizovou připravenost škol. Významnou úlohu sehrávají také technické normy, jako jsou ČSN 73 4400 a ČSN ISO 31000, které napomáhají systematickému zavádění bezpečnostních opatření do školního prostředí.

Kapitola dále zdůrazňuje význam metodických dokumentů, které slouží jako opora pro školy a jejich zřizovatele při zavádění a udržování bezpečnostních opatření. Mezi nejdůležitější materiály patří Metodické doporučení k ochraně měkkých cílů a Minimální standard bezpečnosti v regionálním školství, které poskytují konkrétní postupy a doporučení pro různé krizové situace. Závěr kapitoly je věnován vymezení základních pojmů, které jsou stěžejní pro pochopení bezpečnostní problematiky.

2 BEZPEČNOSTNÍ HROZBA A RIZIKO

Bezpečnostní hrozby a rizika patří mezi stěžejní a zároveň rozsáhlé pojmy v oblasti bezpečnostního managementu, a proto jsou detailně rozpracovány v samostatné kapitole. Tyto jevy jsou v rámci mezinárodních vztahů úzce propojené a často se vzájemně překrývají. Základem každé bezpečnostní politiky je jejich systematická analýza, která se zaměřuje na povahu hrozeb, jejich pravděpodobnost a potenciální dopady. Hodnocení naléhavosti a závažnosti rizik tvoří klíčový podklad pro rozhodovací procesy v oblasti bezpečnostní strategie. Tyto rozhodovací pravomoci náleží zejména státním aktérům a mezinárodním organizacím, které určují směry a priority v oblasti bezpečnosti. [19]

2.1 Bezpečnostní hrozba

Bezpečnostní hrozba představuje objektivní jev, který působí nezávisle na prostředí, v němž se vyskytuje, a také nezávisle na vůli subjektů, kterých se týká. Její aktivace probíhá bez ohledu na přání nebo úmysly ohrožené strany a vyžaduje přijetí adekvátních opatření k omezení jejích dopadů. Hrozby mohou mít různorodou podobu, od fyzických útoků a kybernetických incidentů až po přírodní katastrofy nebo destabilizační jevy v ekonomické či sociální sféře. [19]

2.1.1 Klasifikace bezpečnostních hrozeb

Generální ředitelství Hasičského záchranného sboru České republiky (MV-GŘ HZS ČR) klasifikuje bezpečnostní hrozby v rámci dokumentu „Analýza hrozeb pro Českou republiku“ do dvou hlavních kategorií [20] [21]:

Naturogenní hrozby (přírodního původu):

- a) Abiotické – povodně, zemětřesení, sesuvy půdy,
- b) Biotické – pandemie, šíření nebezpečných chorob a virů,
- c) Kosmické – dopad kosmických těles, sluneční erupce.

Antropogenní hrozby (způsobené člověkem):

- a) Technogenní – průmyslové havárie, dopravní nehody, výpadky infrastruktury,
- b) Sociogenní – terorismus, násilné útoky, občanské nepokoje,
- c) Ekonomické – finanční krize, kolapsy trhu.

2.2 Bezpečnostní riziko

Bezpečnostní riziko má subjektivní charakter a vždy souvisí s rozhodováním a jednáním aktéra, který čelí určité hrozbě. Jeho výše závisí na tom, jak subjekt na tuto hrozbu zareaguje, jaká opatření přijme a jak účinná opatření budou. Riziko by nemělo být zaměňováno s událostmi, které nelze ovlivnit. Termín má smysl pouze tam, kde je výsledek do určité míry ovlivnitelný lidským jednáním nebo rozhodnutím. [19]

Z bezpečnostního hlediska vyjadřuje riziko pravděpodobnost, že dojde k nežádoucí události, která může ohrozit chráněné hodnoty, těmi jsou např. majetek, bezpečnost státu, zdraví nebo i život člověka. Riziko může přímo vycházet z konkrétní identifikované hrozby, nebo se může jednat o důsledek zranitelnosti systému vůči širšímu spektru ohrožení. [19] [22]

Posouzení rizika je základní součástí každého bezpečnostního řízení. Využívá se analýza rizik, která hodnotí pravděpodobnost a dopad hrozby ve vztahu k aktuální zranitelnosti systému a připravenosti subjektu reagovat. Výsledkem této analýzy je identifikace klíčových slabín a návrh odpovídajících preventivních nebo reaktivních opatření. [19] [22]

V oblasti krizového řízení a bezpečnostního managementu se často uplatňuje zjednodušený a v praxi využitelný přístup k vyhodnocení rizika. Riziko je zde chápáno jako součin dvou základních faktorů, a to pravděpodobnosti výskytu určité hrozby a závažnosti jejího dopadu. Tento model umožňuje vyjádřit riziko v číselné podobě a srovnávat ho v kontextu různých typů ohrožení. [19]

2.2.1 Potenciální rizika a jejich zdroje

Školní prostředí sdružuje žáky, učitele i další personál, přičemž se zde konají nejen běžné výukové aktivity, ale i akce s vyšší koncentrací osob (např. třídní schůzky, sportovní události, kulturní vystoupení). Tato koncentrace zvyšuje možnost vzniku krizových situací, které mohou ohrozit osoby, majetek, systémy i provoz školy. [23]

Přehled hlavních rizik:

- **Extrémní vnější vlivy** – klimatické jevy (bouřky, vichřice, povodně) a další havárie (úniky látek, epidemie, výbuchy).
- **Požár** – ohrožení života a zdraví, škody na majetku, nutnost evakuace.

- **Výpadky energií** – elektřina, voda, plyn, topení, internet, informační systémy.
- **Únik nebo ztráta citlivých dat** – osobní údaje žáků a zaměstnanců, napadení školní IT infrastruktury.
- **Neoprávněné vniknutí, vandalismus** – krádeže, poškození vybavení, zásah do dokumentace.
- **Podvodné jednání, sabotáž** – manipulace s výsledky, škody způsobené úmyslně.
- **Narušení během veřejných akcí** – protesty, neplánované shromáždění, obsazení školy.
- **Násilí a kriminalita** – ozbrojený útok, šikana, vydírání, únosy, teroristické hrozby.
- **Ergonomická a hygienická rizika** – nevhodné osvětlení, nábytek, větrání, přetížení zaměstnanců.
- **Biologická rizika** – kontakt s plísněmi, viry, bakteriemi, které mohou způsobit onemocnění.

2.3 Teoretický rámec managementu rizik

Management rizik představuje strukturovaný a systematický proces, jehož cílem je identifikovat, analyzovat a následně minimalizovat potenciální hrozby, které mohou negativně ovlivnit fungování organizace, její klíčová aktiva nebo zájmy. Tento proces zahrnuje soubor preventivních opatření a strategií zaměřených na snížení pravděpodobnosti výskytu nežádoucích událostí a zároveň na omezení jejich možných dopadů. [24]

V rámci tohoto přístupu organizace identifikuje aktuální nebo předpokládané hrozby, zhodnocuje jejich potenciální dopady a navrhuje vhodná bezpečnostní opatření. Tato opatření mohou mít technický, organizační i administrativní charakter a jejich efektivita by měla být průběžně vyhodnocována. Výsledkem dobře nastaveného řízení rizik je posílení odolnosti organizace, ochrana jejích zdrojů a stabilní bezpečnostní prostředí pro její činnost. [25]

Tento proces je zvláště významný v kontextu ochrany tzv. měkkých cílů a prvků kritické infrastruktury, jako jsou veřejné instituce, dopravní terminály či datová centra, kde může narušení bezpečnosti vést k závažným následkům.

Teoretický rámec managementu rizik je zakotven především v mezinárodní normě **ČSN ISO 31000** – Management rizik, která stanovuje obecně platné zásady a postupy pro systematické řízení rizik v jakémkoli typu organizace.

Norma ČSN ISO 31000 – Management rizik popisuje obecné zásady, rámec a procesy pro efektivní řízení rizik v organizacích. Je určena pro všechny typy organizací, bez ohledu na jejich velikost, odvětví nebo činnost. Hlavním cílem této normy je pomoci organizacím zvýšit pravděpodobnost dosažení jejich cílů, identifikovat příležitosti a hrozby a efektivně spravovat zdroje při řešení rizik. [26] Klíčové prvky normy jsou:

Zásady řízení rizik – musí být dodrženy pro efektivní řízení rizik. Tyto zásady zahrnují:

- integraci řízení rizik do všech organizačních procesů,
- přizpůsobení řízení rizik specifickému kontextu organizace,
- systematický, strukturovaný a včasný přístup,
- transparentnost a zapojení zainteresovaných stran,
- neustálé zlepšování na základě zkušeností.

Rámec řízení rizik – umožní integraci řízení rizik do celkového vedení organizace, její strategie, plánování a rozhodovacích procesů. Tento rámec zahrnuje:

- zavedení politiky řízení rizik,
- přidělení odpovědností a zdrojů,
- vytvoření procesů pro komunikaci a konzultace o rizicích.

Proces řízení rizik – je systematický a skládá se z následujících kroků:

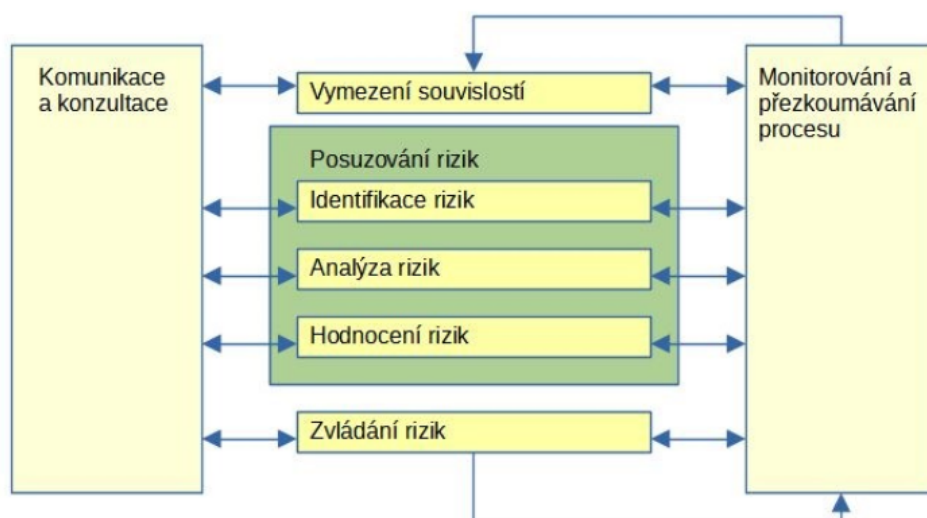
- komunikace a konzultace,
- stanovení kontextu,
- posuzování rizika,
- šetření,
- monitorování a přezkum,
- zaznamenávání.

Norma ČSN ISO 31000 zdůrazňuje, že riziko je definováno jako účinek nejistoty na cíle, přičemž tento účinek může být jak negativní (hrozba), tak pozitivní (příležitost). Implementace této normy podporuje proaktivní přístup k řízení nejistot, což přispívá

k lepšímu rozhodování, efektivnímu využívání zdrojů a dlouhodobé udržitelnosti organizací. [10]

2.4 Řízení rizik

Pro efektivní řízení rizik je nezbytné porozumět základním pojmům, především rozdílům mezi samotným rizikem a hrozbou. Klíčovými termíny jsou zejména hrozba (nebo také nebezpečí), chráněný zájem (aktivum) a riziko. [27]



Obrázek 1 Proces řízení rizik

(zdroj: [28])

2.4.1 Identifikace rizik

Identifikace rizik představuje úvodní a zároveň klíčovou fází procesu řízení rizik. Jejím cílem je systematicky rozpoznat potenciální hrozby, které mohou negativně ovlivnit chod organizace, bezpečnost osob, stabilitu klíčových procesů nebo ekonomickou výkonnost.

Proces začíná vymezením rozsahu analýzy, tedy určením, které aktivity, oblasti nebo aktiva budou předmětem hodnocení. Následuje sběr relevantních informací, a to jak z interních zdrojů (např. provozní dokumentace, incidenty z minulosti), tak z externích (oborové studie, konzultace s odborníky, benchmarking). Využívají se i metody jako brainstorming, strukturované rozhovory nebo analýza scénářů. [27] [28]

Pro lepší orientaci se rizika obvykle rozdělují do kategorií, jak bude zmíněno v kapitole 2.5 Typy analýzy rizik. Identifikaci napomáhá i využití specializovaných nástrojů, jako jsou

kontrolní seznamy, HAZOP (Hazard and Operability Analysis), FMEA (Failure Mode and Effects Analysis) nebo analýzy "co když". [27]

Výstupem je přehledně strukturovaný seznam rizik, který tvoří základ pro jejich další hodnocení. Správně provedená identifikace umožňuje organizaci cíleně reagovat na předvídatelná ohrožení a posiluje její připravenost na krizové situace. [28]

2.4.2 Analýza rizik

Analýza rizik je klíčovým nástrojem pro identifikaci, hodnocení a řízení potenciálních hrozeb, které mohou ovlivnit organizace, procesy nebo systémy. Správné pochopení a aplikace metod analýzy rizik umožňuje efektivně předcházet negativním dopadům a minimalizovat škody. Tato kapitola poskytuje podrobný přehled o různých typech analýzy rizik, metodách používaných k jejich provádění, specifických technikách analýzy, rámcích a standardech, které se v oblasti řízení rizik uplatňují. [27]

Základní postup při analýze rizik

Při tvoření analýzy rizik je nezbytné dodržovat následující kroky, které jsou na sobě závislé, jen tak lze dosáhnout co nejobjektivnějších výsledků:

Stanovení hranice analýzy rizik

Prvním krokem je vymezení hranice analýzy rizik, tedy určení, která aktiva budou či nebudou do analýzy zahrnuta. Tato hranice odděluje relativní aktiva a určuje se tak jejich důležitost.

Rozsah analýzy se stanovuje na základě záměrů managementu nebo úvodní studie. Klíčová aktiva související s cíli organizace budou analyzována, zatímco ostatní zůstávají mimo rozsah analýzy. [29]

Identifikace aktiv

Bezpečnostní analýza začíná identifikací aktiv, která mohou být ohrožena a která mají pro organizaci specifickou hodnotu. Aktiva zahrnují vše, co má pro organizaci hodnotu, a co může být ovlivněno hrozbou, ať už přímo nebo nepřímo. [30]

Aktivum je definováno jako prvek nebo část systému, která má pro organizaci určitou hodnotu, je ohrožena působením hrozeb a vyžaduje ochranu.

Aktiva se dělí na:

- a) Hmotná aktiva** – budovy, vybavení, zařízení, peněžní prostředky.

- b) **Nehmotná aktiva** – informace, pověst, know-how, softwarové licence, autorská práva.
- c) **Lidská aktiva** – zaměstnanci a jejich odborné znalosti, morálka, loajalita.
- d) **Organizační aktiva** – procesy, struktury a kultura organizace.

Je důležité chápat, že aktivem může být i samotná organizace jako celek, neboť hrozby mohou působit na její samotnou existenci. [30]

Identifikace hrozeb

V této fázi se stanovují potenciální hrozby, které by mohly ohrozit alespoň jedno ze zvolených aktiv. [29] [30]

Hrozby lze identifikovat na základě:

- a) **Seznamů hrozeb uvedených v literatuře,**
- b) **Vlastních zkušeností a analýz,**
- c) **Statutu organizace** (např. podnikatelský subjekt, veřejná instituce).

Pro systematickou identifikaci hrozeb lze využít metody, jako je brainstorming nebo metoda Delphi.

Analýza hrozeb a zranitelností

Každá hrozba se hodnotí ve vztahu ke konkrétním aktivům nebo jejich skupinám. U aktiv, která mohou být ohrožena, se stanovuje:

- **Úroveň hrozby** – míra nebezpečnosti, motivace útočníka a jeho přístup
- **Úroveň zranitelnosti** – citlivost a kritičnost aktiva vůči dané hrozbě.

Součástí analýzy je také zohlednění již existujících protiopatření, která mohou úroveň hrozeb i zranitelností snižovat. Výstupem této fáze je seznam dvojic "hrozba – aktivum", u kterých je stanovena úroveň ohrožení. [30]

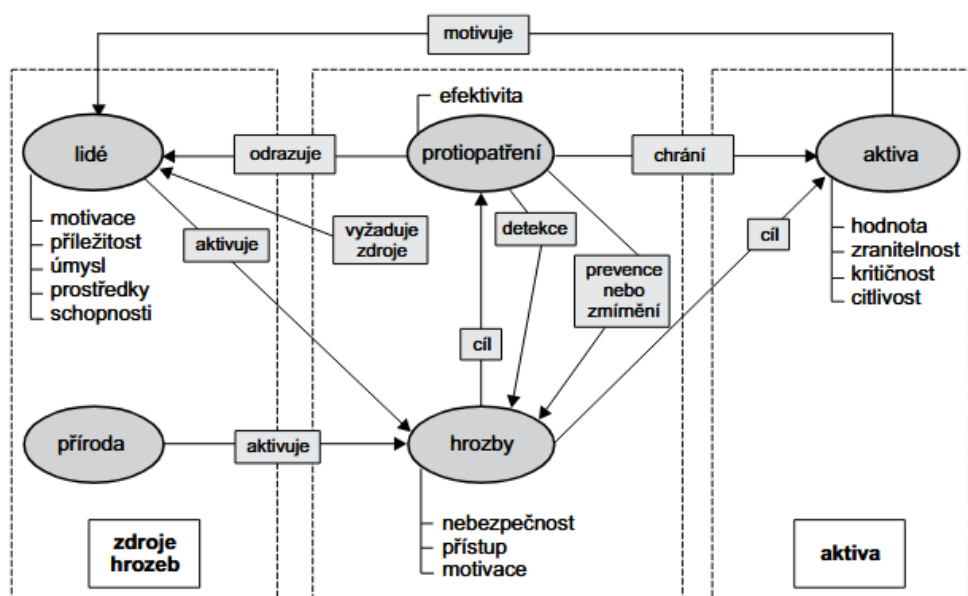
Stanovení pravděpodobnosti výskytu jevu

Zde se hodnotí pravděpodobnost, s jakou může daná hrozba ovlivnit analyzovaná aktiva. Pro její určení se využívají např. historická data a statistiky o výskytu podobných hrozeb, faktory ovlivňující úmyslné hrozby (motivace, schopnosti útočníka, přístup k cílům), faktory ovlivňující náhodné hrozby (geografická poloha, extrémní povětrnostní podmínky, lidská selhání) a úroveň existujících protiopatření a jejich efektivita. [30]

Měření rizika

Riziko se měří kombinací tří hlavních faktorů:

- I. Hodnota aktiva
- II. Úroveň hrozby
- III. Úroveň zranitelnosti aktiva



Obrázek 2 Schéma vztahů v řízení rizik

(zdroj: [30])

2.4.3 Hodnocení rizik

Hodnocení rizik je považováno také za zcela klíčový proces v rámci řízení rizik, který umožňuje organizacím určit pravděpodobnost a závažnost identifikovaných hrozeb. Tento proces poskytuje základ pro rozhodování o opatřeních, která povedou k minimalizaci negativních dopadů na aktiva, bezpečnost osob či plynulost provozu.

Hodnocení rizik obvykle probíhá v několika fázích. Nejprve se analyzuje pravděpodobnost výskytu rizika a jeho možný dopad na analyzovaný objekt či organizaci. Pro kvantifikaci těchto faktorů se často používají různé metody, jako je riziková matice, bodovací systémy nebo statistické analýzy. Následně se přistupuje ke klasifikaci rizik, která umožňuje rozlišit, zda se jedná o nízké, střední nebo vysoké riziko. [27] [30]

K hodnocení rizik lze využít různé nástroje, například analýzu scénářů, metodu Failure Mode and Effects Analysis (FMEA) nebo Hazard and Operability Study (HAZOP). Tyto metody pomáhají nejen s odhadem závažnosti a pravděpodobnosti, ale také umožňují efektivněji identifikovat možné způsoby snižování rizika. [27]

Výstupem hodnocení rizik je přehledná analýza, která poskytuje podklady pro další fázi řízení rizik. Správně provedené hodnocení umožňuje organizaci zaměřit se na prioritní oblasti, optimalizovat opatření a předejít možným krizovým situacím. [30]

2.4.4 Zmírnění rizik

Tato část se zaměřuje na kategorizaci, výběr a implementaci bezpečnostních opatření, jejichž cílem je systematicky snižovat identifikovaná rizika a minimalizovat jejich negativní dopady na chráněná aktiva organizace.

Kategorizace bezpečnostní opatření

Bezpečnostní opatření představují základní nástroj pro snížení úrovně rizik, která byla identifikována a analyzována v předchozích fázích řízení rizik. Tato opatření lze rozdělit do několika základních kategorií podle jejich povahy a způsobu účinku:

- **Fyzická bezpečnost** – zahrnuje veškerá opatření a technologie, jejichž cílem je zabránit fyzickému přístupu neoprávněných osob k chráněným aktivům organizace.
- **Organizační opatření** – spočívají v nastavení procesních pravidel, interních směrnic, bezpečnostních protokolů, rozdělení pravomocí a odpovědností.
- **Administrativní opatření** – např. školení, řízení přístupových práv, bezpečnostní audity, bezpečnostní kulturu organizace.
- **Personální opatření** – zaměřená na výběr, prověřování a proškolení zaměstnanců, včetně vytvoření bezpečnostně orientovaného firemního prostředí.

Tato opatření mohou být vzájemně kombinována s cílem dosáhnout požadovaného stupně ochrany. Úspěšné bezpečnostní strategie vyžadují vždy vícevrstvý přístup (princip obrany v hloubce - „defense in depth“). [31]

2.4.5 Zvládání rizik

Zvládání rizik představuje postup, jehož cílem je minimalizovat pravděpodobnost výskytu rizikových událostí a omezit jejich potenciální dopady na organizaci. Zvládání rizik zahrnuje

výběr a implementaci vhodných opatření, která zajistí efektivní řízení rizik v souladu s definovanými cíli a tolerancí rizika. [27]

Strategie zvládání rizik

Pro zvládání rizik existuje několik osvědčených a uznávaných strategií, které objekty a organizace volí na základě míry akceptovatelnosti daného rizika a jeho potenciálního dopadu [27]:

- a) **Vyhýbání se riziku (Risk Avoidance)** – Eliminace rizikové činnosti nebo její nahrazení bezpečnější alternativou.
- b) **Snížování rizika (Risk Reduction)** – Zavedení opatření (např. technických, organizačních, školení), která omezí pravděpodobnost výskytu nebo dopad.
- c) **Přenos rizika (Risk Transfer)** – Přenesení odpovědnosti na třetí stranu, např. pojištěním nebo outsourcingem.
- d) **Akceptace rizika (Risk Retention)** – Vědomé přijetí rizika v případech, kdy je nízké, nebo je jeho odstranění neproveditelné. Řízení probíhá skrze plánování a prevenci. [27]

2.4.6 Ověření připravenosti v praxi

Ověření připravenosti organizace na krizové situace je důležitým krokem v rámci řízení rizik. Nestačí vytvořit pouze teoretické postupy a krizové plány, ale je nezbytné je také otestovat v praxi. Systémy řízení musí být navrženy, zavedeny a otestovány již v předstihu, tedy dříve, než nastane reálná krizová situace. Zdůrazňuje se opakovaně slovo vyzkoušeny, neboť je známo mnoho případů, kdy to, co se jevílo na papíře bezchybně, bylo v praxi naprostým selháním. [30]

V rámci hodnocení úrovně připravenosti školského zařízení je potřeba věnovat pozornost nejen krizovým plánům, ale rovněž provázanosti těchto dokumentů se systémy včasného varování a celkovou schopností organizace správně reagovat na vznik mimořádné události. Důležité je správně vyhodnotit signály potencionální hrozby a následně ověřit důvěryhodnost těchto signálů. Na základě těchto zjištění by měla být přijata adekvátní opatření k řízení mimořádné situace, a to včetně nácviků připravenosti, vyhlášení příslušného stupně pohotovosti a zajištění informovanosti všech dotčených osob. [30]

Simulace a nácviky krizových scénářů tvoří nezbytnou součást přípravy. Prostřednictvím nich lze ověřit nejen připravenost jednotlivců, ale i celých organizací. Organizace a její jednotlivé složky by měly implementovat a udržovat tréninkové programy tak, aby se ujistily, že jejich BCM (Business Continuity Management – řízení kontinuity činností) a krizové řízení jsou dostačující, aktualizované a šité na míru. [30] [32]

Proces ověřování připravenosti přesahuje rámec pouhého testování již existujících opatření. Mezi stěžejní schopnosti krizového managementu patří dovednost předvídat možné scénáře mimořádných událostí a přijímat opatření s předstihem. Efektivní krizový manažer nepřistupuje k hrozbám pouze reaktivně, ale systematicky analyzuje potenciální rizika ještě před jejich samotným vznikem. V rámci této činnosti zvažuje různé varianty vývoje událostí, posuzuje jejich možné dopady a přijímá taková opatření, která umožňují udržet nad mimořádnými situacemi co největší míru kontroly. [30] [32]

Praxe ukazuje, že bez reálného ověření a procvičení zůstávají i sebelepší plány neúčinné. Je známo mnoho případů, kdy organizace disponovaly perfektními krizovými plány, ale v okamžiku skutečné krize selhaly z důvodů špatného nácviku nebo absence praktického ověření připravenosti. [32]

Z těchto důvodů je ověřování připravenosti prostřednictvím experimentů, modelových situací a nácviků nezbytnou součástí krizového řízení.

2.5 Typy analýzy rizik

Existuje několik typů analýzy rizik, které se používají v závislosti na specifické povaze subjektu a činnostech ovlivňujících riziko. Mezi nejčastěji používané metody patří:

a) Kvalitativní analýza rizik

Kvalitativní analýza rizik se zaměřuje na popisné hodnocení rizik pomocí kategorií, jako jsou "nízké", "střední" a "vysoké". Tento typ analýzy je vhodný pro situace, kdy chybí dostatečná data pro kvantitativní hodnocení nebo kdy je hlavním cílem rychlé posouzení rizik. Kvalitativní přístup je často využíván v oblasti řízení provozních rizik, kde experti na bezpečnost hodnotí možné scénáře na základě svých zkušeností a odborného úsudku.

Kvalitativní analýza rizik se nejvíce uplatňuje v situacích, kdy je potřeba rychlé rozhodování bez složitých matematických modelů. [27]

b) Semikvantitativní analýza rizik

Semikvantitativní analýza rizik kombinuje prvky kvalitativní a kvantitativní analýzy. Přidává číselné hodnoty ke kvalitativním kategoriím, čímž umožňuje lepší porovnání různých typů rizik. Například pravděpodobnost výskytu určitého rizika může být hodnocena na stupnici od 1 do 5, zatímco dopad může být vyjádřen jako finanční ztráta nebo ohrožení lidských životů.

Tento přístup je často využíván v oblasti fyzické bezpečnosti, kde je potřeba hodnotit různé typy hrozeb, jako jsou přírodní katastrofy, neoprávněné vniknutí nebo technologická selhání. Semikvantitativní analýza umožňuje organizacím přiřadit prioritní úroveň jednotlivým hrozbám a lépe plánovat opatření na jejich zmírnění. [27]

c) Kvantitativní analýza rizik

Kvantitativní analýza rizik se opírá o numerická data a statistické metody pro přesné vyčíslení pravděpodobnosti a dopadů rizika. Tento přístup je často využíván v průmyslovém a finančním sektoru, kde je důležité mít přesné údaje pro rozhodování. Kvantitativní analýza zahrnuje metodu, jako jsou analýza stromu událostí (ETA).

Pro přesné finanční nebo technické hodnocení rizika je právě kvantitativní analýza velice důležitá. Například při hodnocení bezpečnosti jaderných elektráren se kvantitativní metody používají k modelování možných havárií a k určení pravděpodobnosti jejich výskytu. Tento přístup vyžaduje rozsáhlá historická data a sofistikované analytické nástroje. [27]

2.5.1 Vybrané metody analýzy rizik

V předchozí části byly představeny základní typy analýzy rizik. Každý z představených přístupů využívá specifické metody a modely, které umožňují identifikovat, hodnotit a řídit rizika podle povahy analyzovaného subjektu a dostupných informací.

Tato kapitola se zaměřuje na dvě vybrané metody CARVER a PNH. Tyto modely představují konkrétní nástroje používané v praxi v rámci uvedených typů analýz a slouží k systematickému posuzování hrozeb, zranitelností a potenciálních dopadů na chráněné hodnoty. Uvedené metody budou dále použity v praktické části této práce k posouzení vybraných rizik.

Metoda CARVER

Mezi kvalitativní metody hodnocení rizik patří např. metoda CARVER, která slouží jako analytický nástroj pro identifikaci a posouzení zranitelných a kritických prvků infrastruktury. Název CARVER vychází z šesti hodnotících kritérií, kteří tvoří tzv. matici.

Matice metody CARVER je účinným nástrojem pro určení míry přijatelnosti rizik, a to na základě uvedených kritérií (kritičnost, přístupnost, obnovitelnost, zranitelnost, dopad a rozpoznatelnost). Matice CARVER je založena na součtu jednotlivých kritériálních hodnot u daného aktiva. [33]

Výpočetní vzorec: $\Sigma = C + A + R1 + V + E + R2$

C – bodové ohodnocení kritičnosti,

A – bodové ohodnocení přístupnosti,

R1 – bodové ohodnocení obnovitelnosti,

V – bodové ohodnocení zranitelnosti,

E – bodové ohodnocení dopadu na obyvatelstvo (např. žáky a zaměstnance),

R2 – bodové ohodnocení rozpoznatelnosti (predikovatelnosti hrozby). [34]

Výsledkem je pak celková hodnota, která umožňuje porovnat jednotlivé cíle/ aktiva objektu mezi sebou, identifikovat ty nejzranitelnější nebo nejvýznamnější prvky, a následně navrhnout nejefektivnější bezpečnostní opatření.

Tato metoda byla původně vyvinuta pro potřeby vojenského plánování. V současnosti nachází široké uplatnění i v civilní sféře např. v oblasti dopravy, zdravotnictví, energetiky, nebo analýze zranitelnosti měkkých cílů. [35]

V praxi se metoda CARVER používá k identifikaci a hodnocení kritických prvků infrastruktury v různých oblastech, ať už v železniční dopravě nebo energetice, jak bylo zmíněno již výše. Každý prvek je hodnocen bodově podle šesti hlavních kritérií, což umožňuje kvantifikovat jeho důležitost a zranitelnost. Tento přístup napomáhá organizacím se zaměřit na nejvíce ohrožené body a plánovat účinná bezpečnostní opatření. [36]

Metoda CARVER poskytuje objektivní a strukturovaný přístup k analýze bezpečnostních hrozeb. Její hlavní výhodou je schopnost upřednostnit rizika a alokovat bezpečnostní zdroje tam, kde jsou nejvíce potřeba. Výstupem analýzy je bodové hodnocení kritických prvků infrastruktury, které slouží jako podklad pro rozhodování o preventivních

opatření. V oblasti zdravotnické infrastruktury se metoda osvědčila při určování nejvíce ohrožených nemocnic a klíčových zdravotnických zařízení. [35]

Metoda PNH

Mezi semi-kvantitativní metody hodnocení rizik lze zařadit také metodu PNH (Preliminary Hazard Analysis), v českém prostředí často označovanou jako předběžná neboli preliminární analýza nebezpečí. Tato metoda je využívána především v počátečních fázích návrhu systémů, procesů či projektů, kdy ještě nejsou k dispozici podrobné technické údaje. Její hlavní výhodou je schopnost rychle identifikovat potenciální hrozby, které by mohly ohrozit bezpečnost osob, majetku či infrastruktury. [37]

V praktickém provedení se metoda PNH zaměřuje na identifikaci potenciálních rizikových faktorů spojených s jednotlivými prvky systému. Posouzení probíhá na základě stanovených charakteristik, jako je kritičnost daného aktiva, jeho přístupnost, schopnost obnovy po incidentu, zranitelnost, dopad na okolní systém a míra rozpoznatelnosti. Každému z těchto kritérií je přiřazena bodová hodnota podle předem definované stupnice, což umožňuje semi-kvantitativní vyjádření míry rizika. Výsledné skóre pak slouží k určení priority rizik a následnému návrhu vhodných preventivních opatření. Tento strukturovaný přístup pomáhá systematicky vyhodnocovat bezpečnostní situaci objektu a rozhodovat o efektivní alokaci ochranných prostředků. [38]

Výpočetní vzorec: $R = P \times N \times H$

P – představuje pravděpodobnost výskytu,

N – závažnost možných následků

H – schopnost odhalení rizika.

Výstupem metody PNH je seznam identifikovaných rizik seřazených dle jejich závažnosti, což usnadňuje stanovení priorit pro přijetí preventivních či zmírňujících opatření. [37]

Shrnutí kapitoly

Kapitola se věnuje problematice bezpečnostních hrozeb a rizik jako klíčových prvků bezpečnostního managementu. Hrozby jsou rozděleny do dvou hlavních kategorií, a to na hrozby přírodního původu a hrozby způsobené lidskou činností. Dále jsou popsány situace, které mohou narušit chod organizace např. přírodní katastrofy, technologické havárie, terorismus, násilí ve školách, výpadky infrastruktury a úniky dat.

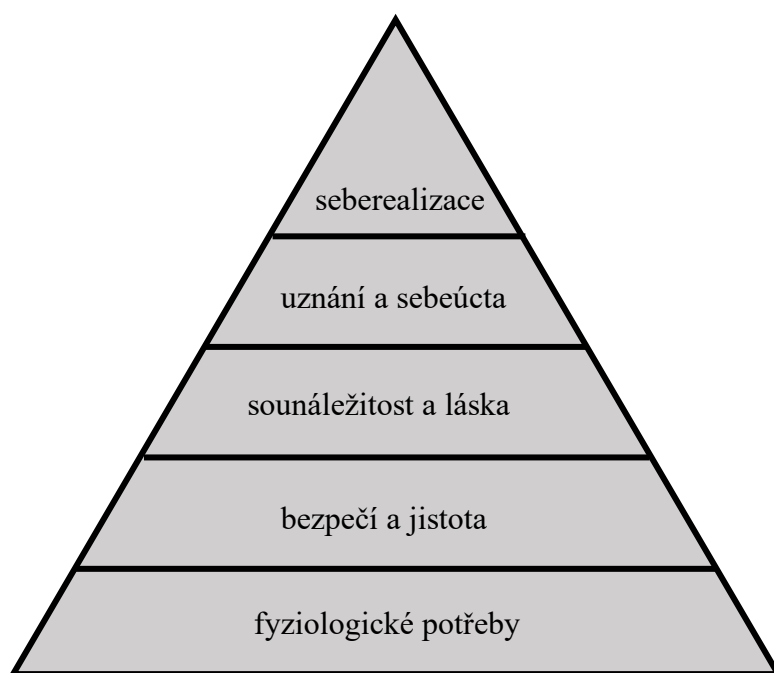
Dále kapitola rozvádí přístup k řízení rizik prostřednictvím mezinárodně uznávané normy ČSN ISO 31000. V kapitole je popsán celý proces řízení rizik, který zahrnuje identifikaci, analýzu, hodnocení rizik, návrh konkrétních bezpečnostních opatření a ověření připravenosti v praxi. Významnou součástí tohoto procesu je i příprava školních zařízení na různé krizové situace s důrazem na plánování, školení zaměstnanců a testování krizových systémů.

V závěrečné části kapitoly jsou představeny tři kategorie analýzy rizik: kvalitativní, semikvantitativní a kvantitativní analýza. Následně jsou podrobněji popsány metoda CARVER (z oblasti kvalitativní analýzy) a metoda PNH (z oblasti semikvantitativní analýzy), které budou využity v praktické části práce.

3 OBECNÁ VÝCHODISKA BEZPEČNOSTI

Pojem „bezpečnost“ vychází z českého výrazu „bez péče“, což vyjadřuje stav bez starostí, mimo nebezpečí. V moderním pojetí jde o komplexní kategorii, která se vztahuje k ochraně a stabilitě systému – ať už jde o stát, organizaci, komunitu nebo jednotlivce. Zahrnuje opatření, procesy a strategie zaměřené na eliminaci nebo minimalizaci hrozeb, které mohou ohrozit chráněné zájmy. [22]

Bezpečnost má také psychologický rozměr. Pocit bezpečí je v zásadě jedna ze základních lidských potřeb. Podle teorie amerického psychologa Abrahama Maslowa je bezpečí, hned po fyziologických potřebách, druhou nejdůležitější podmínkou pro stabilní a kvalitní život. Teprve po jejím naplnění může člověk usilovat o vyšší potřeby např. sociální vztahy, uznání a seberealizaci. [39]



Obrázek 3 Maslowova pyramida potřeb

(zdroj: [39])

V současné době nabývá problematika bezpečnosti na významu napříč všemi úrovněmi, od státní správy až po jednotlivé organizace, instituce a podniky. Bezpečnostní politika představuje nástroj řízení, jehož cílem je stanovit jasné priority, metody, analýzy a postupy pro identifikaci, prevenci a minimalizaci různých typů hrozeb. Slouží jako rámec

pro systematické zabezpečení chráněných hodnot, a to jak v oblasti fyzické bezpečnosti, tak v oblasti informační, provozní či personální ochrany. [23]

3.1 Dělení bezpečnosti

Bezpečnost lze členit podle několika kritérií, a to podle charakteru, původu hrozeb i typu ohrožení. Toto členění pomáhá volit odpovídající strategie ochrany a vhodná opatření.

3.1.1 Security vs. Safety

V některých jazycích, např. anglickém a francouzském, se bezpečnost rozlišuje na dva termíny:

- a) **Security / sécurité** označuje ochranu před záměrnými hrozbami jako jsou útoky, kriminalita nebo sabotáže – tedy fyzická, informační nebo personální bezpečnost.
- b) **Safety / sûreté** se vztahuje k ochraně před neúmyslnými nebo technickými riziky jako jsou nehody, požáry, technologické havárie nebo selhání zařízení.

Toto rozlišení je důležité i pro volbu vhodných bezpečnostních opatření, zejména při tvorbě bezpečnostních plánů pro měkké cíle. [40] [41] Např. mechanická zábrana proti vjezdu vozidel je typickým příkladem *security*, zatímco detektory kouře spadají do oblasti *safety*.

3.1.2 Vnitřní a vnější bezpečnost

Z hlediska objektu, jehož ochrana má být zajištěna, lze bezpečnost rozdělit na dvě hlavní kategorie:

- a) **Vnitřní bezpečnost** se zaměřuje na ochranu, prevenci a eliminaci rizik pocházejících zevnitř daného objektu např. technické poruchy, lidské selhání, škodlivé jednání personálu.
- b) **Vnější bezpečnost** zahrnuje ochranu, prevenci a eliminaci rizik přicházejících z vnějšího prostředí jako jsou teroristické útoky, vandalismus, násilné činy nebo narušení veřejného pořádku. [22]

3.2 Fyzická bezpečnost

Fyzická bezpečnost je klíčovou složkou celkového bezpečnostního systému každé organizace. Jejím hlavním cílem je zabránit přístupu neoprávněným osobám, odhalit

případné pokusy o narušení a zajistit bezpečí osob, majetku a infrastruktury v objektu. V kontextu školního prostředí představuje základní linii obrany před hrozbami vnějšího i vnitřního charakteru. [42]

3.2.1 Struktura fyzické bezpečnosti dle prostorové charakteristiky

Moderní koncepce fyzické bezpečnosti se opírá o vícevrstvý model ochrany, kdy každá vrstva plní specifickou funkci a posiluje celkovou odolnost systému. Takové uspořádání bývá označováno jako obrana v hloubce („defense in depth“). [31] [43]

Z hlediska praktické aplikace v objektech typu škol se využívá dělení na tyto čtyři úrovně:

a) Plášťová ochrana

První kontaktní vrstva chrání perimetr objektu. Zajišťuje odstranění snadného přístupu a vizuální signalizaci hranic [31, 43]:

- oplocení areálu, brány, závory,
- vnější osvětlení prostor,
- detektory pohybu,
- kamerové systémy zaměřené na vnější perimetr.

b) Perimetrická ochrana

Zajišťuje kontrolu nad vstupem do areálu či budovy. Opatření na této úrovni se zaměřují na regulaci přístupu a odlišení oprávněných a neoprávněných osob [31] [43]:

- vrátnice, turnikety, recepce,
- elektronické přístupové systémy (RFID čtečky, kódové zámky),
- registrace návštěv, školení vrátných.

c) Prostorová ochrana

Zahrnuje dispozice uvnitř objektu – školní budovy a jejích částí. Cílem je omezit volný pohyb a zpomalit postup útočníka [31] [43]:

- zónování budovy (např. oddělení tříd, kabinetů, serveroven),
- vnitřní kamery a pohybová čidla,
- uzamykatelné místnosti, skříně a dveře s vyšší bezpečnostní třídou.

d) Objektová ochrana

Nejvnitřnější vrstva zabezpečení, která se vztahuje ke konkrétním cenným nebo citlivým místům [31] [43]:

- trezory, učitelské dokumentace, informační systémy,
- místnosti s chemikáliemi, laboratoře, archivy,
- vstup jen pro vybrané osoby, biometrická identifikace, alarmy.

Toto dělení pomáhá při plánování a správném rozmístění prostředků ochrany a umožňuje cíleně alokovat rozpočtové a personální zdroje. V prostředí školy přispívá také ke zvýšení pocitu bezpečí mezi žáky, pedagogy i rodiči [43] [44].

3.3 Současné trendy v oblasti bezpečnosti

Oblast fyzické bezpečnosti v posledních letech prochází dynamickým rozvojem, v němž klíčovou roli hrají nové technologie, zejména umělá inteligence (AI – Artificial Intelligence), pokročilé kamerové systémy a automatizované zabezpečovací systémy. Významně se prosazují také technologie strojového učení (ML – Machine Learning), datové analýzy a Edge computing (distribuovaný výpočetní model, který přesouvá výpočetní výkon a zpracování dat blíže ke zdroji jejich vzniku, například k IoT zařízením, senzorům či lokálním serverům). Tyto pokročilé technologie umožňují přesnější detekci hrozeb, rychlejší reakce na incidenty a prediktivní ochranu před riziky. [45] [46]

Vývoj kriminality přitom potvrzují i aktuální statistiky Policie ČR. V oblasti násilné kriminality byl v roce 2024 zaznamenán mírný nárůst o 4,5 %, zejména u nebezpečného vyhrožování (nárůst o 19,1 %), vydírání (nárůst o 17,3 %) a nebezpečného pronásledování (nárůst o 20,9 %). Celkem bylo registrováno 12 919 skutků, což je o 570 více než v předchozím roce 2023. [47]

V reakci na tyto bezpečnostní výzvy stále více organizací zavádí inovativní technologie a hybridní bezpečnostní strategie, které kombinují lidský faktor s pokročilými technologiemi. Díky využití umělé inteligence, moderních kamerových systémů, automatizace a technologií Edge computingu je dnes možné nejen výrazně zvýšit efektivitu bezpečnostních opatření, ale také lépe předvídat a rychleji reagovat na potenciální hrozby. Tento dynamický vývoj přináší nové příležitosti, jak chránit objekty, instituce i kritickou

infrastrukturu v prostředí, které je čím dál komplexnější a náročnější z hlediska bezpečnosti. [45]

3.3.1 Chytré kamerové systémy

Umělá inteligence (AI) a strojové učení (ML) se v posledních letech stávají klíčovými prvky moderních bezpečnostních systémů. Tyto technologie umožňují provádět real-time analýzu chování, identifikaci anomálií a automatické upozorňování na potenciální hrozby. Například AI systémy dokážou detekovat neobvyklé pohyby nebo shlukování osob v oblastech, kde to není běžné, a okamžitě informovat bezpečnostní personál. Tím se snižuje závislost na lidském dohledu a výrazně se zvyšuje efektivita reakce na incidenty. [46]

V současné době lze VSS, neboli video surveillance systém, přirovnat k nikdy nekončícímu filmu. S rostoucím počtem instalovaných kamer narůstají i nároky na monitorování, což vyžaduje stále více lidských zdrojů. Vyšetřování a dokumentace incidentů obvykle znamená pracné procházení záznamů. AI systémy přinášejí budoucnost v podobě inteligentního, real-time videodohledu, kdy automatizované analýzy chování včas identifikují potenciální hrozby a podezřelé aktivity a okamžitě upozorňují operátory. [48]

Další přínos AI spočívá v eliminaci nadbytečných poplachů. Operátoři jsou často zahlceni množstvím falešných alarmů, což může vést k jejich otupení vůči skutečným hrozbám. Snížením počtu nerelevantních upozornění AI zvyšuje efektivitu bezpečnostních operací a umožňuje je škálovat bez neúměrného navyšování lidských zdrojů. [49]

Kamerové systémy od Axis Communications

Reálným příkladem integrace AI jsou kamerové systémy AXIS. Tyto kamery využívají pokročilé technologie videoanalýzy, detekce pohybu a rozpoznávání objektů v reálném čase. Vysoké rozlišení obrazu a funkce jako Lightfinder 2.0 a Forensic WDR umožňují kvalitní monitorování za jakýchkoli světelných podmínek, přičemž zařízení podporují napájení přes Ethernet (PoE). Díky tomu je i instalace systému mnohem snadnější. [50]

Pro školská zařízení je vhodným modelem například AXIS M4216-LV, což je IP kamera odolná vůči vandalismu, ideální pro monitorování vstupních prostor, školních hřišť a okolí budov. Tento model nabízí technologie Lightfinder 2.0 pro lepší barevné vidění za tmy, Forensic WDR pro vyrovnávání kontrastů, integrované IR přisvícení a pokročilou videoanalytiku s využitím umělé inteligence. [50]

Významnou součástí Axis řešení je právě Axis Object Analytics – sofistikovaná platforma pro inteligentní analýzu objektů. Tento software umožňuje kamerám AXIS automaticky určovat a rozlišit různé typy objektů, například lidi, vozidla atd., na základě specifických scénářů přizpůsobených potřebám uživatele. Díky tomu lze lépe filtrovat relevantní události, eliminovat falešné poplachy, a ještě přesněji identifikovat potenciální hrozby v reálném čase. [51]

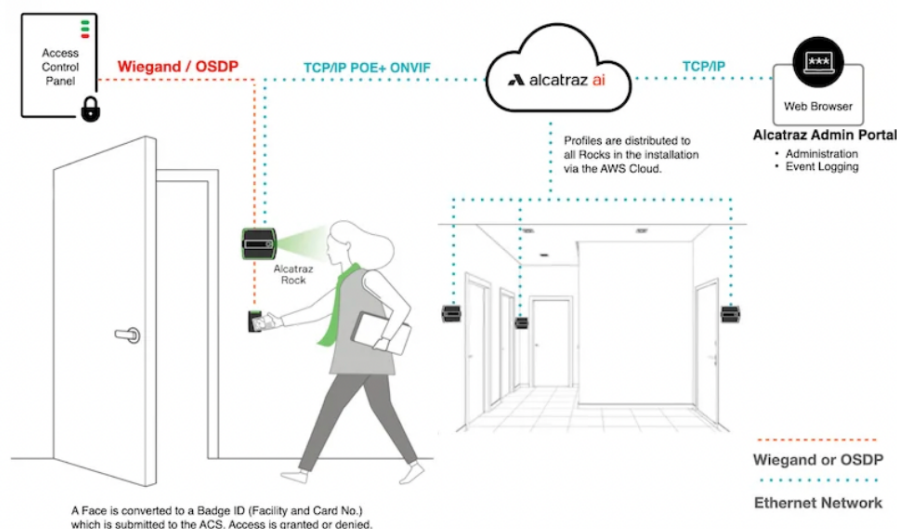
3.3.2 Pokročilé systémy kontroly přístupu

Moderní systémy kontroly přístupu dnes stále častěji nahrazují tradiční metody, jako jsou fyzické klíče či přístupové karty, pokročilými technologiemi, které zvyšují úroveň zabezpečení i uživatelský komfort. Mezi nejvýznamnější trendy patří biometrická autentizace např. rozpoznávání otisků prstů, obličeje nebo oční duhovky a využívání mobilních aplikací jako bezpečnostních klíčů. Tyto technologie minimalizují riziko neoprávněného vstupu a zároveň zjednodušují správu přístupových práv, například umožněním jejich vzdálené správy v dynamických pracovních prostředích. [52]

Kombinace tradičních a biometrických metod vytváří vícevrstvý systém ověřování identity, který je výrazně odolnější vůči běžným hrozbám, jako je ztráta nebo krádež přístupových karet. Moderní řešení tak nejen chrání majetek a osoby, ale také přispívají k efektivnější správě budov a infrastruktury.

Kontrola přístupu The Rock od společnosti Alcatraz AI

Mezi špičkové produkty v oblasti biometrické kontroly přístupu patří zařízení The Rock od americké společnosti Alcatraz AI. Jde o all-in-one (vše v jednom) řešení, které kombinuje rozpoznávání obličeje, umělou inteligenci a strojové učení pro maximální bezpečnost a uživatelský komfort. Systém umožňuje bezkontaktní vstup, minimalizuje fronty a eliminuje potřebu používání fyzických karet nebo klíčů. Díky pokročilým algoritmům dokáže rozpoznat uživatele i v náročných podmínkách a lze jej snadno integrovat do stávající infrastruktury přístupových systémů. [53]



Obrázek 4 Schéma zabezpečení

(zdroj: [53])

3.3.3 IoT a chytré senzory

Internet věcí (IoT) a chytré senzory hrají klíčovou roli v moderních systémech fyzické bezpečnosti a správy budov. Integrací různých zařízení a senzorů do jednotného systému umožňují komplexní monitorování a řízení prostředí, což zvyšuje efektivitu a rychlost reakce na potenciální hrozby. [46]

Inteligentní detekce v rámci elektrické požární signalizace (EPS)

Moderní systémy elektrické požární signalizace (EPS) procházejí zásadní proměnou díky začlenění prvků umělé inteligence, pokročilé analýzy dat a konektivity v rámci IoT. Inteligentní detekce v EPS přináší vyšší úroveň bezpečnosti, přesnosti a schopnosti včasné reakce na riziko požáru. Tradiční kouřové a teplotní hlásiče jsou dnes doplňovány sofistikovanými multisenzorovými detektory, které dokážou kombinovat více typů signálů např. v podobě kouře, teploty a oxidu uhelnatého, a na základě integrované analýzy dat minimalizují výskyt falešných poplachů. [54]

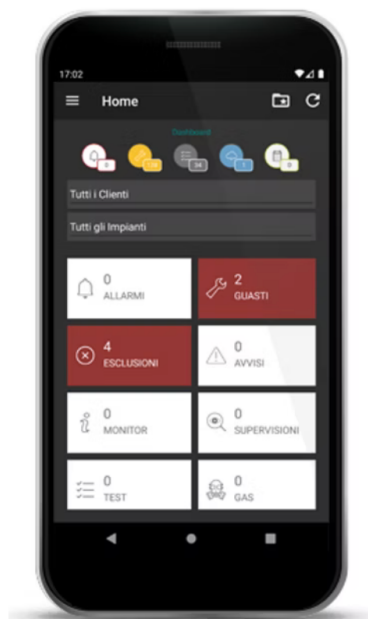
Moderní EPS systémy s inteligentními algoritmy dokážou detekovat odchylky v typu kouře či teplotního profilu a porovnají je s historickými daty, čímž se zvyšuje pravděpodobnost správného vyhodnocení rizika. Zásadní výhodou tohoto systému je komunikace v reálném čase se systémem řízení budov tzv. BMS (Building Management Systems), který zajišťuje automatizované reakce v podobě spuštění evakuačního režimu,

uzavření požárních uzávěr nebo aktivaci hasicích systémů. Tyto inteligentní EPS systémy jsou dnes běžně využívány nejen v komerčních objektech, ale i ve školách, nemocnicích a průmyslových areálech, kde je kladen vysoký důraz na prevenci a rychlost reakce. [55]



Obrázek 5 Multisenzorový detektor

(zdroj: [54])



Obrázek 6 Mobilní aplikace pro správu EPS

(zdroj: [54])

Magnetické zámky s funkcí fail-safe v požárních a nouzových systémech

Dalším důležitým prvkem moderní fyzické bezpečnosti jsou magnetické zámky s funkcí fail-safe, které hrají důležitou roli v rámci evakuace osob z budovy. Princip fail-safe zajišťuje, že v případě výpadku napájení nebo aktivace požárního poplachu dojde automaticky k odemčení zámku, čímž je umožněn pohyb osob bez rizika překážky v únikových koridorech. [54]

Moderní magnetické zámky jsou dnes konstruovány nejen s důrazem na bezpečnost, ale i na jednoduchou integraci do systému kontroly přístupů a EPS systémů. Kromě základní funkce udržení dveří v uzavřené poloze nabízejí i pokročilé funkce jako stavové výstupy, signalizaci stavu dveří, možnost vzdáleného odblokování či propojení s biometrickými čtečkami. Ve spojení s inteligentními EPS a přístupovými systémy tak tyto zámky tvoří komplexní řešení. [52] [54]

Shrnutí kapitoly

Kapitola se zabývá teoretickým vymezením pojmu bezpečnost a jeho významem v kontextu ochrany osob, majetku a infrastruktury, a to zejména ve školském prostředí. Zvláštní pozornost je věnována rozdílu mezi pojmy „security“ a „safety“, rozlišení vnitřní a vnější bezpečnosti a fyzické bezpečnosti. V rámci ní je popsána struktura dle prostorové charakteristiky, do které patří plášťová, perimetrická, prostorová a objektová ochrana.

Druhá část kapitoly se zaměřuje na současné trendy v oblasti bezpečnosti, které jsou stále více ovlivňovány moderními technologiemi, zejména umělou inteligencí, strojovým učením a konceptem internetu věcí (IoT). Detailně jsou popsány chytré kamerové systémy s pokročilou videoanalytikou, moderní přístupové systémy s biometrickou autentizací i inteligentní požární signalizace s možností prediktivního vyhodnocování rizik. Součástí je také zmínka o magnetických zámcích s funkcí fail-safe, které jsou při evakuaci osob zásadní.

4 OCHRANA MĚKKÝCH CÍLŮ

Pojem „měkké cíle“ (soft targets) sice nemá jednotnou nebo oficiální definici, nicméně v bezpečnostní sféře se běžně používá k označení míst s velkou koncentrací lidí a zároveň nízkou úrovní zabezpečení proti násilným útokům. Právě kvůli těmto charakteristikám se stávají častým terčem útoků, zejména pak útoků teroristických. Oproti nim stojí tzv. „tvrdé cíle“ (hard targets), tedy objekty, které jsou výrazně lépe chráněny a zabezpečeny, například státní instituce, vojenské areály, zařízení bezpečnostních složek, ale i některé soukromé či komerční objekty se zvýšeným stupněm ochrany.

Rozdělení na měkké a tvrdé cíle je klíčové i při tvorbě bezpečnostních strategií, protože reflektuje pohled potenciálního útočníka. Zatímco tradiční přístupy se soustředí na význam objektu pro společnost nebo na možné následky útoku, tato perspektiva klade důraz na pravděpodobnost výběru cíle. Díky tomu upozorňuje i na ty subjekty, které by jinak zůstaly mimo zorné pole běžných bezpečnostních opatření. [18]

Typickými příklady měkkých cílů jsou školy, nemocnice, nákupní centra, kulturní zařízení, ale i veřejná prostranství. Ochrana těchto cílů vyžaduje specifický přístup spojující preventivní, technická i organizační opatření, která musí reflektovat lokální podmínky a reálnou míru ohrožení. [56]

Koncepce ochrany měkkých cílů na období 2017–2020, kterou zpracovalo Ministerstvem vnitra ČR, se zaměřuje na systematické zvyšování bezpečnostní úrovně těchto prostor. Hlavními pilíři dokumentu jsou posílení prevence, zvyšování bezpečnostního povědomí a rozvoj spolupráce mezi státní správou, soukromým sektorem a bezpečnostními složkami. Dokument zároveň analyzuje současný stav zabezpečení měkkých cílů, identifikuje hlavní rizika a navrhuje konkrétní opatření vedoucí ke zvýšení odolnosti vůči bezpečnostním hrozbám. [58]

4.1 Základy ochrany měkkých cílů

Hrozby směřující vůči měkkým cílům mají různé podoby. Nejde pouze o teroristické útoky s ideologickým pozadím, ale často také o činy jednotlivců motivovaných osobními problémy či psychickou poruchou. Tzv. modus operandi útočníků může zahrnovat použití chladných nebo střelných zbraní, vozidel, improvizovaných výbušných zařízení či chemických látek. Útočníci často cílí na lokality s vysokou symbolickou nebo mediální hodnotou a minimálními překážkami pro vstup. Významným trendem je nárůst útoků spáchaných tzv.

osamělými vlky, kteří nejsou součástí organizovaných struktur, což výrazně komplikuje predikci a prevenci incidentů. [44]

Ochrana měkkých cílů je vícevrstevným procesem založeným na třech klíčových pilířích:

- I. Fyzická bezpečnost** – zahrnující opatření jako kontrola vstupů, kamerové systémy nebo bariéry.
- II. Organizační a režimová opatření** – pravidla pro pohyb osob, návštěvnické režimy a postupy pro krizové situace.
- III. Připravenost a vzdělávání** – zahrnuje nácviky evakuace, školení personálu a komunikaci při krizových situacích.

Všechny tyto prvky musí být propojeny v rámci komplexního bezpečnostního systému, který reaguje na specifika daného místa. [44]

Kvalitní ochrana měkkého cíle začíná jeho identifikací a následným hodnocením atraktivity a zranitelnosti. Hodnotí se faktory jako otevřenost prostoru, přítomnost bezpečnostního personálu, počet a koncentrace osob, dostupnost únikových cest, přítomnost symboliky, ale i potenciální mediální dopad útoku. Výsledkem této analýzy je stanovení míry ohrožení, která slouží jako podklad pro výběr a prioritizaci bezpečnostních opatření. [56]

Ochrana měkkých cílů je společenskou odpovědností, která přesahuje rámec jednoho správce či provozovatele. Nezbytná je úzká spolupráce s Policií ČR, složkami IZS a samosprávou. Policie může sehrát klíčovou roli při konzultacích ohledně zajištění akcí, realizaci bezpečnostních opatření nebo vyhodnocování rizik. V případě incidentu pak přebírá velení a koordinuje krizové řízení. Otevřená komunikace a výměna informací jsou klíčovými nástroji k posílení bezpečnostního prostředí. [56]

Ochrana měkkých cílů čelí několika výzvám. Jednou z hlavních je nutnost najít rovnováhu mezi bezpečností a zachováním otevřenosti a dostupnosti těchto míst pro veřejnost. Dále je problematická absence legislativního rámce, která snižuje závaznost opatření. Velkou výzvou je také schopnost adaptace na měnící se hrozby, a to zejména s příchodem nových technologií nebo taktik útočníků. Odpovědné osoby se často potýkají s nedostatkem zdrojů, odborných kapacit či metodické podpory. [44]

4.2 Principy ochrany měkkých cílů

Po vymezení základních východisek ochrany měkkých cílů přináší tato kapitola systematický přehled principů, které tvoří rámec pro aplikaci bezpečnostních opatření v praxi. Opírá se o metodické dokumenty Ministerstva vnitra ČR a slouží jako teoretické vodítko pro nastavení konkrétních kroků směřujících k posílení bezpečnosti měkkých cílů. Ochrana je zde nahlížena jako vícevrstvý proces, založený na kombinaci preventivních, technických a organizačních nástrojů.

Tyto oblasti zahrnují opatření, jež se společně podílejí na snížení rizika útoku a zároveň na zmírnění jeho případných dopadů. Je důležité zdůraznit, že implementace těchto opatření není zpravidla nařízena plošně státem, ale závisí na dobrovolném rozhodnutí samotných správců či vlastníků měkkých cílů. [23]

Základní kroky ochrany:

- a) **Identifikace chráněných zájmů** – Základním krokem je určení, co má být chráněno. V kontextu ochrany měkkých cílů jde primárně o ochranu života a zdraví osob. Vedle toho může být chráněným zájmem také majetek, informace nebo dobré jméno organizace. Klíčové je vnímat měkký cíl jako prostor, kde přítomné osoby mohou být náhle vystaveny násilnému jednání. [57]
- b) **Analýza hrozeb a rizik** – Na základě identifikace chráněných zájmů se dále vyhodnocují potenciální hrozby. Ty mohou pocházet od jednotlivců (např. psychicky nemocných osob), organizovaných skupin (např. extremisté) nebo být důsledkem obecné bezpečnostní situace. Vyhodnocení míry ohroženosti umožňuje správně alokovat bezpečnostní opatření a zaměřit se na hrozby s nejvyšší pravděpodobností výskytu a nejzávažnějšími dopady. [58]
- c) **Nastavení bezpečnostních opatření** – Opatření musí odpovídat specifikům měkkého cíle, jeho provozu, počtu návštěvníků i dostupným zdrojům. Mezi klíčové principy patří přiměřenost (neomezující běžný chod), kompatibilita (s ostatními opatřeními) a flexibilita (s ohledem na měnící se hrozby). Opatření mohou být fyzická (např. bezpečnostní personál), technická (např. kamerový systém) či organizační (např. školení zaměstnanců). [23]
- d) **Tvorba bezpečnostního plánu** – Bezpečnostní plán je souhrnný dokument, který definuje pravidla prevence, reakce na incident a následné kroky – jako je evakuace,

krizová komunikace či spolupráce s integrovaným záchranným systémem. Obsahuje standardizované postupy, které pomáhají zmírnit dopad incidentu a umožňují rychlý návrat do rutinního provozu. [59]

4.3 Specifika škol jako měkkých cílů

Školy a školská zařízení představují zvláštní kategorii tzv. měkkých cílů, neboť se jedná o objekty s omezenými možnostmi ochrany, vysokou koncentrací osob a každodenním veřejným provozem. Jejich otevřenost a vnitřní kultura zakládající si na důvěře však představují bezpečnostní slabinu, která je zneužitelná nejen externími pachateli, ale i zevnitř samotného školního prostředí.

Ve snaze porozumět specifické zranitelnosti škol jako měkkých cílů je nezbytné vycházet z metodického rámce, který pro hodnocení měkkých cílů stanovilo Ministerstvo vnitra ČR. Tento rámec určuje, že volba vhodných bezpečnostních opatření musí být založena na individuálním posouzení každého objektu, a to se zohledněním funkce zařízení, ale zejména s ujasněním tzv. bezpečnostně relevantních diagnostických faktorů. Tyto faktory mají zásadní význam při hodnocení dvou klíčových kritérií [23] [60]:

a) Atraktivita cíle z pohledu útočníka

b) Reálné možnosti zabezpečení cíle

V tomto smyslu byly uvedené faktory aplikovány na prostředí škol a školských zařízení, které tímto způsobem získávají svůj specifický bezpečnostní profil. [23] [60]

4.3.1 Atraktivita cíle z pohledu útočníka

Pro útočníka není výběr cíle náhodný a vždy se rozhoduje podle kombinace několika faktorů, které zvyšují šanci na úspěch útoku a jeho dopad. Školy jako měkké cíle splňují mnoho z těchto podmínek např. jsou přístupné, málo chráněné, s vysokou koncentrací osob a s minimální přítomností bezpečnostních složek. Navíc útok na školu vyvolává silnou společenskou a mediální odezvu, čímž zvyšuje atraktivitu takového cíle v očích útočníka. [23]

Jednotlivé faktory, které ovlivňují atraktivitu škol jako potenciálních cílů jsou následující:

a) Otevřenost pro veřejnost

Školy jsou ze své podstaty veřejnými institucemi s volným pohybem žáků, rodičů, dodavatelů, servisních pracovníků a dalších návštěvníků. Většina škol má minimální

režimová opatření. Vstup často není kontrolován, chybí kontrola nebo identifikace. To zvyšuje možnost nenápadného průniku útočníka do budovy.

b) Bezpečnostní personál

Na rozdíl od některých jiných objektů (např. obchodních center nebo kulturních zařízení), školy obvykle nedisponují specializovaným bezpečnostním pracovníkem. Většinou je přítomen pouze školník nebo hospodářka, kteří však často nemají potřebné školení pro řešení rizikových a krizových situací. To výrazně omezuje schopnost školy detekovat hrozbu v počáteční fázi.

c) Množství a koncentrace osob

V době vyučování se v budově školy nachází vysoký počet osob, z nichž většinu tvoří děti, v případě zvláštních škol skupina dětí se sníženou schopností vlastní ochrany. Navíc se většina osob soustřeďuje v konkrétních časech (příchody, přestávky, obědy), což zvyšuje efekt útočnickovy snahy způsobit co největší škodu.

d) Přítomnost policie

Běžná přítomnost policie ve školách není obvyklá, pokud se nejedná o výjimečné události nebo zvýšenou bezpečnostní hrozbu. Z hlediska útočníka to znamená nižší pravděpodobnost okamžitého zásahu bezpečnostních složek.

e) Přítomnost médií

V případě útoku na školu lze očekávat výraznou mediální odezvu – školy mají vysoký společenský a symbolický význam. To zvyšuje mediální atraktivitu cíle a může působit jako motivační prvek pro útočníka, který usiluje o pozornost.

f) Symboličnost cíle

Škola je symbolem hodnot, jako jsou vzdělávání, dětství, společenský rozvoj, budoucnost. Útok na školu proto nemá jen praktický dopad, ale i psychologický a kulturní rozměr. Je vnímán jako útok na společnost jako celek [23] [60].

4.3.2 Reálné možnosti zabezpečení cíle

Schopnost školy bránit se útoku je ovlivněna řadou praktických aspektů, a to od organizační struktury přes dostupné finanční a technické prostředky až po míru připravenosti personálu. I přes zvyšující se povědomí o důležitosti bezpečnosti zůstává realita mnohdy daleko za jejich potřebami.

Schopnost škol účinně reagovat na jejich ohrožení je současně podporována i limitována následujícími faktory [23] [60]:

a) Organizační struktura

Školy mají jasnou vnitřní hierarchii, která může v krizových situacích sehrát pozitivní roli, tedy pokud je připravena. Zásadní je, aby vedení školy vědělo, kdo je za co zodpovědný, mělo stanovené role při incidentu a komunikaci s IZS. Bez jasného plánu však tato struktura selhává.

b) Zdroje a prostředky na bezpečnost

Většina škol má jen omezený rozpočet, protože fungují jako příspěvkové organizace (mnoho veřejných škol v České republice je zřizována obcemi, kraji nebo státem a funguje jako příspěvková organizace podle zákona č. 250/2000 Sb). Kvůli tomu bývá bezpečnost až na druhé koleji. Školám chybí peníze na technické zabezpečení, jako jsou kamery, elektronické zámky, kontrola vstupu nebo pravidelná školení pro zaměstnance. Ve většině případů si nemohou dovolit ani fyzickou ostrahu.

c) Schopnost identifikace vlastních rizikových situací

Tato schopnost vyžaduje především vyškolený personál, jasné stanovené postupy a bezpečnostní povědomí u všech zaměstnanců. V mnoha školách však stále chybí základní prevence jako jsou pravidelné nácviky evakuace, krizová komunikace, nebo stanovení „lock-down“ procedur. Bez těchto základů škola nedokáže včas rozpoznat varovné signály a adekvátně reagovat. [23] [60]

4.4 Zásady ochrany škol

Ze specifik uvedených v předchozích kapitolách vyplývá nutnost přistupovat k jejich ochraně s pečlivostí, systematičností a důrazem na prevenci. Školy nejsou pouze prostory pro vzdělávání, ale představují zároveň místa denního setkávání dětí, pedagogů, nepedagogických pracovníků a často také veřejnosti. Tato otevřenost, spolu s jejich symbolickým významem, klade vysoké nároky na jejich zabezpečení a připravenost čelit možným hrozbám.

Cílem této podkapitoly je představit hlavní principy ochrany škol jako měkkých cílů v kontextu současných bezpečnostních doporučení Ministerstva vnitra ČR. Tato doporučení vycházejí především z dokumentu „10 principů zodolnění měkkého cíle“, který shrnuje

klíčové prvky zvyšování odolnosti objektů, a zároveň z technické normy ČSN 73 4400, jež stanovuje systémový rámec pro řízení bezpečnosti škol a školských zařízení.

Zatímco „10 principů z odolnosti měkkého cíle“ poskytuje praktická obecně platná doporučení vhodná i pro personál bez bezpečnostního vzdělání, norma ČSN 73 4400 rozpracovává jednotlivé oblasti do konkrétních opatření, a to od dispozičního řešení budov až po organizaci školení a kontrolu funkčnosti bezpečnostních systémů. Kombinací obou přístupů lze dosáhnout efektivní, komplexní a realisticky proveditelné strategie ochrany škol. [61]

V následujících bodech budou vybrané principy rozvedeny tak, aby reflektovaly jak obecné zásady, tak konkrétní aplikace v prostředí škol:

a) Poznání bezpečnostní charakteristiky a ohrožení

Škola by měla nejprve přesně definovat, co je třeba chránit. Především zdraví a životy dětí, pedagogů, nepedagogů a návštěvníků. Současně je nutné analyzovat možné hrozby, a to jak vnitřní (např. konfliktní žák, zaměstnanec), tak vnější (aktivní útočník, kriminální čin). Brožura doporučuje využít metody jako je riziková analýza a mapování slabin.

Podle normy ČSN 73 4400 je třeba vypracovat posouzení rizik, které zahrnuje pravděpodobnost a dopady konkrétních scénářů (např. útok střelnou zbraní, vniknutí nepovolané osoby, výhružný telefonát). Rizika musí být vyhodnocena v kontextu lokality, provozního režimu školy a bezpečnostní historie objektu. [61] [62]

b) Prevence a zmírnění dopadu útoku

Preventivní opatření mohou zahrnovat fyzické zabezpečení vstupů, kamerové systémy, přístupové karty, přehledné uspořádání vstupních prostor a umístění bezpečnostních prvků tak, aby bylo možné hrozby detekovat včas. Brožura zdůrazňuje nutnost „myslet dopředu“ a zavést opatření, která útok ztíží nebo mu zcela zabrání. [61]

ČSN 73 4400 se detailně věnuje dispozičnímu řešení budovy, perimetru a technické ochraně. Doporučuje například oddělení veřejně přístupných částí od ostatních, kontrolu zásobovacích vstupů, vytvoření úkrytových zón („safe haven“) a přehlednost prostor z důvodu rychlé evakuace. [62]

c) Školení personálu, příprava koordinačního plánu a standardizování postupů

Bezpečnostní systém školy nemůže být účinný bez proškoleného personálu. Brožura doporučuje každoroční školení, nácvik scénářů a jasně popsané standardní operační postupy.

Důraz je kladen i na koordinaci mezi více osobami a stanovení konkrétních rolí v případě incidentu. [40]

Norma ČSN 73 4400 vyžaduje pravidelné školení personálu (včetně krizové komunikace), testování a aktualizaci postupů a vedení záznamů o bezpečnostních incidentech. Také doporučuje vypracování krizových scénářů a koordinaci více osob, která se v kritických situacích osvědčuje jako efektivní model. [62]

d) Spolupráce s Policií ČR a IZS

Brožura doporučuje aktivní spolupráci s místní policií a dalšími složkami IZS, nejen v době incidentu, ale i při jeho přípravě a prevenci. Je vhodné nabídnout prohlídku objektu, sdílet informace o rizicích a konzultovat bezpečnostní plány. [61]

Norma ČSN 73 4400 výslovně doporučuje navázání spolupráce s Policií ČR a Hasičským záchranným sborem – ideálně formou písemného kontaktu a pravidelnými konzultacemi. Také podporuje začlenění těchto složek do taktických nácviků. [62]

e) Využití nástroje „lock-down“, „safe haven“ a scénáře „run-hide-fight“

V kritických situacích se doporučuje používat standardizované scénáře chování, známé pod anglickým označením „Run-Hide-Fight“ (Uteč–Schovej se–Bojuj). Brožura radí připravit místnosti typu „safe haven“, tedy bezpečné místnosti, kde lze přečkat útok. [61]

Norma ČSN 73 4400 tyto principy nejen potvrzuje, ale navrhuje jejich architektonické začlenění do provozu školy. Lock-down je popsán jako uzamčení objektu, safe haven má být speciálně upravená místnost se základním vybavením (světlo, ventilace, komunikace). Scénáře útoků mají být součástí školení personálu i žáků. [62]

4.5 Vybrané metodiky

Škola a neštěstí: Jsme připraveni!

Metodický dokument s názvem Škola a neštěstí: Jsme připraveni! vydalo Ministerstvo školství, mládeže a tělovýchovy ČR ve spolupráci s odborníky na krizové řízení, školní psychologii a prevenci rizikového chování z Generálního ředitelství Hasičského záchranného systému. Tento materiál představuje praktického průvodce pro školy a jejich pracovníky při zvládání mimořádných a krizových událostí, jako jsou úmrtí, přírodní katastrofy, násilné činy nebo dlouhodobě zatěžující situace (např. pandemie, šikana či válka). [64]

Dokument zdůrazňuje, že prevence sama o sobě nestačí. Bohužel se přes veškerou snahu neštěstí dějí a budou dít. Hlavním cílem metodiky je zvýšit připravenost škol tak, aby každý člen školní komunity, od vedení školy po žáky, věděl, jak v krizové situaci jednat. Metodika se opírá o zkušenost, sdílenou odpovědnost a schopnost reagovat pružně a smysluplně. Klíčovým přínosem je srozumitelnost, použitelnost v praxi a důraz na spolupráci a komunikaci. [64]

Metodika je členěna do tří hlavních částí, které reflektují tzv. katastrofický cyklus [64]:

- a) **Jsme zasažení** – První část se věnuje období bezprostředně po události. Nabízí praktické postupy, jak zvládnout první dny – od zajištění bezpečí po informování, koordinaci a zvládání dopadů. Obsahuje tzv. taháky, tedy kontrolní seznamy pro dospělé i jednotlivé role (ředitel, učitel, žák, rodič, pracovník vnější podpory). Tyto pomůcky jsou označeny ikonami, usnadňují orientaci a umožňují rychlou akci i ve stresu.
- b) **Obnovujeme** – Druhá část metodiky se zabývá střednědobými a dlouhodobými důsledky událostí. Pomáhá školám obnovit prostředí a vztahy, reflektovat zkušenosti a poskytovat podporu i v méně nápadných případech (např. dlouhodobá nemoc učitele, dopady šikany). Důležitý je důraz na aktivní rozhodnutí pomáhat a vědomé navazování na hodnoty školy.
- c) **Připravujeme se** – Třetí část se orientuje na budoucnost. Věnuje se prevenci a tvorbě plánů připravenosti. Zahrnuje zásady, jak se školní klima může stát odolnějším prostřednictvím participace celé komunity. Metodika připomíná, že i nepřímo zasažené školy jsou součástí širšího dění (např. regionální katastrofy). Součástí jsou i reflexe a příklady, jak budovat pružnost a tvořivost při plánování.

V závěru dokument nabízí přehled doporučených postupů „Co dělat, když...“ a přehled kontaktů a tipů. To umožňuje rychlou orientaci a oporu při plánování i zásahu.

Významnou přidanou hodnotou metodiky je její jazyková a vizuální přístupnost. Používá srozumitelný jazyk, vyhýbá se odbornému žargonu, nabízí příklady z praxe a zapojuje ikonografii (např. deštník = ochrana, hvězdička = příklad). Pracuje se začleňujícím jazykem „my“, což posiluje pocit sdílené odpovědnosti a motivuje jednotlivce ke spolupráci a zapojení se. [64]

Manuál bezpečné školy

Dokument s názvem „Manuál bezpečné školy“ vydalo Ministerstvo vnitra České republiky, konkrétně Odbor prevence kriminality, ve spolupráci s Asociací bezpečná škola. Tento dokument představuje metodický materiál zaměřený na podporu implementace technické normy ČSN 73 4400 „Prevence kriminality – řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení“. Jeho cílem je nabídnout školám a jejich zřizovatelům praktický návod, jak krok za krokem zavádět systémová opatření, která zvyšují bezpečnost školního prostředí. [10]

Manuál reaguje na aktuální bezpečnostní hrozby, včetně případů násilných útoků ve školách, a snaží se poskytnout komplexní návod pro preventivní činnost, která přesahuje rámec klasické sociální prevence. Podporuje zavádění konkrétních organizačních, režimových, technických a vzdělávacích opatření, která společně přispívají k ochraně žáků, studentů, pedagogů i dalších osob pohybujících se ve školních prostorách. Dokument slouží jako most mezi standardizačním přístupem vyjádřeným v normě ČSN 73 4400 a praktickými potřebami jednotlivých škol. [10]

Publikace je rozdělena do sedmi hlavních kapitol a několika příloh. Její obsah je logicky strukturován od obecného přehledu bezpečnostních hrozeb a teoretického základu bezpečnosti ve školách, přes popis metodiky implementace bezpečnostních opatření, až po praktické rady a výběr vhodných technických prostředků. Klíčové kapitoly zahrnují [10]:

- 1) **Bezpečnostní kontext a hrozby** – Představuje příklady útoků na školách a definuje základní otázku: před čím mají být školy chráněny.
- 2) **Vyrovnaná bezpečnostní opatření** – Rozvádí princip, že technická opatření mají smysl až tehdy, jsou-li doplněna organizačními a vzdělávacími aktivitami.
- 3) **Metodika aplikace normy ČSN 73 4400** – Nabízí praktické kroky pro provedení auditu, implementaci nápravných opatření, školení a informování.
- 4) **Úskalí aplikace normy** – Reflektuje na limity jako je právní nevymahatelnost normy, finanční náročnost nebo střety s jinými předpisy.
- 5) **Vzdělávání** – Popisuje školení a semináře, které podporují rozvoj bezpečnostního vědomí ve školách.

- 6) **Instalace technických prostředků** – Přináší doporučení k výběru a instalaci vhodných technologií jako jsou kamerové systémy, poplachová zařízení či přístupové systémy.
- 7) **Psychologické aspekty** – Věnuje se varovným signálům v chování žáků a psychologii krizového rozhodování.

Na závěr dokument obsahuje přílohu s rozбором postavení normy ČSN 73 4400 v kontextu evropského standardizačního úsilí a recenze odborníků, které potvrzují jeho význam.

Hlavní přínos Manuálu bezpečné školy spočívá v jeho srozumitelnosti, praktičnosti a komplexnosti. Dokument netvoří pouze teoretický výklad normy, ale přináší konkrétní návody a příklady dobré praxe. Jeho struktura umožňuje školám snadno se v materiálu orientovat a adaptovat jej na vlastní podmínky. Významným prvkem je i otevřené pojmenování úskalí realizace normy, což zvyšuje důvěryhodnost dokumentu a připravuje uživatele na možné komplikace. Manuál se tak stává neocenitelným nástrojem pro ředitele škol, zřizovatele, architekty, projektanty, bezpečnostní experty i pedagogy, kteří chtějí systematicky zvyšovat úroveň bezpečnosti svých institucí. [10]

Shrnutí kapitoly

Kapitola se zaměřuje na problematiku ochrany měkkých cílů. V textu je popsáno, proč jsou tato místa častým cílem útoků, a upozorňuje na potřebu specifických přístupů k jejich ochraně. Dále jsou zmíněny různé formy ohrožení včetně útoků jednotlivců a ideologicky motivovaných činů. Zdůrazňuje se zde nutnost kombinovat fyzická opatření, režimová pravidla a příprava personálu a veřejnosti. Kapitola se věnuje také koncepci ochrany měkkých cílů, kterou vypracovalo Ministerstvo vnitra ČR.

V další části kapitoly jsou popsány principy ochrany měkkých cílů, které vycházejí z metodických dokumentů a doporučení. V textu jsou popsány ohrožené zájmy, vyhodnocení rizik a plánování bezpečnostních opatření. Je zdůrazněna role spolupráce mezi veřejným a soukromým sektorem, včetně koordinace s Policií ČR a složkami integrovaného záchranného systému. Zvláštní pozornost je věnována školám, jejich provozní zvláštnostem a praktickým omezením při zajišťování bezpečnosti. Kapitola ukazuje, že školy mají řadu zranitelných míst a často nedisponují dostatečnými prostředky, vedením ani odborně připraveným personálem.

Závěr kapitoly představuje praktické metodiky, které školám pomáhají zavádět účinná bezpečnostní opatření. Představeny jsou dva materiály, jedná se o příručku Škola a neštěstí: Jsme připraveni!, která podporuje krizovou připravenost a reakce na mimořádné situace a Manuál bezpečné školy, který nabízí postupy pro zavádění bezpečnostních standardů podle normy ČSN 73 4400. Oba materiály zdůrazňují význam prevence, krizových plánů, spolupráce s bezpečnostními složkami a zvyšování bezpečnostního povědomí uvnitř školních kolektivů.

5 ZÁVĚR TEORETICKÉ ČÁSTI

Teoretická část této diplomové práce poskytuje komplexní přehled oblastí souvisejících s bezpečností školských zařízení, přičemž každá kapitola přinesla důležité poznatky, které tvoří základ pro návrh konkrétních opatření pro praktickou část.

Úvodní kapitola se věnovala právnímu rámci, jenž upravuje bezpečnostní problematiku ve školách v České republice. Zároveň byly představeny obecně závazné právní předpisy, prováděcí vyhlášky, technické normy a metodické dokumenty, které poskytují školám a jejich zřizovatelům důležitou oporu při zavádění a řízení bezpečnostních opatření. Zvláštní důraz byl kladen na normy ČSN 73 4400 a ČSN ISO 31000, které představují základní pilíře systematického řízení bezpečnostních rizik a nastavují postupy pro minimalizaci hrozeb v různých fázích provozu školského zařízení. Kromě zmíněného byl v kapitole vymezen také terminologický rámec.

Další část práce se zaměřila na teoretické uchopení problematiky hrozeb a rizik a jejich dělení. Text rozvíjel myšlenku, že pro efektivní zvládání rizik je nezbytné osvojit si strukturovaný přístup podle mezinárodně uznávaných standardů. V tomto kontextu byla detailně představena již zmíněná norma ČSN ISO 31000, která definuje jednotlivé fáze řízení rizik. K aplikaci těchto principů byly popsány dvě analýzy rizik, a to kvalitativní metoda CARVER a semikvantitativní metoda PNH.

Třetí kapitola se soustředila na samotný pojem bezpečnost v kontextu školského prostředí. Byla objasněna důležitost rozlišení mezi bezpečností typu „security“ a „safety“, přičemž obě složky tvoří nedílnou součást komplexního zabezpečení školního objektu. Popsaná byla také vícevrstvá struktura fyzické ochrany. Velká část kapitoly byla věnována moderním trendům a technologiím, jako jsou AI kamerové systémy, inteligentní přístupové technologie, IoT a chytrá požární signalizace.

Závěrečná teoretická kapitola se zaměřila na problematiku ochrany měkkých cílů, kam školská zařízení nepochybně patří. Kapitola reflektovala zvyšující se počet útoků na veřejná a snadno dostupná místa a popisovala, proč jsou školy považovány za zranitelné objekty vyžadující zvláštní pozornost. Podstatná část kapitoly byla věnována metodikám, jako jsou příručka Škola a neštěstí: Jsme připraveni! a Manuál bezpečné školy, které představují funkční opory pro každodenní praxi i krizovou připravenost školských zařízení.

II PRAKTICKÁ ČÁST

6 CHARAKTERISTIKA VYBRANÉHO OBJEKTU

Z důvodu ochrany bezpečnostních zájmů školy a minimalizace rizika zneužití citlivých informací je v diplomové práci vybraný objekt částečně anonymizován. V textu budou využity pouze takové podklady a informace, které neumožní jednoznačnou identifikaci konkrétní školní instituce. Veškeré podklady byly získány na základě předchozí dohody s vedením školy, přičemž podmínky spolupráce byly smluvně upraveny tak, aby byly vyhovující pro obě strany. Zmíněný postup zároveň zajišťuje respektování ochrany citlivých údajů. O těchto krocích byl vyrozuměn rovněž vedoucí diplomové práce, s nímž byla celá práce konzultována.

6.1 Obecné informace

Posuzovaná školní instituce poskytuje základní a odborné vzdělávání žákům se speciálními vzdělávacími potřebami. Má dlouhou historii sahající až do poloviny 20. století. Od svého vzniku, v roce 1950, prošla budova řadou zásadních stavebních i organizačních změn, které byly vždy reakcí na měnící se požadavky v oblasti vzdělávání dětí a mladistvých se zdravotním znevýhodněním.

V průběhu desetiletí docházelo k postupnému rozšiřování objektu a přizpůsobování jeho vnitřních dispozic aktuálnímu počtu a potřebám žáků či personálu. Mezi zásadní momenty patří realizace půdní vestavby v 90. letech. Tato úprava přinesla nové výukové prostory a zároveň vytvořila podmínky pro zřízení prostor pro speciálně pedagogické centrum. Centrum od té doby poskytuje nejen přímou podporu žákům školy, ale také formu služeb pro děti mimo zařízení, jejich rodiče i pedagogické pracovníky v regionu.

V současnosti představuje budova funkčně ucelený komplex, který musí splňovat náročné požadavky nejen z pohledu vzdělávání, ale také z hlediska ochrany zdraví a bezpečí žáků. Vzhledem k tomu, že se jedná o základní školu speciální je nutné posuzovat rizika, která se pojí s provozem takového zařízení.

Je také nezbytné věnovat zvýšenou pozornost plánování opatření v oblasti ochrany osob a majetku, prevence krizových situací a nastavení funkčního systému včasného varování, evakuace a komunikace s externími složkami, zejména Integrovaným záchranným systémem. Současný technický a dispoziční stav budovy poskytuje výchozí rámec pro navrhování efektivních bezpečnostních opatření v souladu s cíli této diplomové práce. [64]

Instituce poskytuje vzdělávání v několika stupních dle míry podpory, kterou žáci vyžadují, přičemž součástí výuky jsou i praktické činnosti, pracovní dovednosti, logopedická péče a rehabilitační programy. Ve škole působí pedagogové se specializací v oblasti speciální pedagogiky, asistenti pedagoga a další odborní pracovníci, kteří se podílí na komplexní podpoře vzdělávacího procesu. [65]

Výuka probíhá ve třídách s malým počtem žáků, což umožňuje individuální přístup a efektivní práci s každým žákem. V rámci vzdělávací nabídky jsou zařazeny také aktivity podporující zdravý životní styl, orientaci v praktickém životě a rozvoj digitálních dovedností. Škola úzce spolupracuje s rodinami žáků i se školskými poradenskými zařízeními s cílem zajistit co nejefektivnější podporu. [66]

Organizační struktura školy odpovídá typu zařízení s rozšířenou péčí a je přizpůsobena jak legislativním požadavkům, tak i praktickým potřebám vzdělávání dětí se specifickými potřebami. [67]

6.2 Umístění objektu

Analyzovaný objekt se tedy nachází v klidné zástavbě menšího města. Jedná se o třípodlažní budovu, která je konstrukčně řešena jako zděná stavba s pravoúhlým půdorysem.

Hlavní vstup je situován směrem do hlavní ulice, která zajišťuje bezproblémový přístup z veřejného prostoru. Vnitřní dispozice objektu je navržena, tak aby byla zachována funkčnost provozu, přehlednost a oddělení jednotlivých zón podle jejich účelu. Objekt pak disponuje dvěma vedlejšími vstupy, z nichž první je umístěn směrem do oploceného školního pozemku. Druhý vedlejší vstup pak směřuje přímo do prostoru sousedícího provozního areálu, čímž "propojuje" školu s externím prostředím mimo kontrolovaný perimetr školního pozemku. Tato skutečnost představuje důležitý bezpečnostní aspekt, neboť z hlediska režimových opatření může znamenat vyšší míru zranitelnosti, zejména při nedostatečném technickém nebo organizačním zajištění tohoto přístupu.



Obrázek 7 Letecký snímek školy

*(zdroj: [68])***Legenda obrázku:**

označení budovy školní instituce



označení školního prostranství, které je po celé délce oplocené

Poloha objektu je z hlediska přístupu složek integrovaného záchranného systému (IZS) relativně příznivá. Nejbližší služebna Policie České republiky je situována přibližně 800 metrů od objektu a je dostupná z hlavní komunikace v řádu jednotek minut. Městská policie, která v dané lokalitě rovněž působí, má stanoviště přibližně 1 kilometr od školy. Obě složky tak mohou v případě potřeby zasáhnout rychle, a to jak při narušení veřejného pořádku, tak i při mimořádné události přímo v areálu školy. Nejbližší zdravotnické zařízení poskytující základní péči, hovoříme o praktickém lékaři, se nachází do 500 metrů chůze. Nemocniční zařízení, které je schopné poskytnout akutní zdravotnickou pomoc (včetně urgentního příjmu) je ve spádovém městě ve vzdálenosti přibližně 15 km. Čas odpovídá tomu dojezdovému, který je u záchranné služby stanoven v řádu 15–20 minut za běžného provozu. V případě potřeby letecké záchranné služby je lokalita dostupná z několika směrů bez přítomnosti vysokých stavebních překážek.

Strategicky důležité dopravní tahy, jako je silnice I. třídy, jsou vzdáleny do 1 km, což umožňuje rychlý příjezd zásahových vozidel v případě mimořádné události. Přístup ke školskému objektu je možný jak po hlavní komunikaci, tak i přes vedlejší příjezdovou trasu, která vede podél železniční tratě.

V bezprostřední blízkosti školy protéká menší vodní tok, který za běžných podmínek nepředstavuje zvýšené riziko, avšak v případě dlouhodobých dešťů či záplav by mohl mít lokální dopad. Zároveň je třeba zohlednit, že vodní tok může představovat potenciální hrozbu i za běžných podmínek, zejména v situaci, kdy by se dítě bez dohledu pedagogického personálu dostalo do jeho těsné blízkosti.

Celkově lze konstatovat, že poloha školského zařízení je z hlediska možnosti efektivního zásahu složek IZS odpovídající požadavkům na bezpečný provoz školského objektu.

6.3 Identifikace aktiv

Proces identifikace aktiv vychází ze zásad uvedených v teoretickém rámci práce, kde byla popsána role aktiv jako výchozího bodu celého řízení rizik. V souladu s tímto přístupem byla nejprve provedena identifikace aktiv, které mají pro školské zařízení hodnotu a které mohou být vystaveny potenciálním hrozbám.

Tabulka 1 Identifikovaná aktiva

1	Žáci se specifickými potřebami
2	Školní speciální pedagogové a asistenti pedagogů
3	Poradkyně z SPC
4	Vedení školy – ředitelka, hospodářka, zástupci
5	Školník
6	Kancelář hospodářky školy vybavena trezorem
7	Provozně-technická místnost (určena primárně školníkovi)
8	Ředitelna
9	Sborovna 1
10	Sborovna 2
11	SPC
12	Dílna technických prací (zaměřená na dřevo)
13	Hlavní rozvodna elektřiny a centrální technické zázemí (vytápění, voda)
14	Učebna PC
15	Účtárna
16	Třídy s multimediální technikou
17	Výtah

18	Tělocvična (evakuační východ a klíče)
19	Hlavní vchod disponující starší verzí intercomu
20	Vedlejší vchod skrz provozně-technickou místnost

(zdroj: vlastní)

6.4 Identifikace hrozeb

Na základě teoretických východisek uvedených v první části diplomové práce byla v praktické části provedena systematická identifikace potenciálních hrozeb, které by mohly ohrozit alespoň jedno z dříve stanovených aktiv školského zařízení.

Tabulka 2 Identifikované hrozby

1.	Neoprávněný vstup cizí osoby bočním vchodem (např. přes areál autoservisu)
2.	Neoprávněný vstup nepovolané osoby hlavním vchodem školy
3.	Útěk žáka z budovy přes hlavní vchod do veřejného prostoru (ulice)
4.	Útěk žáka zadním východem směrem k řece nebo na volné prostranství za školou
5.	Útěk žáka přes technické zázemí školy (např. dílna školníka)
6.	Ztráta nebo krádež klíčů od únikových východů nebo zabezpečených prostor
7.	Krádež školního vybavení cizí osobou během přítomnosti ve škole
8.	Krádež školního vybavení nebo pomůcek samotným žákem
9.	Vypnutí hlavního jističe (pojistek) žákem nebo nepovolanou osobou
10.	Neoprávněný přístup do školní počítačové sítě a zcizení dat (digitální incident)
11.	Ztráta citlivých digitálních dokumentů o žácích (např. dokumentace z SPC)
12.	Požár způsobený neopatrností (např. v dílně)
13.	Vstup cizí osoby do školy v doprovodu jiného žáka či zaměstnance (zneužití důvěry)
14.	Únik informací z emailové komunikace školy (např. narušení GDPR)
15.	Vznik konfliktu mezi žáky vedoucího k fyzickému napadení
16.	Sociálně patologické chování žáků na sociálních sítích
17.	(Ne)úmyslné uzamčení prostoru s žákem nebo osobou se zdravotním omezením
18.	Vniknutí cizí osoby pod smyšlenou legendou
19.	Přítomnost agresivního zákonného zástupce

20.	Selhání evakuačního postupu během cvičení nebo skutečné události
21.	Vstup ozbrojené osoby do školy s úmyslem ublížit (aktivní útočník)
22.	Zneužití slavnostních dnů školy (např. dny otevřených dveří) k průzkumu prostor pro pozdější útok nebo krádež.
23.	Dlouhodobé sledování a zmapování režimu školy (čas vstupu/výstupu, pohyb žáků) za účelem naplánování narušení.
24.	Cílený útok na školu (např. kvůli jejímu zaměření, minoritnímu složení žáků, inkluzi apod.)
25.	Fyzické napadení pedagoga, asistenta nebo jiného zaměstnance školy ze strany třetí osoby (např. rodič, bývalý zaměstnanec)
26.	Zasílání nebezpečného nebo podezřelého balíčku na adresu školy
27.	Využití jinak nezajištěných provozních částí školy pro vstup či úkryt osoby – např. sklep, půda, technická místnost.
28.	Pokus o vydírání pracovníka školy
29.	Cílené narušení školní akce konané mimo budovu školy (např. výlet, exkurze, sportovní turnaj)
30.	Záměrné zablokování přístupu záchranným složkám (např. zaparkované vozidlo, manipulace s bránou či vstupem)

(zdroj: vlastní)

Shrnutí kapitoly

Šestá kapitola se zaměřovala na obecnou charakteristiku vybraného školského zařízení, které je z důvodu ochrany citlivých údajů v práci anonymizováno. Úvodní část popisovala historický vývoj školy, její současnou organizační strukturu, vzdělávací zaměření a specifika práce s žáky se speciálními vzdělávacími potřebami. Dále byla popsána lokalita objektu a jeho stavebně-dispoziční řešení.

V další části kapitoly byla provedena identifikace aktiv a hrozeb. Mezi hlavní aktiva patří jak osoby (žáci, pedagogický a nepedagogický personál). Navazující identifikace hrozeb pak odhalila celou škálu scénářů, které mohou negativně ovlivnit bezpečnostní situaci v objektu, a to od neoprávněného vstupu, přes digitální incidenty, až po krizové události typu požáru či útoku aktivního útočníka. Tato část vytvořila základ pro aplikaci analytických metod CARVER a PNH, které budou využity v následující kapitole při hodnocení rizik a návrhu bezpečnostních opatření.

7 ANALÝZA RIZIK

Tato kapitola navazuje na teoretický rámec diplomové práce, kde byl podrobně popsán proces řízení rizik včetně jednotlivých fází. V praktické části je vybraný objekt analyzován pomocí následujících metod. Přestože je konkrétní budova v práci anonymizována, slouží jako modelový příklad pro posouzení objektů obdobného charakteru.

Cílem této kapitoly je přehledně a systematicky zhodnotit úroveň bezpečnosti v objektu, a tím poukázat na zjištěné nedostatky.

7.1 Metoda CARVER

Metoda CARVER se řadí mezi kvalitativní metody využívající matici rizik. Tímto způsobem se dá snáz určit míra přijatelnosti rizik, a to na základě níže uvedených kritérií. U každého z kritérií se hodnotitelem stanoví hodnota od 1 do 5. Součtem těchto hodnot získáme tzv. CARVER skóre, které se následně vyhodnotí.

Kritičnost (Criticality)

Kritičnost znamená cílovou hodnotu. Jedná se o primární hledisko při cílení. Cíl je kritický, pokud jeho zničení nebo poškození má významný dopad na vojenské, politické nebo ekonomické zájmy.

- Čas: Jak rychle se negativní dopad projeví.
- Rozsah: Jak velká část provozu bude omezena.
- Náhrady: Existují alternativní prostředky nebo služby?
- Relativní význam: Jak důležitý je cíl v rámci celého systému? [33] [69]

Tabulka 3 Kritérium kritičnosti

Kritérium kritičnosti		
Kritičnost	Hodnoty	Kritéria
Velmi nízká	1	Poškození bez dopadu na chod školy, případně řešitelné obratem
Nízká	2	Omezení některých činností (např. výdej stravy, školní družina)
Střední	3	Dočasné přerušení výuky pro většinu tříd (1–2 dny), ztráta klíčových prostor
Vysoká	4	Významné omezení provozu (50–100 %), nelze zabezpečit výuku v hlavních částech

Velmi vysoká	5	Poškození způsobí úplné přerušení provozu školy; znemožnění výuky a evakuace (zdroj: vlastní)
--------------	---	---

Přístupnost (Accessibility)

Posuzuje se, zda je možné se k cíli fyzicky dostat s potřebným vybavením a personálem. Zohledňuje se i případná pomoc zevnitř (např. znalost vnitřního uspořádání). Přístupnost může být zajištěna i tehdy, pokud je nezbytná asistence informovaných osob zevnitř systému. Při hodnocení přístupnosti se pohlíží i na ovlivňující faktory:

- ochranná zařízení pro detekci osob,
- aktivní a pasivní systémy včasného varování,
- přístupové možnosti. [69]

Tabulka 4 Kritérium přístupnosti

Kritérium přístupnosti		
Kritičnost	Hodnoty	Kritéria
Velmi nízká	1	Prakticky nepřístupný bez speciálních nástrojů, silné zabezpečení, dohled
Nízká	2	Přístup vyžaduje překonání mechanických zábranných systém či jiných opatření
Střední	3	Přístup je obtížnější, značný počet překážek a bezpečnostních opatření
Vysoká	4	Přístup je jednoduchý, malý počet překážek a bezpečnostních opatření
Velmi vysoká	5	Cíl zcela volně přístupný zvenčí bez jakýchkoli bariér (např. hlavní vstup bez zajištění)

(zdroj: vlastní)

Obnovitelnost (Recuperability)

Obnovitelnost cíle je hodnocena na základě času potřebného k jeho nahrazení či opravě konkrétních aktiv. Tento faktor je závislý na dostupnosti náhradních komponentů, druhu cílových zařízení, lidského faktoru a technologií. [69]

Tabulka 5 - Kritérium obnovitelnosti

Kritérium obnovitelnosti		
Kritičnost	Hodnoty	Kritéria
Velmi nízká	1	Obnova v rámci několika hodin nebo ihned díky záloze (např. náhradní klíče, technika)
Nízká	2	Obnova do 48 hodin, provoz částečně zachován

Střední	3	Obnova trvá 3–5 pracovních dnů, zajištěna náhradní výuka
Vysoká	4	Obnova trvá týdny, škola musí omezit výuku nebo přejít do nouzového režimu
Velmi vysoká	5	Obnova není možná v průběhu školního roku; vyžaduje rozsáhlou rekonstrukci, jedná se o časově náročnou záležitost

(zdroj: vlastní)

Zranitelnost (Vulnerability)

Kritérium zranitelnosti aktiva udává, jak snadno je možné napadnout či poškodit určitý cíl, pokud se k němu útočník dostane. Při hodnocení zranitelnosti se hodnotí například:

- jestli je cíl snadno zničitelný i bez odborných znalostí nebo naopak velmi odolný,
- z čeho je aktivum postaveno (např. pevné zdi vs. skleněné dveře),
- počet prostředků, které by útočník potřeboval. [33] [69]

Tabulka 6 Kritérium zranitelnosti

Kritérium zranitelnosti		
Kritičnost	Hodnoty	Kritéria
Velmi nízká	1	Vysoká odolnost – bezpečnostní třída, dohled, elektronická ochrana, kontrola vstupů
Nízká	2	Přítomnost aktivních prvků ochrany (CCTV, alarm), běžné narušení nepravděpodobné
Střední	3	Kombinace mechanického zábranného systému (např. mříže + uzamčení)
Vysoká	4	Základní prvky fyzické bezpečnosti, ale bez aktivních prvků (např. jen mechanický zámek)
Velmi vysoká	5	Cíl lze poškodit běžným nářadím (páčidlo, kámen); žádná technická ani fyzická bezpečnost

(zdroj: vlastní)

Vliv na chod instituce (Effect)

Jedná se o kritérium, které udává výši ztráty při narušení daného cíle. V tomto případě může mít útok jak ekonomický, psychologický, tak sociální dopad. [33]

Tabulka 7 Kritérium vliv na chod instituce

Kritérium vliv na chod instituce		
Kritičnost	Hodnoty	Kritéria
Velmi nízká	1	Žádné vážné následky; běžné řešení v rámci interních kapacit

Nízká	2	Ovlivněn chod školy, veřejnost částečně informována
Střední	3	Kombinace mechanického zábranného systému (např. mříže + uzamčení)
Vysoká	4	Významný psychologický, sociální a provozní dopad, škola musí přerušit výuku na dny
Velmi vysoká	5	Ohrožení života dětí/zaměstnanců, panika, mediální masáž, dlouhodobé uzavření školy

(zdroj: vlastní)

Rozpoznatelnost (Recognizability)

Kritériem rozpoznatelnosti se hodnotí, jak snadno je cíl identifikovatelný k potencionálnímu útoku. Rozpoznatelnost závisí na tom, jaké informace může potenciální útočník o objektu zjistit – například během předchozího sledování nebo běžného pohybu v okolí. V případě školského zařízení se může jednat o veřejně dostupné údaje, jako je počet žáků, doba příchodů a odchodů, harmonogram vyučování, rozsah mimoškolních aktivit či viditelnost vstupů a východů. [33] [69]

Tabulka 8 Kritérium rozpoznatelnosti

Kritérium rozpoznatelnosti		
Kritičnost	Hodnoty	Kritéria
Velmi nízká	1	Velmi malá znalost cíle, pachatel vynaloží velmi velké úsilí
Nízká	2	Malá znalost cíle, pachatel vynaloží poměrně velké úsilí
Střední	3	Částečná znalost cíle, nejsou zjištěny všechny informace, ale dá se to odvodit logicky, pachatel vynaloží střední úsilí
Vysoká	4	Velká znalost cíle, pachatel vynaloží malé množství úsilí
Velmi vysoká	5	Kompletní znalost cíle, zároveň je viditelný a známý, pachatel vynaloží velmi malé množství úsilí

(zdroj: vlastní)

7.1.1 Aplikace metody CARVER

Tabulka 9 Aplikace metody CARVER

Vybraný cíl		C	A	R ₁	V	E	R ₂	CARVER skóre
1	Žáci se specifickými potřebami	5	4	4	4	5	3	25
2	Školní speciální pedagogové a asistenti pedagogů	4	4	4	4	5	3	24
3	Poradkyně z SPC	3	5	3	4	5	3	23

4	Vedení školy – ředitelka, hospodářka, zástupci	3	4	4	4	5	3	23
5	Školník	2	3	2	4	2	3	16
6	Kancelář hospodářky školy vybavena trezorem	2	3	4	4	3	3	19
7	Provozně-technická místnost (určena primárně školníkovi)	2	3	2	4	2	3	16
8	Ředitelna	3	3	3	4	5	2	20
9	Sborovna 1	4	3	3	4	5	3	22
10	Sborovna 2	4	3	3	4	5	3	22
11	SPC	2	3	3	4	5	3	20
12	Dílna technických prací (zaměřená na dřevo)	1	3	2	4	2	4	16
13	Hlavní rozvodna elektřiny a centrální technické zázemí (vytápění, voda)	2	3	4	4	5	3	21
14	Učebna PC	1	3	2	4	2	3	15
15	Účtárna	2	3	2	4	3	4	18
16	Třídy s multimediální technikou	1	3	2	4	3	4	17
17	Výtah	1	3	2	4	2	4	16
18	Tělocvična (evakuační východ a klíče)	3	3	2	4	2	3	17
19	Hlavní vchod disponující starší verzí interkomu	4	4	4	5	5	5	27
20	Vedlejší vchod skrz provozně-technickou místnost	1	5	3	4	2	4	19
21	Digitální záznamy o zdravotním stavu a potřebách žáků	3	3	4	3	5	2	20
22	Emailová komunikace školy s rodiči a institucemi (GDPR dopad)	4	3	4	3	4	2	20
23	Webové stránky školy + oficiální Facebook/Instagram profil	2	3	4	3	3	4	19
24	EPS	3	3	3	4	2	4	19
25	PZTS + Alarm JABLOTRON	3	3	3	4	3	5	21

(zdroj: vlastní)

Výsledné skóre u každého aktiva je barevně označeno podle hodnotící tabulky, která přiřazuje konkrétní barvy jednotlivým úrovním rizika.

Tabulka 10 Hodnotící tabulka CARVER

Hodnotící tabulka		
6–14 bodů	Nízké riziko	Cíl je málo zranitelný, málo významný nebo dobře chráněný; přijatelné.
15–19 bodů	Mírné riziko	Riziko je přijatelné, ale doporučuje se minimální kontrolní opatření.
20–24 bodů	Zvýšené riziko	Cíl vyžaduje zvýšenou pozornost, je vhodné zvážit preventivní opatření.

25–29 bodů	Vysoké riziko	Vysoká zranitelnost nebo význam; nutné navrhnout konkrétní opatření.
30 a více bodů	Kritické riziko	Cíl představuje velmi vysoké ohrožení; nepřijatelné bez zásahu.

(zdroj: vlastní)

7.1.2 Vyhodnocení metody CARVER

Na základě provedené analýzy vybraných aktiv školního zařízení pomocí metody CARVER bylo možné objektivně stanovit jejich míru rizikovosti. Při analýze bylo posuzováno šest hodnotících kritérií, jako je kritičnost, přístupnost, obnovitelnost, zranitelnost, vliv na chod instituce a rozpoznatelnost.

Výsledky analýzy ukazují, že kritického rizika (30 bodů a více) nebylo v analyzovaných aktivech dosaženo, což lze považovat za pozitivní výsledek. Přesto se v rámci hodnocení objevují aktiva spadající do kategorie vysokého rizika (25–29 bodů), a to konkrétně:

- Hlavní vchod disponující starší verzí interkomu (27 bodů),
- Žáci se specifickými vzdělávacími potřebami (25 bodů).

Tyto výsledky odrážejí vysokou zranitelnost a význam těchto aktiv pro bezpečnost školy. Hlavní vchod představuje strategický bod, to z toho důvodu, že se jedná o místo, které může zajistit kontroly přístupu a jeho zranitelnost může výrazně ovlivnit ochranu měkkého cíle. Žáci se specifickými potřebami jsou navíc skupinou osob vyžadující zvýšenou pozornost.

Zvýšené riziko (20–24 bodů) bylo zaznamenáno u několika dalších významných aktiv, mezi které patří:

- Školní speciální pedagogové a asistenti pedagogů (24 bodů),
- Poradkyně z SPC (23 bodů),
- Vedení školy – ředitelka, hospodárka, zástupci (23 bodů),
- Sborovny, ředitelna, školní poradenské centrum (SPC),
- Digitální záznamy o zdravotním stavu žáků a emailová komunikace školy.

Tato aktiva hrají zásadní roli ve vybrané školní instituci, ochraně a podpoře žáků. Narušení jejich bezpečnosti by mělo výrazné dopady na fungování školy. Výsledky ukazují, že zaměstnanci a data patří mezi aktiva, která vyžadují více preventivních opatření a kontroly.

Mírné riziko (15–19 bodů) bylo identifikováno u technických prostor a běžných učeben, například:

- Učebna výpočetní techniky,
- Dílna technických prací,
- Provozně-technická místnost,
- Vedlejší vchod.

Přestože tyto prostory nepředstavují bezprostřední vysokou hrozbu, jejich ochrana nesmí být opomíjena. Je důležité si uvědomit, že i aktiva, která v rámci analýzy nevykazovala vysokou míru zranitelnosti, mohou v případě svého narušení představovat závažné sekundární riziko pro další aktiva školy. Tímto způsobem může dojít k eskalaci dopadů a narušení celkové integrity bezpečnostního systému. Preventivní opatření, jako je omezení přístupu, zabezpečení technických zařízení nebo pravidelný monitoring, mohou významně přispět ke snížení celkové úrovně rizika.

Analýza dále ukázala, že nízké riziko (6–14 bodů) nebylo u žádného hodnoceného prvku zaznamenáno.

Z výsledků jsou rovněž patrné opakující se slabiny jako např.:

- vysoká přístupnost určitých prostor,
- nedostatečné fyzické zabezpečení důležitých bodů,
- absence speciálních krizových scénářů pro chráněné osoby,
- nedostatek technických a organizačních opatření,
- zranitelnost informačních systémů a citlivých údajů.

Tato zjištění potvrzují, že řada hrozeb sdílí společné příčiny, a proto je možné účinně zvyšovat úroveň bezpečnosti implementací systémových opatření, která budou mít dopad na více oblastí současně. To by pro školu znamenalo menší finanční náklady.

Závěrem lze konstatovat, že analýza metodou CARVER významně přispěla k odhalení skrytých bezpečnostních nedostatků v provozu školy a poskytla důležitá data pro návrh následných bezpečnostních opatření. Zjištěné skutečnosti budou využity jako podklad pro vytvoření konkrétního souboru technických a organizačních návrhů opatření.

7.2 Metoda PNH

Metoda PNH, jinými slovy posouzení nebezpečí a hrozeb, je nástroj, který slouží k identifikaci a hodnocení potencionálních bezpečnostních hrozeb.

Pro účely analýzy vybraného školského zařízení je v první řadě nezbytné vytvořit hodnotící tabulky pro pravděpodobnost výskytu hrozby, závažnost jejích následků a subjektivní názor hodnotitele. Tyto tabulky slouží jako základní rámec pro následné bodové hodnocení rizik a jejich porovnání.

Tabulka 11 - Pravděpodobnost vzniku nebezpečí

Pravděpodobnost vzniku nebezpečí	
Hodnota	Popis
1	Výskyt je vysoce nepravděpodobný, téměř náhodný.
2	Riziko je málo pravděpodobné, ale nelze jej zcela vyloučit.
3	Výskyt je možný za určitých podmínek.
4	Událost je velmi pravděpodobná.
5	Riziko je přítomné trvale nebo pravidelně vyskytující se.

(zdroj: vlastní)

Tabulka 12 Závažnost následků

Závažnost následků		
Hodnota	Popis	
1	Drobné zranění bez nutnosti pracovní neschopnosti.	Minimální škoda (do 5 000 Kč), např. poškození školních pomůcek.
2	Mírné zranění vyžadující krátkodobou nepřítomnost (např. pohmoždění).	Nízká škoda (do 20 000 Kč), např. poškození nábytku či menší techniky.
3	Závažnější úraz vyžadující lékařské ošetření či hospitalizaci.	Střední škoda (20 000 – 100 000 Kč), např. škody na vybavení učeben.
4	Těžký úraz s trvalými následky.	Vysoká škoda (100 000 – 500 000 Kč), např. požár v části objektu.
5	Smrtelný úraz nebo incident s fatálním dopadem.	Kritická škoda (nad 500 000 Kč), např. zničení části budovy či IT infrastruktury.

(zdroj: vlastní)

Tabulka 13 Názor hodnotitele

Názor hodnotitele	
Hodnota	Popis
1	Zanedbatelný vliv – prostředí a podmínky nemají téměř žádný dopad na riziko.
2	Mírný vliv – některé podmínky mírně zvyšují riziko.

3	Velký vliv – riziko je ovlivněno více faktory.
4	Významný vliv – přítomno více zhoršujících okolností.
5	Kritický vliv – riziko je výrazně zhoršeno souběhem rizikových faktorů.

(zdroj: vlastní)

7.2.1 Aplikace metody PNH

Kompletní výstup hodnocení rizik metodou PNH je k dispozici v příloze P I diplomové práce. V následující části textu je pak stručně popsán postup a hlavní zjištění vyplývající z aplikace této metody.

7.2.2 Vyhodnocení metody PNH

Na základě provedené analýzy identifikovaných nebezpečí ve školním zařízení a následného vyhodnocení míry rizikovosti lze konstatovat, že školní instituce čelí celé řadě hrozeb.

V diplomové práci bylo detailněji analyzováno 30 hrozeb s hodnotami $R = 12\text{--}100$, přičemž 6 hrozeb spadá do kategorie II (nežádoucí) a 24 do kategorie III (mírné). Žádná hrozba nedosáhla nepřijatelné úrovně I (>100). Výsledky odhalily nedostatky v bezpečnostním managementu, které vyžadují okamžitá opatření.

Jak již bylo v úvodu zmíněno pro každé identifikované riziko byla stanovena pravděpodobnost výskytu (P), možné následky (N) a schopnost odhalení (H), přičemž výsledná míra rizika (R) byla vypočítána $R = P \times N \times H$ a tím byla následně zařazena do rizikových kategorií. Hodnocení probíhalo v souladu s pětistupňovou klasifikací, která byla zpracována hodnotitelem, viz Tabulka 12 Závažnost následků.

Výsledky ukazují, že mezi nejzávažnější zjištěné problémy patří neoprávněný vstup cizích osob do školy, zejména:

- a) Vniknutí cizí osoby pod smyšlenou legendou ($R = 100$),
- b) Vstup cizí osoby v doprovodu žáka či zaměstnance ($R = 100$),
- c) Neoprávněný vstup přes hlavní vchod školy ($R = 75$).

Výše zmíněné hrozby byly vyhodnoceny jako nežádoucí. Zároveň odhalily slabiny v systému kontroly vstupu, evidenci návštěv a fyzické ochraně perimetru školy. Pro snížení těchto rizik je nezbytné implementovat kombinaci technických a organizačních opatření. Jedná se například o přístupové systémy, instalace kamerových systémů (CCTV), zavést důsledné režimové opatření a zvýšit počet fyzických kontrol u vstupních dveří do školní

instituce. Detailnější přehled návrhu bezpečnostních opatření jsou zpracována v následující kapitole.

Další velké riziko představují hrozby digitálního/kybernetického charakteru, konkrétně neoprávněný přístup do školní počítačové sítě ($R = 60$) a únik citlivých dat žáků ($R = 50$). Při zpracování bylo pohlíženo na úroveň bezpečnosti informací v digitální podobě a edukaci/proškolení zaměstnanců školní instituce.

Zároveň hodnocení zahrnovalo související nešifrovanou komunikaci zaměstnanců a neoprávněný přístup k síti. Ztráta citlivých dat žáků ($R=50$) navíc představuje právní riziko v kontextu GDPR. Tyto skutečnosti potvrzují nutnost posílení kybernetické bezpečnosti školy prostřednictvím pravidelného školení personálu a zavedení technických bezpečnostních opatření.

Analýza také odhalila opakující se možnosti hrozeb spojených s útekem žáků z budovy (např. hlavním vchodem nebo vedlejšími vchody) a ztrátou kontroly nad jejich pohybem. Tato rizika ($R = 27-36$) sice nespadá do nejvyšších stupňů, ale jejich výskyt ukazuje na nutnost plánovaného zlepšení bezpečnostních podmínek, zejména v oblasti uzamykání vchodů, fyzického zabezpečení venkovních prostor nebo navýšení počtu dozorujících pedagogů během přestávek. Zároveň se podobným incidentům dá předcházet instalací technických prostředků, které zamezují samovolný průchod nepovolaným osobám.

Pozornost si rovněž zaslouží hrozby zahrnující násilí, ať už ve formě fyzického napadení pedagoga ($R = 32$) nebo potenciálního vstupu ozbrojené osoby do školy ($R = 30$). Přestože hrozby dosahují nižší míry podle stanovených kritérií, jejich potenciální následky jsou natolik vážné, že je nezbytné jim věnovat zvýšenou pozornost při tvorbě krizových plánů a provádění nácviků evakuace.

Z analýzy dále vyplynulo, že určité druhy ohrožení a slabín se opakují napříč více scénáři. Typickými příklady jsou:

a) Nedostatečná kontrola vstupů - (43 % rizik)

Hlavním nedostatkem je absence kamerového systému (CCTV) a zároveň CCTV s pokročilými funkcemi, jako je detekce podezřelého chování nebo rozpoznávání obličejů, které by umožnily včasné vyhodnocení a reakci na rizikové situace v reálném čase.

b) Nedostatečná prevence digitálních rizik - (30 %)

Mezi hlavní nedostatky patří nedostatek pravidelného školení zaměstnanců v oblasti kybernetické bezpečnosti, což výrazně snižuje jejich schopnost rozpoznat a adekvátně reagovat na digitální hrozby, jako jsou phishingové útoky (kybernetických útok, jehož cílem je získat citlivá data) nebo narušení dat.

c) Krizová připravenost (27 %)

V rámci provedené analýzy byla identifikována řada slabých míst v oblasti bezpečnostní připravenosti školského zařízení, která mohou výrazně ovlivnit schopnost školy adekvátně reagovat na mimořádné události. Jedním z klíčových zjištění je nedostatečná připravenost zaměstnanců na identifikaci a správný postup při výskytu neznámé osoby v budově, což představuje významné riziko zejména v případě neoprávněného vniknutí.

Pomocí obou analýz byly zjištěny systémové nedostatky, které sice nebyly na první pohled patrné, avšak prostřednictvím podrobných zkoumání, vlastní observací a zjištěných informací prostřednictvím vedoucího pracovníka, byly detekovány. Analýza tak významně přispěla k odhalení skrytých slabin v oblasti bezpečnostního řízení školy. Tyto slabiny je nutné bezodkladně zahrnout do návrhů na zlepšení bezpečnostních opatření v dalším kroku plánování.

7.2.3 Zjištěné skutečnosti na základě analýzy rizik

Pomocí výše uvedených vyhodnocení obou metod aplikovaných v rámci analýzy rizik byly identifikovány bezpečnostní nedostatky a zranitelná místa školského zařízení. Zde je přehled zjištění, které je potřeba zajistit:

- zvýšit ochranu všech vstupů do školy prostřednictvím technických a organizačních opatření,
- posílit digitální bezpečnost,
- zvýšit krizovou připravenost školy formou školení, pravidelných cvičení a tvorby krizových plánů,
- zaměřit se na školení a edukaci personálu a žáků,
- systematicky budovat kulturu bezpečnosti ve všech oblastech provozu školy.

Výše uvedené výsledky mohou být řešeny dle principu ALARP, např.:

- **Krátkodobé (0–3 měsíce):** Instalace bezpečnostních zámků na hlavní vchody, zavedení povinné registrace návštěv s digitální evidencí.
- **Střednědobé (3–12 měsíců):** Implementace prediktivních analytických nástrojů.
- **Dlouhodobé (>12 měsíců):** Pravidelná aktualizace krizových plánů sbírání poznatků o aktuálním bezpečnostním stavu.

7.3 Experiment

Cílem experimentu bylo ověřit, jak jsou reálně zaměstnanci školního zařízení připraveni na situaci, když do objektu pronikne neznámá osoba se záměrem poškodit určitá aktiva školy. Takový scénář je v dnešní době velmi pravděpodobný, a to nejen v souvislosti se stoupající kriminalitou, ale i s obecně narůstajícím počtem bezpečnostních incidentů ve školském prostředí. Jako student bezpečnostního managementu upřednostňuji preventivní činnosti, které často dokážou předcházet reálným hrozbám. Proto jsem se rozhodla provést jednoduchý experiment, který měl simulovat neoprávněný pohyb cizí osoby po škole.

Rozhodně nebylo cílem „nachytat“ personál či ztrapnit vedení školy, ale objektivně zjistit, jak reálně fungují zavedená opatření, jak zaměstnanci vnímají bezpečnost ve svém pracovním prostředí a jestli by byli schopni adekvátně reagovat na podezřelou situaci. Dílčím cílem bylo transparentně ukázat vedení školy, že je potřeba klást větší nárok na své zaměstnance a zároveň zvýšit úroveň bezpečnosti ve škole.

Experiment má kromě zmíněných věcí také sloužit jako impuls pro zvýšení preventivních opatření, neboť doposud nebylo vedení školy ani zaměstnanci příliš aktivní v těchto záležitostech.

7.3.1 Hypotéza

V rámci tohoto experimentu byla předem stanovena hypotéza, která zní následovně: Zaměstnanci školy nejsou schopni včas rozpoznat přítomnost nepovolané osoby v prostorách objektu a adekvátně na tuto situaci reagovat. Bez povšimnutí se neoprávněná osoba dostane do vnitřních prostor školy, kde se bude pohybovat dostatečnou dobu pro provedení nežádoucích aktivit.

Tato hypotéza vychází z dlouhodobějšího monitoringu školy, z konzultací s vedením školy a vlastní obhlídky objektu. Předpokládá se, že hypotéza bude naplněna, i když se v inkriminované době bude ve škole nacházet větší množství osob (pedagogický i nepedagogický personál, asistenti, rodiče, návštěvy). Objekt není střežen žádnou fyzickou ostrahou, vstupní dveře bývají v určitých hodinách otevřené a přístup do jednotlivých částí školy není nijak kontrolován. Z tohoto důvodu bylo předpokládáno, že cizí osoba by mohla projít objektem bez povšimnutí, což by v praxi představovalo značné bezpečnostní riziko.

7.3.2 Použitá metoda

Pro ověření výše uvedené hypotézy je zvolena metoda tzv. inscenačního experimentu. Jedná se o simulaci bezpečnostního incidentu v reálném prostředí, bez předchozího upozornění osob, jejichž chování má být testováno. V tomto případě vědělo o experimentu pouze vedení školy, se kterým byla sepsána smlouva o provedení experimentu a analýzy objektu. Lze konstatovat, že inscenační experiment je běžně využíván např. v oblasti testování připravenosti bezpečnostního personálu nebo zaměstnanců institucí, kde je nutné prověřit schopnost vnímat okolí a rychle se rozhodovat.

Po skončení celého procesu dojde k debriefingu a zpětné vazbě všem zúčastněným. Etické zásady experimentu byly dodrženy – nikdo nebyl zesměšněn, situace nevyvolala stres či paniku a žádná osoba nebyla vystavena riziku. Cílem bylo poukázat na realitu každodenního fungování školy a její možné zranitelnosti.

7.3.3 Popis scénáře experimentu

Scénář byl navržen tak, aby co nejvíce odpovídal reálné situaci, která by mohla nastat v běžném školním provozu. Figurant, který zastával roli osoby s nekalým úmyslem (jedná se o nejmenovaného příslušníka Policie České republiky), vstoupil do budovy školy v poledních hodinách, kdy probíhala standardní výuka a v objektu se nacházelo přibližně 90 osob.

Do školy vstoupil vedlejším, běžně nepoužívaným vchodem, který je situován v části objektu sousedící s přilehlým autoservisem. Figurant využil legendu technického pracovníka a podle toho zvolil i vhodné oblečení a rekvizity, tzn. pracovní oděv a velkou tašku přes rameno. Prostor autoservisu prošel bez povšimnutí a podařilo se mu dostat až k bočním dveřím školy.

Vstupní dveře byly v danou chvíli otevřené a nezabezpečené, čímž došlo k narušení první bezpečnostní bariéry, tedy neoprávněnému vstupu do vnitřních prostor školy. Figurant se tak dostal do technické místnosti, kde se v daném okamžiku nikdo ze zaměstnanců nenacházel. Přibližně po dobu čtyř minut tam mohl nerušeně provádět obhlídku místnosti s rizikovým vybavením.

Následně pokračoval do školního atria, odkud vstoupil do prostoru šaten, kde se v tu dobu pohybovali žáci. Bez povšimnutí tam setrval asi tři minuty. Poté se vrátil zpět do atria, použil výtah a přemístil se do prvního nadzemního podlaží. Po další obhlídce pokračoval po schodišti do druhého podlaží ke sborovně.

Zde byl poprvé kontaktován zaměstnancem školy, který se zeptal, zda hledá konkrétní osobu. Figurant odpověděl, že byl již „nasměrován“, čímž vyvolal dojem legitimního pohybu po budově. Provedl další nenápadnou obhlídku prostor a opět se přesunul do prvního podlaží.

Vstoupil do učebny s počítačovým vybavením, která byla v té době bez dohledu a nezajištěná, a symbolicky „odcizil“ výrobek vytvořený žáky. Poté figurant pokračoval v pohybu po budově, a nakonec se bez potíží dostal do sborovny, kde přímo oslovil ředitelku školy a informoval ji, že se po škole pohyboval zcela bez povšimnutí. Celý scénář trval přibližně 15 minut. Tím byl celý inscenační scénář ukončen.

7.3.4 Subjekty experimentu

V experimentu byl aktivně zapojen pouze jeden figurant, který sehrál roli nepovolané osoby. Před uskutečněním experimentu bylo informováno vedení školy, které bylo seznámeno o průběhu a poskytlo k němu potřebné souhlasy. Ostatní zaměstnanci školy (učitelé, asistenti, správní pracovníci, školník, kuchařky) o experimentu nevěděli, čímž bylo zajištěno zachování autenticity a přirozenosti průběhu.

7.3.5 Výsledky experimentu

Výsledky experimentu ukázaly, že aktuální bezpečnostní a organizační procesy školy neumožňují včasné rozpoznání pohybu nepovolaných osob. Jednalo se např. o nepozorovaný pohyb figuranta po budově, vstup do několika místností, použití výtahu a konečné „doručení důkazního materiálu“ vedení školy, které poukazují na nízkou úroveň ostražitosti a zároveň i edukace zaměstnanců v dané problematice.

Příkladem může být situace, kdy figurant prošel kolem sborovny v druhém podlaží (po cca 12 min), kde byl následně dotazován zaměstnancem, zda nechce poradit s orientací v objektu. Figurant zodpověděl, že již s dotyčnou osobou hovořil a pokračoval dál v pohybu po budově školy. Zaměstnanec udělal chybu, že si jeho odpověď neověřil a nebyl v dotazování dál aktivní.

I přesto je třeba ocenit, že alespoň jeden ze zaměstnanců projevil zájem o neznámou osobu. V případě skutečného incidentu či narušení bezpečnosti školy, by tak mohl dotyčný sehrát důležitou roli při popisu neznámého pachatele.

Přesto však nebyla zaznamenána žádná aktivní reakce na podezřelé chování. Výsledky experimentu tak potvrdily platnost stanovené hypotézy a zároveň odhalily konkrétní slabá místa. Ukázalo se, že současné nastavení kontroly vstupů a obezřetnost zaměstnanců nejsou dostatečné. Zjištění poukazují na potřebu posílení bezpečnostních opatření, zavedení preventivních mechanismů a pravidelného školení personálu.

7.3.6 Závěr a hodnocení zjištěných skutečností

Závěrem lze konstatovat, že zaměstnanci školy nejsou v současnosti připraveni efektivně reagovat podobné incidenty. Absence jakýchkoliv základních bezpečnostních opatření, jako je kontrola vstupu, identifikace návštěvníků nebo jednotná pravidla pro hlášení podezřelých situací, výrazně snižuje celkovou úroveň bezpečnosti školského zařízení.

7.3.7 Zjištěné skutečnosti v rámci experimentu

- 1) Nezajištěný vedlejší vstup představuje vážnou slabinu fyzického zabezpečení objektu. Přístup z veřejného prostoru nebyl nijak kontrolován, což umožnilo snadný vstup neoprávněné osoby.
- 2) Absence kontroly provedené personálem umožnila figurantovi pohybovat se bez ověření totožnosti a účelu návštěvy.
- 3) Nedostatečný monitoring společných prostor a absence kamerového systému znemožnila včasné odhalení podezřelého pohybu.
- 4) Omezená informovanost zaměstnanců o tom, kdo se v budově má nacházet, vedla k tomu, že jediný kontakt s figurantem proběhl bez následných potřebných kroků.
- 5) Volně přístupné učebny s technickým vybavením nejsou z hlediska ochrany majetku dostatečně zabezpečené.

- 6) Místnost určena pro školníka/ údržbáře nebyla zajištěna, jak z vnějšího prostranství, tak z vnitřních prostor. Zde je potřeba zdůraznit, že škola je zaměřena na žáky se speciálními potřebami, a z toho důvodu je riziko o to větší. V tomto případě mohlo dojít nejen k nežádoucí manipulaci s vybavením ze strany figuranta, ale také ze strany žáků, kteří by mohli do místnosti volně vstoupit a následně bez dozoru opustit školu přes zmíněný vedlejší východ.

7.4 Dílčí experiment

Před realizací hlavního experimentu byl záměrně proveden menší dílčí pokus, jehož cílem bylo prověřit aktuální fungování režimových opatření v oblasti hlavního vstupu do budovy školského zařízení. Konkrétně bylo testováno, zda je možné proniknout do objektu hlavním vchodem bez jakékoliv formy osobního ověření a jakým způsobem reagují zaměstnanci na osobu, která není předem ohlášena ani jim známá.

Experiment proběhl přibližně deset minut před plánovaným experimentem. Přistoupila jsem ke vstupním dveřím školy, vstoupila do vestibulu a následně pomocí zvonkového systému, resp. interkomu zazvonila na sborovnu. Po představení se jako návštěvník, který přichází za paní ředitelkou, došlo k okamžitému automatickému odemčení vstupních dveří. K tomu došlo bez jakýchkoli ověřovacích dotazů, vizuálního kontaktu nebo fyzické identifikace.

V době pokusu se ve vestibulu nebyl přítomen žádný pedagog ani jiná dozorující osoba. Přítomní žáci můj příchod zaznamenali, přesto mi nevěnovali pozornost. Nepokusili se mě oslovit, navést ani informovat personál. Po otevření dveří jsem se bez omezení pohybovala po budově, včetně prostor v blízkosti učeben a administrativních kanceláří.

Je vhodné doplnit, že jsem objekt již v minulosti navštívila, což teoreticky mohlo ovlivnit celou situaci uvnitř budovy. Nicméně samotný experiment byl zaměřen výhradně na prověření první úrovně zabezpečení, tzn. vstupu nepovolané osoby do objektu. Dílčí experiment proběhl bez jakéhokoliv ověřovacího mechanismu.

Z pohledu řízení bezpečnostních rizik je tento stav hodnocen jako rizikový. Absence režimu pro kontrolu vstupujících osob znamená, že k obdobné situaci by s vysokou pravděpodobností mohlo dojít opakovaně. Zaměstnanci školy nemají k dispozici jednotný postup ani nástroje, které by umožnily identifikovat a případně zastavit neznámého návštěvníka ještě před vstupem do vnitřních prostor.

Z výše uvedeného vyplývá, že v daném případě dochází k tzv. systémovému selhání, tedy chybě na úrovni nastavení pravidel, nikoliv individuálního pochybení jednotlivce. Absence technických či organizačních opatření znemožňuje účinnou prevenci vniknutí a zvyšuje pravděpodobnost incidentu s dopadem na bezpečnost žáků i zaměstnanců školy. Standardem by mělo být alespoň základní ověření totožnosti osob vstupujících do objektu, zavedení jednoduchého kontrolního mechanismu a zajištění odpovídajícího školení personálu.

Shrnutí kapitoly

Sedmá kapitola s názvem „Analýza rizik“ představovala zásadní část praktického zhodnocení bezpečnosti vybraného školského zařízení. Jejím hlavním cílem bylo provést systematické posouzení úrovně zabezpečení objektu, identifikovat jeho slabá místa a určit oblasti, které vyžadují posílení. Pro naplnění tohoto cíle byly aplikovány dvě odlišné, ale vzájemně se doplňující analytické metody.

Metoda CARVER, původně vyvinutá pro armádní účely, byla přizpůsobena pro prostředí školy a umožnila vyhodnotit míru rizikovosti jednotlivých aktiv na základě šesti kritérií (např. kritičnost, přístupnost, zranitelnost). Výsledky ukázaly, že nejzranitelnějšími prvky jsou hlavní vchod a žáci se speciálními vzdělávacími potřebami, což reflektuje jak technické, tak organizační nedostatky současného zabezpečení.

Druhá použitá metoda, PNH (Posouzení nebezpečí a hrozeb), umožnila kvantifikovat identifikovaná rizika a rozřadit je podle závažnosti. Hodnoceno bylo celkem 30 hrozeb, z nichž většina spadala do kategorie mírného nebo nežádoucího rizika. Nejvyšší pozornost si zasloužily scénáře neoprávněného vstupu do budovy.

Výsledky zároveň odhalily opakující se slabiny v oblasti fyzického zabezpečení, režimových opatření i kybernetické ochrany. Důležitým doplňkem analýzy rizik byl experiment, který v reálném čase simuloval scénář neoprávněného vstupu cizí osoby do objektu školy. Výsledky experimentu potvrdily platnost hypotézy, tzn. zaměstnanci nebyli schopni včas detekovat a adekvátně reagovat na přítomnost neznámého člověka ve škole. Tento experiment, společně s předchozími analytickými metodami ukázal na systémové slabiny v oblasti fyzické bezpečnosti a připravenosti personálu. Výsledky celé kapitoly proto slouží jako pevný základ pro návrh cílených technických a organizačních opatření, jejichž implementace bude předmětem následující části práce.

8 POPIS AKTUÁLNÍHO STAVU ZABEZPEČENÍ A DISPOZIČNÍHO USPOŘÁDÁNÍ VYBRANÉHO OBJEKTU

Kapitola se zaměřuje na popis dispozičního a provozního uspořádání vybraného objektu. Současně je zde popsán stav fyzického zabezpečení budovy. Kapitola se dále věnuje otázce ochrany specifického měkkého cíle. Cílem je zhodnotit, jak je objekt prostorově organizován a jaká bezpečnostní opatření jsou v současnosti k dispozici.

Informace o aktuálním stavu zabezpečení byly zjištěny vlastní observací školní instituce, dále na základě konzultace s vedením školy a v neposlední řadě byly poznatky získány z konzultace s bezpečnostním technikem PTZS. Kromě těchto zdrojů byly využity také volně dostupné informace o instituci.

Cílem této části není pouze popis technických prostředků, ale také krátké zhodnocení jejich umístění a efektivity z hlediska možných bezpečnostních hrozeb, s důrazem na jejich praktické využití v každodenním provozu školy.

Zabezpečení objektu je rozčleněno do čtyř základních úrovní, jedná se konkrétně o ochranu perimetru, pláště budovy, vnitřních prostor a samotných objektů uvnitř. V souladu s teoretickým rámcem práce lze tato opatření zařadit mezi technické, organizační, režimové a fyzické formy ochrany. Následující část se proto detailněji věnuje jednotlivým prostředkům, které jsou ve školním objektu aktuálně využívány k zajištění jeho bezpečnosti.

8.1.1 Perimetrická ochrana

Samotný objekt vybrané školní instituce se nachází v prostoru, jehož větší část je majetkem města. To přirozeně omezuje možnosti rozsáhlejšího zajištění perimetrické ochrany. Vzhledem k těmto prostorovým a legislativním limitům není tato ochrana příliš silnou stránkou instituce. Z mechanických prvků je využito oplocení, které se nachází na obou stranách budovy v zadní části, tzn. prostor za školou směrem k řece. Tento úsek vymezuje soukromý pozemek školy a zároveň slouží jako mechanický zábranný systém proti nedovolenému vstupu. Pravá strana budovy je napojena na pozemek autoservisu, se kterým sdílí příjezdovou cestu. Příjezdová cesta slouží také jako nástupní plocha pro složky IZS.

V některých místech je plot, oddělující školní prostranství od přilehlého autoservisu, viditelně v nevyhovujícím technickém stavu. Drátěné oplocení je poničeno a částečně povoleno, čímž dochází ke ztrátě jeho funkce, v tomto případě mechanické zábranné bariéry.

Vzhledem k blízkosti provozní plochy autoservisu je nutné jeho opravu urychlit, z důvodu zajištění bezpečného prostředí pro pohyb žáků.



Obrázek 8 Nevyhovující stav plotu na hranici s autoservisem

(zdroj: vlastní)

Plot, který ohraničuje perimetr vybraného objektu, splňuje doporučenou výšku, která se pohybuje v rozmezí přibližně 1,2 až 2 metrů. Tato výška je v souladu s běžnými bezpečnostními standardy pro školská zařízení a představuje minimální bariéru proti neoprávněnému vstupu na pozemek. Oplocení je navíc vizuálně přehledné a umožňuje jednoduchou kontrolu pohybu v blízkosti objektu.

Na konci školního pozemku, na odvrácené straně budovy, se nachází také oplocení, které vymezuje hranici mezi areálem školy a přilehlým městským pozemkem. Zároveň zabraňuje samovolnému vstupu žáků k nedaleké řece.



Obrázek 9 Plot oddělující prostranství školy a městský pozemek

(zdroj: vlastní)

Perimetrická ochrana nedisponuje žádným prvkem elektronického zabezpečovacího systému ani kamerového systému.

8.1.2 Plášťová ochrana

Plášťová ochrana objektu, tedy zabezpečení vnějších konstrukčních částí budovy (oken, dveří a vstupních bodů), není v případě vybrané instituce řešena nikterak zvláštním způsobem. Většina vstupů a okenních otvorů je chráněna pouze základními prvky, jako jsou běžné zámky či zámkové mechanismy.

Okna nejsou opatřena mřížemi ani bezpečnostní folií a nedisponují detektory tříštění. Hlavní vstup je opatřen standardním zámkem, chybí však prvky elektronické kontroly přístupu nebo doplňkové technické prostředky, které by zajišťovaly vyšší stupeň zabezpečení pláště budovy. Vzhledem k tomu, že se jedná o školní zařízení, které se nachází v relativně klidné lokalitě, nebyla zatím identifikována nutnost sofistikovanějšího řešení této

formy ochrany. I přesto však absence pokročilejších bezpečnostních prvků může představovat riziko, zejména mimo provozní dobu školy.

8.1.3 Prostorová ochrana

Prostorová ochrana představuje důležitou část zabezpečení objektu, jejímž cílem je monitorování vnitřních prostor budovy s cílem včasného zachycení neoprávněného pohybu. Ve vybrané školní instituci je tato forma zabezpečení zajištěna pomocí 14 PIR detektorů značky JABLOTRON, které jsou rozmístěny v důležitých částech objektu. Konkrétně se jedná o JA-110P sběrníkový PIR detektor pohybu.

Tyto detektory jsou součástí Poplachového zabezpečovacího a tísňového systému (PTZS) a jsou schopné zachytit jakýkoliv pohyb ve střežených zónách, typicky v chodbách, učebnách nebo vstupních prostorech, primárně mimo provozní dobu. V případě detekce narušení jsou detektory napojeny na systém signalizace, který aktivuje výstražné zařízení, čímž dochází ke spuštění akustického alarmu. [13] V tomto případě je využívána JA-111A Sběrníková siréna venkovní a JA-110A Sběrníková siréna vnitřní. Venkovní siréna je umístěna na severní straně budovy směrem na školní pozemek, vnitřní siréna pak v 1. poschodí v těsné blízkosti ústředny, která se nachází vedle kabinetu hospodářky školy.

Venkovní umístění bylo zvoleno záměrně, protože opačná strana objektu je orientována k hlavní komunikaci, a z důvodu dopravnímu ruchu by siréna nemusela jít slyšet. Umístěním sirény do klidnější části areálu je zajištěno, že zvukový signál bude v případě spuštění lépe slyšet i v nedalekém centru města. Zmíněný PTZS byl instalovaný v době mé obhlídky objektu, tudíž se jedná o novou záležitost a vedení školy teprve testuje efektivitu této formy zabezpečení. Nasazení těchto detektorů však významně zvyšuje efektivitu vnitřní ochrany objektu a slouží jako preventivní prvek proti neoprávněnému vstupu cizí osobou.

Přízemí budovy

Přízemí objektu plní zejména vstupní, provozní a částečně výukové funkce. Hlavní vstup je situován v pravém křídle budovy, a ústí do vestibulu školy, který je opatřen dalšími dveřmi disponující starší verzí interkomu. Dveře oddělující vestibul od vnitřních prostor školy jsou vybaveny kováním v provedení klika–koule, které zajišťuje, že při jejich zavření není možné vstoupit bez použití klíče. V praxi však dochází k situacím, kdy jsou dveře po odemčení ponechány otevřené, čímž je narušena jejich bezpečnostní funkce a umožněn volný, nekontrolovaný vstup do vnitřních prostor školy. Dveře jsou zároveň opatřeny bezpečnostním kováním s překrytím cylindrické vložky, které zvyšuje jejich odolnost vůči

neoprávněnému vniknutí. Tento typ zabezpečení se běžně využívá v objektech, kde je třeba kontrolovat pohyb osob, a přispívá ke zvýšení celkové úrovně fyzické ochrany budovy.

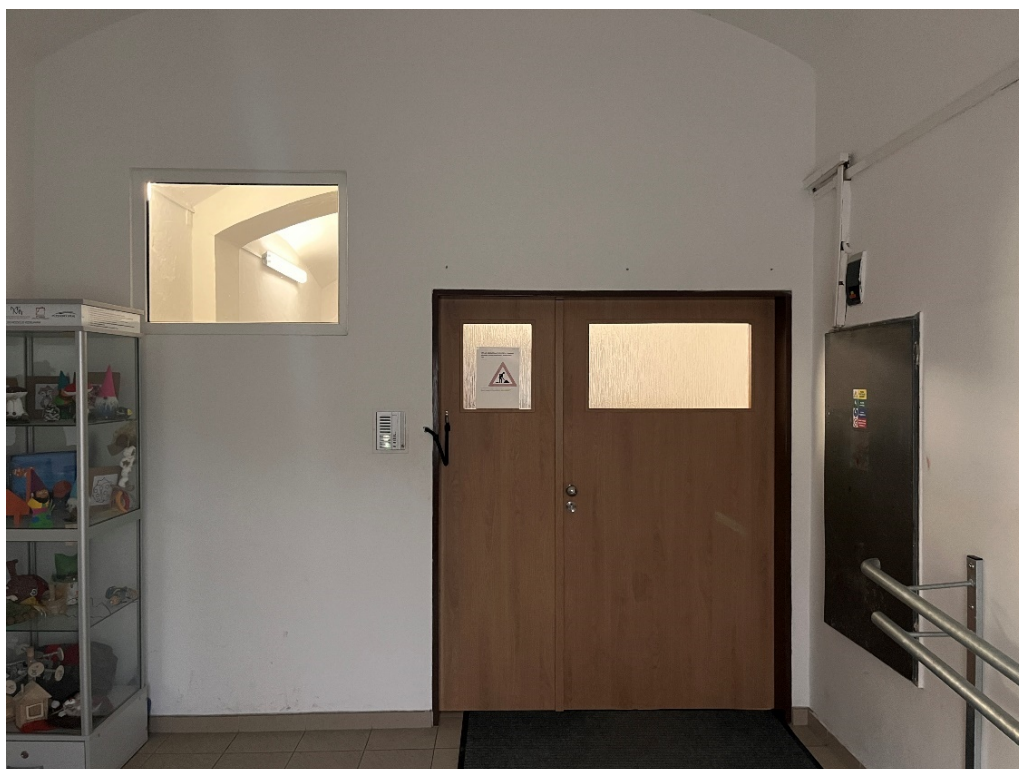
Problém se zajištěním dveří vyplývá ze specifík provozu školní instituce. V časovém rozmezí od 11:00 do cca 16:00 jsou dveře běžně odemčeny z důvodu odchodů žáků. Nepřetržité hlídání hlavního vstupu by bylo v tomto časovém období personálně i organizačně náročné. Výsledkem je zvýšené riziko vstupu nepovolaných osob do budovy. V uvedeném čase dochází k pohybu rodičů přicházejících pro své děti a návštěv Speciálního pedagogického centra, přičemž v mnoha případech není zajištěna jejich identifikace. Neprověřené osoby se tak mohou volně pohybovat po prostorách školy, což představuje bezpečnostní riziko.

Pro lepší pochopení orientaci v popisu prostorového uspořádání budovy jsou níže přiloženy evakuační plány jednotlivých podlaží.



Obrázek 10 Evakuační plán objektu – přízemí

(zdroj: vlastní)



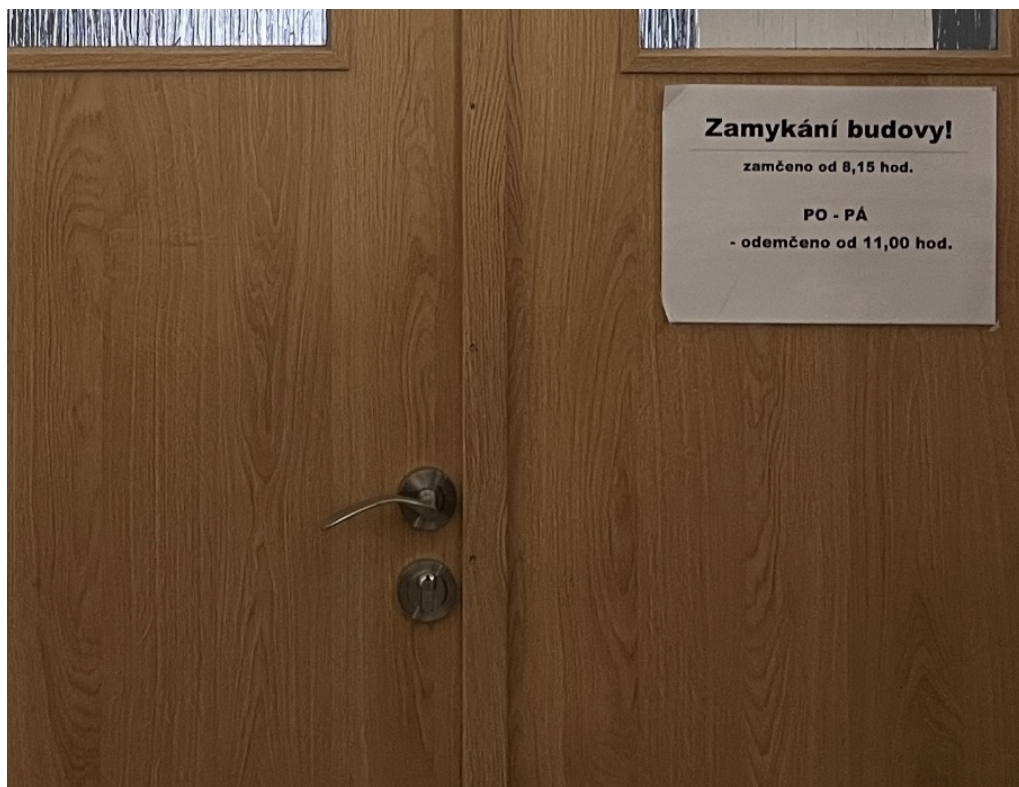
Obrázek 11 Hlavní dveře ve vstupním vestibulu

(zdroj: vlastní)



Obrázek 12 Interkom u hlavních dveří ve vestibulu

(zdroj: vlastní)



Obrázek 13 Informace na hlavních dveřích

(zdroj: vlastní)

Navazující prostor z dveří vestibulu je vybaven šatnami, které slouží k odkládání obuvi a svrchního oblečení žáků. Prostor je důležitým bodem, neboť je v něm velká fluktuace osob při příchodu a odchodu z budovy, zejména v ranních a odpoledních hodinách. Zároveň bylo zjištěno, že šatny nebývají zamčeny, tudíž jsou odložené věci žáků také vystaveny riziku odcizení či poškození.

V pravém křídle přízemí se nachází školní kuchyňka, která slouží výhradně zaměstnancům školy. Součástí této části budovy je rovněž školní dílna určená pro dřevařské práce. Tento prostor je specifický nejen svou funkcí, ale také riziky, která se s ní pojí. V dílně se běžně nachází elektrické nářadí, ostré pracovní pomůcky a další předměty, které mohou být v mnoha případech nebezpečné. Během obhlídky bylo zjištěno, že je potřeba zvýšit úroveň bezpečnosti směrem k žákům, kteří se místnosti pohybovali i bez přímého dohledu. Pokud hovoříme o rizicích spojených se zmíněnou dílnou, jedná se o níže uvedené:

1. Nezajištěné pracovní pomůcky a nářadí, které mohou být snadno dostupné a zneužitelné, pokud nejsou řádně uzamčeny.

2. Nevhodné skladování materiálů, například dřevěného odpadu nebo hořlavin, které mohou v kombinaci s elektrickým nářadím zvýšit riziko požáru.

3. Možnost úrazů žáků v době výuky, kdy pedagogický pracovník nedbá příliš na bezpečnost žáků.

4. Ztráta nebo odcizení vybavení, které může být následně využito k úmyslnému poškození majetku nebo ohrožení osob.

Ze školních šaten vede přímý koridor k tělocvičně. Ta je mimo dobu výuky či jiné plánované aktivity standardně zamčena. To z toho důvodu, aby se předešlo neoprávněnému vstupu a případnému zneužití prostoru. Z tělocvičny vede únikový východ na školní prostranství, kde je situováno centrální shromážděště. Klíče od uvedených dveří jsou uloženy za popisovou tabulkou, viz obrázek č. 14.



Obrázek 14 Úschova klíčů od únikového východu

(zdroj: vlastní)

Další důležitou částí přízemí tvoří atrium, které propojuje jednotlivé části budovy a slouží jako hlavní "uzel" tohoto podlaží. Z atria je přímý přístup do zmiňovaného koridoru mezi šatnami a tělocvičnou. Propojující dveře plní funkci únikového východu. Nad těmito

dveřmi se nachází klíče zavěšené na magnetickém držáku, které jsou volně dostupné bez jakéhokoliv zabezpečení nebo kontroly, viz obrázek č. 15.

Tato skutečnost představuje významné bezpečnostní riziko. Klíče nejsou chráněny proti neoprávněnému použití a jejich umístění je snadno dostupné nejen pro pracovníky školy, ale i pro žáky či jiné osoby pohybující se v prostorách školy. Hrozí tak možnost neoprávněnému otevření únikových dveří, což může vést k narušení bezpečnostního režimu, úniku osob z objektu, nebo naopak k usnadnění vstupu zvenčí. V případě krizové situace navíc není zaručeno, že klíče budou na svém místě, což může zkomplikovat celou evakuaci školy.



Obrázek 15 Úschova klíčů od výše uvedených dveří

(zdroj: vlastní)

Z atria dále vede výtah, jež vertikálně propojuje všechna podlaží budovy, což znamená přízemí, první a druhé nadzemní podlaží. Výtah nedisponuje žádným bezpečnostním prvkem spadající do režimového opatření. Z toho důvodu jej může využívat kdokoli bez toho, aniž by si toho někdo všiml.



Obrázek 16 Vstup do výtahu v atriu

(zdroj: vlastní)

Vedle výtahu jsou plechové dveře vedoucí do kotelny a technických místnosti, včetně dílny školního údržbáře. Z hlediska bezpečnostního posouzení představuje tato oblast jedno z nejrizikovějších míst celé budovy. Klíče od těchto dveří vlastní pouze školní údržbář a vedení školy. Při obhlídce objektu bylo zjištěno, že dveře do dané místnosti zůstaly odemčené, a to i v době, kdy se školní údržbář v prostorách nenacházel.



Obrázek 17 Dveře mezi atriem a kotelnou

(zdroj: vlastní)

Při vstupu je zřejmé, že prostor není dostatečně zabezpečen proti nepovolenému vniknutí. Dveře z dílny vedou přímo na volně přístupné prostranství přilehlého autoservisu, což znamená, že k nim mají přímý přístup i cizí osoby. Při několika návštěvách bylo opakovaně zaznamenáno, že tyto dveře byly zcela otevřené. Tato skutečnost výrazně zvyšuje riziko neoprávněného vstupu do objektu, a to nejen z hlediska majetkového ohrožení, ale i z hlediska bezpečnosti osob nacházejících se v budově.



Obrázek 18 Pohled při vstupu do kotelny

(zdroj: vlastní)

Součástí samotného prostoru kotelny se nachází řada technických zařízení (např. plynové kotle, expanzní nádoby), k nimž by v žádném případě neměly mít přístup nepovolané osoby. V místnosti je zároveň uloženo větší množství různorodého nářadí, pracovních pomůcek, chemických látek a dalších předmětů, které mohou představovat bezpečnostní riziko – ať už ve smyslu možnosti úrazu, manipulace s nebezpečnými látkami, nebo odcizení nářadí.



Obrázek 19 Pohled při vstupu do kotelny II.

(zdroj: vlastní)



Obrázek 20 Technická dílna školníka

(zdroj: vlastní)



Obrázek 21 Technická dílna školníka – východ

(zdroj: vlastní)



Obrázek 22 - Technická dílna školníka – pohled z východu na autoservis

(zdroj: vlastní)



Obrázek 23 - Technická dílna školníka – pohled na dveře z venku

(zdroj: vlastní)

První nadzemní podlaží

První nadzemní podlaží budovy slouží převážně pro vzdělávací a administrativní účely. Jeho dispoziční řešení je uspořádáno kolem centrální chodby a atria, na které navazuje hlavní schodiště propojující všechna patra objektu. Na tomto podlaží se nachází celkem devět učeben určených pro běžnou výuku a jedna učebna určena pro hodiny informatiky.

Nejvýznamnější část tohoto podlaží je situována v těsné blízkosti kanceláře vedení školy, odkud se zajišťuje koordinace a provozní dohled nad chodem celé instituce. Ve zmíněném prostoru se taktéž nachází výtah propojující centrální atrium a všechna nadzemní podlaží. Tento úsek chodby je z hlediska fyzické bezpečnosti vybaven několika prvky technické ochrany, zejména PIR detektory napojených na PTZS, dále je tam instalovaná jedna ze dvou sirén. V neposlední řadě je tam také umístěn detektor elektronické požární signalizace (EPS), který slouží k včasné detekci požáru a zajištění evakuační bezpečnosti.

Dále se tam nachází kancelář hospodárky, ve které je umístěn jeden ze čtyř zvonků, který je součástí interkomu u hlavních dveří. Hospodárka školy částečně vykonává dohled nad pohybem osob vstupujících do objektu. Z toho vyplývá, že hospodárka je osoba, která má přehled o vstupu žáků a jejich rodičů.

Další dispoziční uspořádání školy je logicky členěné, přehledné a umožňuje plynulý pohyb osob po budově. Díky přímému propojení centrální chodby s hlavním schodištěm lze považovat uspořádání za funkční jak z provozního, tak orientačního hlediska.



Obrázek 24 Evakuační plán objektu - 1. poschodí

(zdroj: vlastní)

Druhé nadzemní podlaží

Druhé nadzemní podlaží plynule navazuje svou funkcí i dispozičním uspořádáním na podlaží první. Patro slouží primárně k výuce a odborné činnosti pedagogických pracovníků.

V levé části budovy se nachází dvě běžné učebny určené pro výuku žáků prvního stupně a dále dvě místnosti vyčleněné pro školní družinu a knihovnu. V těsné blízkosti hlavního schodiště je situována kancelář zástupce ředitele, která plní funkci vedení pedagogického provozu v rámci běžného chodu školy. Zároveň se tam nachází Sborovna č.1, která je vybavena druhým vnitřním telefonem napojeným na interkom u hlavních dveří.

V pravém křídle druhého nadzemního podlaží se nachází prostory Speciálně pedagogického centra (SPC) Tyto místnosti slouží k individuální či skupinové práci s dětmi

se speciálními vzdělávacími potřebami. Prostory jsou využívány nejen interními žáky školy, ale rovněž externími klienty, tzn. dětmi docházejícími z jiných školských zařízení, často v doprovodu rodičů.

Centrum je vybaveno třetím vnitřním telefonem propojeným s interkomem. Problém však nastává v návaznosti na provozní režim školy, kdy většina konzultací a poradenských činností probíhá v poledních nebo odpoledních hodinách, kdy jsou hlavní dveře zpravidla odemčené. V této době tak návštěvníci centra vstupují do budovy bez předchozí kontroly a pohybují se samostatně v prostorách školy, což může představovat bezpečnostní riziko.

Kromě SPC se tam nachází také běžné učebny určené pro výuku a sborovna číslo 2, která slouží jako zázemí pro pedagogický personál. Tato místnost je rovněž vybavena vnitřním telefonem. Díky tomu mají zaměstnanci možnost alespoň částečně monitorovat pohyb osob přicházejících do školy.

Třetí podlaží, půdní vestavba, je veřejnosti i žákům běžně nepřístupná. Slouží z části jako technické zázemí a sklad.



Obrázek 25 Evakuační plán objektu - 2. poschodí

(zdroj: vlastní)

Shrnutí kapitoly

Kapitola osmá se věnovala podrobnému popisu aktuálního stavu zabezpečení a dispozičního uspořádání školní budovy. Popis byl strukturován podle čtyř základních úrovní fyzické ochrany a vycházel z několika osobních návštěv školy, konzultací s vedením instituce a s odborníkem na bezpečnostní systémy.

Zjištěné informace ukazují, že zabezpečení objektu je sice částečně funkční, ale vykazuje řadu slabin, které je potřeba urgentně řešit. Slabiny jsou zejména v oblasti kontroly vstupů, technického stavu oplocení a absence pokročilých bezpečnostních prvků jako jsou kamerové a sofistikované přístupové systémy. V kapitole bylo upozorněno na problémy se snadno dostupnými únikovými klíči, nezajištěnými technickými prostory a na slabé organizační kontroly nad pohybem cizích osob po budově.

Dispozičně je škola uspořádána přehledně a účelně. Přízemí slouží pro vstupní a provozní činnosti, vyšší patra pro výuku, administrativu a činnosti speciálně pedagogického centra (SPC). Toto členění usnadňuje orientaci i plynulý pohyb osob, nicméně odhaluje konkrétní riziková místa např. dílny s volně přístupným nářadím, nehlídané šatny či nedostatečně uzavřené boční vstupy. Zvláštní pozornost byla věnována prostorám SPC, které jsou využívány i veřejností – kde se ukazuje, že režim vstupu těchto návštěvníků není vždy dostatečně kontrolován.

V kapitole byla identifikována potřeba posílení fyzické i režimové bezpečnosti a tyto nedostatky budou sloužit pro návrh konkrétních opatření ke zvýšení bezpečnostní úrovně školského zařízení.

9 NÁVRH BEZPEČNOSTNÍCH OPATŘENÍ

Na základě výsledků analýz PNH a CARVER, experimentálního ověření a posouzení aktuálního stavu zabezpečení byla navržena bezpečnostních opatření, která by měla zvýšit celkovou bezpečnostní úroveň školního zařízení. Návrhy zároveň vycházejí z hodnocení měkkých cílů, které stanovilo Ministerstvo vnitra ČR. Jak již bylo uvedeno v kapitole Ochrana měkkých cílů, je nezbytné uplatňovat strategii „myslet dopředu“ a tím potencionálním hrozbám předcházet.

Součástí návrhů bezpečnostních opatření není pouze fyzická či technická ochrana, ale také důsledná edukace a průběžná osvěta všech osob, které se v objektu školy pravidelně pohybují. Jedná se především o informovanost pedagogických a nepedagogických zaměstnanců, ale také žáků. Je z principu důležité dělat osvětu o základních principech bezpečného chování v případě potenciální hrozby.

Zejména ve školním prostředí je žádoucí zvyšovat úroveň bezpečnosti, která spočívá v pravidelné osvětě, instruktáže a školení. Tyto aktivity mohou být realizovány jak interně (např. školním metodikem prevence), tak externími specialisty zaměřenými na krizovou připravenost, prevenci násilného chování nebo reakce na specifické typy hrozeb. Doporučuje se zařazení vzdělávacího programu, jehož součástí mohou být tematické bloky zaměřené např. na rozpoznání podezřelého chování osob, základní pravidla evakuace, popř. ukrytí, správný postup při výskytu neznámé osoby v objektu školy, krizovou komunikaci a nácvik tísňového volání a postupy při výskytu aktivního střelce ve škole. Vzdělávání by mělo být přizpůsobeno cílové skupině, tzn. žákům by měly být informace předávány srozumitelnou a věku přiměřenou formou, zatímco zaměstnanci školy musí detailně znát bezpečnostní protokoly a umět aplikovat předepsané postupy v praxi.

Osvětová činnost zároveň podporuje všímavost a včasné informování, což může být rozhodující zejména v situacích, kdy dochází k narušení bezpečnosti ze strany cizí osoby, nebo v případě výskytu nečekané krizové události. Pedagogové a další pracovníci by tak měli být schopni rychle identifikovat varovné signály a efektivně reagovat. Z hlediska bezpečnostního managementu lze konstatovat, že systematická edukace a osvěta významně přispívají ke snížení zranitelnosti objektu, posilují vnitřní odolnost školy vůči hrozbám a tvoří jeden z pilířů účinné prevence.

9.1 Návrh připravenosti a vzdělávání

Dle zásad ochrany měkkých cílů patří připravenost a vzdělávání mezi tři klíčové pilíře. Z tohoto důvodu se vedení školy doporučuje zavést pravidelné školení, preventivní program a aktuální krizový plán školy. Krizový plán by měl být strukturován podle cílových skupin a aktualizován minimálně jednou ročně. Právě tato forma preventivního působení patří mezi nejefektivnější a zároveň finančně nejméně náročná opatření. Jedná se především o následující typy mimořádných událostí:

Identifikace a postup při výskytu neznámé osoby v budově

Jedním ze základních scénářů krizové připravenosti školy je situace neoprávněného vstupu cizí osoby do budovy školy. Aby se předešlo možnému riziku, je nezbytné zavést jasně stanovená preventivní a organizační opatření. Hlavní vstup do školy by měl být pod stálým dohledem určené provozní osoby, která zajišťuje kontrolu nad tím, kdo do budovy vstupuje. Ostatní vstupy by měly být trvale uzamčeny, aby se minimalizovalo riziko průniku zvenčí. Zaměstnanci školy mají výslovný zákaz vpouštět do objektu kohokoli, kdo není oprávněn ke vstupu, a to ani při společném příchodu. Pokud cizí osoba projeví zájem o vstup, je nutné ji zastavit, zjistit účel její návštěvy a neprodleně o tom informovat vedení školy nebo jiného pověřeného pracovníka.

Zaměstnanci školy by měli být zároveň vedeni k tomu, aby si všímali pohybu neznámých či podezřelých osob v budově. V případě, že se taková osoba pohybuje v prostorách školy je nutné situaci vyhodnotit a reagovat podle jejího charakteru. Ve většině případů není vhodné osobu přímo konfrontovat, ale je nezbytné její přítomnost neprodleně nahlásit vedení školy. Při jakémkoli podezřelém chování je důležité dodržovat tzv. bezpečnostní zónu, tedy udržet si od podezřelé osoby dostatečný odstup, ideálně několik metrů. Pokud to situace dovolí, doporučuje se uchýlit se do jiné místnosti, zevnitř ji uzamknout a vyčkat příjezdu Policie ČR. V mimoškolní době by měl být celý objekt střežen elektronickým zabezpečovacím systémem. Pokud by přesto došlo k narušení objektu a existovalo by důvodné podezření, že přítomná osoba může být nebezpečná, je zaměstnanec povinen okamžitě kontaktovat Policii ČR, a poté bez prodlení informovat ředitele školy či jeho zástupce. Do příjezdu policie musí zaměstnanec zajistit klid, bezpečnost okolí a umožnit bezpečnostním složkám přístup do objektu. Tato doporučení by měla být součástí pravidelné školní dokumentace a interních směrnic, s nimiž by měli být zaměstnanci pravidelně seznamováni. [70] [71]

Aktivní útočník

Aktivní útočník je jedinec, který se z vlastní iniciativy rozhodne násilně zaútočit na osoby ve svém okolí. Jeho čin bývá náhlý, intenzivní a často extrémně brutální. Na základě dosavadních případů lze říci, že útoky jsou zpravidla předem plánované, zaměřené na co největší počet obětí a probíhají v místech s vysokou koncentrací lidí, jako jsou například školy. Útočníci si vybírají oběti náhodně, používají různé typy zbraní a jejich cílem nebývá střet s policií, přičemž celý incident zpravidla trvá jen několik minut. [71]

Reakce při útoku aktivního střelce

V případě útoku aktivního pachatele je doporučeno postupovat podle tří základních principů krizové reakce, které jsou přizpůsobeny aktuální situaci a možnostem přítomných osob [71] [72]:

- a) **Únik z prostoru** – pokud je dostupná bezpečná cesta, je prioritou okamžitý odchod z ohrožené zóny.
 - Při úniku by se nemělo zdržovat sběrem osobních věcí.
 - Pokud to situace dovolí, je vhodné pomoci ostatním osobám s evakuací.
 - Pokud je to možné, upozornit ostatní na přítomné nebezpečí a varovat je, aby se do oblasti nevydávali.
 - Po přemístění se na bezpečné místo, kontaktovat tísňovou linku Policie ČR (158) a stručně popsat situaci.
- b) **Úkryt** – pokud útěk není možný, je nutné nalézt úkryt, který minimalizuje riziko odhalení.
 - Zajistit uzamčení nebo mechanické zablokování vstupních dveří do místnosti.
 - Vyhledat pevné prostředky, které mohou sloužit jako bariéra.
 - Ztišit mobilní telefon a zůstat naprosto potichu, aby nedošlo k prozrazení polohy.
 - Pokud je situace stabilní, je třeba opět kontaktovat Policii ČR a sdělit svou polohu a průběh incidentu.
- c) **Sebeobrana** – pokud již nelze uniknout ani se ukryt a život je bezprostředně ohrožen, je nezbytné aktivně se bránit.

- Pokusit se útočníka zastavit jakýmkoliv dostupnými prostředky.
- Při útoku jednat rázně, rozhodně a s maximálním nasazením.
- Využít předměty v okolí, které lze improvizovaně použít jako zbraň.
- Důležité je jednat bez váhání, cíleně a koordinovaně s cílem eliminovat hrozbu.

Požár

V případě zjištění požáru je nezbytné zachovat klid a jednat s rozvahou. Panice je třeba předejít a řídit se pokyny pověřených osob. Okamžitě je nutné informovat odpovědné zaměstnance školy, například vedení školy nebo pedagogického pracovníka. V případě, že jsou ve škole k dispozici tlačítkové hlásiče požáru, je možná i tato varianta. Zároveň se ohrožení oznámí hlasitým voláním „Hoří!“ nebo použitím jiného domluveného hesla/signálu. Učitelé přebírají zodpovědnost za vedení třídy a instruují žáky k evakuaci. Třída se řadí ke dveřím, učitel provádí kontrolu a ujistí se, že nikdo nezůstal v učebně. Následně probíhá organizovaná evakuace. Všichni musí mít na paměti, že se nesmí používat výtah, únikové cesty musí zůstat volné a jasně označené. Pokud se při evakuaci musí projít zakouřenými prostory, je třeba se pohybovat při zemi a chránit si dýchací cesty. Pokud je to možné, zavírejte za sebou dveře, aby se zpomalilo šíření požáru. [71]

Po evakuaci se všechny osoby shromáždí na předem stanoveném místě, tzv. "shromážděště" mimo budovu, kde učitel zkontroluje přítomnost žáků a nahlásí aktuální stav vedení školy nebo přímo příslušníkům hasičského záchranného sboru. Nikdo se nesmí vracet do budovy bez výslovného souhlasu záchranných složek. Pokud jsou mezi evakuovanými zranění nebo chybějící osoby, je třeba tuto skutečnost okamžitě nahlásit. Záchranným složkám je nutné nebránit v činnosti a řídit se jejich pokyny.

Tísňovou linku 150 (Hasičský záchranný sbor) nebo univerzální linku 112 je vhodné volat ihned poté, co dojde k identifikaci. V hovoru je důležité uvést všechny potřebné informace. [70] [73]

Teroristický čin

V případě anonymního oznámení o uložení výbušniny ve škole je nezbytné zachovat klid a postupovat podle stanovených pravidel. Pokud je oznámení učiněno telefonicky, je třeba co nejpřesněji zaznamenat znění sdělení včetně uvedení místa a typu výbušniny. V případě písemné nebo elektronické formy se dokumentace neodstraňuje, ale uchovává pro potřeby dalšího šetření. Následně je nutné bezodkladně kontaktovat složky integrovaného

záchranného systému prostřednictvím tísňové linky 112, případně přímo Hasičský záchranný sbor (150) nebo Policii ČR (158). Pokud se v prostorách školy v době oznámení nacházejí osoby, musí být okamžitě zahájena evakuace podle předem připraveného požárního evakuačního plánu. Podezřelých předmětů se nesmí nikdo dotýkat a všichni přítomní jsou povinni dodržovat pokyny zasahujících složek. [71]

Zvýšená obezřetnost je rovněž namístě při přijetí podezřelé zásilky. Mezi varovné signály patří zejména zásilka od neznámého odesílatele, přítomnost výhružného textu, neobvyklý zápach nebo obsah v podobě prášku či jiného podezřelého předmětu. Pokud se taková zásilka objeví, nesmí být s jejím obsahem manipulováno – je nutné s ní netřepat ani ji neotevírat. Místnost je potřeba ihned opustit, dotčená osoba by se měla omýt vodou a mýdlem a vše následně nahlásit na linku 150 nebo 158. Ještě před voláním je vhodné zhodnotit, zda existují konkrétní okolnosti, které naznačují, že zásilka může představovat reálnou hrozbu. V obou případech je klíčové neprodleně informovat vedení školy a nezasahovat do práce bezpečnostních složek. [70]

Vedení školy doporučují další tematické okruhy pro edukaci:

a) Pro zaměstnance školy (pedagogické a nepedagogické pracovníky)

- postupy při evakuaci, ukrytí, přivolání IZS,
- komunikační protokol při incidentu (vnitřní a vnější sdělení),
- řešení stresových reakcí a krizová intervence pro pedagogy,
- simulace incidentu aktivního útočníka v prostorách škol.

Četnost těchto školení je minimálně 2× ročně, přičemž jednou v úvodu školního roku a jednou v průběhu. Co se týče formy, nejlepší variantou jsou školení, instruktáže, modelové situace a krizové nácviky.

b) Pro žáky

Zde jsou tematické okruhy pro vzdělávání:

- Jak se chovat při krizových situacích (např. požár, cizí osoba),
- všímavost a oznámení podezřelého chování dospělému/odpovědnému pracovníkovi,
- pravidla osobní bezpečnosti a pohybu po škol,

- práce s emocemi a stresovými situacemi.

Četnost školení pro žáky je minimálně 1× ročně, například formou projektového dne, následně pak individuálně každá třída v rámci třídnických hodin. Pro žáky je potřeba volit odlišnou formu edukace, a to například interaktivní besedy, diskuze, informační letáky, edukační videa, případové studie, pracovní listy či jiné podpůrné materiály k vypracování.

9.2 Návrhy pro zvýšení fyzické bezpečnosti

V této podkapitole navrhuji konkrétní opatření pro zvýšení fyzické bezpečnosti školy, a to na základě zjištění z praktické části diplomové práce a vlastního posouzení aktuálního stavu zabezpečení.

Elektronická požární signalizace

Škola v současné době disponuje základním systémem elektronické požární signalizace (EPS), který zajišťuje detekci kouře a vyvolání požárního poplachu. Pro zvýšení úrovně bezpečnosti a efektivity evakuace je však nezbytné tento systém dále rozšířit, a to zejména o ručně ovládané tlačítkové hlásiče požáru (ROP), které dále aktivuje evakuační režim při identifikaci mimořádné události. Následně je navrhováno doplnění evakuačních východů o magnetické zámky s tzv. fail-safe funkcí. Napojením magnetických zámků na systém EPS bude zajištěna jejich automatická deaktivace při požárním poplachu, čímž se okamžitě uvolní únikové cesty.

Uvedené technické řešení by nahrazovalo to dosavadní provizorní opatření, tzn. klíče od evakuačních východů nemusí být uschovány za popisovou tabulkou v tělocvičně.



Obrázek 26 Tlačítkový hlásič

(zdroj: [54])

Kamerové systémy

Jedná se o jeden z nejdůležitějších a zároveň nejefektivnějších technických návrhů v rámci zvyšování bezpečnostní úrovně školního zařízení.

Kamerové systémy navrhuji umístit:

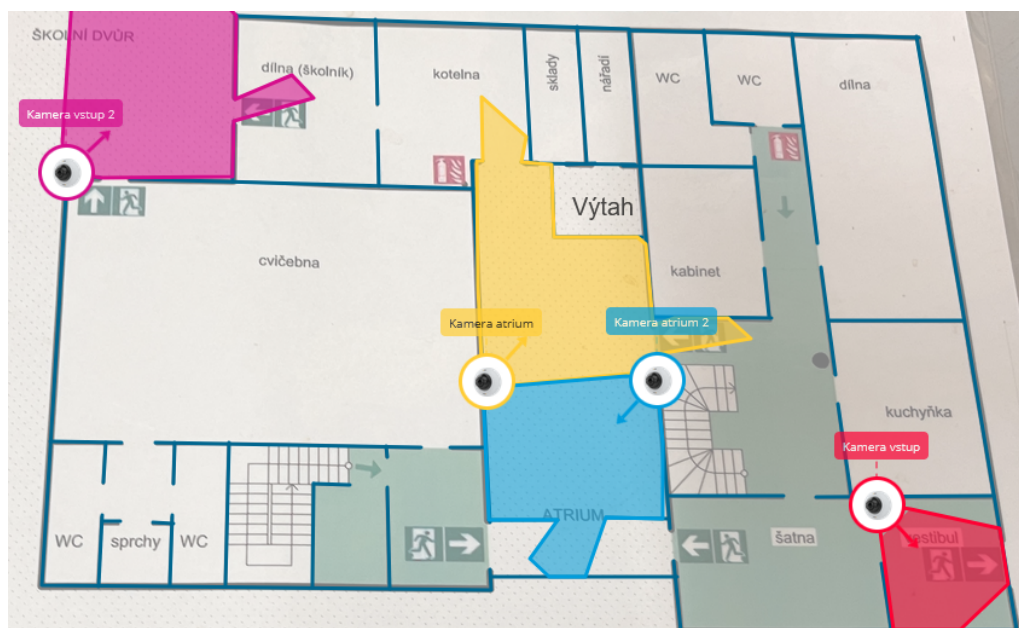
1. u hlavního vchodu ve vestibulu u systému interkom,
2. u obou vedlejších vchodů,
3. v atriu.

Doporučené modely:

AXIS M4216-LV – je vhodná pro monitoring vstupních i vnitřních prostor školy díky 4MP rozlišení (2304×1728) a objektivu (3–6 mm) s možností vzdáleného ostření a optickému přiblížení. Disponuje IR přísvitem s dosahem až 20 metrů pro noční vidění, funkcí WDR a technologií Lightfinder pro kvalitní obraz i za špatných světelných podmínek. Kamera je odolná proti vandalismu (IK08) a částečně proti vlhkosti (IP42). Vestavěná analytika na bázi deep learningu umožňuje detekci osob, podezřelého chování či počítání průchodů. Díky připojení přes PoE a možnosti integrace s přístupovými a monitorovacími systémy patří tato kamera mezi nejefektivnější technická opatření pro zvýšení fyzické bezpečnosti ve školním prostředí. [50]

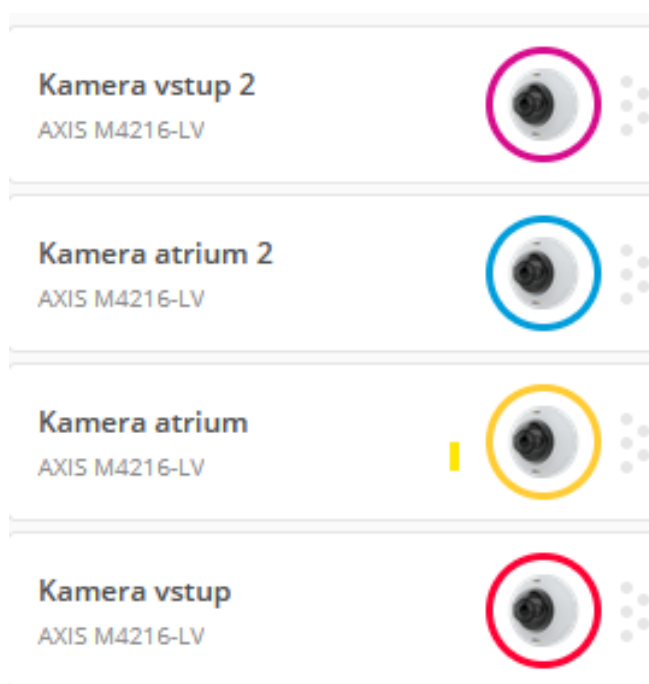
Další možnosti:

- Rhombus R200 / R360 - R200 pro vstupy, R360 ideální pro vestibul s 360° záběrem.
- Verkada CD52 / CD52-E – cloudová správa, dlouhá záruka, možnost vzdáleného dohledu a archivace.



Obrázek 27 Plán rozmístění kamer AXIS

(zdroj: vlastní)



Obrázek 28 Použité kamery v návrhu

(zdroj: vlastní)

V souladu se současnými trendy v oblasti fyzické bezpečnosti, jak bylo uvedeno v teoretické části této práce, by bylo do budoucna vhodné zvážit rozšíření kamerového systému o doplňkové bezpečnostní prvky, jako jsou například AI detekce zbraní, integrace s přístupovým systémem nebo automatizované varovné protokoly.

Elektronická kontrola vstupu

Jedním ze zásadních opatření ke zvýšení fyzické bezpečnosti školního zařízení je zavedení přístupového systému založeného na technologii RFID. Vzhledem k charakteru objektu navrhuji využít vysokofrekvenční RFID systémy pracující na frekvenci 13,56 MHz, které nabízejí vyšší úroveň zabezpečení a podporu šifrování. Za nejbezpečnější řešení se považuje technologie MIFARE DESFire EV2 nebo EV3, která splňuje bezpečnostní certifikaci EAL5+ a umožňuje víceúrovňovou šifrovací ochranu (DES, 3DES, AES128). [74]

Since je pořizovací cena vyšší, ale jak již bylo zmíněno, má nejlepší úroveň bezpečnosti a je dlouhodobě spolehlivý. Doporučuji instalaci u všech strategických vstupů, tzn. hlavní vchod, vedlejší vstupy do objektu a výtah. Přístup by byl umožněn pouze oprávněným osobám prostřednictvím RFID karet nebo čipů, jednalo by se především o zaměstnance a žáky se specifickými potřebami, kteří pro pohyb ve škole využívají výtah.

Do budoucna by stálo za zvážení, zda nezajistit možnost přístupu pomocí čipu i dalším žákům. Tento krok by mohl snížit zatížení zaměstnanců v oblasti režimových opatření a současně posílit samostatnost žáků při pohybu po objektu.

Mechanické zábranné systémy

Co se týče návrhu spadajících do mechanických zábranných systému, je potřeba implementovat prvky bezpečnostní třídy RC.3/RC.4, které poskytují zvýšenou ochranu proti vniknutí a jsou vhodná pro rizikové objekty jako je škola. V první řadě se jedná o doplnění nebo výměnu dveřního kování, konkrétně hovoříme o klikách a koulích u všech vstupních dveří. U hlavních dveří bych volila kombinaci pevné, či otočné koule na rozetě s klikou zevnitř. Nejvhodnější materiál je nerezová ocel, hliník nebo slitina zamak. [11]

Alternativní způsob řešení je použití madla, které může v určitých případech nahradit kouli nebo klasický klíčový systém.

Zvýšenou pozornost je třeba věnovat vnitřním dveřím, hovoříme například o vstupu do technické místnosti/kotelny, počítačové učebny, ředitelny nebo kanceláře hospodářky. Tam je namístě instalace zesíleného kování a cylindrických vložek vyšší bezpečnostní třídy, čímž se výrazně sníží riziko neoprávněného vstupu a zároveň dojde ke zvýšení celkové úrovně fyzické bezpečnosti v rámci objektu. [11]

9.3 Organizační a režimové opatření

Pro zvýšení bezpečnosti provozu školy navrhuji zavést cílená organizační a režimová opatření, která zajistí vyšší kontrolu pohybu osob a včasné odhalení podezřelého chování. U vstupu do budovy bude návštěvník povinen vyvolat hovor pomocí interkomu, čímž se zvýší dohled nad vstupujícími osobami. Před vstupem do objektu bude návštěvník jednoznačně identifikován, pomocí nainstalovaných kamerových systémů.

S ohledem na vytíženost vestibulu v ranních hodinách bude u vstupu přítomen kompetentní zaměstnanec školy, který bude dohlížet na režim vstupu a v případě potřeby reagovat na vzniklou situaci. Po tomto časovém okně budou vstupní dveře uzamčeny a přístup do budovy bude umožněn výhradně oprávněným osobám, tzn. buď prostřednictvím identifikační karty, čipu, nebo stávajících klíčů.

Ve frekventovaných časech během dne, zejména při obědových pauzách, bude dohled zajištěn v okolí šaten a chodeb, opět za přítomnosti určeného pracovníka. Pracovníci se mohou v rámci služby střídat, avšak musí být předem poučeni, jak se zachovat případě krizové nebo mimořádné situace. S tímto opatřením doporučuji zřídit bezpečnostní komisi, která bude pravidelně koordinovat bezpečnostní opatření a vyhodnocovat incidenty. Vybrané prostory, jako jsou technické místnosti, půdy, atrium, kotelna či výtah, mohou být nadále přístupné pouze oprávněným osobám. Tyto prostory by měly být zabezpečeny buď čipovým přístupem, nebo fyzickým uzamčením. Výtah by mohl být nadále přístupný pouze pro zaměstnance a žáky se specifickými potřebami.

9.4 Podpora ze strany zřizovatele a místní samosprávy

Vzhledem k charakteru školského zařízení, jakožto měkkého cíle a potřebě posílení jeho úrovně bezpečnosti se nabízí také aktivní zapojení zřizovatele školy do plánovaného procesu zabezpečení. Na základě telefonické komunikace s příslušnými pracovníky zřizovatelského úřadu bylo zjištěno, že daný subjekt je otevřený diskuzi na téma posilování bezpečnosti školských zařízení a ochotný jednat o případných možnostech financování konkrétních bezpečnostních opatření. Podmínkou je však potřeba připravit dokument, tzv. projektový záměr, který by obsahoval analýzu současného stavu, identifikovaná rizika a návrhy konkrétních řešení. Zároveň bylo zjištěno, že zřizovatel je otevřený k debatě zapojení školy do národní iniciativy zaměřené na prevenci a bezpečnost ve školním prostředí. Jedná se například o projekt Bezpečná škola vedený příslušnou odbornou asociací.

Tato forma zapojení by nejen posílila důvěryhodnost předloženého návrhu, ale zároveň by škole umožnila čerpat metodickou podporu, kterou by mohli využívat zaměstnanci školy pro svou edukaci a následné prezentování žákům školy.

Jako další finanční zdroj se nabízí obec s rozšířenou působností, kde škola sídlí. Po konzultaci s představiteli místní samosprávy bylo zjištěno, že i zde jsou otevřeni k debatě na toto téma. V tomto případě je možné uvažovat o spolufinancování bezpečnostních opatření, zejména v případě, že by návrh schválil příslušný orgán samosprávy (např. rada města). Tato možnost by mohla být vhodným doplňkem k podpoře zajištěné zřizovatelem.

Z výše uvedeného vyplývá, že není potřeba aby škola hradila všechny náklady ze svých finančních prostředků, ale může využít této formy spolufinancování. Doporučuji tedy vedení školy iniciovat přípravu souhrnného podkladu, který bude sloužit jako výchozí materiál pro jednání se zřizovatelem i se zástupci místní samosprávy. Dokument by měl obsahovat nejen výsledky bezpečnostní analýzy a návrhy opatření, ale i rámcový rozpočet a návrh harmonogramu realizace.

9.5 Ekonomický rámec návrhů bezpečnostních opatření

S ohledem na navrhovaná bezpečnostní opatření byl vytvořen orientační přehled nákladů, které by mohly být spojeny s jejich realizací. Cílem této části je poskytnout rámcový ekonomický odhad pro rozhodování vedení školy a zřizovatele. Konkrétní částky se mohou lišit v závislosti na dodavatelích, rozsahu realizace či možnostech spolufinancování.

Tabulka 14 - Kalkulace zabezpečení

Opatření	Množství	Jednotková cena (Kč)	Celkem (Kč)
IP kamera AXIS M4216-LV	4	13 000	52 000
Montáž kamerového systému	1	15 000	15 000
UTP kabeláž Cat5e (50 m/kamera)	4	439	1 756
Napájecí kabely a drobné příslušenství	4	300	1 200
Patch panel, zásuvky, koncovky, boxy	1	2 000	2 000

Magnetické zámky s EPS (fail-safe)	3	5 500	16 500
Kabeláž pro EPS	3	685	2 055
RFID přístupový systém	3 vstupy	11 000	33 000
Kabeláž pro čtečky	3	189	567
Montáž a konfigurace přístupového systému	1	8 000	8 000
Bezpečnostní kování RC.3/RC.4 (kliky, koule)	6	1 000	6 000
EKV systém pro výtah (modul, čtečka, montáž, kabeláž)	1	15 000	15 000
Školení zaměstnanců (externí lektor)	2 akce	7 000	14 000
Osvětové programy pro žáky	1 akce	4 000	4 000
Projektová dokumentace a krizový plán	1	8 000	8 000
Rezerva (cca 10 % na nečekané výdaje)	-	-	18 000
Celkem			198 078 (bez DPH)

(zdroj: vlastní)

Návrh vychází z rámcových cen běžně dostupných produktů a služeb na českém trhu. Vzhledem k tomu, že školské zařízení může žádat o finanční podporu ze strany zřizovatele nebo zapojení do dotačních programů (např. Bezpečná škola), není nutné, aby veškeré výdaje byly kryty výhradně z rozpočtu školy.

Při konzultaci s vedením školy bylo dohodnuto, že větší část navrhovaných opatření bude akceptována a jejich implementace bude řešena buď okamžitě, nebo postupně podle aktuálních priorit a finančních možností školy.

Shrnutí kapitoly

Poslední kapitola diplomové práce se zaměřovala na návrhy bezpečnostních opatření, která vycházela z komplexního vyhodnocení rizikových analýz metod CARVER a PNH,

z výsledků experimentu připravenosti zaměstnanců a také z posouzení současného stavu zabezpečení školního objektu.

Hlavním cílem navrhovaných opatření je především posílit celkovou úroveň bezpečnosti školského zařízení v souladu s principy ochrany měkkých cílů, jak je doporučuje Ministerstvo vnitra ČR. Základním stavebním kamenem těchto opatření je prevence a systematická práce s riziky. Kapitola kladla důraz nejen na zavádění nových technologií, ale také na osvětu, školení a pravidelnou edukaci všech osob, které se ve škole pohybují. Prevence prostřednictvím vzdělávání je v tomto případě zásadní, jedná se o finančně nenáročný a dlouhodobě nejúčinnější nástroj k předcházení krizovým situacím.

Mezi navrhovaná technická opatření patří rozšíření systému elektronické požární signalizace (EPS) o tlačítkové hlásiče a magnetické zámky na únikových východech, instalace kamerového systému s analytickými funkcemi a zavedení přístupového systému na bázi RFID technologie. Kapitola rovněž reflektovala potřebu posílit mechanické zabezpečení. Důležitou součástí návrhů jsou organizační a režimová opatření jako je dohled nad vstupem v ranních hodinách, rotace dozorujících zaměstnanců během dne a zřízení bezpečnostní komise školy.

V závěru kapitoly byl představen ekonomický rámec návrhů, který potvrzuje, že bezpečnost lze zvyšovat efektivně, a to i s ohledem na finanční možnosti školy. Opatření byla konzultována s vedením školy, které projevilo zájem o jejich realizaci. V úplném závěru byla navržena také doporučení na zapojení zřizovatele školy a místní samosprávy v metodické a finanční rovině.

10 ZÁVĚR PRAKTICKÉ ČÁSTI

Závěr praktické části diplomové práce shrnuje klíčové poznatky vyplývající z komplexního bezpečnostního posouzení vybraného školského zařízení, které bylo podrobeno důkladné analýze z hlediska fyzického zabezpečení, připravenosti zaměstnanců, efektivity nastavených režimových a organizačních opatření.

Pátá kapitola poskytla obecnou charakteristiku školského zařízení, včetně popisu jeho vzdělávacího zaměření, specifik práce s žáky se speciálními potřebami a dispozičního uspořádání objektu. V jejím rámci byla provedena úvodní identifikace aktiv a potenciálních hrozeb, které se staly základem pro aplikaci analytických metod v následujících částech.

Šestá kapitola se věnovala podrobné analýze rizik, která proběhla aplikací metod CARVER a PNH. Výsledky těchto nástrojů potvrdily, že mezi nejrizikovější prvky patří hlavní vstup do budovy a přítomnost žáků se specifickými potřebami. Dále byly identifikovány další slabiny, zejména v oblasti fyzické ochrany, informační bezpečnosti a režimových opatření. Provedený experiment navíc prokázal nízkou připravenost personálu čelit mimořádným situacím a nedostatečnou schopnost rozpoznat podezřelé chování ve školním prostředí.

Sedmá kapitola podrobně popsala aktuální stav zabezpečení objektu. Zjištěné poznatky poukázaly na řadu zásadních nedostatků, např. nevyhovující oplocení, absenci kontrolovaného vstupu, špatně zabezpečené technické prostory nebo nedostatečnou kontrolu nad pohybem osob po budově. Zvláštní pozornost byla věnována prostorám Speciálně pedagogického centra, kde chybí dostatečný režim vstupu návštěv, což s sebou přináší další rizika.

Poslední kapitola, tedy osmá, představila návrh bezpečnostních opatření členěných do několika tematických oblastí. Opatření zahrnují návrhy připravenosti a vzdělávání, posílení fyzické bezpečnosti, implementaci režimových a organizačních prvků. Hlavním přínosem těchto opatření je jejich provázanost, realistická proveditelnost a důraz na dlouhodobou udržitelnost. Zvláště důležité je preventivní působení a systematické vzdělávání všech aktérů školního provozu, včetně aktivního zapojení vedení školy, zřizovatele i místní samosprávy.

Závěrem lze konstatovat, že praktická část diplomové práce poskytla ucelený, na důkazech založený pohled aktuálního stavu bezpečnosti vybraného školského zařízení a nabídla konkrétní, realizovatelná a v praxi využitelná doporučení pro její posílení.

Výsledky ukazují, že i relativně jednoduchými a cílenými kroky lze výrazně zvýšit úroveň bezpečnosti a připravenosti školy na mimořádné události.

ZÁVĚR

Diplomová práce se zabývá problematikou zajištění bezpečnosti ve školském prostředí, konkrétně v základní škole speciální, která představuje mimořádně zranitelný měkký cíl. Vzhledem ke zvýšeným požadavkům na ochranu osob a prevenci bezpečnostních incidentů ve školách byl hlavním cílem práce analyzovat aktuální stav fyzického zabezpečení vybraného objektu, identifikovat klíčová aktiva a možné hrozby a na základě zjištěných skutečností navrhnout konkrétní opatření ke zvýšení úrovně ochrany.

V teoretické části byl vymezen právní a metodický rámec problematiky, popsány principy fyzické bezpečnosti a podrobně rozpracovány dvě metody řízení rizik, které byly následně aplikovány v praktické části. Ta se zaměřila na analýzu vybraného školního zařízení, které bylo z důvodu ochrany citlivých informací anonymizováno.

Na základě této analýzy byly určeny konkrétní rizikové oblasti, které mohou ohrozit bezpečný provoz školy. Jedním z dalších důležitých výstupů práce bylo experimentální ověření připravenosti zaměstnanců školy na modelovou krizovou situaci. Tento experiment přinesl cenné poznatky o skutečném stavu zvládání mimořádných událostí, upozornil na slabá místa v oblasti režimových opatření a zároveň potvrdil zásadní roli lidského faktoru v bezpečnostním systému školského zařízení. Výsledky jasně ukázaly, že i přes snahu o bezpečný provoz mohou být některé postupy formální nebo nedostatečně řešené, což v krizové situaci výrazně snižuje efektivitu reakce.

Na základě všech zjištění byl vypracován návrh konkrétních bezpečnostních opatření, který reaguje na konkrétní rizika identifikovaná pomocí metod CARVER a PNH, na výsledky experimentálního ověření připravenosti zaměstnanců školy a na zjištění vyplývající z aktuálního stavu zabezpečení objektu. Návrh zahrnuje jak technická a organizační opatření, tak doporučení v oblasti školení zaměstnanců a krizové připravenosti. Výsledkem těchto návrhů je nejen zvýšení bezpečnosti žáků a zaměstnanců, ale i celkové posílení důvěry v instituci jako stabilní a připravené místo pro výchovu a vzdělávání.

Celý návrh je doplněn orientačním ekonomickým rámcem, který umožňuje vedení školy lépe plánovat případné investice a rozhodovat o prioritách v oblasti zabezpečení. Přínosem práce je nejen samotný návrh opatření, ale také metodický přístup, který lze aplikovat i na jiná školská zařízení podobného typu, a který může sloužit jako východisko pro systematictější práci s riziky ve školním prostředí.

SEZNAM POUŽITÉ LITERATURY

- [1] ČESKO. Ústava České republiky. Ústavní zákon č. 1/1993 Sb., ve znění pozdějších předpisů [online]. Dostupné z: <https://www.psp.cz/docs/laws/constitution.html> [cit. 2025-01-10].
- [2] CONEVITEOSKOLE.CZ. Důležité paragrafy pro školu. [online] Dostupné z: <https://www.coneviteoskole.cz/dulezite-paragrafy/> [cit. 2025-01-10].
- [3] MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY. Bezpečnost na školách. Praha: MŠMT, 2025. [online] Dostupné z: <https://edu.gov.cz/wp-content/uploads/2025/01/Bezpecnost-na-skolach.pdf> [cit. 2025-01-10].
- [4] DOKUMENTACEBOZP.CZ. Povinnosti školy – požární ochrana. [online]. Dostupné z: <https://www.dokumentacebozp.cz/aktuality/povinnosti-skoly-pozarni-ochrana/> [cit. 2025-01-18].
- [5] ČESKO. Zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů [online]. Zákony pro lidi. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-239> [cit. 2025-01-18].
- [6] ČESKO. Vyhláška č. 23/2008 Sb., o technických podmínkách požární ochrany staveb [online]. Ministerstvo školství, mládeže a tělovýchovy. Dostupné z: <https://msmt.gov.cz/dokumenty/vyhlasaka-c-23-2008-sb-o-technickych-podminkach-pozarni> [cit. 2025-01-18].
- [7] ČESKO. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků [online]. Zákony pro lidi. Dostupné z: <https://www.zakonyprolidi.cz/cs/2005-528> [cit. 2025-01-18].
- [8] ČESKO. Vyhláška č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci), ve znění účinném k 1. 1. 2022 [online]. Zákony pro lidi. Dostupné z: <https://www.zakonyprolidi.cz/cs/2001-246/zneni-20220101> [cit. 2025-02-05].
- [9] SLADKÝ, Libor; BREČKA, Tibor A. a kol. Manuál bezpečné školy: Bezpečná škola a školské zařízení v kontextu ČSN 73 4400. Praha: Asociace bezpečná škola z.s., 2022. ISBN 978-80-908515-2-8.

- [10] BHP.cz. Řízení rizik podle nové normy ČSN ISO 31000:2018 [online]. BHP.cz, 2018. Dostupné z: <https://www.bhp.cz/clanky/8534/rizeni-rizik-podle-nove-normy-csn-iso-31000-2018> [cit. 2025-02-05].
- [11] IVANKA, Ján. Mechanické zábranné systémy. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 978-80-7318-910-5.
- [12] TECHNICKE-NORMY-CSN.CZ. Technické normy ČSN. [online]. Dostupné z: <https://www.technicke-normy-csn.cz/technicke-normy-csn/#> [cit. 2025-02-05].
- [13] LOVEČEK, Tomáš; VELAS, Andrej a ĎUROVEC, Martin. Bezpečnostné systémy: poplachové systémy. Vysokoškolské učebnice. V Žiline: Žilinská univerzita, EDIS-vydavateľské centrum ŽU, 2015. ISBN 978-80-554-1144-6.
- [14] Metodické doporučení v oblasti bezpečnosti a ochrany škol a školských zařízení jako měkkých cílů. 2. doplněné vydání, březen 2021. Zpracoval kolektiv autorů PMVIA s.r.o. pod vedením Ing. Petra Šramatého [online]. Dostupné z: https://www.prahaskolska.eu/wp-content/uploads/2024/01/Metodika_pro_skoly_ochrana_mekkych_cilu.pdf [cit. 2025-02-15].
- [15] Minimální standard bezpečnosti v regionálním školství: metodické doporučení [online]. Ministerstvo školství, mládeže a tělovýchovy, 2024. Dostupné z: <https://edu.gov.cz/methodology/minimalni-standard-bezpecnosti-v-regionalnim-skolstvi-metodicke-doporuceni/> [cit. 2025-02-15].
- [16] Škola a neštěstí: Jsme připraveni! Metodické doporučení pro školy a školská zařízení [online]. Ministerstvo školství, mládeže a tělovýchovy, 2024. Dostupné z: <https://edu.gov.cz/metodicke-doporuceni-pro-skoly-a-skolska-zarizeni-skola-a-nestesti-jsme-pripraveni/> [cit. 2025-02-15].
- [17] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Odbor bezpečnostní politiky a prevence kriminality. Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu [online]. Praha, 2016. Dostupné z: <https://mv.gov.cz/soubor/terminologicky-slovník-mv-verze-ke-stazeni.aspx> [cit. 2025-02-22].

- [18] MINISTERSTVO VNITRA ČR. Ochrana měkkých cílů [online]. Dostupné z: <https://mv.gov.cz/clanek/ochrana-mekkych-cilu.aspx> [cit. 2025-02-22].
- [19] KARAFFA, Vladimír; HRINKO, Martin a ZŮNA, Jaromír. Vybrané kapitoly o bezpečnosti. Praha: CEVRO Institut (vysoká škola), 2022. ISBN 978-80-87125-35-9.
- [20] HASIČSKÝ ZÁCHRANNÝ SBOR ČESKÉ REPUBLIKY. Roční zpráva o činnosti HZS ČR 2008 [online]. Dostupné z: <https://www.hzscr.cz/soubor/rocnizprava-o-cinnosti-hzs-cr-08-final-pdf.aspx> [cit. 2025-03-01].
- [21] PAULUS, František, Antonín KRÖMER, Jan PETR, Jaroslav ČERNÝ. Analýza hrozeb pro Českou republiku: závěrečná zpráva [online]. Hasičský záchranný sbor České republiky, Praha, 2015. Dostupné z: <https://www.hzscr.cz/soubor/analyza-hrozeb-zprava-pdf.aspx> [cit. 2025-03-01].
- [22] ZEMAN, Petr, ed. Česká bezpečnostní terminologie: výklad základních pojmů. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002. ISBN 80-210-3037-2.
- [23] MINISTERSTVO VNITRA ČR. Základy ochrany měkkých cílů: metodika. Praha: Ministerstvo vnitra, 2016. [online]. Dostupné z: <https://mv.gov.cz/chh/soubor/terorismus-web-dokumenty-metodika-zaklady-ochrany-mekkych-cilu-pdf.aspx> [cit. 2025-03-01].
- [24] ŘEHÁK, David; MARTÍNEK, Bohumír a LEGIERSKÁ, Petra. Ochrana obyvatelstva v kontextu aktuálních bezpečnostních hrozeb. 2. rozšířené vydání. SPBI Spektrum. Červená řada. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2019. ISBN 978-80-7385-220-7.
- [25] KINGSLEY-HEFTY, John. Physical Security Strategy and Process: A Guide for Corporate and Government Security Professionals. 1st ed. Amsterdam: Elsevier, 2013. ISBN 978-0-12-417237-1.
- [26] Technické normy ČSN. ČSN ISO 31000 (010351) Management rizik - Principy a směrnice [online]. Česká Agentura pro Standardizaci, 2010. Dostupné z: <https://www.technicke-normy-csn.cz/csn-iso-31000-010351-158308.html> [cit. 2025-03-05].

- [27] POPOV, Georgi; LYON, Bruce K. a HOLLCROFT, Bruce. Risk assessment: a practical guide to assessing operational risks. Second edition. Hoboken, New Jersey: Wiley, [2022]. ISBN 978-1-119-75594-4.
- [28] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management II. Zlín: VeRBuM, 2012. ISBN 978-80-87500-19-4.
- [29] KORECKÝ, Michal a TRKOVSKÝ, Václav. Management rizik projektů: se zaměřením na projekty v průmyslových podnicích. Expert. Praha: Grada, 2011. ISBN 978-80-247-3221-3.
- [30] SMEJKAL, Vladimír a RAIS, Karel. Řízení rizik ve firmách a jiných organizacích. 4., aktualizované a rozšířené vydání. Praha: Grada, 2013. 488 s. Expert. ISBN 978-80-247-4644-9
- [31] BAKER, Paul R. a Daniel J. BENNY. The Complete Guide to Physical Security. Boca Raton: CRC Press, Taylor & Francis Group, 2013. ISBN 978-1-4200-9963-8
- [32] PŮČEK, Milan Jan a PÁLENÍKOVÁ, Markéta. Řízení rizik a využívání příležitostí jako nástroj pro zlepšení řízení a kontroly veřejných financí [online]. Brno: Masarykova univerzita, Ekonomicko-správní fakulta, 2022. Projekt pro Ministerstvo financí ČR. Dostupné z: https://www.mfcr.cz/assets/attachments/2022-09-27_Priloha-c-2-k-Analyze-vnitrnich-kontrolnich-systemu-Rizeni-rizik-a-prilezitosti.pdf [cit. 2025-03-12].
- [33] Risk Management in Engineering Projects. [online]. Istanbul: Yildiz Technical University, [s. a.]. Dostupné z: <https://sigma.yildiz.edu.tr/storage/upload/pdfs/1635947323-en.pdf> [cit. 2025-03-12].
- [34] UNITED STATES DEPARTMENT OF AGRICULTURE. 2015 Food and Agriculture Sector-Specific Plan. [online]. Washington, D.C.: USDA, 2015. Dostupné z: <https://www.usda.gov/sites/default/files/documents/2015-food-and-agriculture-sector-specific-plan.pdf> [cit. 2025-03-12].
- [35] NEŠPOROVÁ, Veronika a TAŠLOVÁ, Jana. Bezpečnost zdravotnické kritické infrastruktury. 2015. [online]. Dostupné

- z: https://www.researchgate.net/publication/282871953_Bezpečnost_zdravotnicke_kriticke_infrastruktury [cit. 2025-03-15].
- [36] SLIVKOVÁ, Silvia. Východiska hodnocení kritických prvků železniční dopravní infrastruktury. 2017. [online]. Dostupné z: https://www.researchgate.net/publication/321174256_Vychodiska_hodnoceni_kritickykh_prvku_zeleznicni_dopravni_infrastruktury [cit. 2025-03-15].
- [37] HAUGEN, Stein a RAUSAND, Marvin. Risk Assessment: 9. Preliminary hazard analysis. Trondheim: Norwegian University of Science and Technology, Department of Production and Quality Engineering, 2021. [online]. Dostupné z: <https://www.ntnu.edu/documents/624876/1277591044/chapt09-pha.pdf> [cit. 2025-03-15].
- [38] Univerzita Tomáše Bati ve Zlíně. Bezpečnostní politika UTB. [online]. Zlín: Univerzita Tomáše Bati ve Zlíně, [s. a.]. Dostupné z: <https://www.utb.cz/univerzita/o-univerzite/struktura/poradni-sbory/vybor-pro-řízení-kyberneticke-bezpecnosti/vydane-politiky/> [cit. 2025-03-22].
- [39] MASLOW, Abraham Harold. O psychologii bytí. Přeložil Hana ANTONÍNOVÁ. Praha: Portál (vydavatelství), 2014. ISBN 978-80-262-0618-7.
- [40] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management III. Zlín: Radim Bačuvčík - VeRBuM, 2013. ISBN 978-80-87500-35-4.
- [41] MADDOX, Maeve. Safety and Security. In: DAILYWRITINGTIPS [online]. London: Daily Writing Tips, 2010. Dostupné z: <https://www.dailywritingtips.com/safety-and-security/> [cit. 2025-03-22].
- [42] ŠČUREK, R. a JARKULIŠ, V. Metodologie fyzické bezpečnosti podniku. 1. vyd. Ostrava: VŠB – Technická univerzita Ostrava, 2023. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/Metodologie_fyzicke_bezpecnosti_podniku.pdf [cit. 2025-03-22].
- [43] LUKÁŠ, Luděk a kol. Bezpečnostní technologie, systémy, management I. Zlín: Radim Bačuvčík – VeRBuM, 2011. ISBN 978-80-87500-05-7.
- [44] Apeltauer, T., Dufek, Z., Vangeli, B., Rosenkranz, J., Hromada, M., Mrázková, L., Lapková, D., Kotek, L., Ljubymenko, K. Ochrana měkkých cílů. Praha: Leges, 2019. 171 s. ISBN 978-80-7502-427-5

- [45] EASYFLOW TECH. The Use Of AI In Physical Security [online].[2024]. Dostupné z: <https://easyflow.tech/ai-in-physical-security/> [cit. 2025-03-22].
- [46] PELCO. Future of Security Technology: Industry Trends of 2025 [online].[2024]. Dostupné z: <https://www.pelco.com/blog/security-technology-trends> [cit. 2025-03-22].
- [47] PREVENCEKRIMINALITY.CZ. Kriminalita klesá: Ukazuje vývoj registrované trestné činnosti v roce 2024 – Prevence hraje klíčovou roli v pozitivním vývoji kyberkriminality [online]. 2024. Dostupné z: <https://prevencekriminality.cz/kriminalita-klesa-ukazuje-vyvoj-registrovane-trestne-cinnosti-v-roce-2024-prevence-hraje-klicovou-roli-v-pozitivnim-vyvoji-kyberkriminality/> [cit. 2025-03-22].
- [48] GARDAWORLD. 8 Top Physical Security Trends to Watch in 2025 [online]. 2025. Dostupné z: <https://www.garda.com/articles/8-top-physical-security-trends-to-watch-in-2025> [cit. 2025-03-22].
- [49] WINDWALKER GROUP. The Future of Physical Security in 2025 [online]. 2025-01-30. Dostupné z: <https://www.windwalker.com/newsandinsights/2025/1/30/the-future-of-physical-security-in-2025> [cit. 2025-03-22].
- [50] AXIS COMMUNICATIONS. AXIS M4216-LV. [online]. Dostupné z: <https://www.axis.com/products/axis-m4216-lv> [cit. 2025-03-26].
- [51] AXIS COMMUNICATIONS. AXIS Object Analytics [online]. 2024. Dostupné z: <https://www.axis.com/products/axis-object-analytics> [cit. 2025-03-26].
- [52] EVALINK. The Future of Access Control, Biometrics and the Evolution of AI Security [online]. 2024. Dostupné z: <https://www.evalink.io/blog/the-future-of-access-control-biometrics-and-the-evolution-of-ai-security> [cit. 2025-03-26].
- [53] ALCATRAZ AI. The Rock [online]. 2024. Dostupné z: <https://alcatraz.ai/the-rock> [cit. 2025-03-26].
- [54] KELCOM International spol. s r.o. Elektrická požární signalizace [online]. Pardubice: KELCOM International. Dostupné z: <https://www.kelcomint.cz/elektricka-pozarni-signalizace> [cit. 2025-03-28].

- [55] HOŠEK, Zdeněk. Aktuální evropské trendy v oblasti požárně bezpečnostních zařízení [online]. Praha: TZB-info, 20. 11. 2017. Dostupné z: <https://www.tzb-info.cz/pozarni-bezpecnost-staveb/16573-aktualni-evropske-trendy-v-oblasti-pozarne-bezpecnostnich-zarizeni> [cit. 2025-03-28].
- [56] Nevrkla, J., Lapková, D., Jenčková, K., Šternová, T., Rožek, D., Mrázková, L., Kotek, L. Měkké cíle: Identifikace, ohroženost a jejich ochrana. Praha, 2019. ISBN 978-80-270-7066-4.
- [57] MINISTERSTVO VNITRA ČR. Koncepce ochrany měkkých cílů pro roky 2017–2020. [online]. Praha: Ministerstvo vnitra, 2017. 32 s. Dostupné z: <https://mv.gov.cz/soubor/koncepce-ochrany-mekkych-cilu-pro-2017-2020-pdf.aspx> [cit. 2025-04-01].
- [58] KALVACH, Zdeněk a Benedikt VANGELI. Vyhodnocení ohroženosti měkkého cíle: metodika. [online]. Praha: Ministerstvo vnitra České republiky, 2018. 38 s. Dostupné z: <https://mv.gov.cz/chh/clanek/vyhodnoceni-ohrozenosti-mekkeho-cile-metodika-ke-stazeni.aspx> [cit. 2025-04-01].
- [59] MINISTERSTVO VNITRA ČR. Bezpečnostní plán měkkého cíle: co by nemělo být opomenuto při jeho zpracování. [online]. Praha: Ministerstvo vnitra České republiky, 2019. 20 s. Dostupné z: <https://www.mvcr.cz/cthh/clanek/terorismus-web-dokumenty-dokumenty.aspx> [cit. 2025-04-01].
- [60] MINISTERSTVO VNITRA ČR. Bezpečnostní standard k ochraně jednoho z měkkých cílů. [online]. Praha: Ministerstvo vnitra ČR, 2016. Dostupné z: <https://mv.gov.cz/clanek/bezpecnostni-standard-k-ochrane-jednoho-z-mekkych-cilu.aspx> [cit. 2025-04-01].
- [61] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. 10 principů zodolnění měkkého cíle [online]. Praha: Centrum proti terorismu a hybridním hrozbám, 2019. Dostupné z: <https://www.mvcr.cz/cthh/clanek/10-principu-zodolneni-mekkeho-cile.aspx>. [cit. 2025-04-01].
- [62] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ. ČSN 73 4400: Prevence kriminality – Řízení bezpečnosti při plánování, realizaci a užívání škol a školských zařízení. Praha: Český normalizační institut, 2016.

- [63] Ministerstvo školství, mládeže a tělovýchovy ČR. Metodické doporučení pro školy a školská zařízení – Škola a neštěstí: Jsme připraveni!. [online]. Praha: MŠMT ve spolupráci s MV–GR HZS, 2023. Dostupné z: https://www.edu.cz/wp-content/uploads/2023/07/Metodika_Skola_a_nestesti_Jsme_pripraveni_2023.pdf [cit. 2025-04-04].
- [64] MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY. Rámcový vzdělávací program pro obor vzdělání – základní škola. [online]. Dostupné z: <https://msmt.gov.cz/vzdelavani/ramcovy-vzdelavaci-program-pro-obor-vzdelani-zakladni-skola> [cit. 2025-04-04].
- [65] MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY. Předměty speciálně pedagogické péče – RVP ZŠS (2010), kapitola 2 a 3. [online]. Dostupné z: <https://www.msmt.cz/vzdelavani/predmety-specialne-pedagogicke-pecerVP> [cit. 2025-04-04].
- [66] NÁRODNÍ PEDAGOGICKÝ INSTITUT ČR. Základní školy speciální – archiv NÚV. [online]. Dostupné z: <https://archiv-nuv.npi.cz/t/zakladni-skoly-specialni.html> [cit. 2025-04-04].
- [67] ČESKO. Zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon). [online]. In: *Zákony pro lidi*. Dostupné z: <https://www.zakonyprolidi.cz/cs/2004-561> [cit. 2024-04-04].
- [68] Seznam.cz. Mapy.cz: satelitní mapa [online]. Praha: Seznam.cz. Dostupné z: <https://mapy.cz> [cit. 2025-04-04].
- [69] UNITED STATES ARMY. Field Manual FM 34-36: Appendix D – Intelligence and Electronic Warfare Operations. [online]. Dostupné z: <https://irp.fas.org/doddir/army/fm34-36/appd.htm> [cit. 2025-01-26].
- [70] ZŠ HUDCOVA. Krizový plán školy. [online]. Dostupné z: <https://www.zshudcova.cz/wp-content/uploads/2022/01/Krizovy-plan-skoly.pdf> [cit. 2025-04-07].
- [71] KYNCL, Jaromír. Bezpečnost objektu ve světle moderních technologií. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.

- [72] POLICIE ČESKÉ REPUBLIKY. Uteč, schovej se, boj. [online]. Dostupné z: <https://policie.gov.cz/clanek/utikej-schovej-se-boj.aspx> [cit. 2025-05-10].
- [73] POŽÁRY.CZ. Učitelé vysvětlují žákům, jak se mají chovat při mimořádných situacích. [online]. Dostupné z: <https://www.pozary.cz/clanek/46-ucitele-vysvetlujizakum-jak-se-maji-chovat-pri-mimoradnych-situacich/> [cit. 2025-05-10].
- [74] ABBAS.CZ. Dominus3 podporuje nejbezpečnější přístupové karty MIFARE DESFire. [online]. Dostupné z: <https://www.abbas.cz/clanky/aktuality/dominus3-podporuje-nejbezpecnejsi-pristupove-karty-mifare-desfire/> [cit. 2024-05-10].

SEZNAM OBRÁZKŮ

Obrázek 1 Proces řízení rizik	27
Obrázek 2 Schéma vztahů v řízení rizik	30
Obrázek 3 Maslowova pyramida potřeb	38
Obrázek 4 Schéma zabezpečení	44
Obrázek 5 Multisenzorový detektor	45
Obrázek 6 Mobilní aplikace pro správu EPS	45
Obrázek 7 Letecký snímek školy	63
Obrázek 8 Nevyhovující stav plotu na hranici s autoservisem	85
Obrázek 9 Plot oddělující prostranství školy a městský pozemek	86
Obrázek 10 Evakuační plán objektu – přízemí	88
Obrázek 11 Hlavní dveře ve vstupním vestibulu	89
Obrázek 12 Interkom u hlavních dveří ve vestibulu	89
Obrázek 13 Informace na hlavních dveřích	90
Obrázek 14 Úschova klíčů od únikového východu	91
Obrázek 15 Úschova klíčů od výše uvedených dveří	92
Obrázek 16 Vstup do výtahu v atriu	93
Obrázek 17 Dveře mezi atriem a kotelnou	94
Obrázek 18 Pohled při vstupu do kotelny	95
Obrázek 19 Pohled při vstupu do kotelny II.	96
Obrázek 20 Technická dílna školníka	96
Obrázek 21 Technická dílna školníka – východ	97
Obrázek 22 - Technická dílna školníka – pohled z východu na autoservis	97
Obrázek 23 - Technická dílna školníka – pohled na dveře z venku	98
Obrázek 24 Evakuační plán objektu - 1. poschodí	99
Obrázek 25 Evakuační plán objektu - 2. poschodí	100
Obrázek 26 Tlačítkový hlásič	107
Obrázek 27 Plán rozmístění kamer AXIS	109
Obrázek 28 Použité kamery v návrhu	109

SEZNAM TABULEK

Tabulka 1 Identifikovaná aktiva	64
Tabulka 2 Identifikované hrozby	65
Tabulka 3 Kritérium kritičnosti	67
Tabulka 4 Kritérium přístupnosti.....	68
Tabulka 5 - Kritérium obnovitelnosti	68
Tabulka 6 Kritérium vliv na chod instituce	69
Tabulka 7 Kritérium rozpoznatelnosti	70
Tabulka 8 Aplikace metody CARVER.....	70
Tabulka 9 Hodnotící tabulka CARVER	71
Tabulka 10 - Pravděpodobnost vzniku nebezpečí	74
Tabulka 11 Závažnost následků.....	74
Tabulka 12 Názor hodnotitele.....	74
Tabulka 13 - Kalkulace zabezpečení	112
Tabulka 14 Aplikace metody PNH.....	133
Tabulka 15 Hodnotící tabulka PNH.....	137

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI	Artificial Intelligence - umělá inteligence
BCM	Business Continuity Management – řízení kontinuity činností
BMS	Building Management System – systém řízení budovy
CARVER	Metoda analýzy rizik
CCTV	Closed-Circuit Television – kamerový systém
ČSN	Česká technická norma
ČSN 73 4400	Norma pro prevenci kriminality ve školách
ČSN EN	Evropská norma přejatá jako ČSN
ČSN EN 1300	Norma pro bezpečnostní zámky
ČSN EN 1627	Norma pro odolnost proti vloupání
ČSN EN 50131	Norma pro poplachové systémy
ČSN EN 50134	Norma pro systémy přivolání pomoci
ČSN EN 62676	Norma pro dohledové kamerové systémy
ČSN ISO 31000	Mezinárodní norma pro řízení rizik
DES / 3DES / AES128	Šifrovací algoritmy
EPS	Elektronický požární systém
ETA	Event Tree Analysis – analýza stromu událostí
EV2 / EV3	Verze bezpečnostních čipových technologií
FMEA	Failure Mode and Effects Analysis
GDPR	General Data Protection Regulation – ochrana osobních údajů
HAZOP	Hazard and Operability Study
HZS	Hasičský záchranný sbor
IK08	Odolnost proti vandalismu
IP42	Krytí proti pevným částicím a vodě
IZS	Integrovaný záchranný systém

MIFARE DESFire	Technologie bezkontaktních karet s šifrováním
ML	Machine Learning – strojové učení
MŠMT	Ministerstvo školství, mládeže a tělovýchovy ČR
MV ČR	Ministerstvo vnitra České republiky
MV-GR HZS ČR	Generální ředitelství Hasičského záchranného sboru MV ČR
např.	Například
NBU	Národní bezpečnostní úřad
PC	Personal Computer – osobní počítač
PČR	Policie České republiky
PIR detektor	Passive Infrared – detektor pohybu
PNH	Preliminary Hazard Analysis – předběžná analýza nebezpečí
PoE	Power over Ethernet – napájení přes Ethernet
PZTS	Poplachový zabezpečovací a tísňový systém
RC.3 / RC.4	Bezpečnostní třídy dle normy EN 1627
RFID	Radio-Frequency Identification – bezdrátová identifikace
SPC	Speciální pedagogické centrum
TNK	Technická normalizační komise
tzn.	To znamená
tzv.	Takzvaně
VSS	Video Surveillance System
WDR	Wide Dynamic Range – zlepšení kontrastu obrazu

SEZNAM PŘÍLOH

Příloha P I: Aplikace metody PNH

PŘÍLOHA P I: APLIKACE METODY PNH

Tabulka 15 Aplikace metody PNH

	Identifikované nebezpečí	Možné následky	Možné opatření	P	N	H	R
1.	Neoprávněný vstup cizí osoby bočním vchodem (např. přes areál autoservisu)	Vniknutí cizí osoby, možnost ohrožení žáků a zaměstnanců, krádež majetku školy.	Uzamčení bočních vchodů či CCTV.	4	5	3	60
2.	Neoprávněný vstup nepovolané osoby hlavním vchodem školy	Neoprávněný přístup do školy, ohrožení žáků, narušení pocitu bezpečí ve škole a v okolí.	Kontrolovaný vstup přes hlavní vchod, registrace návštěv.	5	5	3	75
3.	Útěk žáka z budovy přes hlavní vchod do veřejného prostoru (ulice)	Ztráta kontroly nad pohybem žáka, možnost zranění nebo únosu, právní odpovědnost školy.	Instalace automatické nebo elektronického uzamykání dveří, dohled nad vstupy	3	4	3	36
4.	Útěk žáka zadním východem směrem k řece nebo na volné prostranství za školou	Ztráta kontroly nad pohybem žáka, riziko utonutí, vážné zranění, reputace školy.	Uzamčení bočních vchodů či CCTV.	3	3	3	27
5.	Útěk žáka přes technické zázemí školy (např. dílna školníka)	Úraz žáka v technické části školy, ohrožení zdraví, právní postih školy.	Uzamčení technických místností, kontrola pohybu žáků. Omezení přístupu do provozních částí školy čipy nebo instalace automatické nebo elektronického uzamykání dveří.	3	3	3	27
6.	Ztráta nebo krádež klíčů od únikových východů nebo zabezpečených prostor	Zneužití ztracených klíčů, znemožnění evakuace, usnadnění vstupu pachatele.	Odstranit volně dostupné klíče, systém čipů s monitorováním vstupů nebo instalace automatické nebo elektronického uzamykání dveří	4	4	4	64
7.	Krádež školního vybavení cizí osobou během	Krádež cenného vybavení školy, finanční škody, narušení provozu	Kontrolovaný vstup přes hlavní vchod, registrace návštěv, interkom či CCTV.	3	3	4	36

	přítomnosti ve škole	školy, následné vyšetřování.					
8.	Krádež školního vybavení nebo pomůcek samotným žákem	Materiální ztráty, poškození školního majetku, ztráta důvěry k žákům, vyšetřování.	Evidence školního majetku, uzamčení učeben mimo výuku, osvěta žákům, pravidelné inventury školního majetku.	3	2	4	24
9.	Vypnutí hlavního jističe (pojistek) žákem nebo nepovolanou osobou	Výpadek elektřiny, zastavení výuky, riziko poruch technických zařízení.	Zajištění elektroinstalace, zamykání rozvaděčů, instalace alarmu při neoprávněné manipulaci.	3	2	2	12
10.	Neoprávněný přístup do školní počítačové sítě a zcizení dat (digitální incident)	Ztráta nebo únik citlivých dat žáků, právní a finanční postihy pro školu.	Školení zaměstnanců v oblasti kybernetické bezpečnosti, omezení přístupu k síťovým zařízením, firewall.	3	4	5	60
11.	Ztráta citlivých digitálních dokumentů o žácích (např. dokumentace z SPC)	Narušení soukromí žáků, riziko vydírání, možné soudní spory, poškození pověsti školy.	Pravidelné zálohování a šifrování dokumentů, omezení fyzického přístupu k osobním údajům.	2	5	5	50
12.	Požár způsobený neopatrností (např. v dílně)	Vypuknutí požáru, evakuace školy, ohrožení zdraví a životů osob.	Zvýšení počtu EPS detektorů, pravidelná cvičení evakuace-požární bezpečnosti.	3	4	2	24
13.	Vstup cizí osoby do školy v doprovodu jiného žáka či zaměstnance (zneužití důvěry)	Neoprávněný vstup do školy, ohrožení žáků a zaměstnanců a také majetku.	Kontrolovaný vstup přes hlavní vchod, registrace návštěv, interkom či CCTV.	4	5	5	100
14.	Únik informací z emailové komunikace školy (např. narušení GDPR)	Únik osobních dat rodičů a žáků, právní a finanční postihy pro školu.	Zabezpečená emailová komunikace, školení GDPR, pravidelné audity bezpečnosti informací.	3	4	4	48

15.	Vznik konfliktu mezi žáky vedoucího k fyzickému napadení	Fyzická i psychická újma žáků, zvýšené napětí mezi žáky, zásah školního managementu, vyšetřování.	Přítomnost dozoru v rizikových lokalitách školy, osvěta žáku, plán pro řešení podobných situací.	2	4	2	16
16.	Sociálně patologické chování žáků na sociálních sítích	Psychická újma žáků, kyberšikana, pokles pocitu bezpečí ve škole.	Program prevence kyberšikany pro žáky – osvěta, konzultace s rodiči o chování žáka (případná medikace, návštěva SPC).	4	3	2	24
17.	(Ne)úmyslné uzavření prostoru s žákem nebo osobou se zdravotním omezením	Ohrožení zdraví žáka, stresová situace, právní a finanční důsledky pro školu.	Pravidelné kontroly uzavřených prostor, navýšit počet PIR detektorů.	3	4	4	48
18.	Vniknutí cizí osoby pod smyšlenou legendou	Vniknutí neprověřené osoby, ohrožení žáků, personálu a majetku školy.	Zavedení povinných průkazů návštěv.	5	5	4	100
19.	Přítomnost agresivního zákonného zástupce	Verbální a fyzické napadení personálu, přerušení výuky psychická újma žáku i učitelů.	Simulace evakuace školy a její vyhodnocení. Zavedení tísňového tlačítka na IZS.	3	4	2	24
20.	Selhání evakuačního postupu během cvičení nebo skutečné události	Špatná evakuace, chaos, zvýšené riziko zranění žáků i zaměstnanců. Napáchání více škody než užítku.	Zkouška evakuace min. 2x do roka, osvěta a edukace studentů a zaměstnanců školy.	5	4	1	20
21.	Vstup ozbrojené osoby do školy s úmyslem ublížit (aktivní útočník)	Masový útok, úmrtí nebo vážná zranění, masivní mediální dopad.	Bezpečnostní školení o aktivním útočnickovi, nácvik krizového plánu při napadení útočníkem.	3	5	2	30
22.	Zneužití slavnostních dnů školy (např. dny otevřených dveří) k průzkumu prostor pro pozdější útok nebo krádež.	Obhlídka školního prostoru, příprava na budoucí útok nebo krádež.	Identifikace podezřelého chování, dohled během slavnostních dnů, průkazky pro návštěvníky během slavnostních dnů.	3	4	3	36

23.	Dlouhodobé sledování a zmapování režimu školy (čas vstupu/výstupu, pohyb žáků) za účelem naplánování narušení.	Narušení režimu školy, riziko násilného činu v budoucnu. Ohrožení zdraví žáka, stresová situace, právní a finanční důsledky pro školu.	Školení pro zaměstnance, edukační hodiny pro žáky pořádané odborníky. Kontrola obvodového zabezpečení školy- např. CCTV.	3	3	5	45
24.	Cílený útok na školu (např. kvůli jejímu zaměření, minoritnímu složení žáků, inkluzi apod.)	Přímý útok na školu, oběti na životech, poškození infrastruktury. Narušení ochrany měkkých cílů. Verbální a fyzické napadení personálu, přerušení výuky psychická újma žáků i učitelů.	Bezpečnostní školení o aktivním útočnickovi, nácvik krizového plánu při napadení útočníkem. Školení pro zaměstnance, edukační hodiny pro žáky pořádané odborníky.	3	5	3	45
25.	Fyzické napadení pedagoga, asistenta nebo jiného zaměstnance školy ze strany třetí osoby (např. rodič, bývalý zaměstnanec)	Fyzické ohrožení pedagoga, psychická újma ostatních zaměstnanců či právní a finanční důsledky pro školu.	Pravidelné školení zaměstnanců, instalace tísňového tlačítka napojeného na PČR.	4	4	2	32
26.	Zasílání nebezpečného nebo podezřelého balíčku na adresu školy	Výbuch nebo chemická kontaminace, těžká zranění, evakuace, zapojení IZS.	Bezpečný plán pro zacházení s podezřelými zásilkami. Školení personálu o zacházení s podezřelými předměty.	2	5	4	40
27.	Využití jinak nezajištěných provozních částí školy pro vstup či úkryt osoby – např. sklep, půda, technická místnost.	Skrytý pohyb osoby, příprava na pozdější útok či krádež.	Kontrola přístupu do technických prostor školy. Instalace většího množství PIR detektorů. Režimové opatření pro technické místnosti.	3	3	4	36
28.	Pokus o vydírání pracovníka školy	Vydírání zaměstnance, únik citlivých dat, reputace školy.	Školení zaměstnanců na detekci nátlaku/vydírání – modelové situace.	2	4	4	32

			Psychologická podpora zaměstnanců při podezření na vydírání.				
29.	Cílené narušení školní akce konané mimo budovu školy (např. výlet, exkurze, sportovní turnaj)	Útok na žáky mimo školní budovu, právní odpovědnost vedení školy	Bezpečnostní plánování školních akcí.	2	5	2	20
30.	Záměrné zablokování přístupu záchranným složkám (např. zaparkované vozidlo, manipulace s bránou či vstupem)	Zpoždění zásahu IZS, znásobení následků mimořádné události.	Vytvoření nouzových koridorů pro zásahové složky. Pravidelná kontrola přístupových cest a školení personálu v oblasti přístupu pro IZS. Transparentně zdůraznit pokutování tohoto činu.	3	4	2	24

(zdroj: vlastní)

Výsledné skóre u každé hrozby je barevně označeno podle hodnotící tabulky, která přiřazuje konkrétní barvy jednotlivým úrovním rizika.

Tabulka 16 Hodnotící tabulka PNH

Hodnotící tabulka		
Rizikový stupeň	R = výsledek	Popis
I.	> 100	Nepříjemné – nutný okamžitý zásah, přerušení provozu
II.	51–100	Nežádoucí – požadována rychlá opatření ke snížení rizika
III.	11–50	Mírné – vyžaduje plánované zlepšení podmínek
IV.	3–10	Akceptovatelné – nevyžaduje okamžitý zásah, ale dohled
V.	<3	Bezvýznamné – není třeba zavádět další opatření

(zdroj: vlastní)