

Zabezpečení objektu s využitím integrovaného bezpečnostního systému

Bc. Vít Worbis



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. Vít Worbis
Osobní číslo:	A22365
Studijní program:	N1032A020003 Bezpečnostní technologie, systémy a management
Specializace:	Bezpečnostní management
Forma studia:	Kombinovaná
Téma práce:	Zabezpečení objektu s využitím integrovaného bezpečnostního systému
Téma práce anglicky:	Securing a Facility Using an Integrated Security System

Zásady pro vypracování

1. Proveďte literární rešerši na předmětné téma.
2. Analyzujte aktuální trendy v oblasti bezpečnostních systémů základních škol s ohledem na velikost školy.
3. Pojednejte o vhodných integrovaných systémech pro zabezpečení základních škol.
4. Realizujte analýzu rizik a bezpečnostního systému konkrétního objektu školy.
5. Navrhněte zvýšení úrovně zabezpečení konkrétního objektu školy.
6. Zpracujte orientační ceny navrhovaných řešení a vyhodnotte možnosti investora.

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

Seznam doporučené literatury:

1. IVANKA, Ján. Mechanické zábranné systémy. Zlín: UTB, 2014. 153 s. ISBN: 978-80-7454-427-9.
2. VALOUCH, Jan. Projektování integrovaných systémů. Zlín: UTB, 2015. 171 s. ISBN: 978-80-7454-557-3.
3. VALOUCH, Jan. Projektování bezpečnostních systémů. Zlín: UTB, 2019. 165 s. ISBN: 978-80-7454-858-1.
4. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. Zlín: Radim Bačuvčík – VeRBuM, 2011. 316 s. ISBN 978-80-87500-05-7.
5. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management II. Zlín: Radim Bačuvčík – VeRBuM, 2012. 386 s. ISBN 978-80-87500-19-4.
6. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management III. Zlín: Radim Bačuvčík – VeRBuM, 2013. 456 s. ISBN 978-80-87500-35-4.
7. NORMAN, Thomas. Electronic access control. Oxford: Butterworth-Heinemann is an imprint of Elsevier, 2012. 444 s. ISBN: 978-0-12-382028-0.
8. LOVEČEK, Tomáš. REITŠPÍŠ, Josef. Prejektovanie a hodnotenie systémov ochrany objektov. Žilina: EDIS 2011. 280 s. ISBN: 978-80-554-0457-8.

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

.....
podpis autora

ABSTRAKT

Cílem diplomové práce je navrhnout zabezpečení objektu s využitím integrovaného bezpečnostního systému. Jako objekt byla vybrána Základní škola Na Kopcích v Třebíči.

Teoretická část se zaměřuje na obecnou literární rešerši současného právního rámce vztahujícího se k bezpečnosti ve školství. Součástí je i analýza rizik, kde jsou představeny různé metody jejich hodnocení. Dále jsou představeny specifické požadavky na zabezpečení základních škol v návaznosti na jejich velikost a jsou rozebrány jednotlivé technické prostředky zabezpečení.

Praktická část diplomové práce se detailně zaměřuje na zabezpečení konkrétní základní školy v Třebíči. Na základě popisů objektu a hlavní budovy je provedena identifikace hlavních aktiv a následně jsou analyzována potenciální rizika. Dle těchto zjištění je navržen konkrétní soubor opatření rozdělený do dvou variant – minimální a optimální. Součástí návrhu je specifikace klíčových komponent použitých pro zvýšení úrovně zabezpečení a rovněž cenová kalkulace.

Klíčová slova: bezpečnost, základní škola, analýza rizik, poplachové zabezpečovací a tísňové systémy, kamerový systém,

ABSTRACT

The aim of the thesis is to design the security of the building using an integrated security system. The object selected was the Na Kopcích Primary School in Třebíč.

The theoretical part focuses on a general literature search of the current legal framework related to security in education. It also includes a risk analysis where different methods of risk assessment were presented. Furthermore, the specific requirements for the security of primary schools in relation to their size are presented and the different technical means of security are discussed.

The practical part of the thesis focuses in detail on the security of a specific primary school in Třebíč. Based on the descriptions of the facility and the main building, the main assets are identified and then the potential risks are analysed. According to these findings, a specific set of measures is proposed, divided into two variants – minimum and optimal. The proposal includes a specification of the key components used to increase the level of security as well as a price calculation.

Keywords: Security, Elementary School, Risk Analysis, Alarm Security and Emergency Systems, Camera System,

Zde je místo pro případné poděkování, popř. motto, úryvky knih atp.

OBSAH

ÚVOD.....	13
I TEORETICKÁ ČÁST	14
1 TERMINOLOGICKÝ A PRÁVNÍ RÁMEC PROBLEMATIKY ZABEZPEČENÍ OBJEKTU	15
1.1 TERMINOLOGIE	15
1.2 NORMY A PŘEDPISY	18
1.3 PRÁVNÍ RÁMEC OCHRANY OSOB A MAJETKU	20
2 ANALÝZA RIZIK	25
2.1 POJEM ANALÝZA RIZIK	25
2.2 VYBRANÉ METODY ANALÝZY RIZIK	26
3 VYBRANÉ TEORETICKÉ ASPEKTY ZABEZPEČENÍ ZÁKLADNÍCH ŠKOL.....	38
3.1 TYPOLOGIE OCHRANY OSOB A MAJETKU	39
3.2 ROZDĚLENÍ TYPU OCHRAN DLE BEZPEČNOSTNÍHO SYSTÉMU	41
3.3 RIZIKA A STUPNĚ ZABEZPEČENÍ OBJEKTU	46
4 VYBRANÉ SYSTÉMY TECHNICKÉ OCHRANY ZÁKLADNÍCH ŠKOL.....	48
4.1 MECHANICKÉ ZÁBRANNÉ SYSTÉMY	48
4.2 DOHLEDOVÉ VIDEO SYSTÉMY.....	50
4.3 ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE	52
4.4 POPLACHOVÉ ZABEZPEČOVACÍ A TÍŠŇOVÉ SYSTÉMY	55
4.5 INTEGRACE TECHNICKÝCH PROSTŘEDKŮ OCHRANY	60
ZÁVĚR TEORETICKÉ ČÁSTI	62
II PRAKTICKÁ ČÁST.....	63
5 POPIS VYBRANÉHO OBJEKTU	64
5.1 CHARAKTERISTIKA ŠKOLY	64
5.2 POPIS OBJEKTU A OKOLÍ	64
6 ANALÝZA RIZIK	72
6.1 IDENTIFIKACE AKTIV	72
6.2 IDENTIFIKACE HROZEB	74
6.3 ANALÝZA METODOU PNH.....	75
6.4 SEZNAM HROZEB	78
7 ANALÝZA AKTUÁLNÍHO STAVU ZABEZPEČENÍ ZÁKLADNÍ ŠKOLY.....	80
7.1 PERIMETRICKÁ OCHRANA.....	80

7.2	PLÁŠŤOVÁ OCHRANA.....	82
7.3	PROSTOROVÁ OCHRANA	83
7.4	PŘEDMĚTOVÁ OCHRANA A FYZICKÁ OSTRHA.....	84
7.5	TECHNICKÁ OCHRANA.....	84
7.6	IDENTIFIKACE NEDOSTATKŮ	86
8	NÁVRH ŘEŠENÍ PRO ZVÝŠENÍ ÚROVNĚ ZABEZPEČENÍ	87
8.1	HROZBY	87
8.2	MINIMÁLNÍ POŽADAVKY TECHNICKÉHO CHARAKTERU PRO ZVÝŠENÍ ÚROVNĚ ZABEZPEČENÍ.....	87
8.3	MINIMÁLNÍ POŽADAVKY NETECHNICKÉHO CHARAKTERU PRO ZVÝŠENÍ ÚROVNĚ ZABEZPEČENÍ.....	98
8.4	VYČÍSLENÍ NÁKLADŮ	99
8.5	NÁVRH OPTIMÁLNÍCH KROKŮ TECHNICKÉHO CHARAKTERU PRO ZVÝŠENÍ ÚROVNĚ ZABEZPEČENÍ.....	100
8.6	OPTIMÁLNÍ POŽADAVKY NETECHNICKÉHO CHARAKTERU PRO ZVÝŠENÍ ÚROVNĚ ZABEZPEČENÍ.....	103
8.7	VYČÍSLENÍ NÁKLADŮ	103
8.8	VÝSTUPNÍ ANALÝZA.....	104
	ZÁVĚR PRAKTICKÉ ČÁSTI	107
	ZÁVĚR.....	108
	SEZNAM POUŽITÉ LITERATURY	109
	SEZNAM OBRÁZKŮ	116
	SEZNAM TABULEK.....	117
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	118
	SEZNAM PŘÍLOH.....	119

ÚVOD

Ochrana objektů, a tím i majetku, je v současné době jedním z klíčových témat. Tím spíše, pokud se jedná o veřejné budovy, ve kterých se pohybují děti. Z tohoto důvodu je nezbytné přistupovat k otázkám bezpečnosti s maximální vážností a usilovat o její neustálé zvyšování. Bezpečnostní hrozby dneška jsou často velmi sofistikované a mohou přicházet z nejrůznějších směrů. Přesto školský sektor na tuto skutečnost mnohdy nereaguje dostatečně, ať už kvůli omezeným finančním prostředkům nebo zastaralému postoji, že podobná opatření nebyla v minulosti potřebná. Události z posledních let však ukazují, že bezpečnost ve školách si zaslouží systematickou a důslednou pozornost.

Tématem této diplomové práce je zabezpečení objektu s využitím integrovaného bezpečnostního systému. Jako objekt jsem si vybral Základní školu Na Kopcích v Třebíči. Hlavním cílem této práce je provést analýzu vybraného objektu z hlediska bezpečnosti a navrhnout taková opatření, která co nejvíce omezí potenciální rizika.

V teoretické části diplomové práce se budu zabývat klíčovými pojmy právního rámce a technických možností v oblasti zabezpečení objektů, se cílem zaměřením na zabezpečení základních škol. Dále zde popíšu jednotlivé metody analýzy rizik a formy ochrany – režimová, fyzická i technická. Na závěr teoretické části rozeberu jednotlivé technické prostředky zabezpečení.

V praktické části diplomové práce se detailně zaměřím na zabezpečení konkrétní základní školy v Třebíči. Budu popisovat objekt školy včetně jeho areálu, technického vybavení a způsobu využití během školního dne i mimo něj. Provedu identifikaci hlavních aktiv a následně analýzu rizik na základě metody PNH. Popíšu současný stavu zabezpečení objektu pomocí metody kontrolního seznamu. Na závěr praktické části diplomové práce bude navržen konkrétní soubor opatření rozdělený do dvou variant – minimální a optimální.

I TEORETICKÁ ČÁST

1 TERMINOLOGICKÝ A PRÁVNÍ RÁMEC PROBLEMATIKY ZABEZPEČENÍ OBJEKTU

V současné době se bezpečnost stala centrálním bodem zájmu jak pro veřejné, tak pro soukromé sektory, přičemž ochrana fyzických a digitálních aktiv je na prvním místě priorit každé organizace. Zabezpečení objektů, od kancelářských budov po průmyslové komplexy a veřejné instituce, je nezbytné pro ochranu majetku, informací, a především lidských životů před širokou škálou hrozeb včetně zločinu, terorismu, neoprávněného přístupu a přírodních katastrof. Využití integrovaných bezpečnostních systémů přináší řadu výhod, včetně zvýšené efektivity, sníženého rizika lidské chyby a lepšího využití dostupných zdrojů. Díky integraci různých technologií, jako je kamerový systém, kontroly přístupu, detekce průniku a systémy požární signalizace, mohou tyto systémy poskytnout ucelený přehled o bezpečnostní situaci objektu v reálném čase, což umožňuje rychlou a koordinovanou reakci na jakékoli incidenty.

Z tohoto důvodu je důležité, abych se v první kapitole diplomové práce věnoval nejen definici klíčových pojmů, ale také podrobnému prozkoumání právního a regulačního rámce, který formuje základ pro návrh, implementaci a provoz integrovaných bezpečnostních systémů. Tento úvod slouží jako základní kámen pro další diskusi o technologických, organizačních a etických aspektech zabezpečení objektu, a umožňuje čtenáři lépe porozumět komplexitě a důležitosti tématu.

1.1 Terminologie

Tato část diskutuje o pojmech, specifických slovech nebo výrazech z oblasti bezpečnosti.

Aktivum

V oblasti bezpečnosti, termín "aktivum" znamená jakýkoli cenný zdroj, který je potřeba chránit. Aktiva mohou být také lidé, jejichž bezpečnost a ochrana jsou zásadní pro fungování organizace. Aktivem je tedy vše, co má pro organizaci určitou hodnotu, jež může být snížena působením hrozby. [1] [2]

Aktiva můžeme rozdělit do dvou skupin:

- aktiva hmotná,
- aktiva nehmotná.

Z pohledu bezpečnosti se aktivum považuje za cokoli, co má pro organizaci hodnotu a co by mohlo být ohroženo různými hrozbami, včetně kybernetických útoků, fyzických vloupání, sabotáže, krádeže, přírodních katastrof, nebo i selhání interních procesů. [1] [2]

Riziko

Riziko se pojímá jako kombinace pravděpodobnosti, že dojde k nežádoucímu jevu, a míry jeho potenciálního škodlivého účinku. Jde o vyhodnocení možnosti vzniku nepříznivé situace a jejích důsledků. Riziko lze posuzovat jak kvantitativně, tak kvalitativně. Když hovoříme o kvantitativním vyjádření, používáme konkrétní jednotky nebo bezrozměrné hodnoty k určení míry rizika. Naopak kvalitativní posouzení rizika popisuje potenciální dopady slovy a zaměřuje se na závažnost těchto dopadů. Riziko nepopisuje, co se již stalo nebo jak k události došlo, ale odhaduje budoucí dopady na daný objekt nebo systém. Toto hodnocení umožňuje vykreslovat hrozby podle vážnosti jejich možných následků. Analýza rizik se zabývá studiem příčin možné expozice a jejich dopadů, přičemž v pravděpodobnostní složce rizika se odhaduje frekvence výskytu narušení. Dále se předpokládá, že k narušení došlo v důsledku využití existující zranitelnosti a selhání ochranných opatření. [1] [2]

Hrozba

Hrozba je faktor nebo činitel, který může přímo způsobit škodu nebo negativně ovlivnit určitý celek, ať už jde o událost, aktivitu, silu, nebo dokonce osobu zapojenou do vzniku potenciální škody. Příklady hrozeb zahrnují požáry, přírodní katastrofy, odcizení zařízení, nebo neautorizovaný přístup k citlivým informacím. [1]

Hrozba může nastat v důsledku selhání stávajících zabezpečovacích opatření, ale může se také objevit během konfliktu nebo při zadržení. Typicky se projevuje prostřednictvím komunikace (verbálně, gesty, postojem, mimikou), demonstrací odhodlání (např. odvážným přiblížením k protivníkovi), hrozbou použití obranného nástroje nebo zbraně (například jejich zobrazením nebo přípravou k použití) nebo demonstrací síly. Nejvýraznějším projevem hrozby je demonstrace dovedností v oblasti sebeobran, která může zahrnovat lehké zranění útočníka. [1] [2]

Hrozba představuje skutečnost (jev se škodícím účinkem), která se svým působením projevuje na určitém celku negativně. Může mu v případě expozice způsobit újmu nebo na něj mít negativní dopad. Jedná se o škodící účinek (působení), které má materiální nebo

nemateriální povahu. Materiální působení může mít fyzikální nebo chemickou povahu. Příkladem takové hrozby je válka, krádež, dopravní nehoda, povodeň, požár atd. Nemateriální hrozba má informační a logickou povahu. Zprostředkovaně se promítá do řady oblastí společnosti i osobního života jedinců. Může mít podobu spojenou s penězi, informacemi, dezinformacemi a zpravodajstvím, ekonomickými procesy, řízením, odstrašením, psychikou. [1] [6]

Zranitelnost

Zranitelnost označuje stupeň, do kterého může být určité aktivum negativně ovlivněno v důsledku jeho nedostatků, což může vést k realizaci hrozby. Tato charakteristika se týká specifického aktiva, na které má potenciální hrozba dopad. Skrze zranitelnost lze odhadnout, jak velkou citlivost má dané aktivum vůči určité hrozbě, a to se projevuje ve všech případech, kdy je aktivum vystaveno potenciálnímu riziku. Hlavním ukazatelem zranitelnosti je její úroveň, která se posuzuje podle dvou hlavních aspektů: citlivosti a kritičnosti aktiva. Citlivost znamená, jak snadno může být aktivum poškozeno hrozbou, zatímco kritičnost ukazuje na význam aktiva pro daný systém nebo subjekt. [1] [7]

Zranitelnost také popisuje, jak moc je referenční objekt vystaven riziku újmy. Jedná se o místa, která mohou být snadno zasažena a vést k porušení bezpečnosti. Rozpoznání a identifikace zranitelností umožňuje cíleně posílit odolnost systému a tím zredukovat nebo odstranit zranitelnost. [6] [7]

Protipatření

Protipatření definují akce, procesy, postupy, technologie nebo jakékoli prvky, které jsou vytvořeny s cílem zmírnit vliv hrozeb, nebo je dokonce zcela odstranit, snížit jejich zranitelnost nebo minimalizovat jejich negativní dopady. Hlavním úkolem těchto opatření je zabránit vzniku jakékoliv škody, a pokud již k škodě dojde, pomoci překonat její důsledky. Účinnost těchto opatření se posuzuje podle dvou hlavních kritérií: jak efektivní jsou v dosahování svého cíle a jaké jsou náklady spojené s jejich implementací. [1] [2]

Referenční objekt

Referenční objekt je pojem, který označuje celek, v rámci, kterého se řeší otázky narušení a zabezpečení. Tento objekt může být hmotný nebo nehmotný a je definován z důvodů sociálního významu, jelikož má pro společnost určitou důležitost. S časem se rozrůstá seznam typů referenčních objektů. Historicky byly referenční objekty většinou hmotné, jako například rodové skupiny, opevněné areály, domy, města nebo státní útvary. S vývojem se

k nim přidávaly různé organizace, mezinárodní subjekty nebo i celé životní prostředí. Na druhou stranu, mezi nehmotné referenční objekty původně patřily tajné informace a čest, zatímco v pozdější době byla k této kategorii zařazena i lidská práva, osobní data, psychické aspekty člověka nebo národní identita. [1] [2]

Bezpečnost

Pojem "bezpečnost" v teorii bezpečnosti je široký a vícevrstevný koncept, který se týká ochrany jednotlivců, skupin, společnosti, států a mezinárodního systému před různými formami hrozeb. Bezpečnost lze chápat v mnoha dimenzích, včetně fyzické, ekonomické, ekologické, politické, sociální, informační a kybernetické bezpečnosti. Nejlépe ji však zvýrazňuje definice:

„Bezpečnost je stav, kdy jsou na nejnižší možnou míru eliminovány hrozby pro objekt (zpravidla stát, organizaci) a jeho zájmy, přičemž tento objekt je efektivně vybaven k redukci, resp. eliminaci stávajících i potencionálních hrozeb a je ochoten při tomto procesu spolupracovat.“ [5] [4]

1.2 Normy a předpisy

V České republice, jakož i ve většině EU, je používání technických norem založeno na principu dobrovolnosti. Tomu odpovídá platná právní úprava v ČR, která stanoví, že „česká technická norma není obecně závazná“ (viz § 4 odst. 1 zákona č. 22/1997 Sb.). [8] [10]

Existují však případy, že povinnost dodržovat požadavky uvedené v českých technických normách vyplývá z jiného právního aktu, např. z právního předpisu (normy na elektrickou požární signalizaci – EPS), smlouvy nebo rozhodnutí správního orgánu. Pro úplnost je třeba uvést, že plnění požadavků stanovených technickými předpisy – zejména českými technickými normami, je jednoznačný a nejjednodušší způsob, jak prokázat kvalitu jednotlivých výrobků, zabezpečovacích systémů či komplexního zabezpečení objektů. Zárukou, že tomu tak skutečně je, je platný certifikát shody, vydaný akreditovaným certifikačním orgánem podle příslušné požadavkové nomy. [8]

Klasifikace norem podle úrovně jejich působnosti nebo geografického rozsahu:

- Česká technická norma (ČSN) - České technické normy jsou vytvářeny a publikovány Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví (zkráceně ÚNMZ) a jsou specifické pro Českou republiku. Tyto normy mohou být založeny na mezinárodních nebo evropských normách, ale mohou také zahrnovat dodatečné specifikace nebo požadavky, které jsou relevantní pouze pro český trh.
- Evropská norma (EN) - Evropské normy jsou vytvářeny evropskými normalizačními organizacemi, jako je Evropský výbor pro normalizaci (CEN), Evropský výbor pro normalizaci v elektrotechnice (CENELEC) a Evropský ústav pro telekomunikační normy (ETSI). Tyto normy jsou přijímány členskými státy Evropské unie a EFTA (Evropské sdružení volného obchodu) a mají za cíl usnadnit obchod a zvýšit interoperabilitu a bezpečnost produktů na jednotném evropském trhu.
- Mezinárodní norma. Tyto normy jsou vytvářeny mezinárodními organizacemi, jako je Mezinárodní organizace pro normalizaci (ISO) nebo Mezinárodní elektrotechnická komise (IEC). Jsou určeny k použití na celosvětové úrovni a zaměřují se na harmonizaci pravidel, specifikací a postupů napříč různými zeměmi a průmyslovými sektory. [9]

Následující evropské normy byly zpracovány technickou komisí CENELEC/TC 79 Poplachové systémy ve spolupráci s technickou komisí CEN/TC 72 Systémy automatické požární signalizace a převedeny do ČSN.

Rozdělení norem:

- ČSN EN 50131 řada – Alarmové systémy pro ochranu před vloupáním a napadením. Tato série norem se vztahuje na různé aspekty zabezpečovacích systémů, včetně požadavků na systémy, komponenty, a také na jejich instalaci a údržbu.
- ČSN EN 50132 řada – CCTV dohledové systémy pro použití v bezpečnostních aplikacích. Série norem pokrývající návrh, instalaci, provoz a údržbu video dohledových systémů. [11] [9]
- ČSN EN 50133 řada – Systémy elektronického přístupového řízení. Tato norma specifikuje požadavky a testovací metody pro elektronické přístupové systémy.[9]
- ČSN EN 50134 řada – Systémy přivolání pomoci. Tato norma se týká systémů pro přivolání pomoci, což jsou systémy určené k poskytování pomoci lidem v nouzi,

obvykle ve zdravotně kompromitovaných nebo rizikových situacích. Tato norma je rozdělena do několika částí, z nichž každá se zabývá různými aspekty sociálních poplachových systémů, včetně návrhu, instalace, provozu a údržby. [11] [9]

- ČSN EN 50135 řada – Poplachové systémy tísňové. Tato norma se zaměřuje na specifikace, požadavky a testovací metody pro tísňové (nebo nouzové) poplachové systémy, které jsou navrženy k ochraně osob a majetku v případě různých druhů hrozeb nebo nouzových situací. [11] [9]
- ČSN EN 50136 řada – Alarmové systémy pro přenos poplachových zpráv. Tato série norem se zabývá požadavky a testovacími metodami pro systémy přenosu poplachu a jejich komponenty. [11] [9]
- ČSN EN 50518 řada – Dohledová a poplachová přijímací centra (ARC – Alarm Receiving Centre). Tato evropská norma stanovuje požadavky, provozní postupy, minimální funkční požadavky a kritéria pro hodnocení a testování ARC. Jejím cílem je zajistit, že tyto střediska fungují na vysoké úrovni spolehlivosti, aby efektivně přijímaly a zpracovávaly poplachové signály zabezpečovacích a bezpečnostních systémů. [11] [9]

Norma pro elektronické požární signalizační systémy (EPS) se v České republice a v mnoha zemích Evropské unie řídí především evropskou normou EN 54. Tato rozsáhlá norma je rozdělena do několika částí, každá specifikuje různé aspekty systémů požární signalizace, včetně komponent, funkčnosti a výkonu. Každá část normy EN 54 podrobně specifikuje technické požadavky a testovací metody pro různé komponenty a funkce EPS systémů, aby se zajistila jejich spolehlivost a efektivita při detekci požárů a varování osob v budovách. [11]

1.3 Právní rámec ochrany osob a majetku

Při zkoumání právního rámce ochrany osob a majetku se zaměřujeme na několik základních právních oblastí, z nichž každá upravuje tuto problematiku prostřednictvím specifických norem a předpisů. Tato část diplomové práce se věnuje právě těmto legislativním úpravám, které se týkají ochrany jednotlivců a jejich majetku. V České republice dosud neexistuje ucelený právní předpis, jenž by tuto oblast komplexně upravoval. Z tohoto důvodu je pozornost věnována především vybraným částem platné legislativy, a to zejména obecným zásadám ochrany osobních údajů a oznamovacím povinnostem, jež vznikají při zavádění dohledových systémů v rámci bezpečnostních opatření. [11] [12]

Občanský zákoník

Občanský zákoník České republiky, zákon č. 89/2012 Sb., který nabyl účinnosti 1. ledna 2014, představuje klíčový právní předpis pro regulaci občanskoprávních vztahů, včetně ochrany osob a majetku. Zákoník se skládá z několika hlavních částí, které pokrývají široký rozsah témat od rodinného práva, práv k nemovitostem, závazkových vztahů, až po dědické právo. Co se týče ochrany osob a majetku, Občanský zákoník obsahuje několik relevantních ustanovení.

Ochrana osobnosti: Občanský zákoník zakotvuje ochranu osobnosti, včetně práva na ochranu zdraví, svobody, cti, důstojnosti a soukromí. Umožňuje jednotlivcům bránit se proti neoprávněným zásahům, a to i po smrti.

Vlastnické právo: Zákoník detailně reguluje vlastnická práva, včetně nabytí, výkonu a ochrany vlastnictví. Tato část zákona se vztahuje na ochranu majetku a stanovuje právní rámec pro jeho převod, užívání a další aspekty související s vlastnictvím.

Odpovědnost za škodu: Občanský zákoník stanovuje pravidla pro odpovědnost za škodu a poskytuje ochranu osobám, které byly poškozeny činy jiných. To zahrnuje jak majetkovou, tak nemajetkovou škodu.

Závazkové právo: Součástí zákoníku je i závazkové právo, které se týká vztahů mezi subjekty, například smluvních vztahů, a stanoví pravidla pro ochranu zájmů stran v těchto vztazích.

Ochrana spotřebitele: Zákoník zahrnuje také ustanovení o ochraně spotřebitele, která mají za cíl ochránit spotřebitele před nekalými obchodními praktikami a zajišťují spravedlivé, transparentní a férové zacházení. [12] [13]

Příklad paragrafu občanského zákoníku:

§ 11 Občanského zákoníku (Ochrana osobnosti): Tento paragraf zakotvuje, že každý má právo na ochranu své osobnosti, zejména svého života a zdraví, občanské cti a důstojnosti, soukromí, jména a projevů osobní povahy. Umožňuje jednotlivcům podnikat kroky proti tomu, kdo by omezil nebo neoprávněně zasáhl do jejich osobních práv. [12]

Občanský zákoník v § 11 a následujících stanovuje ochranu osobnosti, včetně práva na soukromí. Podle těchto ustanovení má každý právo na ochranu svého soukromého života, a jakýkoliv zásah do tohoto práva, který není zákonně oprávněn, může být považován

za neoprávněný. To zahrnuje i pořízení záznamu bez souhlasu osoby, jejíž soukromí je záznamem dotčeno. V případech, kdy je záznam pořízen bez oprávněného důvodu nebo bez souhlasu dotčené osoby, může tato osoba požadovat jeho odstranění, zakázání jeho šíření a v některých případech i náhradu škody. [12]

Zákon o Policii České republiky

Zákon č. 273/2008 Sb., o Policii České republiky, je klíčovým právním předpisem, který upravuje postavení, působnost, organizaci a činnost Policie ČR. Tento zákon se věnuje širokému spektru témat spojených s veřejným pořádkem, bezpečností a ochranou práv a svobod občanů, včetně ochrany osob a majetku. [13] [14]

V kontextu ochrany osob a majetku se Policie ČR zaměřuje na řadu činností, které zahrnují:

- Vyšetřování trestných činů a přestupků, jejichž cílem je způsobit škodu na majetku nebo zdraví osob.
- Přijímání opatření k zamezení protiprávního jednání, které by mohlo ohrozit bezpečnost osob nebo majetku.
- Spolupráce s jinými bezpečnostními složkami a institucemi v rámci ochrany veřejného pořádku a bezpečnosti.

Je důležité poznamenat, že činnost Policie ČR je regulována nejen tímto zákonem, ale i dalšími právními předpisy, včetně Občanského zákoníku, Trestního zákoníku a zákonů týkajících se ochrany osobních údajů a soukromí. Policie musí při své činnosti respektovat práva a svobody jednotlivců, jak jsou stanovena ústavou a mezinárodními smlouvami o lidských právech, ke kterým se Česká republika připojila. Tento zákon tedy představuje základní rámec pro činnost Policie ČR ve vztahu k ochraně právního státu, veřejného pořádku a bezpečnosti, včetně ochrany osob a majetku. [14]

Trestní zákoník

Trestní zákoník České republiky, zákon č. 40/2009 Sb., je klíčovým právním dokumentem, který definuje trestné činy, stanovuje tresty a jiné trestněprávní sankce za protiprávní jednání. V kontextu ochrany osob a majetku se Trestní zákoník zabývá širokým spektrem trestných činů, které ohrožují tyto dvě základní hodnoty. [15]

Zde je několik příkladů relevantních částí a paragrafů, které se týkají ochrany osob a majetku:

§ 111 a následující – Trestné činy proti životu a zdraví, včetně vraždy, ublížení na zdraví, ohrožení pod vlivem návykové látky a další.

§ 205 a následující – Trestné činy proti majetku, což zahrnuje krádež, loupež, zpronevěru, poškození cizí věci, a další. [13] [15]

Obecné nařízení o ochraně osobních údajů (GDPR)

GDPR, plným názvem Nařízení (EU) 2016/679, je nařízení Evropské unie, které se zaměřuje na ochranu osobních údajů a soukromí občanů EU. Nařízení nabývá přímé aplikace ve všech členských státech EU od 25. května 2018 a přináší s sebou řadu povinností pro organizace, které zpracovávají osobní údaje občanů EU, ať už mají sídlo v EU nebo mimo ni, pokud nabízejí zboží či služby osobám v EU nebo sledují jejich chování. [16]

GDPR klade důraz na principy jako jsou transparentnost zpracování, minimalizace údajů, přesnost, omezení účelu, integrita a důvěrnost, stejně jako na právo subjektů údajů na přístup k údajům, jejich opravu, výmaz (právo být zapomenut), omezení zpracování a na přenositelnost údajů. Dále GDPR stanovuje, že zpracování osobních údajů musí být vždy založeno na některém z právních důvodů, jako je souhlas subjektu údajů, plnění smlouvy, zákonná povinnost, životní zájmy, veřejný zájem nebo oprávněné zájmy zpracovatele. Ačkoli hlavním cílem GDPR není přímo ochrana majetku, jeho ustanovení a principy mají významný dopad i na ochranu majetku, zejména v digitální sféře. GDPR klade důraz na zabezpečení osobních údajů, což nepřímě přispívá k ochraně majetku organizací a jednotlivců tím, že zvyšuje celkovou kybernetickou a informační bezpečnost. [16] [17]

Zákon o zpracování osobních údajů

Zákon č. 110/2019 Sb., o zpracování osobních údajů, je českým národním právním předpisem, který doplňuje a upřesňuje některé aspekty Obecného nařízení o ochraně osobních údajů (GDPR) ve světle specifík českého právního a administrativního prostředí. Tento zákon byl přijat s cílem zajistit soulad českého právního řádu s GDPR a řeší řadu otázek spojených se zpracováním osobních údajů, které GDPR nechává na uvážení jednotlivých členských států. [18]

Zákon č. 110/2019 Sb. je tedy zásadní pro všechny subjekty zpracovávající osobní údaje v České republice, poskytuje jim návod, jak správně postupovat při zpracování osobních údajů a jak zajistit ochranu práv a svobod jednotlivců v souladu s evropskými i národními předpisy.

Kromě těchto hlavních oblastí mohou existovat i specifické zákony a nařízení vztahující se k určitým sektorům nebo situacím, například zákony týkající se kybernetické bezpečnosti, regulace užívání veřejného prostoru, ochrana před domácím násilím atd.

Shrnutí první kapitoly

Zabezpečení základních škol je širokou oblastí, která vyžaduje propojení technologií s právními normami. Ačkoliv v České republice neexistuje jednotný zákon upravující tuto problematiku, lze se opřít o platnou legislativu – například občanský zákoník, trestní zákoník, zákon o Policii ČR nebo GDPR – a o technické normy (např. ČSN EN 50131 či 50132). Ty poskytují rámec pro efektivní návrh a provoz bezpečnostních systémů.

Zásadními prvky zůstávají správná identifikace rizik, posouzení zranitelností a zavedení přiměřených protiopatření. Přitom je nutné dbát na rovnováhu mezi bezpečností a ochranou práv jednotlivců, zejména v oblasti zpracování osobních údajů.

2 ANALÝZA RIZIK

Klíčem k zabezpečení objektu s využitím integrovaného bezpečnostního systému je provést důkladnou analýzu potenciálních rizik, což umožní identifikovat hrozby, proti kterým je ochrana nevyhnutelná. Z tohoto důvodu se druhá kapitola této diplomové práce zaměřuje na analýzu rizik, přičemž úvodní část představuje její základní rysy a pokračuje výpisem některých preferovaných metod. V praktické části této práce se podrobněji věnuji metodě Checklist (Kontrolní seznam) a metodě PNH. Získané informace z analýzy rizik se stávají základem pro práci na praktické části diplomového projektu.

2.1 Pojem Analýza rizik

Základ chybného plánování a organizace jakékoli ochrany spočívá většinou v chybné, nebo dokonce ve špatné analýze bezpečnostních potřeb. Při analýze musejí být definovány úseky ochrany, druhy hrozcích nebezpečí, jejich potencionální zdroje a možné následky. Prvním krokem analýzy musí být tedy konstatování:

- a) co má být chráněno (budovy, místnosti, zařízení atd.),
- b) před čím (vloupáním, požárem atd.),
- c) které osoby musí být chráněny,
- d) jakým způsobem ochranu zajistit.

Při analýze možných původců událostí musíme rozlišovat osoby nejen na oprávněné, částečně oprávněné a neoprávněné, nýbrž i podle jejich původu či poslání, např. vlastní pracovníci (učitelé, asistenti atd.), studenti, žáci, návštěvníci, dodavatelé, servisní technici. Je důležité, aby jednotlivá rizika byla posouzena z hlediska pravděpodobnosti jejich výskytu, neboť nebezpečí číhá všude a možných následků může být mnoho. Jestliže je analýza rizik určena například jen pro plánování systému kontroly přístupu, lze některá zásadní rizika a jejich možné původce uvést v závorkách, tj. nebrat na ně zřetel. Mají však význam pro plánování ostatních ochranných opatření a pro pojištění. Jestliže například nosičům dat a paměťovým médiím (počítačům, terminálům, ústředně kontroly přístupu) hrozí všechna rizika, jsou jiné hodnoty (pozemky, budovy) vystaveny zpravidla jen některým rizikům, např. živelním pohromám, průmyslovým haváriím, požárům apod. [19] [20]

Analýzou rizik se tedy rozumí:

- stanovení chráněných prvků,
- identifikace nebezpečí a zdrojů rizika,
- odhad pravděpodobnosti vzniku protiprávního činu,
- odhad důsledků protiprávního jednání.

Metod analýzy rizik existuje celá řada, výběr pak závisí na konkrétním prostředí, kterého se analýza týká. V praxi se většinou využívá kombinace více metod aplikovaných na jednotlivé činnosti bezpečnostních procedur. Bývají použity buď současně, nebo jednotlivě s kontinuální návazností. K vyhodnocování rizik jsou využívány i počítačové metody, včetně specializovaného softwaru, který dokáže na základě vložených dat modelovat jakékoli mimořádné situace. Výstupy z bezpečnostního modelování a analýzy rizik jsou v závěrečné fázi porovnávány se statistickými daty. [19] [20]



Obrázek 1 Analýza rizik

(zdroj: [21])

2.2 Vybrané metody analýzy rizik

Způsob vyjádření veličin, s nimiž se v analýze rizik pracuje, lze použít jako základní hledisko pro rozdělení těchto metod. Existují při tom dva základní přístupy k jejímu řešení:

kvantitativní a kvalitativní metody vyjádření veličin analýzy rizik. V analýze rizik se používá buď jeden z těchto dvou přístupů, nebo jejich kombinace. [22]

Kvalitativní metody

Kvalitativní metody jsou postaveny na popisu závažnosti potenciálního dopadu a na pravděpodobnosti, že daná událost nastane. Vyznačují se tím, že rizika jsou vyjádřena v určitém rozsahu, například jsou obodována (1 až 10) nebo určena pravděpodobností (0; 1) nebo slovně (malé, střední, velké) apod. Úroveň je obvykle určována kvalifikovaným odhadem. Kvalitativní metody jsou jednodušší a rychlejší, ale více subjektivní. Obvykle přinášejí problémy v oblasti zvládnutí rizik, při posuzování přijatelnosti finančních nákladů nutných k eliminaci hrozby, která může být kvalitativní metodou charakterizována třeba jako „velká až kritická“. Tím, že chybí jednoznačné finanční vyjádření, se kontrola efektivnosti nákladů znesnadňuje. [6] [22]

Kvalitativní metody jsou například:

- Bezpečnostní kontrola (Safety audit)
- SWOT analýza.
- What If – Analýza toho, co se stane, když.....
- CLA – Check List Analysis – analýza pomocí kontrolního seznamu.
- HAZOP – Analýza ohrožení a provozuschopnosti.

Bezpečnostní kontrola (Safety audit)

Bezpečnostní kontrola patří mezi nejstarší metody. Je založena na inspekčních pochůzkách v existujícím zařízení nebo posuzování výkresů v době projektování, často se využívá před spuštěním procesu. Při bezpečnostní kontrole se vyhledávají potenciálně rizikové faktory, nehody, provozní problémy a jiné nebezpečné situace. Jedná se zkrátka o jakýsi BOZP audit, při kterém se kontrolor zaměřuje zejména na detailní prohlídku zařízení, strojů, nástrojů atd. Bezpečnostní audit pracoviště v tomto případě provádí zkušený pracovník, ideálně se zaměřením na bezpečnost práce. Pokud je na pracovišti nové zařízení, provádí kontrolující posouzení technické dokumentace, a to ještě před jeho samotným zapojením a uvedením do provozu. Cílem této kontroly je hlavně zjistit podmínky a okolnosti, které by mohly vést ke zranění, pracovnímu úrazu či jiné nehodě. Je možné použít připravený seznam otázek a maticí pro skórování rizika. Výsledkem je kvalitativní popis možných bezpečnostních problémů a nápravné činnosti. [20] [23]

SWOT analýza

SWOT analýza je rozšířená metodika používaná k identifikaci a vyhodnocení vnitřních a vnějších aspektů, které ovlivňují úspěch organizace či jakéhokoli hodnoceného systému. Často se využívá v oblasti strategického managementu k posouzení určitého strategického plánu. Tuto techniku vytvořil Albert HUMPHREY v 60. letech 20. století. V rámci SWOT analýzy se hodnotí vnitřní a vnější faktory. Vnitřní faktory zahrnují silné stránky (Strengths) a slabé stránky (Weaknesses) organizace nebo systému. Vnější faktory zahrnují příležitosti (Opportunities) a hrozby (Threats), které souvisí s okolním prostředím organizace nebo systému. Zkratka SWOT pochází z prvních písmen anglických názvů těchto faktorů. Hlavním cílem SWOT analýzy je určit zásadní silné a slabé stránky, jakož i hlavní příležitosti a hrozby, které působí z vnějšku. [6] [24]



Obrázek 2 SWOT analýza rizik

(zdroj: [25])

What If – Analýza toho, co se stane, když

Tato v průmyslu často užívaná metoda je založena na brainstormingu, kdy zkušený tým identifikuje havarijní situace na základě kladení otázek typu: “Co se stane, když ... ,,. Studie se provádí formou pracovních porad, všechny otázky jsou zapisovány a tým společně hledá odpovědi na formulované otázky, následky odchylek a doporučuje opatření. U větších procesů je lepší celý systém rozdělit na menší subsystemy, samostatné části provozu a ty hodnotit samostatně. Metoda What If – v praxi relativně oblíbená, neboť neklade vysoké nároky na čas. Je však nutno počítat s tím, že nižší časová náročnost studie má kořeny v intuitivním, méně systematickém postupu. Tato metoda je velmi efektivní a účinná, pokud

má pracovní tým provozní zkušenosti a současně má aplikační zkušenosti s touto metodou. Naproti tomu výhodou metody je nízká časová náročnost, možnost použití v kterékoli fázi života zařízení. Výsledky studie je možno zapisovat pomocí podpůrného softwaru. [6] [20]

CLA – Check List Analysis – analýza pomocí kontrolního seznamu

Kontrolní seznam, známý také jako Checklist, je nástroj založený na systematickém přezkumu, umožňující postupně zaškrtnout a vykonávat určená opatření. Jeho sestavení vychází z pracovních aktivit a technologických postupů, jež se vyskytují na konkrétním pracovišti. Důležitou součástí je pravidelná revize a aktualizace kontrolního seznamu. Analýza prostřednictvím stávajícího seznamu je efektivní metoda, která identifikuje slabiny a rozdíly v operačních procedurách, čímž umožňuje navrhnout zlepšení v bezpečnosti. Při vytváření nového seznamu analytik čerpá z relevantních norem a pravidel, a kvalita seznamu je zvyšována zapojením zkušeného týmu. Náročnost vytvoření seznamu závisí na jeho účelu, podkladech a komplexnosti systému. Tento nástroj lze využít v jakékoli etapě procesu, často se používá během plánování pro zajištění souladu s normami. Kontrolní seznam se může kombinovat i s jinými metodami (např. metoda "Co se stane, když ..."). [6] [20]

HAZOP – Analýza ohrožení a provozuschopnosti

Metoda HAZOP (Hazard Operation Process) je postup založený na pravděpodobnostním hodnocení ohrožení a z nich plynoucích rizik. Jde o týmovou expertní víceoborovou metodu. Hlavním cílem analýzy je identifikace scénářů potenciálního rizika. Experti pracují na společném zasedání formou brainstormingu. Soustředí se na posouzení rizika a provozní schopnosti systému (operability problems). Pracovním nástrojem jsou tabulkové pracovní výkazy a dohodnuté vodící výrazy (guidewords). Identifikované neplánované nebo nepřijatelné dopady jsou formulovány v závěrečném doporučení, které směřuje ke zlepšení procesu. [6]

Při porovnání s ostatními metodami spočívá základní přínos metody HAZOP především v systematickém a metodicky propracovaném návodu prohlídek, při kterých se příčiny hledají klasickou otázkou: „co mohlo způsobit, že ...?“ a následky obdobnou otázkou „co se stane, když. ... ?“. [20]

Cílem HAZOP studie složitého procesního zařízení je identifikace nebezpečných stavů, která se mohou na zařízení vyskytnout. Postup analýzy zahrnuje tyto kroky:

odhalení příčin – odhad možných následků – návrhy opatření – ocenění [20]

Kvantitativní metody

Kvantitativní metody jsou založeny na matematickém výpočtu rizika z frekvence výskytu hrozby a jejího dopadu. Používají číselné ocenění jak v případě pravděpodobnosti vzniku události (či lépe řečeno incidentu), tak i při ocenění dopadu dané události. Vyjadřují dopad obvykle ve finančních termínech, například „tisíce Kč“. Nejčastěji je riziko vyjádřeno ve formě roční předpokládané ztráty, která je vyjádřena finanční částkou. Kvantitativní metody jsou více exaktní než kvalitativní. Jejich provedení sice vyžaduje více času a úsilí, poskytují však finanční vyjádření rizik, které je pro jejich zvládnutí výhodnější. Nevýhodou kvantitativních metod je kromě jejich náročnosti na provedení a zpracování výsledků často vysoce formalizovaný postup, jenž může vést k tomu, že nebudou postihnuta specifika posuzovaného subjektu, která mohou vést k jeho vysoké zranitelnosti, a to z důvodu „zahlcení“ hodnotitele značným objemem formálně strukturovaných dat. Kvalita výsledků těchto metod úzce souvisí s relevantností získaných údajů. [6] [22]

Kvantitativní metody jsou například:

- FMEA – Analýza příčin a následků poruch
- HRA – Analýza lidské spolehlivosti
- QRA – Analýza kvantitativních rizik procesů
- FTA – Analýza stromu poruchových stavů

FMEA – Analýza příčin a následků poruch

Metoda sestavuje tabulku příčin poruch a jejich následků na systém nebo podnik. FMEA identifikuje jednoduché poruchy, které mohou významně přispívat k havárii, ale nehodí se na vyčerpávající seznam poruch. Je snadno použitelná při změnách a modifikacích procesu. Může být provedena jedním analytikem, ale měla by být zkontrolována jiným. Výsledkem je kvalitativní systematický seznam zařízení, jejich poruch a následků, s možností kvantifikace. Zahrnuje i odhad nejhorších případů následků. Obvykle je dokumentována v tabulkové formě s doporučením pro zlepšení bezpečnosti. [20] [23]

Analýzu příčin a následků poruch je nutné pro maximální efektivnost realizovat v týmové spolupráci s lidmi, kteří jsou z různých úrovní postavení firmy a ideálně i napříč více obory. Není sice nijak složitá, ale vyžaduje relativně veliké zkušenosti, a hlavně perfektní znalost zkoumaného produktu. [23]

Cílem metody je:

- vyhodnocení důsledků a posloupnost úkonů či jevů, které vedou k poruše,
- vyhodnocení závažnosti důsledků poruchy s přihlédnutím na správný výkon funkce,
- zařazení do klasifikace poruch dle podmínek diagnostiky,
- identifikace ukazatelů závažnosti a pravděpodobnosti vzniku poruchy. [23]

Metoda FMEA se hodí pro situace, kde je třeba posoudit specifické komponenty systému, jejichž selhání by mohlo ohrozit fungování celého systému. U velmi složitých systémů s mnoha prvky však použití této metody nedoporučujeme. Analýza FMEA také vyžaduje použití počítače, specializovaného softwaru a specificky zaměřené databáze. [23]

HRA – Analýza lidské spolehlivosti

HRA neboli Human Reliability Analysis je analýza lidské spolehlivosti, která se používá pro hodnocení a posouzení, jaký má člověk, jako pracovník, vliv na výskyt potenciálních rizik, včetně havárií, živelních pohrom, nehod nebo dokonce útoků. Koncept analýzy lidské spolehlivosti HRA směřuje k systematickému posouzení lidského faktoru (Human Factors) a lidské chyby (Human Error). Zahrnuje přístupy mikro ergonomické (vztah „člověk-stroj“) a makro ergonomické (vztah systému „člověk-technologie“). Analýza HRA má těsnou vazbu na aktuálně platné pracovní předpisy především z hlediska bezpečnosti práce. Uplatnění metody HRA musí vždy tvořit integrovaný problém bezpečnosti provozu a lidského faktoru v mezních situacích různých havarijních scénářů, tzn. paralelně a nezávisle s další metodou rizikové analýzy. Metoda je obvykle používána ve spojení s jinými metodami (např. FTA). Výsledky ve formě stromu chyb a úspěchů operátora jsou kvalitativní, ale mohou být kvantifikovány. [20] [23]

Metoda lidské spolehlivosti má za cíl:

- kvantitativně analyzovat lidské jednání a odhalit tak možné chyby,
- odhalit slabá místa systému a tím vytvořit prostor pro relevantní opatření,
- zvýšit poměr spolehlivosti a pohotovosti technického systému v důsledku omezení potenciálních chyb člověka. [23]

QRA – Analýza kvantitativních rizik procesů

Metoda QRA (Process Quantitative Risk Analysis) představuje formální a systematický přístup k odhadu pravděpodobnosti a následků nebezpečných událostí a kvantitativní vyjádření výsledků jako například rizik při práci, životního prostředí, majetků společnosti apod. Analýza QRA rovněž hodnotí robustnost a platnost kvantitativních výsledků tím, že identifikuje kritické předpoklady a prvky řízení rizik. Kvantitativní posuzování rizika je systematický a komplexní přístup pro predikci odhadu četnosti a dopadů nehod pro zařízení nebo provoz systému. Procesní kvantitativní analýza rizika rozšiřuje tradiční kvalitativní (obvykle verbální) hodnocení o numerické hodnoty, přičemž integruje různé známé koncepty a usiluje o stanovení kritérií pro rozhodování, strategie a programy pro efektivní řízení rizik. Tento postup vyžaduje rozsáhlou databázi a podporu specializovaného softwaru.[20] [23]

Cílem analýzy kvantitativních rizik procesu je:

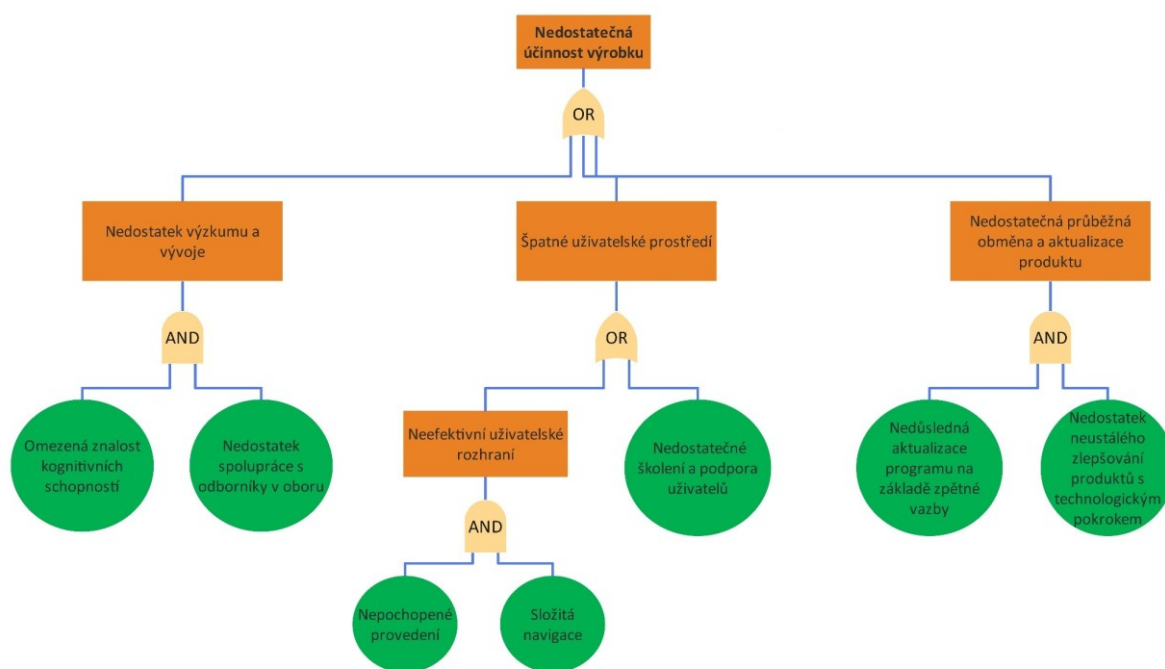
- identifikovat nebezpečí spojená se zařízením,
- určit potenciální frekvence a důsledky zjištěných rizik,
- určit systémovou dostupnost ochranných systémů,
- kvantifikovat rizika spojená se zařízením (např. rizikové obrysy, individuální riziko za rok, potenciální ztráta života apod.). [23]

FTA – Analýza stromu poruchových stavů

Metoda FTA (Fault Tree Analysis) je deduktivní metoda, která vyhledává jednotlivé havárie nebo systémové poruchy a určuje příčiny těchto událostí. FTA je grafický model různých kombinací poruch zařízení a lidských chyb, které mohou vyústit v hlavní systémovou poruchu nazývanou „vrcholová událost“. Dobře se hodí i na rozsáhlé systémy, může stanovit

úplný výčet minimálních poruch. To umožní se zaměřit na preventivní a eliminační opatření, vztahující se na relevantní primární příčiny tak, aby byla minimalizována pravděpodobnost vzniku nehody. Technika FTA je standardizována dle ČSN EN 61025 Analýza stromu poruchových stavů a při její aplikaci se doporučuje uvádět terminologii z této normy. [6] [26]

Model je založen na Booleovské algebře (hradla „a“, „nebo“ a jiné) anglicky – AND a OR, při vyhledávání minimální poruchy vedoucí k vrcholové události. Výsledkem jsou typy poruch a kvantitativně přiřazené pravděpodobnosti poruch systémů, pokud známe pravděpodobnosti primárních příčin. Studii může provádět jeden nebo více analytiků, kteří mohou doporučit bezpečnostní zlepšení procesu. Metoda se nehodí pro rané fáze projektování, je náročná na čas a náročnost se zvyšuje v závislosti na složitosti systému. [6]



Obrázek 3 Ukázka FTA analýzy

(zdroj: vlastní)

Semikvantitativní metoda

Při semikvantitativní metodě jsou ke kvalitativní stupnici přiřazeny odpovídající hodnoty, tzn. bodová škála stupnice (viz Tabulka 1). Cílem je vytvořit širší stupnici hodnocení, než která je obvykle užívána při kvalitativní metodě, ne však navrhnout realistické hodnoty pro výpočet rizika jako tomu je v případě kvantitativní metody. Realizaci semikvantitativní metody je třeba věnovat zvýšenou pozornost, protože vybraná čísla nemusí adekvátně odpovídat skutečnosti, což může vést k rozporupným, odchylujícím se nebo nepřiměřeným výsledkům. Semikvantitativní metoda nemusí správně rozlišit rizika, zvláště když dopad nebo pravděpodobnost dosahují extrémních hodnot. [6]

Tabulka 1 Příklad vyjádření hodnot při jednotlivých typech analýzy rizik

	Kvalitativní metoda	Semikvantitativní metoda	Kvantitativní metoda
Pravděpodobnost výskytu	vysoká	5	90 %
Závažnost dopadu	střední	2,5	100 000,- Kč

(zdroj: vlastní)

Jednoduchá bodová polo-kvantitativní metoda „PNH“

Metoda PNH patří k základním nástrojům pro analýzu rizik. Je vhodná pro situace, kdy nejsou vyžadovány komplexnější techniky, nebo když jsou omezení časová či finanční. Tato polo kvantitativní bodová metoda zahrnuje tři klíčové aspekty: P – pravděpodobnost vzniku, N – pravděpodobnost následků (závažnost) a H – názor hodnotitelů.

Bodování se stanovuje dle individuálních potřeb, přičemž nejběžnější škála má rozmezí od 1 do 5, kde jsou míra, úroveň a kritéria jednotlivých nebezpečí a ohrožení zahrnuty v zjednodušené formě. (viz Tabulka 2) [20] [27]

Když máme jednotlivé kroky obodované tak je mezi sebou vynásobíme dle vzorce:

$$R = P \times N \times H \text{ [20]}$$

Pravděpodobnost vzniku (P) – jedná se o hodnocení pravděpodobnosti, se kterou dané nebezpečí vznikne. Stanovuje se na stupnici 1–5. [20]

Tabulka 2 Pravděpodobnost vzniku rizika

Zanedbatelná	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Téměř jistá	5

(zdroj: [27])

Pravděpodobnost následků (závažnost, N) – stejně jako u pravděpodobnosti vzniku nebezpečí se jedná o hodnocení, které se stanovuje na stupnici 1–5. (viz Tabulka 3) [20]

Tabulka 3 Možné následky ohrožení

Bez následků	1
Mírné následky	2
Významné následky	3
Velmi významné následky	4
Katastrofické následky	5

(zdroj: [27])

Názor hodnotitele (H) – zde je důležité zohlednit míru závažnosti ohrožení, počet ohrožených osob, čas působení ohrožení, stáří a technický stav technologických zařízení, úroveň údržby, kumulace rizik, dynamičnost rizika, možnost zajištění první pomoci, vliv pracovního systému, pracovního prostředí a pracovních podmínek, psychosociální rizikové faktory apod. (viz Tabulka 4) [20] [27]

Tabulka 4 Názor hodnotitelů

Zanedbatelný vliv na míru nebezpečí a ohrožení	1
Malý vliv na míru nebezpečí a ohrožení	2
Větší, zanedbatelný vliv na míru ohrožení a nebezpečí	3
Velký a významný vliv na míru ohrožení a nebezpečí	4
Více významných a nepříznivých vlivů na závažnost a následky ohrožení a nebezpečí	5

(zdroj: [27])

Celkové hodnocení rizika se zjistí následovně: $R = P * N * H$

Tabulka 5 Celkové hodnocení rizika

Rizikový stupeň	R	Míra rizika
I.	>100	Nepřijatelné riziko
II.	51 ÷ 100	Nežádoucí riziko
III.	21 ÷ 50	Mírné riziko
IV.	9 ÷ 20	Akceptovatelné riziko
V.	<8	Bezvýznamné riziko

(zdroj: [27])

Rizikový stupeň

I. - Riziko s katastrofickými následky, které je nepřijatelné a vyžaduje okamžité přerušení činnosti a odstavení z provozu. Provoz může být obnoven až po provedení nezbytných opatření a opětovném posouzení rizik. Práce nesmí být zahájena ani pokračována, dokud nebude riziko sníženo na přijatelnou úroveň. [27]

II. - Nepříjemné riziko, které si vyžaduje rychlé zavedení vhodných bezpečnostních opatření za účelem snížení rizika na přijatelnou úroveň. K zajištění tohoto snížení je nutné vyčlenit odpovídající zdroje. [27]

III. - Jedná se o mírné riziko, u kterého není potřeba okamžitých opatření tak naléhavá jako u rizik kategorie II. Bezpečnostní opatření by měla být obvykle realizována na základě schváleného plánu podle rozhodnutí vedení podniku. Prostředky ke snížení rizika musí být implementovány v určeném časovém rámci. Pokud je toto riziko spojeno s vážnými možnými následky, je nezbytné provést dodatečné hodnocení s cílem přesněji určit pravděpodobnost úrazu a rozhodnout o nutnosti dalších opatření ke snížení rizika. [27]

IV. - Akceptovatelné riziko je takové, které je přijatelné se souhlasem vedení. Při jeho řešení je třeba zvážit náklady na případná opatření nebo zlepšení. Pokud není možné snížit riziko technickými bezpečnostními opatřeními, je nutné zavést vhodná organizační opatření. [27]

V. - Bezvýznamné riziko nevyžaduje žádná zvláštní opatření. Přestože riziko není zcela eliminováno, je nutné na jeho existenci upozornit a specifikovat například vhodná organizační nebo výchovná opatření, která je třeba přijmout.[27]

Shrnutí druhé kapitoly

Druhá kapitola diplomové práce se zabývá analýzou rizik. Tento proces je klíčový pro přípravu efektivních opatření. Díky analýze rizik získáme ucelený pohled na situaci, identifikujeme potenciální hrozby a rizika, kterým je třeba se věnovat a která musí systém efektivně řešit. Analýzy se dělí na dva základní druhy, a to na kvantitativní a kvalitativní. Dále se používají různé kombinované metody anebo metody semikvantitativní, které používají bodovou škálu stupnice a mezi které jsem zahrnul i metodu PNH, poněvadž tato metoda přímo nepatří mezi kvantitativní ani mezi kvalitativní metody. Dále bude tato metoda použita v praktické části této diplomové práce. Kvantitativní nástroje využívají systematický a komplexní přístup, který poskytuje detailnější pohled na situaci prostřednictvím číselných údajů. Mezi vybrané kvantitativní metody se řadí analýza FMEA, HRA, QRA a FTA. Kvalitativní metody využívají slovní proměnné a někdy mohou být jejich výsledky omezené. Proto se často kombinují s kvantitativními metodami, aby se dosáhlo komplexnějšího a robustnějšího poznání. Mezi příklady kvalitativních metod se řadí analýzy jako Bezpečnostní kontrola, SWOT, What If, CLA a HAZOP.

3 VYBRANÉ TEORETICKÉ ASPEKTY ZABEZPEČENÍ ZÁKLADNÍCH ŠKOL

K zajištění ochrany objektu před vniknutím pachatelů se obvykle využívají tradiční technické bezpečnostní systémy společně s režimovými opatřeními. Chráničem proti potenciálnímu útoku nestabilních či agresivních osob nebo dokonce teroristickým hrozbám mohou být sofistikovaná bezpečnostní řešení jako detektory kovů a bezpečnostní rentgeny, která jsou podpořena striktními režimovými pravidly. Tato zařízení jsou účinná proti vniknutí pachatelů s nebezpečnými předměty a zbraněmi, což zvyšuje celkovou bezpečnost školního prostředí. Míra bezpečnosti v základních školách by měla být přizpůsobena podle úrovně kriminality v dané lokalitě.

Je vhodné kategorizovat základní školy podle jejich velikosti, s klíčovým parametrem ve formě počtu žáků, které škola vyučuje. Toto rozdělení pak umožňuje klasifikaci škol do tří skupin: malé, střední a velké školy.

Typicky vesnický charakter má malá škola s počtem žáků nepřesahujícím sto, zahrnující výuku od první až po pátou třídu. Škola obvykle provozuje také školní družinu a mateřskou školu a organizuje sporadické akce jako soutěže nebo karnevaly. Malá škola má tu výhodu jednoduché organizační struktury a díky základním bezpečnostním opatřením je riziko neoprávněného vstupu minimální. Žáci v doprovodu rodinných příslušníků obvykle přicházejí do školy v ranních hodinách, kde u vchodu na ně čeká školník, který dohlíží na vstup a osobně zná všechny žáky i rodiče. Po opuštění budovy všemi osobami se provádí uzamčení školy.

Středně velká základní škola se typicky nachází v menších městech či spádových oblastech a vyučuje mezi sto a čtyři sta žáky. Rozdělení školy zahrnuje první stupeň od prvního do pátého ročníku a druhý stupeň od šestého do devátého ročníku. Součástí jsou mateřská škola a školní družina s omezeným rozsahem aktivit. Velké školy mají více než čtyři sta žáků a nabízejí základní výuku, školní družinu, mateřskou školu a školní jídelnu, která slouží i externím strávníkům. Tyto školy mají komplexní organizaci a pravidelně plánované aktivity.

V případě středně velkých a velkých škol, které se liší od malých škol, není možné, aby školník či jiný zaměstnanec školy poznal všechny studenty. Proto po příchodu žáků do školy dojde k uzamčení hlavního vstupu, a osoba, která si přeje vstoupit do budovy po jejím uzamčení, musí zazvonit a počkat na rozhodnutí školníka nebo administrativního

pracovníka, zda ji do budovy vpustí. Pokud škola poskytuje stravovací služby externím strávníkům, existuje pro tento účel speciální vchod vybavený jednoduchým identifikačním systémem. Tento vchod je vyhrazen pouze pro externí strávníky, kteří jsou opatřeni příslušnými identifikačními kartami nebo čipy. Školní jídelna je od ostatních částí školy oddělena a externím strávníkům není umožněn přístup do jiných prostor. Zabezpečení školy je zajištěno mechanickým ochranným systémem budov na přízemí a vnitřními prostory pomocí systémů PZTS a elektronickým bezpečnostním systémem, který je aktivován, jakmile objekt opustí všichni žáci a zaměstnanci.

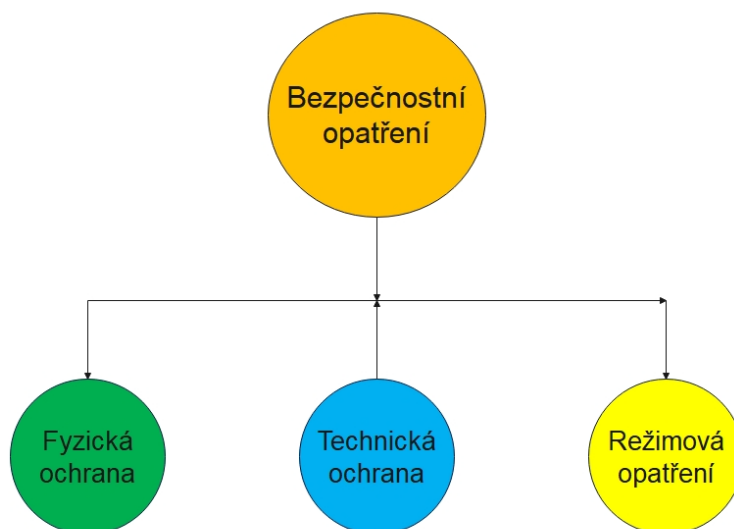
3.1 Typologie ochrany osob a majetku

Bezpečnost subjektu je chápána jako stav, kde rizika plynoucí z hrozeb jsou minimalizována na akceptovatelnou úroveň. Má-li se subjektu zajistit bezpečnost, musí být známy základní hrozby, které mu mohou způsobit újmu. Mezi základní hrozby v současnosti patří činnost kriminálních živlů či jiných osob, jejichž cílem je zcizení, neoprávněné nakládání, poškození nebo úplné zničení chráněných aktiv. Způsob provedení či naplnění hrozby určuje opatření, jimiž se zajišťuje ochrana proti jejich účinku. Ochrana v obecném pojetí představuje proces vytváření bezpečného prostředí pro daný subjekt, popř. podrobněji: proces vytváření stabilního, relativně předvídatelného prostředí, ve kterém může jedinec (skupina) sledovat své cíle bez rušení a ohrožení, bez strachu z vměšování nebo násilí. [28]

Bezpečnostní opatření, realizovaná ve formě systému fyzické bezpečnosti, jsou schopna potenciálního narušitele odradit od jeho činu, zamezit jeho provedení, případně jej zpomalit při zcizení aktiv. [2]

Rozdělujeme tři základní typy ochrany objektů:

- režimová opatření,
- fyzickou ochranu (činnost fyzické ostrahy),
- technickou ochranu (technické prostředky systému fyzické bezpečnosti) [2]



Obrázek 4 Bezpečnostní opatření

(zdroj: vlastní)

Režimová opatření

Režimová opatření představují soubor pravidel a postupů k zajištění požadovaného stupně bezpečnosti na všech úrovních, a to v závislosti na funkcích zabezpečovacích systémů a požadovaných zásadách zejména pro:

- oprávnění osob a dopravních prostředků pro vstup a vjezd do objektu, výstup a výjezd z objektu a způsob kontroly,
- podmínky a způsob kontroly vynášení a vyvážení věcí nebo utajovaných skutečností z objektu,
- režim pohybu osob, věcí, dopravních prostředků a utajovaných skutečností v objektu a jeho jednotlivých částech v pracovní a mimopracovní době,
- režim manipulace s klíči, identifikačními prostředky a médii, které se používají pro systémy zabezpečení vstupů a jimiž se zejména určuje systém a způsob označování, přidělování a odevzdávání klíčů, jejich úschovy a evidence, uložení duplikátů a způsob jejich použití,
- režim manipulace s technickými prostředky a jejich používání. [2] [19]

Režimová opatření by měla být navržena tak, aby příliš neomezovala pohyb osob v objektu organizace a současně zajistila požadovaný stupeň bezpečnosti. Významnou roli v této oblasti sehrává systém kontroly vstupu (přístupový systém). [2]

Fyzická ochrana (činnost fyzické ostrahy)

Fyzická bezpečnost je tradiční a stále nejčastěji využívaným způsobem ochrany majetku a objektů. Různé bezpečnostní incidenty vyžadují v rámci fyzické ochrany různorodé odpovědi. Tyto situace jsou řešeny osoby, které jsou pro tento účel speciálně vyškolené a připravené efektivně zabezpečit chráněná aktiva s minimálními následky. Strážci, kteří poskytují fyzickou ochranu, hrají klíčovou roli v ochraně objektů, buď na stálé nebo dočasné bázi, a jsou schopni v souladu s bezpečnostními opatřeními zajistit ochranu majetku. To obvykle zahrnuje detekci a zadržení případných vetřelců, prevenci krádeže aktiv, implementaci opatření pro případ požáru a havárií atd. Fyzickou ochranu často zajišťují strážníci, hlídači, bezpečnostní agentury nebo policisté. Většina organizací si tuto službu zajišťuje od externích dodavatelů, obvykle soukromých bezpečnostních agentur. Fyzické zajištění ochrany je obvykle finančně nejnáročnějším způsobem zabezpečení. [2] [19]

Technická ochrana (technické prostředky systému fyzické bezpečnosti)

Technická ochrana budov zahrnuje soubor bezpečnostních opatření, která zabraňují, ztěžují nebo signalizují narušení bezpečnosti objektu a chráněné oblasti. Spolu s fyzickou ostrahou tvoří technické prostředky fyzické bezpečnosti klíčová opatření pro ochranu budovy. Cílem těchto prostředků je podporovat režimová opatření, zlepšovat práci fyzické ostrahy a odradit potenciální narušitele, případně výrazně ztížit jejich činnost a prodloužit čas potřebný k přístupu k chráněným aktivům. Základní technické prostředky fyzické bezpečnosti zahrnují mechanické zábranné systémy a elektronické bezpečnostní systémy. Mechanické zábranné systémy, jako jsou dveře, zámky, ploty, mříže a ostnaté dráty, brání fyzickému pohybu narušitelů. Elektronické bezpečnostní systémy se zaměřují na řízení přístupu k aktivům organizace a detekci neoprávněných přístupů. Mezi hlavní elektronické bezpečnostní systémy patří systémy kontroly vstupu, elektronická požární signalizace, kamerové systémy a poplachové zabezpečovací systémy. [2] [19]

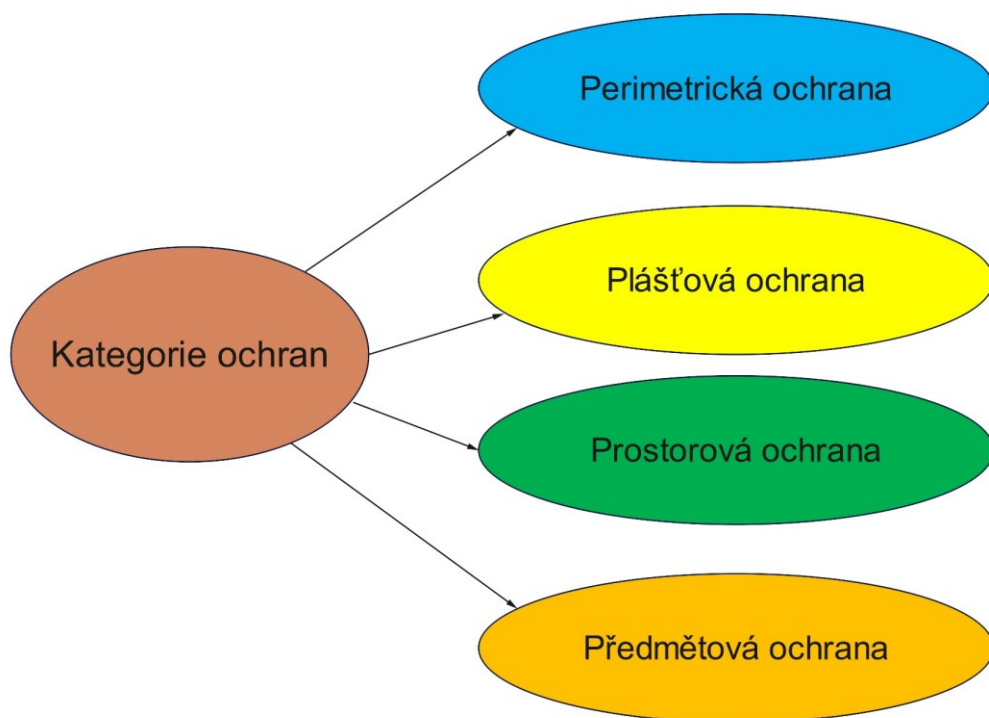
3.2 Rozdělení typu ochran dle bezpečnostního systému

Optimalizace bezpečnostního systému objektu vede k definování principů, které jsou aplikovány při jeho návrhu a realizaci. Jedním z těchto principů je princip víceúrovňové ochrany. Tento princip spočívá v tom, že zajištění fyzické bezpečnosti se rozděluje do několika úrovní, které představují určité bariéry, oblasti nebo domény, jež musí narušitel překonat na své cestě k cílovému objektu. [2] [6]

Základní kategorie ochran jsou:

- perimetrická ochrana,
- plášťová ochrana,
- prostorová ochrana,
- předmětová ochrana.

Každý z výše zmíněných kategorií ochrany má své specifické vlastnosti, které vyplývají z jeho účelu, pořadí a prostorového uspořádání. Technické prostředky použité k zajištění této ochrany musí splňovat určité požadavky. Pokud jde o detektory narušení, je důležité zohlednit typ sledovaných příznaků narušitele, tvar a dosah detekční charakteristiky, stejně jako citlivost a odolnost vůči falešným poplachům. [2] [6]



Obrázek 5 Kategorie ochran

(zdroj: vlastní)

Perimetrická ochrana

Perimetrická ochrana zahrnuje soubor bezpečnostních opatření fyzické ochrany, která se uplatňují na hranici pozemku chráněného objektu a v prostoru mezi touto hranicí a samotnou budovou. Perimetr neboli obvod objektu, je definován katastrální hranicí, která může být vymezena přirozenými nebo umělými překážkami, jako jsou ploty, zdi či vodní toky. Hlavním cílem perimetrické ochrany je odradit, odhalit a zpomalit pohyb narušitele. Tato ochrana by měla zajistit včasné varování při narušení obvodu objektu. Detekční systémy používané v perimetrické ochraně jsou zpravidla navrženy s delším dosahem a užší detekční charakteristikou. Musí být odolné vůči nepříznivým klimatickým podmínkám a zároveň minimalizovat riziko falešných poplachů. Nicméně, vzhledem k různorodému venkovnímu prostředí a široké škále pohybujících se objektů zůstává eliminace planých poplachů jednou z hlavních výzev. V současné době se perimetrická ochrana vyvíjí jako samostatná oblast technické bezpečnosti. Výrobci se zaměřují na inovaci a zavádění pokročilých technologií, které umožňují komplexní zajištění obvodové ochrany. [29] [3]



Obrázek 6 Perimetrická ochrana

(zdroj: [30])

Plášťová ochrana

Plášťová ochrana zahrnuje soubor bezpečnostních opatření fyzické ochrany, která se aplikují na vnější obálku chráněného objektu, obvykle budovy. Jejím hlavním účelem je odradit, zabránit průniku, zpomalit a odhalit narušitele. Plášťová ochrana slouží k detekci narušení konstrukce budovy. Mezi prvky plášťové ochrany patří stěny, okna, dveře, zámky a jejich systémy, mříže, bezpečnostní fólie, kamerové systémy či detektory narušení. Tyto detekční prvky bývají zpravidla instalovány uvnitř budovy. Detektory narušení mají plošnou, ale širší detekční charakteristiku s kratším dosahem. Pokud jsou umístěny vně budovy, musí splňovat požadavky na zvýšenou odolnost vůči klimatickým vlivům. [29] [3]



Obrázek 7 Plášťová ochrana – vytvořená podle AI

(zdroj: [31])

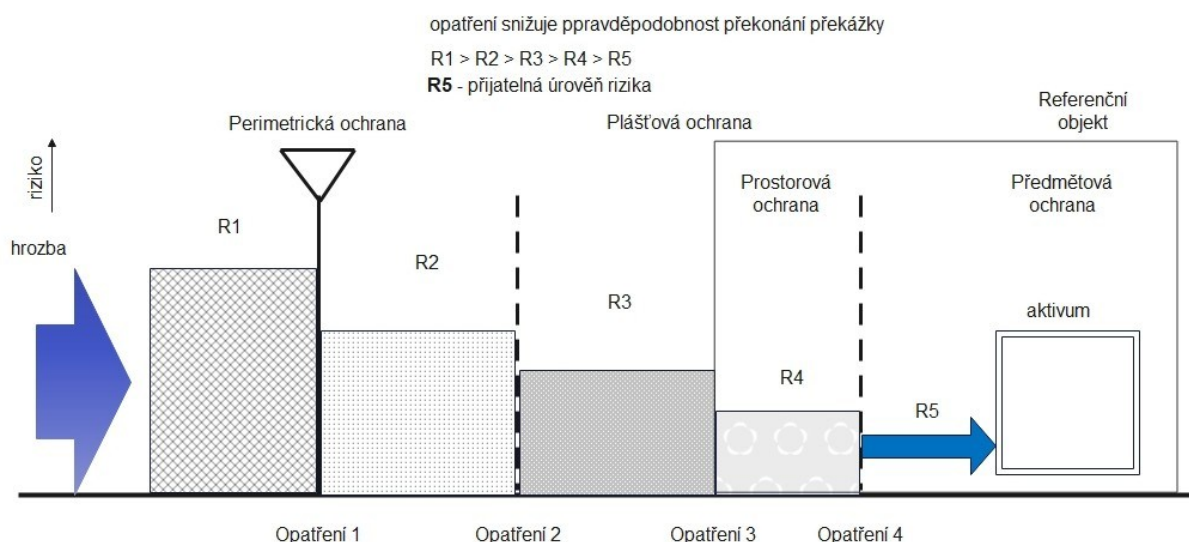
Prostorová ochrana

Hlavním účelem prostorové ochrany je zpomalit a odhalit pohyb narušitele uvnitř střežené budovy. Tato bezpečnostní opatření jsou implementována v interiéru objektu, nejčastěji na chodbách, schodištích a v jednotlivých místnostech. Prostorová ochrana zahrnuje prvky jako dveře, mříže, zámky a jejich systémy, kamerové systémy, přístupové kontrolní systémy a poplachové zabezpečovací systémy s detektory narušení. Tyto detektory by měly spolehlivě signalizovat neoprávněný vstup do vnitřních prostor budovy. Obvykle mají detektory kratší

dosah a širší kuželovou detekční charakteristiku. Jejich konstrukce musí odpovídat požadavkům na provoz v interiérovém prostředí. [29] [3]

Předmětová ochrana

Předmětová ochrana zahrnuje opatření zaměřená na prevenci odcizení a neoprávněné manipulace s chráněnými aktivy. Mezi tyto aktiva patří finanční prostředky, cennosti, utajované informace či technická zařízení s citlivým charakterem. K zajištění předmětové ochrany se využívají vitríny, skleněné tabule, kamerové systémy a poplachová zabezpečovací zařízení. Detektory narušení slouží k identifikaci přítomnosti neoprávněné osoby v bezprostřední blízkosti chráněného objektu nebo jakékoliv manipulace s ním. Detektory určené k monitorování pohybu narušitelů mívají širokoúhlý a plošný detekční rozsah s krátkým dosahem. Úroveň ochrany by měla být přiměřená hodnotě chráněných aktiv a požadovanému stupni zabezpečení. Investice do bezpečnostních opatření by neměly převyšovat hodnotu samotných aktiv. Navíc by úroveň zabezpečení měla odpovídat schopnostem potenciálního narušitele. [29] [3]



Obrázek 8 Bezpečnost objektu podle stupně ochran

(zdroj: vlastní)

3.3 Rizika a stupně zabezpečení objektu

Každý objekt je při realizaci jeho zabezpečení nutné posuzovat nejen z hlediska míry rizika, ale také s ohledem na prostředí, ve kterém se nachází. Toto hledisko představuje základní výchozí bod pro bezpečnostní posouzení konkrétního objektu. Evropská norma ČSN EN 50131-1 ED.2 definuje pět stupňů zabezpečení (viz Tabulka č. 6) a klasifikaci chráněných objektů z hlediska prostředí (viz Tabulka č.7). Tyto klasifikace jsou klíčové pro správný výběr prvků, které budou v daném prostředí fungovat. Zároveň ovlivňují nastavení jednotlivých pojistek i výši pojistných částek. Norma stanovuje systémové požadavky na poplachové zabezpečovací a tísňové systémy, přičemž specifikuje požadavky na jejich provedení a vlastnosti. Neobsahuje však specifikace pro návrh, projekci, instalaci, provoz a údržbu – tyto aspekty jsou upraveny normou ČSN CLC/TS 50131-7. Systémové požadavky této normy se vztahují na poplachové zabezpečovací a tísňové systémy, které sdílejí prostředky pro detekci, vzájemné propojení, ovládání, komunikaci a napájení s jinými systémy. Přestože norma stanovuje stupně zabezpečení a třídy prostředí, neuvádí konkrétní požadavky na jednotlivé komponenty těchto systémů. [29] [32]

Tabulka 6 Úroveň rizika a stupeň zabezpečení

Úroveň zabezpečení	Úroveň rizika	Preventivní opatření
1	velmi nízké	Jednoduché mechanické zabezpečení
2	nízké	Zvýšené mechanické zabezpečení
3	střední	Zvýšené mechanické zabezpečení a minimální elektronické zabezpečení
4	vysoké	Rozsáhlé mechanické zabezpečení a střední elektronické zabezpečení
5	velmi vysoké	Rozsáhlé mechanické zabezpečení a vysoké elektronické zabezpečení

(zdroj: vlastní)

Tabulka 7 Rozdělení chráněných objektů z hlediska prostředí

Třída zařízení	Definice prostředí
I.	Vnitřní (s omezením na prostředí obytných nebo kancelářských prostorů)
II.	Všeobecné vnitřní (například prodejní prostory, obchody, restaurace, schodiště, výrobní a montážní prostory a sklady)
III.	Venkovní (chráněné proti přímému dešti a slunci, nebo vnitřní s extrémními podmínkami okolního prostředí)
IV.	Všeobecné venkovní (nechráněné proti povětrnostním podmínkám)

(zdroj: vlastní)

Shrnutí třetí kapitoly

Třetí kapitola diplomové práce se zabývá teoretickými aspekty k zabezpečení základních škol, které se liší podle jejich velikosti a míry rizika v dané lokalitě. Malé školy, obvykle vesnického charakteru, mají jednodušší organizační strukturu a bezpečnostní opatření, často postačí školník, který zná všechny žáky a rodiče a kontroluje vstup. U středních a velkých škol, kde to již není možné, se využívají sofistikovanější systémy, jako je uzamykání hlavního vstupu, elektronická kontrola přístupu nebo identifikační systémy pro externí strávníky. Ochrana objektů se dělí na režimová opatření, fyzickou ochranu a technickou ochranu. Režimová opatření stanovují pravidla pro vstup, pohyb osob či manipulaci s klíči. Fyzická ochrana zahrnuje přítomnost ostrahy, která reaguje na krizové situace. Technická ochrana spočívá v elektronických a mechanických bezpečnostních systémech, jako jsou zámky, kamerové systémy nebo alarmy. Pro zajištění maximální ochrany se bezpečnostní opatření dělí do čtyř stupňů – perimetrická ochrana zajišťuje bezpečnost na hranici pozemku, plášťová ochrana se soustředí na samotnou budovu, prostorová ochrana monitoruje vnitřní prostory a předmětová ochrana chrání cenné nebo citlivé objekty. Celkově je důležité, aby zabezpečení školního prostředí bylo komplexní a kombinovalo mechanická, elektronická a organizační opatření.

4 VYBRANÉ SYSTÉMY TECHNICKÉ OCHRANY ZÁKLADNÍCH ŠKOL

Moderní bezpečnostní systémy se stále více propojují do jednotných integrovaných řešení, která umožňují jejich centrální správu a monitoring. Díky softwarové analýze mohou bezpečnostní pracovníci efektivněji vyhodnocovat rizika, reagovat na incidenty v reálném čase a mít kompletní přehled o dění v objektu. Tato řešení se často propojují s pulty centrální ochrany, kde bezpečnostní agentury nebo složky integrovaného záchranného systému (hasiči, policie, záchranná služba) mohou v případě nouze okamžitě zasáhnout. Díky moderním technologiím je dnes možné všechny tyto systémy integrovat do jednoho celku, což výrazně zvyšuje jejich efektivitu a umožňuje snadnější správu bezpečnosti v jakémkoli prostředí. Integrace zabezpečovacích systémů představuje moderní přístup k využití technologických možností různých bezpečnostních prvků, jako jsou zabezpečovací, kamerové, přístupové a tísňové systémy, včetně systémů přivolání pomoci. Tyto aplikace lze vzájemně propojit nebo rozšířit o nepoplachové systémy, čímž se umožní efektivní automatizace procesů v jakémkoliv objektu, který je zapotřebí zabezpečit. Zabezpečení základních škol je zásadním aspektem ochrany žáků, pedagogů i majetku. Vzhledem k rostoucím bezpečnostním rizikům je nutné kombinovat mechanická, elektronická a organizační opatření, která minimalizují hrozby neoprávněného vstupu, vandalismu nebo jiných incidentů.

Mezi vybrané technické systémy fyzické ochrany řadíme:

- mechanické zábranné systémy (MZS),
- dohledové video systémy (DV),
- elektrická požární signalizace (EPS),
- poplachové zabezpečovací a tísňové systémy (PZTS). [19][33]

4.1 Mechanické zábranné systémy

Mechanické zábranné systémy (MZS) považujeme za základní prvek ochrany objektů a osob v průmyslu komerční bezpečnosti. Pod mechanické zábranné systémy řadíme veškeré mechanické prvky, které stěžují násilné vniknutí nepovolané osoby do chráněné zóny nebo objektu především přes oplocení nebo cestou dveřních nebo okenních otvorů, případně

manipulací nepovolané osoby s chráněnými předměty v zabezpečeném objektu. Z tohoto důvodu můžeme říct, že mechanické zábranné systémy jsou základním pilířem pro komplexní zabezpečení bytových i nebytových objektů. [6]

Kromě tradičních mechanických zabezpečovacích prvků, jako jsou bezpečnostní dveře, zámky, rolety, mříže a bezpečnostní skla, patří do kategorie klasické ochrany také vjezdové závory, automatická vrata, bariéry proti vozidlům, osobní turnikety, propouštěcí branky a oplocení. Mechanickou ochranu tvoří rovněž některé konstrukční prvky budov, které již svou povahou představují fyzickou překážku proti neoprávněnému vniknutí. Mezi ně se řadí například dveřní, okenní a balkonové výplně, obvodové zdi, stropy, podlahy a střechy přízemních objektů, zejména tam, kde střecha zároveň slouží jako hlavní nosná konstrukce. Mechanické zábranné prostředky však samy o sobě nedokážou zajistit absolutní ochranu objektu. Jejich účinnost závisí především na materiálu, z něhož jsou vyrobeny, jeho pevnosti, tloušťce a dalších fyzikálních vlastnostech. Proto se při jejich hodnocení používá tzv. zpoždovací faktor, který určuje, jak dlouho je daný prvek schopen odolávat pokusu o překonání za použití běžně dostupných metod a nástrojů. Tento časový interval hraje klíčovou roli v bezpečnostní strategii, protože poskytuje pracovníkům fyzické ostrahy dostatek času k adekvátní reakci a provedení účinného zásahu proti narušiteli. [19]

Výraz zní následovně:

$$\Delta t = t_2 - t_1 \text{ [min]} \quad [29]$$

kde jsou následující parametry:

Δt – je časový interval potřebný k překonání překážky

t_1 – je čas zahájení útoku na překážku

t_2 – je čas konečného překonání překážky

Mechanické zábranné systémy můžeme rozdělit na:

- obvodová ochrana,
- plášťová ochrana,
- předmětová ochrana. [29] [34]

Obvodová ochrana

Obvodová ochrana zahrnuje opatření sloužící k zabezpečení vymezeného území a okolního prostoru chráněného objektu. Obvod objektu je definován jeho katastrálními hranicemi, které jsou obvykle vymezeny přírodními nebo umělými překážkami, jako jsou vodní toky, ploty či zdi. Na přilehlých pozemcích se k ochraně primárně využívají mechanické zábrany speciálně navržené pro tento účel. [29]

Plášťová ochrana

Plášťová ochrana slouží k zabránění jakéhokoli narušení standardních i nestandardních vstupních bodů objektu. Zahrnuje zabezpečení všech stavebních otvorů, jako jsou dveře, okna, balkonová okna, sklepní okna, vikýře či zásobovací a energetické šachty. Někdy je označována také jako objektová ochrana. Tento typ zabezpečení se zaměřuje na ochranu vnějšího pláště budovy nebo chráněného objektu. Detekční systém je umístěn přímo na budově, což umožňuje rychlejší reakci na případné narušení ještě předtím, než by útočník pronikl dovnitř. [29]

Předmětová ochrana

Předmětová ochrana slouží k zabezpečení prostor nebo úschovných míst, kde se uchovávají peníze, cennosti, utajované informace či technická zařízení s citlivým charakterem. Jejím cílem je zabránit krádeži nebo neoprávněné manipulaci. Do této kategorie ochrany spadají, jak menší úložné prvky, například pokladničky a pokladny, tak i robustnější zabezpečovací systémy, jako jsou trezorové skříně a komorové trezory. [29]

4.2 Dohledové video systémy

Dohledové video systémy (Video Surveillance System, VSS) jsou systémy zahrnující kamerová zařízení, úložné jednotky, monitorovací vybavení a související technologie pro přenos obrazu a jeho ovládání. V bezpečnostních aplikacích slouží k identifikaci, rozpoznávání, detekci a monitorování zájmových oblastí ve sledovaném prostoru. Dynamický rozvoj informačních a komunikačních technologií (ICT) usnadňuje integraci těchto systémů do stále širšího spektra praktických aplikací. Moderní VSS umožňují získávání sémantické informace z videosekvencí, což otevírá cestu k autonomním inteligentním systémům nové generace. [4] [6]

Původně používaný termín CCTV systémy byl definován podobně jako systémy sestávající z kamerového zařízení, monitorovacích prvků a přidružených zařízení sloužících k přenosu a řízení obrazu. V bezpečnostních aplikacích se jednalo o systémy určené k dohledu nad chráněným prostorem. V současné terminologii se upřednostňuje širší pojem dohledové video systémy (VSS), přičemž CCTV systémy jsou nyní vnímány jako jedna ze součástí této obecnější kategorie. [4] [6]

Uzavřený televizní okruh je systém umožňující monitorování vybraných oblastí střeženého prostoru s možností ukládání a následného zpracování záznamu. Díky strategicky rozmístěným kamerám lze efektivně sledovat různé aktivity, včetně pohybu osob, vozidel či výrobků. Základním prvkem systému je kamera s odpovídajícím objektivem, který určuje šířku záběru a umožňuje zvolit mezi detailním snímáním nebo širším přehledem sledované scény. Pokud je požadována možnost zpětného přehrávání, je nutné systém doplnit o záznamové zařízení určené k archivaci a následné analýze zaznamenaných událostí. Funkce exportu na externí média umožňuje přenos záznamů mimo objekt. Moderní kamerové systémy umožňují, za určitých podmínek, nejen vzdálený přístup k uloženým záznamům, ale i přímé připojení k systému odkudkoliv na světě, kde je dostupné internetové připojení. Sledování může probíhat prostřednictvím mobilního telefonu, tabletu nebo počítače. [35]

Kamerové systémy jsou členěny podle způsobu přenosu signálu:

- analogové,
- digitální,
- hybridní [36]

Analogové kamerové systémy

Signál z kamery je přenášen v analogové podobě prostřednictvím konektorů, jako jsou BNC nebo cinch. Nejčastěji se k přenosu používají koaxiální kabely zakončené BNC konektory. Jejich nevýhodou je omezená maximální délka přenosu, která činí přibližně 100 metrů. Analogové kamerové systémy využívají analogový videosignál, přičemž jejich základním prvkem je kamera s analogovým výstupem. Tento typ technologie nepřenáší obraz jako celek, ale postupně jej přenáší podle normy určující formát videa. Mezi nejrozšířenější televizní normy pro přenos analogového videosignálu patří **PAL, NTSC a SECAM**. [37]

Analogový kamerový systém se síťovým DVR (Digital Video Recorder) kombinuje tradiční analogové kamery s moderními digitálními technologiemi. Umožňuje propojení analogových kamer s DVR rekordérem, který podporuje síťové připojení a vzdálený přístup přes internet nebo lokální síť.

Digitální kamerové systémy

Tyto systémy v zásadě nemají žádné teoretické omezení maximálního rozlišení obrazu z kamer. Výsledná kvalita obrazu je určena především použitou kamerou, kapacitou záznamového zařízení a propustností datové sítě. Digitální kamerové systémy využívají standardní přenosový protokol TCP/IP, což umožňuje jejich integraci do běžných ethernetových sítí. Kamery určené pro tento typ přenosu, známé jako IP kamery (webkamery), obsahují vestavěný video server s klasickým LAN výstupem. Na rozdíl od analogových systémů digitální kamerové systémy pracují na principu číslicového zpracování signálu. Obraz není přenášen řádkově, ale jako celek ve formě datových paketů, což zajišťuje vyšší kvalitu a stabilitu přenosu. Pro distribuci digitálního videa se využívá běžná síťová infrastruktura, což umožňuje snadnou rozšiřitelnost a vzdálený přístup. [36] [37]

Hybridní kamerové systémy

Hybridní kamerové systémy představují kombinaci analogových a digitálních (IP) kamer v jednom dohledovém systému. Umožňují postupnou modernizaci starších analogových systémů bez nutnosti okamžité výměny veškeré infrastruktury. Důvodem vytváření hybridního systému je rozšíření stávajícího (funkčního a vyhovujícího) o další kamery. Ty už se použijí digitální. [37]

4.3 Elektrická požární signalizace

Elektrická požární signalizace (EPS) je systém určený k včasné detekci a případné prevenci vzniku požáru. Tyto systémy nacházejí široké uplatnění v průmyslových objektech, obchodních centrech, administrativních budovách i obytných domech. EPS funguje jako plně automatizovaný systém, který nejen upozorňuje osoby v ohrožené oblasti, ale také aktivuje hasicí zařízení, například sprinklery, a pomáhá zajistit bezpečné únikové cesty. Jeho klíčovou funkcí je rovněž automatické přivolání hasičského záchranného sboru (HZS). [3][7]

Tento systém lze definovat jako soustavu vzájemně propojených prvků, které přesně identifikují místo požáru a předávají tuto informaci dalším složkám pro co nejrychlejší reakci. Spolehlivost EPS hraje zásadní roli nejen v protipožární ochraně, ale také při hašení požáru a bezpečné evakuaci osob. [3] [7]

Rozlišujeme několik druhů EPS:

- a) jednostupňové EPS – mají jednu nebo více hlavních ústředn, na které jsou připojeny samočinné a tlačítkové hlásiče požáru; na ústřednu jsou napojena ovládací a doplňující zařízení; jednostupňové EPS nemají vedlejší ústřednu, [19]
- b) vícestupňové EPS – mají hlavní a vedlejší ústředny, na které jsou připojeny samočinné a tlačítkové hlásiče požáru a vedlejší ústředny nižšího stupně, [19]
- c) EPS s kolektivní adresací – u systému EPS s kolektivní adresací je sice ústředna schopna rozlišit, z které hlásící linky přišel signál POŽÁR, ale nezjistí, od kterého konkrétního hlásiče; vzniká tak problém s určením místa vzniku požáru, [38]
- d) EPS s individuální adresací – tento systém umožňuje identifikaci stavu jednotlivých hlásičů na hlásící lince, a to tím, že prvky komunikují vzájemně mezi sebou, je tak možné rychle odhalit prvek, který hlásí požár. [38]

Základní konfigurace systému EPS je tvořena:

- ústřednou EPS,
- hlásiči požáru,
- signalizačními a doplňujícími zařízeními EPS.

Ústředna EPS

Ústředna EPS je zařízení, které přijímá a vyhodnocuje výstupní elektrické signály hlásičů, signalizuje a vysílá informace o vlastním provozním stavu, ovládá doplňující zařízení EPS a přímo či nepřímo ovládá zařízení bránící rozšíření požáru, popř. zařízení provádějící samočinně protipožární zásah. Mezi běžné funkce ústředn EPS patří i návaznost na centrální ozvučovací systém budovy, klimatizaci, požární odvětrávání, výtahy, únikové východy apod. [19]

Hlavním úkolem ústředny EPS jsou tři základní stavy: PROVOZ, PORUCHA, POŽÁR. Ústředna EPS může požár signalizovat různě. Jendou z možností je, že ho bude

signalizovat obsluhu, signalizovat objektu nebo jen jeho části. Signalizace požáru tak může být jednostupňová nebo dvoustupňová. [38]

Hlásiče požáru

Hlásiče požáru jsou zařízení, které reakcí na daný signál vytváří výstupní elektrický signál, a to buď samočinně, nebo jsou uvedeny do činnosti osobou.

Dělíme je na:

- tlačítkové hlásiče
- samočinné hlásiče

U **tlačítkových hlásičů** vyhodnocuje změnu fyzikálních parametrů člověk, která nastalé změny vyhodnocuje a musí stisknout tlačítko hlásiče, který poté předá údaj do ústředny EPS. Oproti tomu **samočinné hlásiče** reagují na výskyt nebo změnu fyzikálních parametrů požáru bez nutnosti zásahu člověka. [38]

Doplňující zařízení EPS

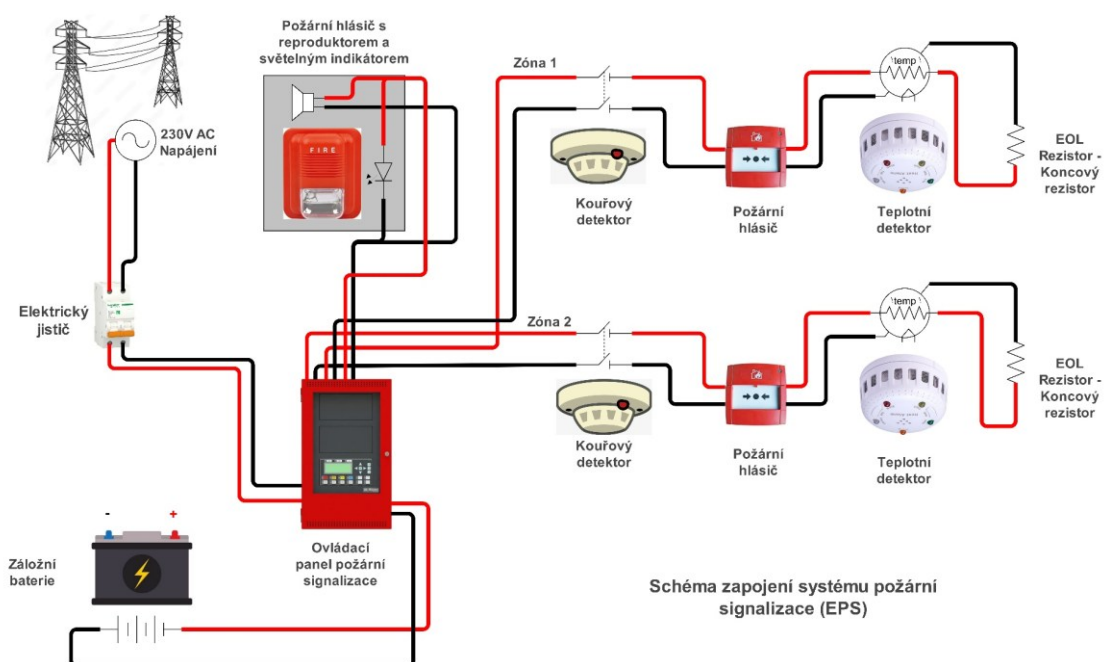
ZDP – zařízení dálkového přenosu, zajišťuje přenos alespoň základních provozních stavů **POŽÁR** a **PORUCHA** na stanovené místo, obvykle na ohlašovnu požárů. Přenos funguje nezávisle na přítomnosti obsluhy a zůstává aktivní i v případě jejího selhání. [38] [19]

OPPO – obslužná pole požární ochrany, pro usnadnění obsluhy ústředny EPS jednotkou PO v případě požáru signalizovaného EPS. [19]

KTPO – klíčový trezor požární ochrany, pro usnadnění vstupu jednotky do objektu, ve kterém je uložen klíč od objektu. [19]

ZOKT – zařízení pro odvod kouře a tepla, je zařízení umožňující automaticky nebo ručně (pomocí tlačítka) otevřít střešní okno, které plní funkci kouřové klapky a odvést tak mimo prostory kouř, plyny a teplo vznikající při požáru. [19]

Protipožární únikové dveře jsou vyráběny ze speciálních dveřních profilů s utěsněním proti prachu, hluku a úniku tepla. Dveře jsou napojeny na EPS a při požáru se samy otevřou. [19]



Obrázek 9 Ukázka – schéma zapojení systému EPS

(zdroj: vlastní)

4.4 Poplachové zabezpečovací a tísňové systémy

Poplachový zabezpečovací a tísňový systém (PZTS), dříve známý jako elektrická zabezpečovací signalizace (EVS), je komplexní soubor technických prostředků sloužících k ochraně objektů před neoprávněným vstupem. Jakmile dojde k pokusu o vniknutí nepovolané osoby, systém jej včas detekuje a spustí výstražnou signalizaci, čímž pomáhá minimalizovat potenciální škody. [19]

PZTS se skládá z ústředny, ovládací klávesnice, detektorů a koncových zařízení. Může být instalován jako samostatný systém nebo integrován do širšího bezpečnostního řešení zahrnujícího například kamerové systémy (VSS), požární signalizaci (EPS) či mechanické zábranné systémy (MZS). Výstražný mechanismus se aktivuje buď analogovou metodou (např. přerušením kabelu), nebo digitálně prostřednictvím pohybových detektorů (např. PIR senzorů). Detektory komunikují s ústřednou kabelově, bezdrátově nebo kombinací obou technologií. [19] [39]

Systém PZTS zajišťuje ochranu okolí objektu, pláště budovy (okna, dveře) i vnitřních prostor. K tomu využívá různé typy senzorů – pohybové detektory, magnetické kontakty pro

dveře a okna a další zabezpečovací prvky. V případě narušení střeženého prostoru se spustí výstražná signalizace prostřednictvím vnitřní a vnější sirény s majákem. Systém také umožňuje automatické odesílání poplachových zpráv na předem definovaná telefonní čísla nebo na dohledová a poplachová přijímací centra. Kromě detekce neoprávněného vniknutí reaguje také na pokusy o poškození jednotlivých senzorů či narušení prostředí silným zářením.[19] [33]

Systém PZTS se může skládat z:

- ústředny,
- ovládacích zařízení,
- komunikátor,
- detektory – snímače,
- zdroje energie
- výstupních prvků,

Ústředna PZTS

Poplachové zabezpečovací systémy jsou zpravidla složeny z ústředny, optických a akustických výstražných prvků, detektorů narušení a přímých spojů, zajišťujících připojení detektorů do ústředny. Ústředna zajišťuje příjem poplachů z jednotlivých detektorů narušení, jejich zaznamenání, vyhodnocení a vyhlášení poplachu – nejčastěji to bývá akustická signalizace – siréna. [3]

Ústředna představuje centrální řídicí jednotku celého zabezpečovacího systému, která zajišťuje nepřetržitý sběr, vyhodnocování a zpracování informací z připojených detektorů, senzorů a ovládacích prvků. Funguje jako hlavní mozek systému, který efektivně řídí veškerou komunikaci mezi jednotlivými komponenty. Toto propojení může být realizováno kabelově, bezdrátově nebo jejich kombinací, přičemž každý způsob přenosu signálu má své výhody – drátové připojení vyniká stabilitou a odolností vůči rušení, zatímco bezdrátové řešení nabízí flexibilitu a snadnou instalaci bez nutnosti složitých stavebních úprav. Ústředna poplachového zabezpečovacího systému může být připojena prostřednictvím poplachového přenosového systému na poplachové přijímací centrum (pult centralizované ochrany). [39]

Zařízení pro ovládání

Ovladač je důležitou součástí zabezpečovacího systému, která slouží nejen k jeho ovládání, ale často i k programování ústředny. Moderní alarmy lze řídit různými způsoby, přičemž nejběžnější variantou je klávesnice s LCD displejem, která uživateli poskytuje plnohodnotný přístup k nastavení systému. Další běžnou metodou ovládání jsou RFID čtečky podporující různé identifikační prvky, jako jsou kontaktní a bezkontaktní čipy, karty, přívěšky či klíčenky. Populární je také dálkové ovládání, které umožňuje pohodlnou aktivaci a deaktivaci systému na dálku. V současnosti nabývají na významu biometrické čtečky otisků prstů, které často fungují v kombinaci s klávesnicí. Tento způsob ověření je velmi efektivní, protože umožňuje dvojitou identifikaci – nejen pomocí otisku prstu, ale také prostřednictvím zadaného PIN kódu. Další možností ovládání je přístup přes internet, obvykle prostřednictvím integrovaného webového rozhraní, ke kterému se uživatel připojí po zadání přihlašovacích údajů. K dispozici je také mobilní ovládání, a to buď prostřednictvím SMS příkazů nebo hlasových hovorů, což umožňuje flexibilní správu systému odkudkoli. [3] [39]

Komunikátor

Komunikátor je klíčovým prvkem zabezpečovacího systému, který zajišťuje přenos informací mimo chráněný objekt. Jeho hlavním úkolem je hlásit narušení objektu nebo upozorňovat na jakékoli odchylky od běžného provozního stavu systému. Informace o stavu zabezpečení jsou předávány různými způsoby, například SMS zprávami, hlasovými hovory nebo odesíláním fotografií pořízených integrovanými detektory. Důležitou funkcí komunikátoru je také možnost připojení k pultu centralizované ochrany (PCO), který umožňuje okamžitou reakci bezpečnostních složek i bez zásahu majitele, správce či jiné oprávněné osoby. [3] [39]

Zajištění spolehlivého přenosu informací

Pro dosažení vysoké spolehlivosti přenosu se běžně využívá kombinace alespoň dvou přenosových kanálů. Často jsou objekty primárně připojeny přes internet, který umožňuje rychlý a cenově dostupný přenos dat, a zároveň jsou vybaveny GSM modulem jako záložním řešením pro případ výpadku internetového spojení. Mnoho výrobců poplachových zabezpečovacích a tísňových systémů (PZTS) reaguje na potřeby uživatelů a integruje GSM komunikátory přímo do základní desky ústředny. Tyto moderní systémy umožňují kompletní správu a ovládání zabezpečení prostřednictvím mobilního telefonu, což zajišťuje uživatelům maximální kontrolu a pohodlí. [3] [39]

Dálkový přístup pro koncového uživatele

Koncový uživatel může ke svému bezpečnostnímu systému přistupovat online, a to pomocí internetu či mobilní aplikace, kde může provést kontrolu stavu systému, upravit nastavení nebo reagovat na poplachové události. Tím získává neustálý přehled o bezpečnosti svého objektu odkudkoli na světě. [3] [39]

Nejčastější typ komunikátoru, který se v současné době používá, je

- **Telefonní komunikátor (PSTN)** – hlášení z objektu jsou přenášeny pevnou telefonní sítí.
- **GSM komunikátor** – přenos dat je uskutečněn pomocí GSM sítě – hovorové pásmo nebo formou SMS.
- **LAN komunikátor** – TCP/IP – oznámení neboli data se z PZTS přenášejí prostřednictvím LAN sítě – přes internet.
- **Rádiové komunikátory** – využívající rádiové sítě s vyhrazenou frekvencí. [3][39]

Detektory – snímače

Detektory, známé také jako bezpečnostní čidla, tvoří zásadní součást poplachových zabezpečovacích a tísňových systémů (PZTS). Jejich hlavním úkolem je monitorovat chráněný prostor a detekovat nežádoucí události, jako je neoprávněný vstup, rozbití skla, vibrace či změny teploty. Jakmile detektor zaznamená narušení, přenese informaci do ústředny, která situaci vyhodnotí a spustí odpovídající reakci – například aktivaci sirény, odeslání poplachové zprávy na mobilní telefon nebo přenos informace na pult centralizované ochrany (PCO). [19] [39]

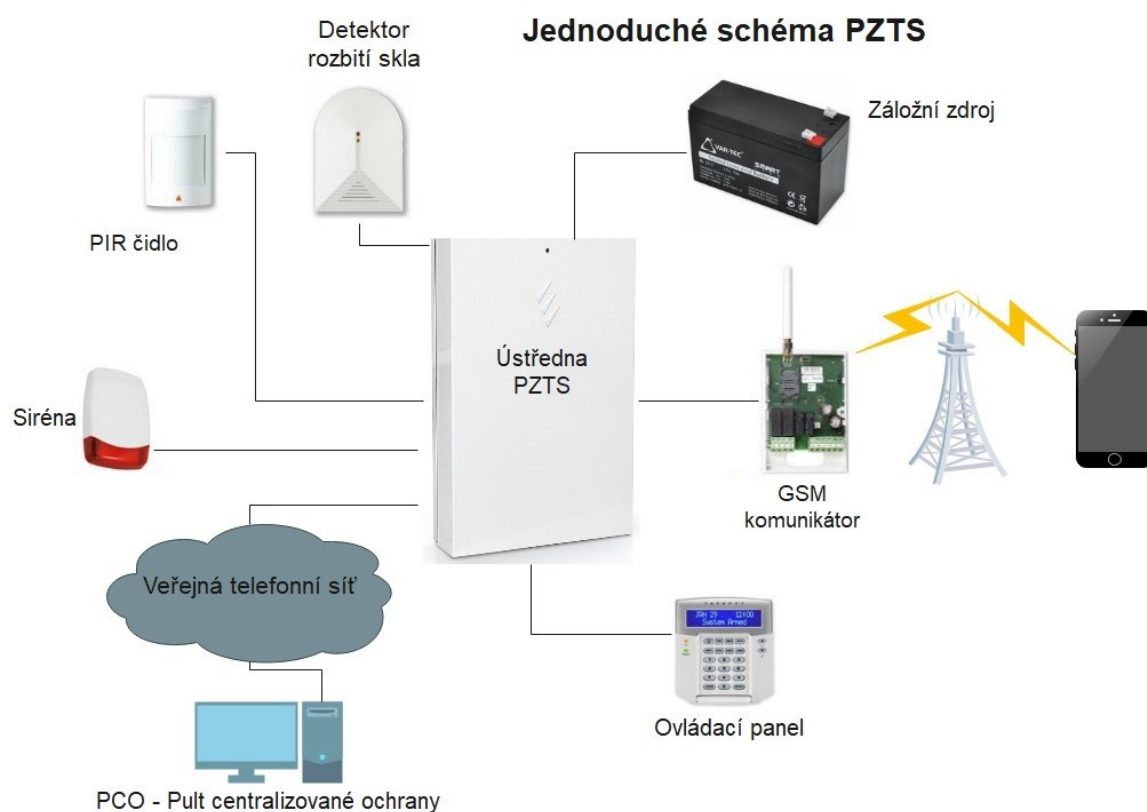
Detektory pracují na různých principech, přičemž jejich činnost je založena na převodu specifických fyzikálních jevů do elektrického poplachového signálu. Mohou reagovat například na přerušení elektrického obvodu, narušení světelného paprsku, změny elektromagnetického pole, magnetické anomálie nebo vibrace. Nejčastěji se využívají magnetické detektory (snímající otevření oken a dveří), elektrické okruhy (signální stěny), radiolokační senzory (pracující na principu elektromagnetických vln), termovizní a infračervené detektory (reagující na teplotní změny) a vibrační čidla (zaznamenávající mechanické otřesy). Detektory narušení se dnes nacházejí stále v komplexnějším využití v ochraně obvodové, plášťové, prostorové i předmětové. [19] [39]

Zdroj energie

V kontextu PZTS lze zdroj energie rozdělit na hlavní a záložní neboli primární a sekundární. V těchto systémech je běžné kombinované napájení, kde hlavním zdrojem je síťové napětí (230 V AC) a v případě výpadku přebírá funkci záložní akumulátor (obvykle 12V baterie). Tento mechanismus zajišťuje nepřetržitou funkčnost systému, a to i při přerušení dodávky elektrické energie.

Výstupní zařízení – Siréna

Siréna jako výstupní zařízení představuje důležitý prvek zabezpečovacího systému, jehož úkolem je upozornit okolí na narušení střeženého prostoru. V případě vyhlášení poplachu je siréna aktivována ústřednou a vydává hlasitý zvukový signál, často doplněný blikajícími světly (majákem). [39]



Obrázek 10 Ukázka – schéma zapojení systému PZTS

(zdroj: vlastní)

4.5 Integrace technických prostředků ochrany

Integrace technických prostředků ochrany představuje proces propojení různých bezpečnostních systémů do jednoho funkčního celku, který umožňuje jejich efektivní a centralizované řízení. Tento přístup se využívá jak v oblasti fyzické bezpečnosti, tak i v ochraně informací a majetku. Cílem integrace je zlepšení funkčnosti jednotlivých systémů, zvýšení úrovně bezpečnosti, snížení provozních nákladů a zefektivnění reakce na mimořádné situace. Mezi technické prostředky ochrany, které lze integrovat, patří poplachové zabezpečovací a tísňové systémy (PZTS), elektronické požární signalizace (EPS), dohledové video systémy (DV), mechanické zábranné systémy (MZS) a rovněž prvky kybernetické bezpečnosti. Integrace probíhá na několika úrovních – od fyzického propojení zařízení přes logické napojení pomocí komunikačních protokolů až po funkční a uživatelskou úroveň, kdy všechny systémy sdílejí informace a reagují koordinovaně. Například při detekci pohybu v hlídaném prostoru může dojít k automatickému přepnutí kamery na danou oblast, spuštění záznamu a uzamčení dveří. Díky centralizovanému řízení má obsluha přehled o všech systémech v reálném čase, což zvyšuje rychlost a přesnost reakcí při řešení krizových situací. Moderní integrované systémy často využívají pokročilé softwarové platformy, které umožňují vizualizaci událostí, správu oprávnění a dlouhodobou analýzu dat. Integrace technických prostředků ochrany je dnes klíčovou součástí komplexního bezpečnostního řešení pro firmy, veřejné instituce i kritickou infrastrukturu.

Shrnutí čtvrté kapitoly

Čtvrtá kapitola diplomové práce je zaměřena na vybrané technické systémy pro zabezpečení základních škol. Vybrané technické systémy jsou mechanické zábranné systémy (MZS), dohledové video systémy (DV) neboli (VSS), elektrická požární signalizace (EPS), poplachové zabezpečovací a tísňové systémy (PZTS). Tato kapitola se věnuje přehledu technických prostředků využívaných pro zajištění bezpečnosti a popisuje, jakým způsobem fungují. Rámcově jsou zde představeny jednotlivé typy ochrany včetně jejich hlavních prvků a zároveň jsou uvedeny konkrétní příklady prostředků používaných pro daný typ zabezpečení. Technické prostředky ochrany slouží jako účinný nástroj pro kontrolu a dozor nad chráněným objektem vůči různým vnějším hrozbám. V praxi se může jednat například o detekci požáru prostřednictvím hlásičů, které aktivují poplach, o vyhodnocení situace

pomocí senzorů ve spojení s dohledovým systémem, nebo o zaznamenání neoprávněného vstupu skrze prvky poplachového zabezpečovacího a tísňového systému (PZTS).

ZÁVĚR TEORETICKÉ ČÁSTI

Teoretická část diplomové práce poskytla ucelený přehled klíčových pojmů, právního rámce a technických možností v oblasti zabezpečení objektů, se zvláštním důrazem na zabezpečení základních škol. V úvodu byly objasněny základní bezpečnostní pojmy jako aktivum, riziko, hrozba, zranitelnost či protiopatření a následně byl popsán legislativní rámec včetně norem ČSN a evropské i mezinárodní regulace. Důležitou součástí byla i analýza rizik, kde byly představeny různé metody jejich hodnocení — kvalitativní, kvantitativní i semikvantitativní — včetně metody PNH, která bude použita v praktické části.

Dále byly představeny specifické požadavky na zabezpečení základních škol v návaznosti na jejich velikost a lokalitu. Popsány byly formy ochrany – režimová, fyzická i technická – a jejich praktické využití v prostředí škol. V neposlední řadě byly rozebrány jednotlivé technické prostředky zabezpečení jako mechanické zábranné systémy, dohledové video systémy, elektrická požární signalizace a poplachové zabezpečovací a tísňové systémy, včetně jejich možností integrace do jednoho funkčního celku.

Tato část vytvořila teoretický základ, na němž staví praktická část práce, jež se zaměřuje na konkrétní aplikaci uvedených poznatků na vybranou základní školu, včetně návrhu odpovídajících bezpečnostních opatření.

II PRAKTICKÁ ČÁST

5 POPIS VYBRANÉHO OBJEKTU

Tato kapitola se zaměřuje na popis současného stavu vybraného objektu a areálu, ve kterém se nachází. Dále budou představeny klíčové informace týkající se tohoto objektu, jenž bude sloužit jako základ pro provedení vstupních analýz v následujících částech práce. Na základě výsledků těchto analýz budou navržena vhodná opatření k zajištění požadované úrovně bezpečnosti veřejné budovy. Pro účely tohoto projektu byla jako zabezpečovaný objekt zvolena základní škola v Třebíči.

Popis si rozdělím na tři části, kdy v první části popíšeme bezprostřední okolí, dále budeme pokračovat popisem areálu a na konec hlavní budovou která je umístěna uvnitř areálu. V každé části se soustředíme na vlastnosti, které jsou specifické pro danou oblast.

5.1 Charakteristika školy

Základní škola a mateřská škola Na Kopcích je vzdělávací institucí zaměřenou na rozšířenou výuku informačních technologií. Svou činnost zahájila 1. září 1996 a stala se tak nejnověji zřízenou základní školou ve městě Třebíč. Mateřská škola byla k areálu připojena o dvanáct let později, konkrétně 1. září 2008. Od roku 2001 nese škola oficiální statut zařízení s rozšířenou výukou výpočetní techniky. Škola se nachází ve východní části města, v oblasti Nové Město. Její areál tvoří budovy základní i mateřské školy, dále sportovní infrastruktura v podobě víceúčelového sportoviště s umělým povrchem, vnitřní kryté tělocvičny a školní jídelny. Spádová oblast školy zahrnuje převážně východní část sídliště Nové Dvory (zejména oblast východně od Velkomeziříčské ulice) a také části sídliště Nové Město – konkrétně lokality Brněnská a Na Kopcích. Kromě toho spadá pod školu také obec Ptáčov. [40]

5.2 Popis objektu a okolí

Základní škola se nachází na sídlišti v samotném centru města. Její spádovou oblast tvoří i několik menších okolních obcí. Za školou bylo vybudováno víceúčelové hřiště, které je přístupné i veřejnosti. Ke škole náleží také oplocený školní pozemek. Budova školní jídelny prošla modernizací – byla vybavena novým konvektomatem, chladičím zařízením, novými bateriemi a myčkou. Mezi největší nedávné investice patří výměna oken a zateplení všech budov školy. [40]

Další budova, která se nachází v celkovém objektu je tělocvična. Jsou zde šatny s nově instalovanými sprchami, kabinety pro učitele tělesné výchovy a nářad'ovna. Tělocvična má parketovou podlahu s protiskluzovým nátěrem a systémem odvětrávání.

Vstupní dveře do hlavní budovy jsou prosklené s klasickými mechanickými zámky. Škola má plastová okna a vchodové dveře, které byly vyměněny již před několika lety. Je však patrné, že mechanické zámky ve dveřích už nevyhovují současným požadavkům.

Po skončení výuky probíhají ve škole zájmové kroužky, které končí v 18 hodin. Následně se objekt uzamyká a aktivuje se systém PZS. Zabezpečení je napojeno na DPPC Městské policie, která v případě narušení objektu provádí kontrolu a ověřuje, zda nejde o falešný poplach. Tento bezpečnostní systém je nainstalován pouze v přízemí budovy.

V nejbližší době čeká školu celková rekonstrukce, která se uskuteční během letních prázdnin, kdy ve škole nejsou přítomni žáci.



Obrázek 11 – Vchod do ZŠ Na Kopcích

(zdroj: [41] upraveno)

Popis areálu

Areál základní školy je chráněn drátěným plotem o celkové délce 318 metrů, přičemž plocha pozemku činí 12 612 m². Plot je klasické konstrukce, ukotvený do země pomocí betonových patek, a dosahuje výšky 1,5 metru. Jeho současný technický stav však již není zcela vyhovující. Budovu školy obklopují dvě vedlejší ulice a před hlavním vchodem se nachází veřejné parkoviště, které je k dispozici zdarma. Vzhledem k oplocení je vstup do areálu

možný pouze hlavním vchodem. Vedlejší vstupy slouží výhradně jako únikové cesty, vstupy pro zaměstnance nebo zásobování.

Uvnitř areálu je vyhrazené parkoviště pro zaměstnance školy. Kromě toho se zde nachází několik samostatně oplocených sportovišť, využívaných jak pro hodiny tělesné výchovy, tak pro volnočasové aktivity žáků.

Hlavní přístup do areálu je zajištěn vstupní bránou umístěnou vedle hlavního vchodu do budovy. Přes hlavní bránu je přístup na zaměstnanecké parkoviště, které je zabezpečeno uzamykatelnou bránou standardní konstrukce, která se otevírá v ranních hodinách před začátkem výuky a uzavírá se přibližně v 18 hodin. Ostatní brány slouží především k údržbě areálu a zásobování.

Před školou je možnost parkování na veřejném parkovišti, případně na trávníku mimo komunikaci. To umožňuje rodičům a návštěvníkům pohodlně přivést děti, ať už ráno nebo při večerních akcích, bez stresu spojeného s hledáním místa k zaparkování.

V blízkosti školního areálu se nachází pivnice, která může být zdrojem potenciálního bezpečnostního rizika pro děti i školu kvůli přítomnosti rizikových osob.



Obrázek 12 Satelitní snímek Třebíč

(zdroj: [42] upraveno)

Popis objektu – hlavní budova

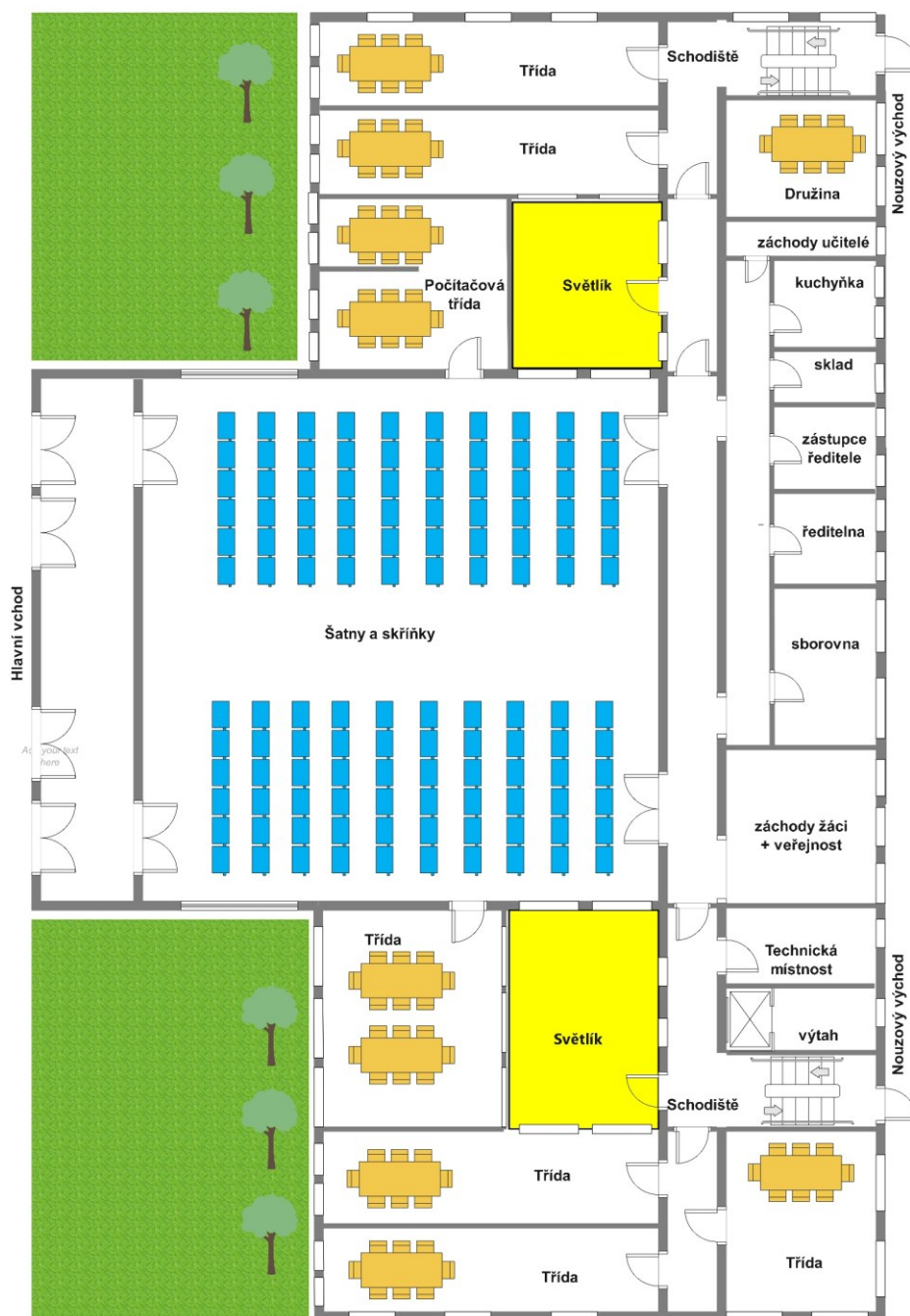
Hlavní budova Základní školy Na Kopcích je třípatrová. V přízemí se nachází hlavní vchod tvořený čtyřmi dvoukřídlými dveřmi, přičemž vstupní stěna je celá prosklená. Po vstupu pokračují návštěvníci přes další dvojce dveře do interiéru budovy. V přízemí je umístěna převlékárna a šatny, které slouží všem žákům školy k odkládání osobních věcí před příchodem do tříd. Součástí přízemí je také počítačová učebna.

Budova je prosvětlena dvěma světlíky, které prochází všemi patry. K dispozici jsou dvě schodiště a jeden výtah. Škola disponuje dvěma nouzovými východy, které slouží jak k evakuaci, tak k zásobování a přístupu zaměstnanců. V přízemí se nachází celkem sedm tříd (včetně počítačové učebny) a školní družina. Dále zde jsou toalety pro žáky i veřejnost, ředitelna, sborovna, sklad vybavení, malá kuchyňka pro zaměstnance a technická místnost pro údržbu a úklid.

Do druhého patra lze vystoupat po schodech nebo využít výtah, který je přizpůsoben i pro osoby se zdravotním postižením. V tomto podlaží je deset vyučovacích tříd a tzv. herna, kde si žáci mohou hrát nebo odpočívat během přestávek. Na chodbě je možnost sednout si na křesla a zahrát si stolní tenis během přestávky. Z druhého patra vede most spojující hlavní budovu se sousedními objekty – tělocvičnou a jídelnou, které však nejsou dále v textu popisovány.

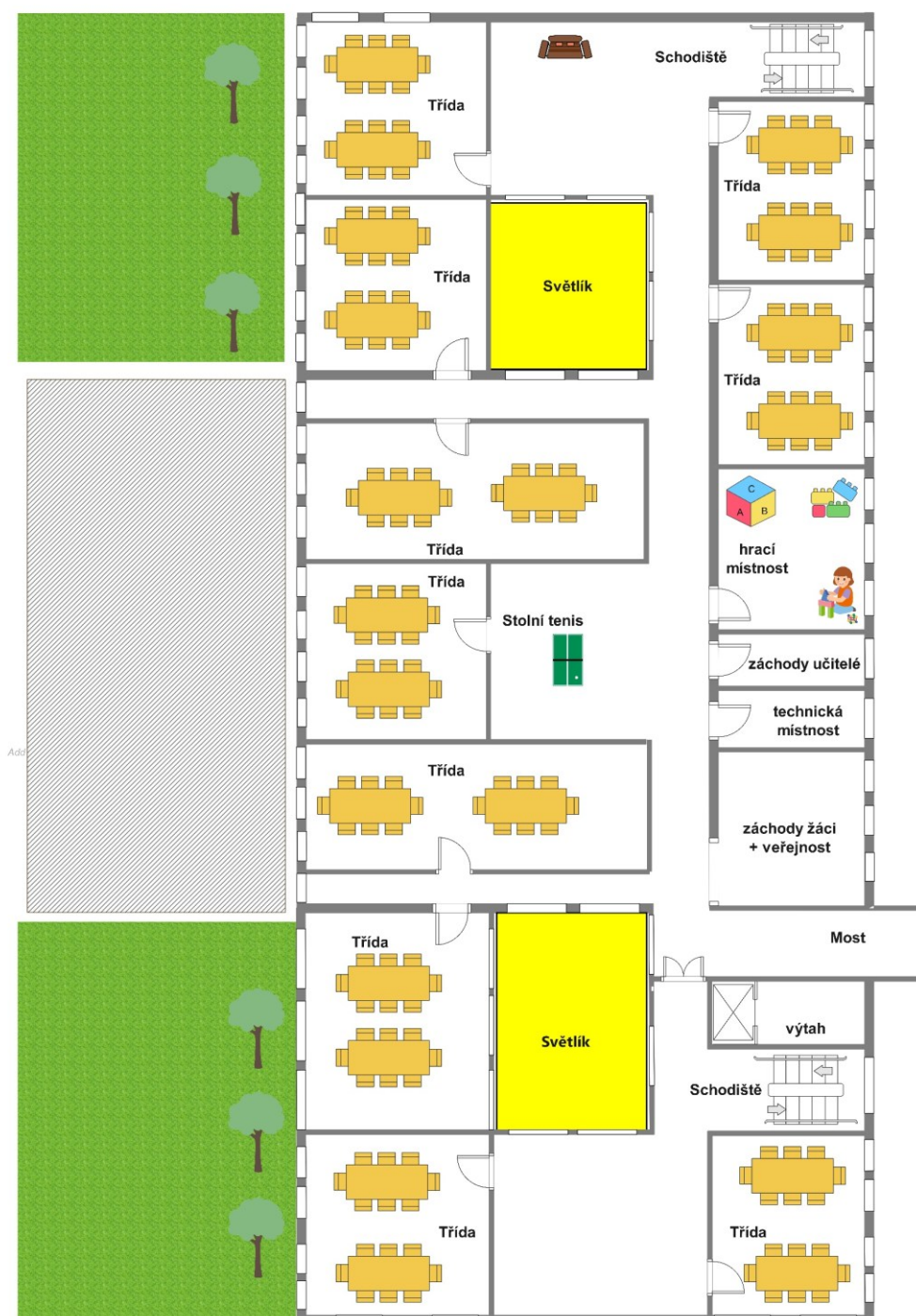
Třetí patro je podobné druhému, avšak bez mostu. Navíc je zde sklad pomůcek sloužící k uložení vybavení pro výuku.

Vzhledem k tomu, že celý areál se skládá z několika budov, není v rámci této práce možné věnovat se všem objektům podrobně. Následující kapitoly se proto zaměřují výhradně na analýzu aktuálního stavu zabezpečení a posouzení dle metody PNH, a to pouze v rozsahu hlavní budovy a areálového oplocení. Ostatní budovy nejsou do tohoto hodnocení zahrnuty.



Obrázek 13 Půdorys hlavní budovy 1.podlaží

(zdroj: vlastní)



Obrázek 14 Půdorys hlavní budovy 2.podlaží

(zdroj: vlastní)

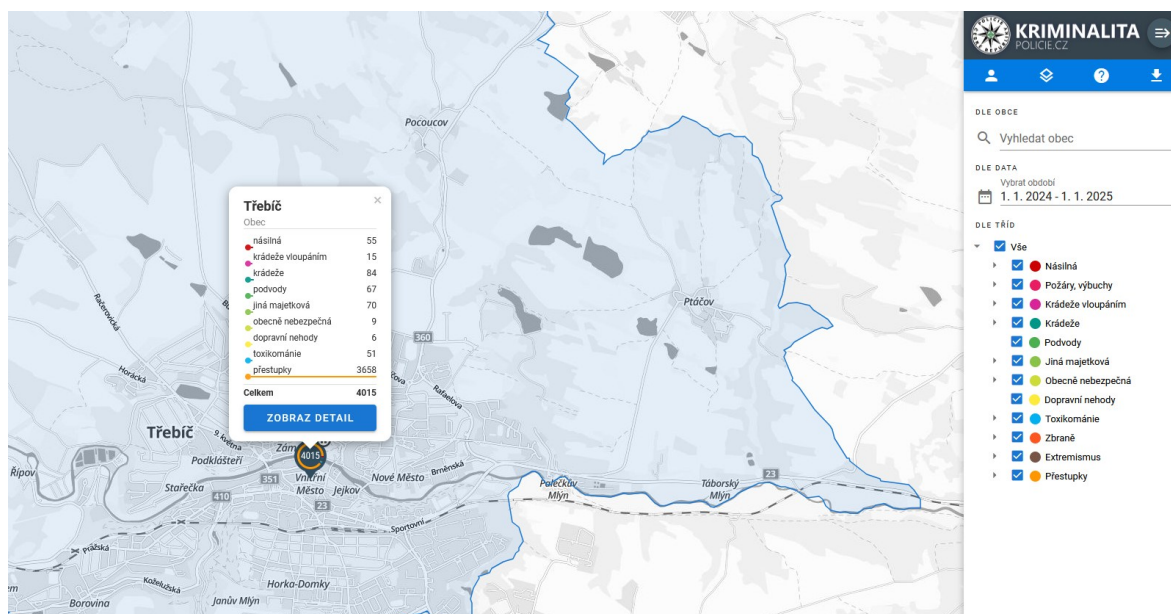


Obrázek 15 Půdorys hlavní budovy 3.podlaží

(zdroj: vlastní)

Mapa kriminality

Obrázek č. 16 graficky znázorňuje míru kriminality v lokalitě umístěné základní školy v Třebíči. V okresním městě Třebíči a jeho nejbližším okolí vyšetřovali policisté v posledním roce (od 1.ledna 2024 do 1.ledna 2025) přes 4015 případů. V drtivé většině přestupky, ale jsou zde i 55 násilné zločiny, 84 krádeží a 67 podvodů. Vyplývá to z policejní mapy (ta však nemusí zobrazovat všechny trestné činy. [43])



Obrázek 16 Mapa kriminality v Třebíči

(zdroj: [43])

Shrnutí páté kapitoly

Tato kapitola se věnuje popisu současného stavu základní školy v Třebíči a jejího areálu, které budou sloužit jako podklad pro další analýzy bezpečnosti. Je zde popsán areál objektu a popis hlavní budovy. Připojené jsou vytvořené půdorysy objektu hlavní budovy.

Kapitolu zakončuje analýza kriminality v oblasti, podle níž bylo v okolí školy v posledním roce vyšetřováno více než 4000 případů, většinou přestupků, ale také násilné trestné činy, krádeže a podvody.

6 ANALÝZA RIZIK

V rámci této části diplomové práce bude provedena identifikace aktiv, kdy budou určena hodnotná aktiva, která je nutné chránit. Uvedená aktiva musí být vyjádřena v nějaké hodnotě. V našem případě bude výhodnější, když hodnota bude vyjádřena v korunách. Následně bude provedena analýza rizik metodou PNH, jejímž výstupem bude rozčlenění hrozeb podle rizikových skupin pro jednotlivá aktiva.

6.1 Identifikace aktiv

Aktiva jsou všechno, co má pro organizaci hodnotu a co je potřeba chránit. "Identifikace aktiv" znamená proces rozpoznání a zaznamenání všech aktiv organizace nebo systému. Dle normy ISO 27001 musíme vědět, co chránit a musíme určit hodnotu aktiv. Tedy zjistím daná aktiva pro hlavní budovu a areál školy. [2]

Hlavní aktiva

Hlavní budova a areál objektu – jedná se o celý pozemek i se všemi budovami v areálu (třídy, tělocvična, jídelna, hřiště), nemovitý majetek, odhadovaná hodnota je do 50 000 000,- Kč

Majetek – majetek se musí rozdělit do jednotlivých skupin. Je rozdíl, zda se bude jednat o majetek školy, zaměstnanců, žáků nebo návštěvníků. Žáci mají své věci uložené v přízemí ve skříňkách, to však neznamená, že tam mají uloženo vše. Batohy s knihami a učebnicemi, či peněženky a mobily mají u sebe. Stejně jako zaměstnanci můžou mít své věci uložené po celé budově. Tudíž rozdělení musí být následující:

- Majetek školy (movitý) – odhadovaná hodnota do 6 500 000,- Kč
- Majetek zaměstnanců – odhadovaná hodnota do 450 000,- Kč
- Majetek žáků – odhadovaná hodnota do 775 000,- Kč

Lidé – rozdělení aktiva bude na zaměstnance a na žáky.

- Zaměstnanci
- Žáci

Peníze – neboli hotovost. Jedná se o fyzicky přítomné peníze v celém areálu. Peníze, které mají u sebe žáci a zaměstnanci. Rozdělení:

- Hotovost u zaměstnanců – odhadovaná hodnota do 120 000,-Kč

- Hotovost u žáků – odhadovaná hodnota do 50 000 Kč

Kontinuita – např. kontinuita provozu – škola funguje dál i při havárii, výpadku elektřiny, pandemii apod. Pokud by nastala některá z událostí, která by bránila provozu základní školy, může to mít za následek schopnost poskytování služeb. Pokud bychom započítali prodlevu na jeden den, částka by mohla klidně v rozmezí od 100 000,- Kč do 1 000 000,- Kč. Záleží, jaký den v měsíci a jaký den v týdnu by se událost stala. Budeme počítat normální pracovní den ve školním týdnu. Tedy 200 000,- Kč

Suma aktiv

Celková suma všech uvedených aktiv. Suma nemusí odpovídat reálné hodnotě, je však důležité vzít v úvahu, že se jedná o značný majetek.

Tabulka 8 Celková suma uvedených aktiv

Hlavní budova a areál objektu	50 000 000,- Kč
Majetek školy	6 500 000,- Kč
Majetek zaměstnanců	450 000,- Kč
Majetek žáků	775 000,- Kč
Hotovost u zaměstnanců	120 000,- Kč
Hotovost u žáků	50 000,- Kč
Kontinuita	200 000,- Kč
Celkem	58 095 000,-Kč

(zdroj: vlastní)

Období

Budeme rozdělovat dvě doby, kterých se bude týkat analýza. V podstatě se jedná dobu, kdy jsou uvnitř žáci a zaměstnanci a dobu mimo ni. Prázdniny a různé volné dny do toho započítávat nebudeme.

- 1–pondělí až pátek od 8:00 do 16:00
- 2–pondělí až pátek od 16:00 do 8:00, sobota a neděle

6.2 Identifikace hrozeb

Hrozba je něco, co by mohlo způsobit škodu na majetku, datech, zdraví lidí nebo fungování organizace. Je to situace, událost nebo činnost, která může negativně ovlivnit to, co se snažíme chránit. Hrozba ještě není samotné poškození – jen možnost, že k němu dojde.

Hrozby

Vybrané hrozby jsou podle místa, kde se Základní škola Na Kopcích nachází. Už podle názvu základní školy nemá význam zahrnout povodeň, mezi hrozby. Ovšem silná vichřice může být zahrnuta jako potenciální hrozba.

- **Krádež** – v rámci celého objektu může dojít ke krádeži, ať už uvnitř objektu (žáci apod.) anebo vnější zásah, škola má několik set žáků a drobné krádeže se mohou stávat,
- **Požár** – jsou zde umístěné hasící přístroje, které jsou dle vyhlášky č. 246/2001 Sb. o požární prevenci povinné, pokud by nastal požár mimo vyučovací dobu, není zde umístěný žádný systém na upozornění,
- **Vandalismus** – vandalismus se zde může objevit, už z důvodu umístění základní školy na sídlišti – poškozený plot, posprejované zdi, počmárané automobily atd.,
- **Výpadek elektrické energie** – pokud by odešel hlavní zdroj energie, škola nemá záložní. Tudíž by nastal blackout – nemožnost vyučování (světlo, zásuvky),
- **Výpadek pitné vody** – pitný režim je důležitý, výpadek pitné vody například v „letní“ den vidím jako závažný problém,
- **Úraz** – při velkém počtu žáků a zaměstnanců je velká pravděpodobnost, že se úraz může vyskytnout (zakopnutí, spadnutí, uklouznutí), úraz při tělocviku,
- **Napadení** – útok na lidskou osobu,
- **Onemocnění větší části učitelského sboru** – může nastat situace kdy onemocnění větší část učitelského sboru (chřipka, pandemie),
- **Silná vichřice** – způsobení poškození budovy,
- **Zničení** – majetku,

Tabulka 9 Zvolená aktiva a hrozby

Aktivum	Hrozby
Hlavní budova a areál objektu	Krádež, Požár, Vandalismus, Silná vichřice, Výpadek elektřiny, Výpadek vody
Majetek	Vandalismus, Požár, Krádež, Zničení, Silná vichřice
Lidé	Úraz, Napadení, Onemocnění
Peníze	Krádež, Požár
Kontinuita	Požár, Výpadek elektřiny, Výpadek vody, Krádež, Úraz, Zničení,

(zdroj: vlastní)

6.3 Analýza metodou PNH

Dle zvolených aktiv a identifikaci hrozeb, jsem vytvořil tabulku pro zpracování analýzy metodou PNH – bodová polo-quantitativní metoda, viz kapitola 2.2.3

Aktivum – Hlavní budova a areál objektu

Zpracované výsledky pro aktivum – Hlavní budova a areál objektu:

Tabulka 10 PNH analýza – Hlavní budova a areál objektu

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Hlavní budova a areál objektu	Krádež	1	3	2	3	24	III.
		2	2	2	3	12	IV.
	Požár	1	3	5	3	45	III.
		2	2	5	3	30	III.
	Vandalismus	1	3	2	2	12	IV.
		2	2	2	2	8	V.
	Silná vichřice	1	1	4	2	8	V.
		2	1	4	3	12	IV.
	Výpadek elektřiny	1	1	4	4	16	IV.
		2	1	4	2	8	V.
	Výpadek vody	1	1	3	3	9	IV.
		2	1	3	3	9	IV.

(zdroj: vlastní)

Aktivum – Majetek školy

Zpracované výsledky pro aktivum – Majetek školy:

Tabulka 11 PNH analýza – Majetek školy

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Majetek školy	Vandalismus	1	3	2	2	12	IV.
		2	2	2	2	8	V.
	Požár	1	3	5	3	45	III.
		2	2	4	3	24	III.
	Krádež	1	3	3	3	27	III.
		2	2	2	2	8	V.
	Silná vichřice	1	1	4	3	12	IV.
		2	1	3	3	9	IV.
	Zničení	1	2	3	2	12	IV.
		2	2	3	2	12	IV.

(zdroj: vlastní)

Aktivum – Majetek zaměstnanců

Zpracované výsledky pro aktivum – Majetek zaměstnanců:

Tabulka 12 PNH analýza – Majetek zaměstnanců

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Majetek zaměstnanců	Vandalismus	1	2	3	2	12	IV.
		2	1	2	2	4	V.
	Požár	1	3	2	3	18	IV.
		2	1	2	2	4	V.
	Krádež	1	3	3	3	27	III.
		2	1	2	2	4	V.
	Silná vichřice	1	1	2	2	4	V.
		2	1	1	2	2	V.
	Zničení	1	2	2	2	8	V.
		2	1	2	2	4	V.

(zdroj: vlastní)

Aktivum – Majetek žáků

Zpracované výsledky pro aktivum – Majetek žáků:

Tabulka 13 PNH analýza – Majetek žáků

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Majetek žáků	Vandalismus	1	3	2	3	18	IV.
		2	1	2	2	4	V.
	Požár	1	2	2	2	8	V.

		2	1	2	2	4	V.
	Krádež	1	3	3	3	27	III.
		2	1	2	2	4	V.
	Silná vichřice	1	1	2	2	4	V.
		2	1	2	2	4	V.
	Zničení	1	3	3	3	27	III.
		2	1	2	2	4	V.

(zdroj: vlastní)

Aktivum – Lidé – Zaměstnanci a žáci

Zpracované výsledky pro aktivum – Lidé:

Tabulka 14 PNH analýza – Lidé

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Lidé – zaměstnanci	Úraz	1	2	4	2	16	IV.
		2	1	4	2	8	V.
	Napadení	1	3	3	3	27	III.
		2	1	3	3	9	IV.
	Onemocnění	1	2	4	1	8	V.
		2	1	4	1	4	V.
Lidé – žáci	Úraz	1	4	2	2	16	IV.
		2	1	2	2	4	V.
	Napadení	1	3	3	3	27	III.
		2	1	3	3	9	IV.
	Onemocnění	1	4	2	1	8	V.
		2	1	2	1	2	V.

(zdroj: vlastní)

Aktivum – Peníze – Hotovost

Zpracované výsledky pro aktivum – Peníze – Hotovost:

Tabulka 15 PNH analýza – Peníze hotovost

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Peníze – hotovost u zaměstnanců	Požár	1	2	2	3	12	IV.
		2	1	1	3	3	V.
	Krádež	1	3	3	3	27	III.
		2	1	1	3	3	V.
Peníze – hotovost u žáků	Požár	1	2	2	3	12	IV.
		2	1	1	3	3	V.
	Krádež	1	4	2	3	24	III.
		2	1	1	3	3	V.

(zdroj: vlastní)

Aktivum – Kontinuita

Zpracované výsledky pro aktivum – Kontinuita:

Tabulka 16 PNH analýza – Kontinuita

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Kontinuita	Požár	1	3	4	3	36	III.
		2	2	4	3	24	III.
	Výpadek elektřiny	1	2	3	3	18	IV.
		2	2	2	2	8	V.
	Výpadek vody	1	1	3	2	6	V.
		2	1	2	2	4	V.
	Krádež	1	3	3	3	27	III.
		2	2	2	2	8	V.
	Úraz	1	3	2	2	12	IV.
		2	1	2	2	4	V.
	Zničení	1	2	2	3	12	IV.
		2	1	2	3	6	V.

(zdroj: vlastní)

6.4 Seznam hrozeb

Dle rozdělení podle rizikového stupně, který je uveden na konci kapitoly 2.2.3, se budu zabývat pouze vyhodnocením I. až III. stupně rizika. Jedná se již o závažnější rizika, která je zapotřebí zvážit a zabývat se jimi. Uvedené hrozby pod IV. a V. stupněm rizika, jsou z mého pohledu zanedbatelné a přijatelné, a proto se jimi nehodlám dále věnovat.

Tabulka 17 PNH analýza rizikové stupně III. až I.

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Hlavní budova a areál objektu	Krádež	1	3	2	3	24	III.
	Požár	1	3	5	3	45	III.
		2	2	5	3	30	III.
Majetek školy	Požár	1	3	5	3	45	III.
		2	2	4	3	24	III.
	Krádež	1	3	3	3	27	III.
Majetek zaměstnanců	Krádež	1	3	3	3	27	III.
Majetek žáků	Krádež	1	3	3	3	27	III.
	Zničení	1	3	3	3	27	III.
Lidé – zaměstnanci	Napadení	1	3	3	3	27	III.
Lidé – žáci	Napadení	1	3	3	3	27	III.
Peníze – hotovost u zaměstnanců	Krádež	1	3	3	3	27	III.
Peníze – hotovost u žáků	Krádež	1	4	2	3	24	III.
Kontinuita	Požár	1	3	4	3	36	III.

		2	2	4	3	24	III.
	Krádež	1	3	3	3	27	III.

(zdroj: vlastní)

Shrnutí šesté kapitoly

Tato kapitola se zaměřuje na analýzu rizik pro Základní školu Na Kopcích. Nejprve byla provedena identifikace aktiv. Následně byla identifikována relevantní hrozby, které mohou tato aktiva ohrozit. Analýza probíhala pomocí metody PNH, která hodnotí pravděpodobnost, následky a hodnotu aktiv, čímž stanovuje výslednou rizikovost. Rizika byla rozdělena podle rizikových stupňů (RS), přičemž se dokument soustředil na ta, která spadají do III. rizikového stupně (střední rizika), protože se jedná o relevantní hrozby, které vyžadují pozornost.

7 ANALÝZA AKTUÁLNÍHO STAVU ZABEZPEČENÍ ZÁKLADNÍ ŠKOLY

V této kapitole se budu zabývat současným stavem zabezpečení základní školy a jejího okolí. Použiji metodu Checklist (Kontrolní seznam), kterým provedu analýzu pomocí kontrolního seznamu. Tuto metodu jsem popisoval ve druhé kapitole této diplomové práce.

K posouzení současného stavu zabezpečení mě poslouží rozdělení úrovně ochran – perimetrická, plášťová, prostorová a předmětová. Tyto úrovně ochran spojím s kontrolním seznamem a více tak popíšu současný stav zabezpečení objektu.

V předchozí kapitole jsem provedl analýzu rizik na základě metody PNH (kapitola 6.3.) podle identifikace hrozeb a jejich zařazení podle úrovně rizika. U rizik od III. stupně závažnosti a nižších (tedy I. a II.) bude nutné navrhnout vhodná opatření, která povedou ke snížení těchto rizik na přijatelnou úroveň. Způsob, jakým budou tato opatření realizována, podrobně popíšu v následující kapitole.

7.1 Perimetrická ochrana

Celý obvod areálu základní školy je ohrazen pletivovým plotem o výšce 1,5 metru. Plot je klasické konstrukce, ukotvený do země pomocí betonových patek. Jeho současný technický stav však již není zcela vyhovující. Jsou zde vidět mechanické poškození a známky po korozi. Jeho překonání by nebyl vůbec žádný problém. Hlavní brána je opatřena klasickým mechanickým zámekem, bez připojení na elektřinu. Brána se otevírá všední dny ráno před začátkem vyučování. Na hlavní bráně je patrné, že se na ni podepsal zub času. Je sice i s ostnatým drátem a její celková výše jsou 2 metry, ale jak je vidět na obrázku 18 Vstup do areálu – Hlavní brána (vlastní), již není zcela ve vyhovujícím stavu.



Obrázek 17 Plot okolo základní školy

(zdroj: vlastní)

Obrázek 18 Vstup do areálu – Hlavní brána

(zdroj: vlastní)

Posouzení perimetrické ochrany

Tabulka 18 Kontrolní seznam – Perimetrická ochrana

Perimetrická ochrana			
P.č.	Otázka	Ano	Ne
1.	Je obvod areálu oplocený?	X	

2.	Je oplocení v technickém stavu, kdy dokáže plnit svou funkci?		X
3.	Je výška plotu dostatečná (1,50m)?		X
4.	Je okolo obvodu pletiva podhrabová deska?		X
5.	Je okolo obvodu pletiva ostnatý drát?		X
6.	Má oplocení doplňkové zábrany?		X
7.	Je hlavní brána uzamykatelná?	X	
8.	Je hlavní brána ve stavu, aby plnila svoji funkci?	X	
9.	Je perimetr sledován kamerovým systémem		X
10.	Je umožněno vjezdu cizím autům na pozemek (zásobování, údržbářské práce apod.)?	X	

(zdroj: vlastní)

Identifikace hrozeb

Dle metody Kontrolní seznam jsem zjistil následující hrozby:

- Areál má nevyhovující oplocení
- Oplocení nemá další doplňkové zábrany
- Areál není monitorován dohledovým kamerovým systémem

7.2 Plášťová ochrana

Plášťová ochrana základní školy je tvořena především otvorovými výplněmi, které představují klíčový prvek pasivní bezpečnosti. Hlavní vstup do budovy je tvořen skleněnými dvoukřídlími dveřmi, které mají klasické mechanické zámky bez certifikace. Je zde pouze klasická cylindrická vložka. Ostatní vstupní dveře či nouzové východy jsou plastové výroby a mají již v sobě zadlabací zámky, cylindrické vložky s kováním. Okna po celé budově jsou plastová, vybavená dvojsklem a opatřena bezpečnostním kováním po celém obvodu.

Nejsou zde instalovány žádné detekční systémy, bezpečnostní folie, mříže, kamerový systém či detektory narušení.

Posouzení plášťové ochrany

Tabulka 19 Kontrolní seznam – Plášťová ochrana

Plášťová ochrana			
P.č.	Otázka	Ano	Ne

1.	Jsou zajištěny vstupy do budovy?	X	
2.	Jsou dveře do budovy v dobrém technickém stavu a jsou schopné plnit svoji funkci?	X	
3.	Jsou vstupy do budovy opatřeny bezpečnostní certifikací?		X
4.	Jsou okna do budovy v dobrém technickém stavu a jsou schopné plnit svoji funkci?	X	
5.	Mají okna v budově bezpečnostní kování?	X	
6.	Jsou na dveřích nebo na oknech umístěny elektronické bezpečnostní prvky?		X
7.	Jsou okna v budově jistěna dalším bezpečnostní složkou (bezpečnostní fólie, mříže)?		X

(zdroj: vlastní)

Identifikace hrozeb

Dle metody Kontrolní seznam jsem zjistil následující hrozby:

- Hlavní vstupy do budovy nemají bezpečnostní certifikaci
- Není zde použito přídavné bezpečnostní zařízení (mříže, bezpečnostní fólie)

7.3 Prostorová ochrana

Poplachové zabezpečovací zařízení představuje účinnou formu prostorové ochrany. Základní škola používá tento systém zabezpečení, ale současný stav systému je však již nevyhovující – jeho komponenty jsou technicky nemoderní a opotřebované, což snižuje jejich spolehlivost. Ochrana je navíc zajištěna pouze v části přízemí objektu.

Posouzení prostorové ochrany

Tabulka 20 Kontrolní seznam – Prostorová ochrana

Prostorová ochrana			
P.č.	Otázka	Ano	Ne
1.	Jsou v rámci plášťové ochrany instalovány prvky PZS?	X	
2.	Jsou prvky PZS v dobrém technickém stavu a jsou schopné plnit svoji funkci?		X
3.	Je systém PZS napojen na DPPC?	X	
4.	Je systém PZS instalován po celé budově?		X
5.	Je zabráněno neoprávněnému otevření dveří či oken?		X

(zdroj: vlastní)

Identifikace hrozeb

- Systém PZS je nemoderní a opotřebovaný, neplní svoji funkci
- Systém PZS není instalován po celé budově, pouze v přízemí

7.4 Předmětová ochrana a Fyzická ostraha

Základní škola disponuje trezorem, který je umístěn v ředitelně. Klíč od trezoru má pouze ředitel a zástupce ředitele. Jsou zde umístěny důležité dokumenty a hotovost.

V areálu i hlavní budově není zajištěna fyzická ostraha, a to ani prostřednictvím vlastních zaměstnanců, ani pomocí najatého externího personálu.

Posouzení předmětové ochrany a fyzické ostrahy

Tabulka 21 Kontrolní seznam – Předmětová ochrana a Fyzická ostraha

Předmětová ochrana a Fyzická ostraha			
P.č.	Otázka	Ano	Ne
1.	Je k dispozici v celém objektu fyzická ostraha?		X
2.	Je kontrolován vchod do areálu?		X
3.	Je kontrolován vjezd do areálu		X
4.	Je uložena hotovost na vyhrazeném místě k tomu určeném?	X	
5.	Je toto místo zabezpečeno předmětovou ochranou	X	
6.	Je ve vnitřních částech objektu instalován kamerový dohled?		X

(zdroj: vlastní)

Identifikace hrozeb

- Ostraha objektu ani areálu není zajištěna bezpečnostní službou.
- Ve vnitřních částech objektu není instalován kamerový dohled.

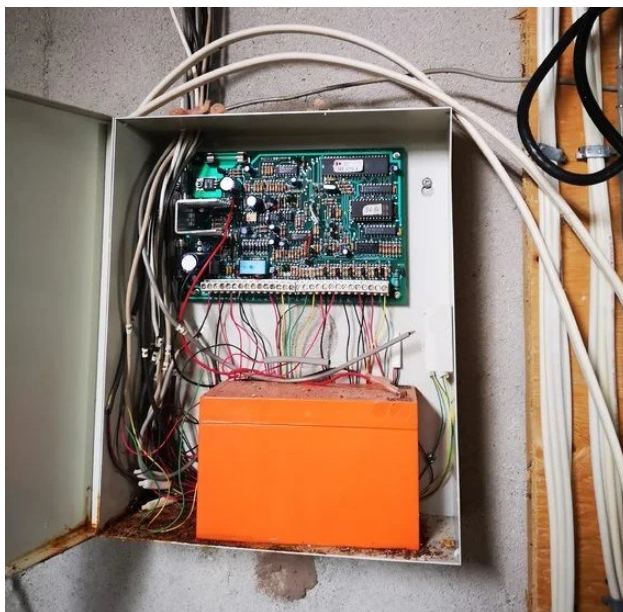
7.5 Technická ochrana

Zde jsem vypsal položky technické ochrany, kterými disponuje Základní škola Na Kopcích

PZS

V přízemí hlavní budovy je instalována ústředna od výrobce DSC – PC2000, která má několik detektorů umístěných na stěnách administrativních prostor v přízemí (např.

ředitelna, zástupce ředitele, sborovna a počítačová učebna). Jde o pohybové PIR detektory napojené pomocí kabeláže v plastových lištách umístěné na omítce budovy. Oknům a dveřím však chybí jakékoliv zabezpečení proti neoprávněnému otevření. Záložní napájení zajišťuje vnitřní baterie, která je dobíjena ze sítě. Ústředna je propojena s DPPC pomocí telefonní linky. Systém je aktivován při odchodu posledního pracovníka ze školy prostřednictvím klávesnice u vchodu.



Obrázek 19 Fotografie umístěného systému PZS

(zdroj: vlastní)

Dohledový video systém – VSS

V objektu se v současné době nenachází žádný kamerový systém. Vnitřní prostory nejsou sledovány ani monitorovány kamerami. Nebyla provedena instalace žádného zařízení pro vizuální dohled. Ochrana objektu prostřednictvím kamerového systému tedy zcela chybí.

Požární ochrana

V objektu není instalován žádný systém elektrické požární signalizace (EPS). Chybí tedy jakákoli technologie, která by automaticky detekovala vznik požáru, například pomocí čidel kouře nebo teploty. V případě vzniku požáru tak nelze očekávat žádné automatické spuštění poplachu či přivolání zásahu. Objekt není napojen na žádný centrální pult požární ochrany.

Protipožární ochrana je zajištěna pouze pomocí ručních hasicích přístrojů. Tyto přístroje jsou rozmístěny na vybraných místech budovy.

7.6 Identifikace nedostatků

Na základě metody kontrolního seznamu jsem identifikoval konkrétní hrozby, kterými se budu zabývat v závěrečné kapitole. Tyto hrozby následně propojuji s výsledky provedené s analýzou rizik PNH, které jsem provedl v přechozí kapitole.

- Areál má nevyhovující oplocení
- Oplocení nemá další doplňkové zábrany
- Areál není monitorován dohledovým kamerovým systémem
- Hlavní vstupy do budovy nemají bezpečnostní certifikaci
- Není zde použito přídatné bezpečnostní zařízení (mříže, bezpečnostní fólie)
- Systém PZS je nemoderní a opotřebovaný, neplní svoji funkci
- Systém PZS není instalován po celé budově, pouze v přízemí
- Ostraha objektu ani areálu není zajištěna bezpečnostní službou.
- Ve vnitřních částech objektu není instalován kamerový dohled.

Shrnutí sedmé kapitoly

Analýza současného stavu zabezpečení Základní školy Na Kopcích ukázala, že zabezpečení objektu je v řadě oblastí nedostatečné a nevyhovuje současným bezpečnostním standardům. Pomocí metody kontrolního seznamu byly zhodnoceny čtyři hlavní úrovně ochrany – perimetrická, plášťová, prostorová a předmětová – a byla identifikována řada konkrétních nedostatků. Celkově lze konstatovat, že zabezpečení objektu je v mnoha ohledech zastaralé, nedostatečné a neodpovídá požadavkům na moderní školské zařízení. V další části práce budou na základě této analýzy navržena konkrétní opatření ke zvýšení úrovně bezpečnosti školy.

8 NÁVRH ŘEŠENÍ PRO ZVÝŠENÍ ÚROVNĚ ZABEZPEČENÍ

Obsahem osmé kapitoly této se budu zabývat návrhem pro zvýšení úrovně zabezpečení základní školy. Pro hrozby, které byly popsány v rámci analýzy PNH a kontrolním seznamem v předchozích kapitolách, navrhnou způsob řešení s cílem snížit výsledný stupeň rizika, na přijatelnou úroveň IV. a V.

Budu navrhovat dvě varianty opatření. První varianta bude spíše vycházet z úsporného řešení, zde budu navrhovat základní opatření, které by byly v rámci bezpečnosti nejvýhodnější pro daný objekt. Druhá varianta nabídne rozšířenou verzi řešení, která sice může být nákladnější, ale stále se bude brát ohled na finanční náročnost s ohledem na hodnotu chráněných aktiv.

Při návrhu obou variant se zaměřím především na cenové odhady zvolených zařízení a tam kde to bude možné, vložím orientační ceny podle dostupných ceníků. Do kalkulací obou variant budou zahrnuty pouze náklady na samotné zařízení, nebudou započítávány výdaje za instalaci, konfiguraci sítě, stavební úpravy.

8.1 Hrozby

Hrozby, které byly zjištěny, jsou zobrazeny v předešlých kapitolách 6.4. a 7.6. Seznam hrozeb

8.2 Minimální požadavky technického charakteru pro zvýšení úrovně zabezpečení

Tato první varianta představuje základní úroveň opatření nezbytných pro zajištění bezpečnosti základní školy. Jedná se o úsporné řešení, které se zaměřuje na klíčové prvky ochrany objektu. Ačkoli některé navržené bezpečnostní komponenty mohou působit finančně náročně, cílem je dosáhnout vyváženého poměru mezi ekonomickou náročností a efektivitou zabezpečení.

Výměna plotových panelů

K výměně celého oplocení by byly použity plotové panely, které by se osadily do nových sloupků. Tím by došlo k požadované obnově oplocení za účelem zvýšení bezpečnosti. Délka jednoho panelu je 2,50 m a výška je 1,83 m. Celková délka plotu činí 318 metrů, což znamená, že pro kompletní výměnu by bylo potřeba 127 plotových dílů a nových 64 sloupků.

Vybraný materiál:

- 127 kusů – plotový panel 2D DOUBLE LIGHT – 183 cm, drát 5/4/5 mm, antracit – 1215,- Kč/kus [44]
- 64 kusů – Sloupek 60x40mm PVC 200 cm – 305,- Kč/kus [45]

Opatření bylo navrženo s ohledem na tyto hrozby:

- Areál má nevyhovující oplocení

Tabulka 22 Hrozby související s výměnou plotových panelů

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Hlavní budova a areál objektu	Krádež	1	3	2	3	24	III.
Majetek školy	Krádež	1	3	3	3	27	III.
Kontinuita	Krádež	1	3	3	3	27	III.

(zdroj: vlastní)

Zabezpečení oken a dveří

V rámci zabezpečení hlavního vstupu do budovy je nutné vybavit vstupní dveře novými zámky s platnou bezpečnostní certifikací. Půjde o kompletní výměnu zámků tak, aby odpovídaly aktuálním bezpečnostním požadavkům. Zároveň je potřeba vyměnit zámek také u hlavní brány, která slouží k vjezdu do areálu. Pro zabezpečení dveří byla zvolena třída RC2.

Bezpečnostní třídy dveří představují standardizovaný systém, který určuje, jak účinně dveře odolávají pokusům o neoprávněný vstup. Nejčastěji používaná klasifikace vychází z evropské normy EN 1627 a označuje se zkratkou RC, přičemž třídy jsou číslovány od RC1 do RC6. Každá třída odpovídá určité úrovni ochrany a splňuje konkrétní požadavky a zátěžové testy.[46]

Třída RC2: Dveře této třídy mají vyšší úroveň odolnosti. Jsou schopny poskytnout ochranu před běžnými pokusy o vloupání, jako je použití jednoduchých nástrojů a fyzická síla. [46]

Dalším bezpečnostním prvkem je instalace bezpečnostní fólie na okna v přízemí. Tato fólie by byla aplikována na okenní tabule a výplně s cílem ztížit neoprávněný vstup a zvýšit odolnost proti vnějším vlivům.

Vybraný materiál pro dveře:

- 5 kusů – Jednostranná cylindrická vložka FAB 2** – 177,- Kč/ kus [47]

- 5 kusů – Bezpečnostní kování – 802 od firmy ROSTEX – 1211,- Kč/ kus [48]

Vybraný materiál pro okna a okenní tabule:

Byla vybrána bezpečnostní fólie Bezpečnostní folie SMC7. Čirá, nezabarvená bezpečnostní fólie se zesílenou ochranou se nejčastěji používá ve školkách, školách, nemocnicích, úřadech, hotelech, domácnostech nebo v potravinářských provozech. Kromě toho poskytuje spolehlivou ochranu i proti krupobití. Je ideálním řešením pro místa, kde hrozí rozbití skla a tím i riziko zranění osob, zejména dětí. [49]

Cena vychází 3 265,- Kč za m². Počet kusů, které je zapotřebí s ohledem velikosti okna:

- 16 kusů - 1200 mm x 2200 mm
- 4 kusy – 2000 mm x 1500 mm

Celkově po zaokrouhlení nahoru se jedná o plochu 55 m², která bude započítána do kalkulace.

Opatření bylo navrženo s ohledem na tyto hrozby:

- Hlavní vstupy do budovy nemají bezpečnostní certifikaci
- Není zde použito přídatné bezpečnostní zařízení (mříže, bezpečnostní fólie)

Tabulka 23 Hrozby související se zabezpečením oken a dveří

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Majetek zaměstnanců	Krádež	1	3	3	3	27	III.
Majetek žáků	Krádež	1	3	3	3	27	III.
Peníze – hotovost u zaměstnanců	Krádež	1	3	3	3	27	III.
Peníze – hotovost u žáků	Krádež	1	4	2	3	24	III.

(zdroj: vlastní)

Kamerový systém – VSS

Navržený kamerový systém bude tvořen celkem třemi kamerami. Jedna vnitřní kamera bude umístěna v přízemí, kde bude monitorovat vstupní prostor. Jejím úkolem bude zaznamenávat příchod žáků a zaměstnanců a bude nasměrována tak, aby pokryla oblast od vstupu směrem k šatnám a administrativní části budovy. Zbylé dvě kamery budou umístěny v exteriéru. První z nich bude instalována na stožáru na střeše budovy a poskytne panoramatický pohled,

čímž zajistí přehled o celém okolí. Druhá venkovní kamera bude umístěna nad hlavním vstupem, kde bude snímat příchozí osoby u vchodu.

Rozmístění kamer bude znázorněno na obrázku 24,25,26, společně se systémy PZTS a EPS.

Uvnitř objektu by se umístila následující technika:

- 1 kus – VIVOTEK FD9189-H-v2 – vnitřní IP kamera, 5MPx rozlišení 2560 x 1920 bodů, 60FPS, H.265, WDR Pro, úhel záběru 103°, zvýšená citlivost v noci, 3D redukce šumu, otočení obrazu, inteligentní IR přísvit na 30 metrů, PoE [50]

Cena – 8390,- Kč

- 1 kus – VIVOTEK ND9323P – záznamové zařízení pro 8 IP kamer, 2x HDD až 16 TB, HDMI (4K) a VGA výstup pro monitor/TV, 2x USB, PoE switch pro 8 kamer, 4x DI / 1x DO, ONVIF, VIVOCLOUD, v českém jazyce [51]

Cena – 7 990,- Kč

- 1 kus – WD RED Plus 4 TB – Pevný disk Western Digital RED Plus 4 TB, [52]

Cena – 3 990,- Kč

Venkovní plášť budovy bude doplněn o tato zařízení:

- 1 kus – VIVOTEK CC9380-HV – venkovní IP kamera, 5MPx rozlišení 2560 x 1920 bodů, 30FPS, H.265, WDR Pro, úhel záběru 180°, zvýšená citlivost v noci, 3D redukce šumu, PoE, IP66 a IK10 [53]

Cena – 12 593,- Kč

- 1 kus – VIVOTEK FD9383-HVF2 – venkovní IP kamera, 5MPx rozlišení 2560 x 1920 bodů, 30FPS, H.265, WDR Pro, úhel záběru 103,4°, SNV, podpora umělé inteligence, inteligentní IR II na 30 metrů, PoE, IP66 a IK10 [54]

Cena - 7 967,- Kč

Opatření bylo navrženo s ohledem na tyto hrozby:

- Areál není monitorován dohledovým kamerovým systémem

Tabulka 24 Hrozby související s kamerovým systémem – VSS

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Hlavní budova a areál objektu	Krádež	1	3	2	3	24	III.
Majetek školy	Krádež	1	3	3	3	27	III.
Majetek zaměstnanců	Krádež	1	3	3	3	27	III.
Majetek žáků	Krádež	1	3	3	3	27	III.
	Zničení	1	3	3	3	27	III.
Lidé – zaměstnanci	Napadení	1	3	3	3	27	III.
Lidé – žáci	Napadení	1	3	3	3	27	III.
Peníze – hotovost u zaměstnanců	Krádež	1	3	3	3	27	III.
Peníze – hotovost u žáků	Krádež	1	4	2	3	24	III.
Kontinuita	Krádež	1	3	3	3	27	III.

(zdroj: vlastní)

Modernizace PZTS

Stávající elektronický zabezpečovací systém (PZS) bude nahrazen moderním poplachovým zabezpečovacím a tísňovým systémem (PZTS), protože současné zařízení již nesplňuje požadované funkce. Nový systém zajistí vyšší úroveň ochrany objektu. Rozmístění čidel a dalších součástí PZTS bude znázorněno na půdorysu budovy viz obrázek 24, 25 a 26, který přehledně zachytí jejich umístění v rámci celkového zabezpečení.

Vnitřní prostory hlavní budovy budou vybaveny těmito zařízeními:

- 1 kus – Zabezpečovací ústředna Paradox MAGELLAN MG5075 – Zabezpečovací ústředna Paradox MAGELLAN MG5075 včetně plastového boxu a zdroje pro bezdrátový i drátový zabezpečovací systém. Ústředna je již na desce osazena bezdrátovým přijímačem 868MHz a má možnost využít 5 vstupů s možností připojit 10 NC zón v ATZ zapojení. Ústřednu je možné rozdělit na dvě oblasti a pro ovládání systému využívat 32 uživatelských kódů / bezdrátových klíčenek. [55] Cena - 4 828,- Kč/kus
- 1 kus – Bezúdržbový akumulátor 12V 7Ah – baterie – Cena 538,- Kč / kus
- 1 kus – Klávesnice Paradox K32 LCD+ – Drátová LCD klávesnice Paradox K32 LCD+ k systémům MAGELLAN, která umožňuje zobrazování všech 32 zón. Stav zón a systému se zobrazuje rolováním na displeji. Pomocí bočních tlačítek lze na LCD listovat v popisech a stavových hláškách. Pomocí LCD klávesnice lze

prohlížet historii událostí ústředny. Připojení po 4drátové komunikační sběrnici [55] – Cena 3 951,- Kč/ kus

- 1 kus – Vnitřní siréna s blikáčem SA 913TF – Vnitřní nezálohovaná siréna s červeným blikáčem, napájení 11–14 V=, proudový odběr 250 mA, akustický výkon 110 dB/m. [55] - Cena 342,- Kč/kus
- 2 kusy – Bezdrátový magnetický kontakt Paradox DCT2-868 - Bezdrátový magnetický kontakt Paradox DCT2 s jedním jazýčkovým relé v miniaturním provedení. [55] Cena 1 123,- Kč/kus
- 2 kusy – Detektor rozbití skla Paradox DG457 – Detektor tříštění skla Paradox GLASSTREK DG457. Čidla detekují dvě frekvence, vzniklé při porušení skla. Nízkofrekvenční vlnu nárazu a vysokou frekvenci tříštění. [55] Cena 986,- Kč/kus
- 11 kusů – PIR detektor pohybu Paradox 476 - Duální infradetektor Paradox 476 pro montáž do rohu i na zeď. Vysoká odolnost proti RF rušení, inteligentní vyhodnocování a zpracování signálu, teplotní kompenzace, automatický čítač pulsů. [55] – Cena 455,- Kč/kus
- 1 kus – Internetový modul PARADOX IP180 MQTT – Připojení na internet je datovým kabelem s RJ45 nebo WiFi. [55] – Cena 3 323,- Kč/kus

Opatření bylo navrženo s ohledem na tyto hrozby:

- Systém PZS je nemoderní a opotřebovaný, neplní svoji funkci
- Systém PZS není instalován po celé budově, pouze v přízemí

Tabulka 25 Hrozby související s ochranou PZTS

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Hlavní budova a areál objektu	Krádež	1	3	2	3	24	III.
Majetek školy	Krádež	1	3	3	3	27	III.
Kontinuita	Krádež	1	3	3	3	27	III.

(zdroj: vlastní)

EPS

V hlavní budově dosud není nainstalován žádný systém elektrické požární signalizace (EPS). Navrhovaný systém je koncipován jako základní řešení, které slouží k detekci požáru a

pokrývá pouze nezbytné prvky. Rozmístění EPS zařízení bude znázorněno na celkovém půdorysu budovy – viz obrázek 24, 25 a 26.

Vnitřní prostory hlavní budovy budou vybaveny těmito zařízeními:

- 1 kus – ústředna B01090-00 "APOLLO F2" - Ústředna s jednou kruhovou linkou s možností rozšíření pro malé aplikace, splňuje normu EN 54, napájení 230 V AC, 50 Hz, max. 2x AKU 26Ah, [56] Cena 30 835,- Kč /kus



Obrázek 20 Ústředna EPS

(zdroj: [56])

- 1 kus – akumulátor – AKU CJ-12/12Ah [57] Cena 842,- Kč/kus
- 3 kusy – požární tlačítko – SA5900-908APO Inteligentní tlačítkový hlásič červený (povrchový) se zadním krytem, s izolátorem. [58] Cena 1 659,- Kč/kus



Obrázek 21 Požární tlačítko

(zdroj: [58])

- 3 kusy – siréna – PSS-0020 - Siréna SONOS, červená, 106 dB, 32 tónů, 9–60 V DC, 6–35 mA, EN 54-3, vysoká patice, IP65 [59] Cena 797,- Kč/kus



Obrázek 22 Siréna

(zdroj: [59])

- 17 kusů – TSD-1 - Kombinovaný detektor (teplotní a kouřový), volitelný režim detekce, hexamřížka proti vniknutí nečistot, paměť poplachu, samoreset, konfigurace pomocí DIP přepínače, univerzální zapojení, detekce znečištění optické komory [60] Cena 812,- Kč/kus



Obrázek 23 Teplotní a kouřový detektor

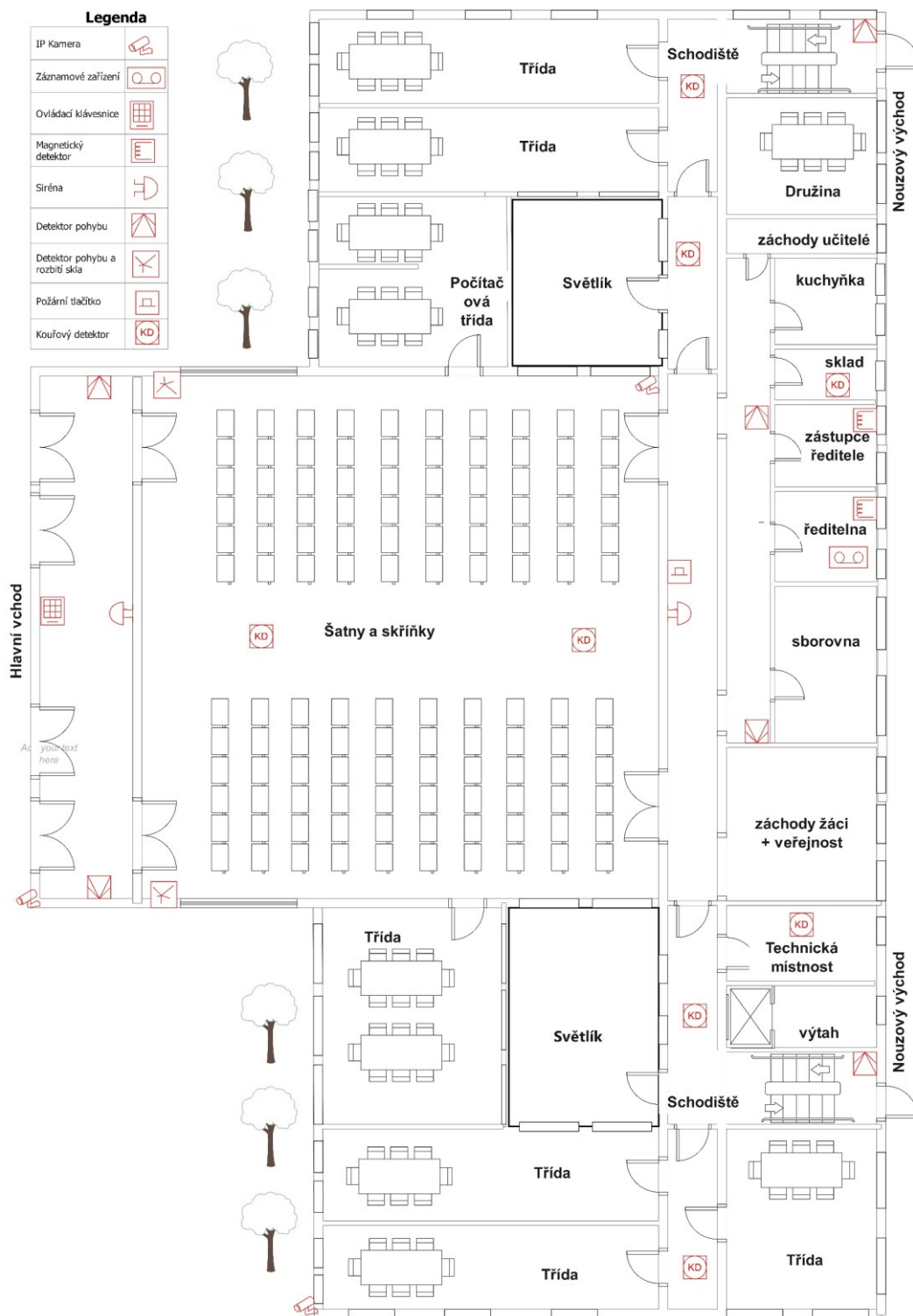
(zdroj: [60])

Opatření bylo navrženo s ohledem na tyto hrozby:

Tabulka 26 Hrozby související s požární ochranou

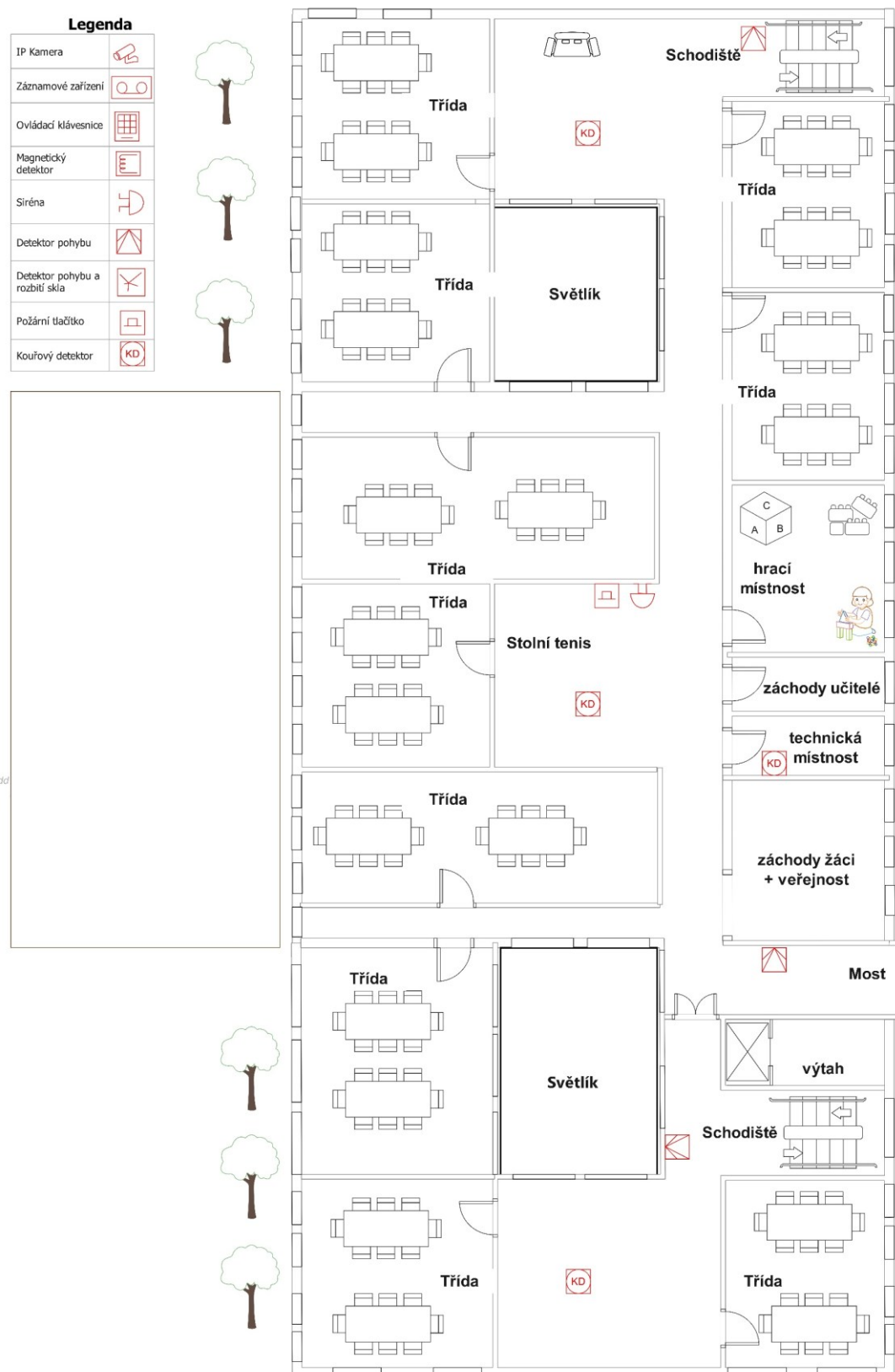
Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Hlavní budova a areál objektu	Požár	1	3	5	3	45	III.
		2	2	5	3	30	III.
Majetek školy	Požár	1	3	5	3	45	III.
		2	2	4	3	24	III.
Kontinuita	Požár	1	3	4	3	36	III.
		2	2	4	3	24	III.

(zdroj: vlastní)



Obrázek 24 Přízemí hlavní budovy s elektronickými zabezpečovacími systémy

(zdroj: vlastní)



Obrázek 25 První patro hlavní budovy s elektronickými zabezpečovacími systémy

(zdroj: vlastní)



Obrázek 26 Druhé patro hlavní budovy s elektronickými zabezpečovacími systémy

(zdroj: vlastní)

8.3 Minimální požadavky netechnického charakteru pro zvýšení úrovně zabezpečení

Požadavky netechnického charakteru jsou taková bezpečnostní nebo organizační opatření, která nezahrnují technické prostředky ani technologická zařízení, ale přesto výrazně přispívají k ochraně osob, majetku nebo informací.

V rámci návrhu zabezpečení Základní školy Na Kopcích se budeme soustředit na minimální opatření, která jsou nutná pro zajištění základní úrovně ochrany s důrazem na požadavky netechnického charakteru.

Fyzická ostraha

V rámci minimálních požadavků nebudeme započítávat fyzickou ostrahu, která by byla pro základní školu finančně náročná, byť užitečná. Budou zde započítány pouze náklady spojené s připojením PZTS na DPPC. Rozšíření o fyzickou ostrahu vložím až do optimálních požadavků.

Požadavky:

- Napojení objektu na PCO – 2 500,- Kč [61]

Opatření bylo navrženo s ohledem na tyto hrozby:

- Ostraha objektu ani areálu není zajištěna bezpečnostní službou.

Tabulka 27 Hrozby související s bezpečnostní službou

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Hlavní budova a areál objektu	Krádež	1	3	2	3	24	III.
	Požár	1	3	5	3	45	III.
Majetek školy	Požár	1	3	5	3	45	III.
	Krádež	1	3	3	3	27	III.
Majetek zaměstnanců	Krádež	1	3	3	3	27	III.
Majetek žáků	Krádež	1	3	3	3	27	III.
	Zničení	1	3	3	3	27	III.
Lidé – zaměstnanci	Napadení	1	3	3	3	27	III.
Lidé – žáci	Napadení	1	3	3	3	27	III.
Peníze – hotovost u zaměstnanců	Krádež	1	3	3	3	27	III.
Peníze – hotovost u žáků	Krádež	1	4	2	3	24	III.
Kontinuita	Požár	1	3	4	3	36	III.
	Krádež	1	3	3	3	27	III.

(zdroj: vlastní)

8.4 Vyčíslení nákladů

V rámci minimálních požadavků na zvýšení úrovně zabezpečení zpracovávám celkový odhad nákladů pro konkrétní základní školu. Jsou zde uvedeny položky, které jsou z bezpečnostního hlediska považovány za základní a nezbytné. Vybraná zařízení byla zvolena s ohledem na dostupnost jak po materiální, tak finanční stránce. Pokud je možné některé práce provést svépomocí, škola je tomuto přístupu nakloněna. Tyto práce proto nebudou započítány do celkové kalkulace, ale budou uvedeny samostatně jako oddělená položka v rozpočtu.

Náklady na montážní práce nejsou do kalkulace zahrnuty, protože jejich rozsah nelze v této fázi návrhu přesně určit – zejména s ohledem na dosud nedefinované kabelové trasy a způsob instalace včetně potřebného materiálu.

Tabulka 28 Náklady – varianta minimální požadavky

Produkt	Počet kusů	Cena za kus v Kč	Cena v Kč
plotový panel 2D DOUBLE LIGHT	127	1 215	154 305
Sloupek 60x40mm PVC 200 cm	64	305	19 520
cylická vložka FAB 2**	5	177	885
Bezpečnostní kování – 802 ROSTEX	5	1 211	6 055
bezpečnostní fólie	55	3 265	179 575
VIVOTEK FD9189-H-v2	1	8 390	8 390
VIVOTEK ND9323P	1	7 990	7 990
WD RED Plus 4 TB	1	3 990	3 990
VIVOTEK CC9380-HV	1	12 593	12 593
VIVOTEK FD9383-HVF2	1	7 967	7 967
Paradox MAGELLAN MG5075	1	4 828	4 828
Bezúdržbový akumulátor 12V	1	538	538
Klávesnice Paradox K32 LCD+	1	3 951	3 951
Vnitřní siréna SA 913TF	1	342	342
Paradox DCT2-868	2	1 123	2 246
Paradox DG457	2	986	1 972
Paradox 476	11	455	5 005
PARADOX IP180 MQTT	1	3 323	3 323
B01090-00 "APOLLO F2"	1	30 835	30 835
AKU CJ-12/12A	1	842	842
SA5900-908APO	3	1 659	4 977
siréna – PSS-0020	3	797	2 391

TSD-1	17	812	13 804
Napojení objektu na PCO	1	2 500	2 500
Cena celkem			478 824

(zdroj: vlastní)

Zhodnocení návrhu

Navržená varianta naplňuje stanovený cíl v rámci základního zabezpečení objektu. Přestože se celkové náklady mohou na první pohled jevit jako vysoké, pokrývají zabezpečení jak celého areálu, tak hlavní budovy. Cílem je snížit rizika identifikovaná v průběhu analýzy. Vynaložené finanční prostředky lze proto vnímat jako smysluplnou investici, která se v budoucnu pozitivně projeví.

8.5 Návrh optimálních kroků technického charakteru pro zvýšení úrovně zabezpečení

Tato varianta staví na minimálních bezpečnostních opatřeních a dále ji rozšiřuje o doplňující opatření, která zvyšují celkovou úroveň zabezpečení.

Podhrabové desky – betonové

Pokud by součástí výměny oplocení za plotové panely byla i náhrada betonových patek za podhrabové desky, došlo by k dalšímu zvýšení úrovně zabezpečení. I když se jedná o nadstandardní investici, v kontextu již probíhající výměny oplocení by šlo o rozumný doplněk, který by přispěl k lepší ochraně objektu. Pokud vezme v úvahu, že je zapotřebí 127 plotových panelů pro výměnu minimalistické variantě návrhu zabezpečení a každý panel má délku 2,5 metru. Je tedy zapotřebí i 127 podhrabových desek.

Vybraný materiál:

- 127 kusů – Podhrabová deska betonová 2500 x 200 x 40 mm – 399,- Kč/kus [62]

Opatření bylo navrženo s ohledem na tyto hrozby:

- Oplocení nemá další doplňkové zábrany

Tabulka 29 Hrozby související s výměnou plotových panelů

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Hlavní budova a areál objektu	Krádež	1	3	2	3	24	III.
Majetek školy	Krádež	1	3	3	3	27	III.
Majetek zaměstnanců	Krádež	1	3	3	3	27	III.

Majetek žáků	Krádež	1	3	3	3	27	III.
	Zničení	1	3	3	3	27	III.

(zdroj: vlastní)

Doplnění kamerového systému

Doplnění kamerové systému spočívá v instalaci dalších kamer. Záznamové zařízení zvolené v předchozí variantě má dostatečnou kapacitu pro připojení dalších čtyř kamer. Tři z nich budou umístěny ve venkovních prostorách a přispějí ke zvýšení celkové bezpečnosti objektu. Čtvrtá kamera bude instalována uvnitř budovy, aby podpořila dohled v klíčových vnitřních částech. Není proto nutné pořizovat nové záznamové zařízení ani rozšiřovat úložnou kapacitu disku. Nově přidávané kamery budou zobrazeny na Obrázku 27 - přízemí hlavní budovy.

Uvnitř objektu by se umístila následující technika:

Venkovní plášť budovy bude doplněn o tato zařízení:

- 3 kusy – VIVOTEK CC9380-HV – venkovní IP kamera, 5MPx rozlišení 2560 x 1920 bodů, 30FPS, H.265, WDR Pro, úhel záběru 180°, zvýšená citlivost v noci, 3D redukce šumu, PoE, IP66 a IK10 [53]

Cena – 12 593,- Kč

Uvnitř objektu by se umístila následující technika:

- 1 kus – VIVOTEK FD9189-H-v2 – vnitřní IP kamera, 5MPx rozlišení 2560 x 1920 bodů, 60FPS, H.265, WDR Pro, úhel záběru 103°, zvýšená citlivost v noci, 3D redukce šumu, otočení obrazu, inteligentní IR přísvit na 30 metrů, PoE [50]

Cena – 8390,- Kč

Opatření bylo navrženo s ohledem na tyto hrozby:

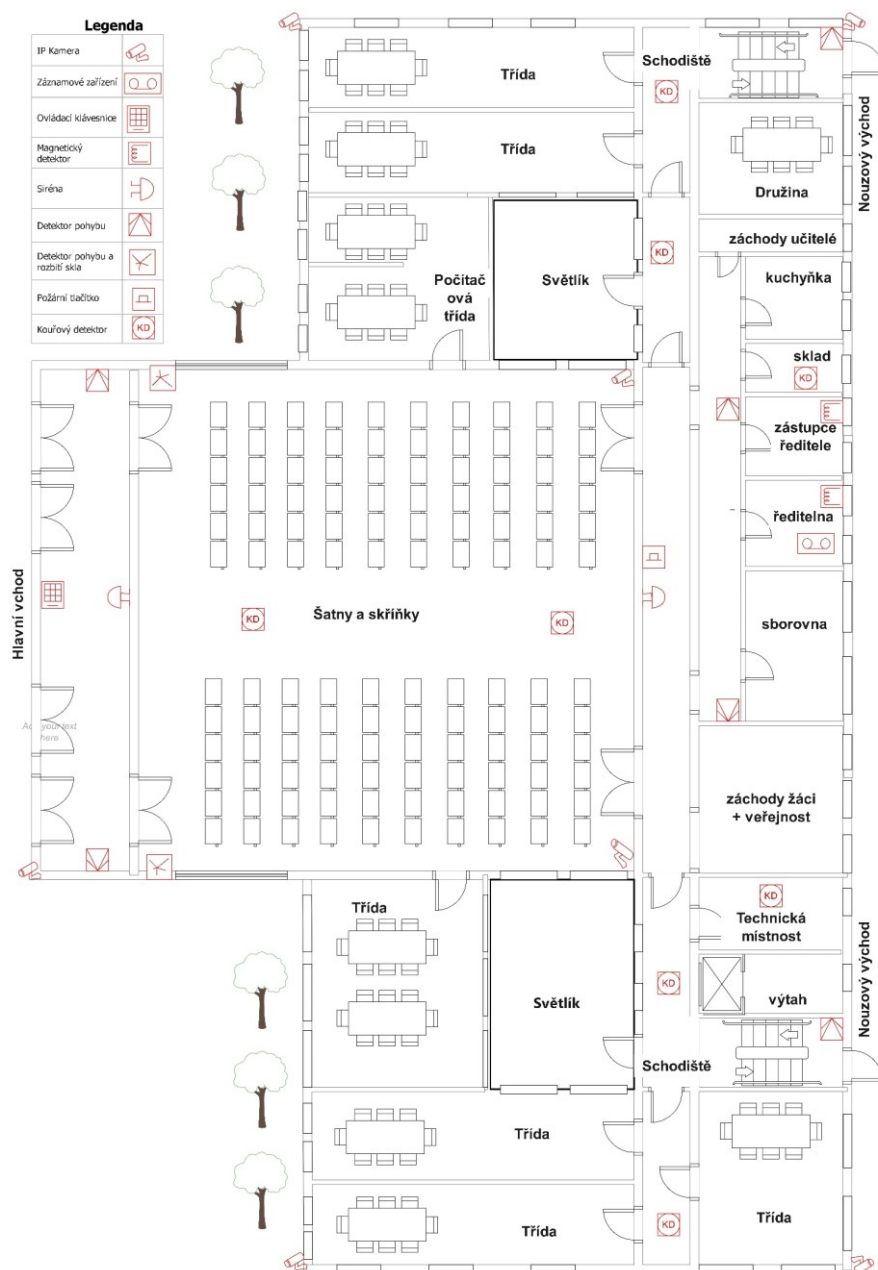
- Areál není monitorován dohledovým kamerovým systémem

Tabulka 30 Hrozby související s kamerovým systémem – VSS

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Hlavní budova a areál objektu	Krádež	1	3	2	3	24	III.
Majetek školy	Krádež	1	3	3	3	27	III.
Majetek zaměstnanců	Krádež	1	3	3	3	27	III.
Majetek žáků	Krádež	1	3	3	3	27	III.
	Zničení	1	3	3	3	27	III.

Lidé – zaměstnanci	Napadení	1	3	3	3	27	III.
Lidé – žáci	Napadení	1	3	3	3	27	III.
Peníze – hotovost u zaměstnanců	Krádež	1	3	3	3	27	III.
Peníze – hotovost u žáků	Krádež	1	4	2	3	24	III.
Kontinuita	Krádež	1	3	3	3	27	III.

(zdroj: vlastní)



Obrázek 27 Doplnění kamerového systému do přízemí hlavní budovy

(zdroj: vlastní)

8.6 Optimální požadavky netechnického charakteru pro zvýšení úrovně zabezpečení

V rámci netechnických opatření navržených pro optimální variantu zabezpečení zde uvádím návrh na zapojení bezpečnostní služby.

Fyzická ostraha

Pokud bychom chtěli do nákladů optimální varianty zabezpečení zahrnout fyzickou ostrahu objektu prostřednictvím bezpečnostní služby, bylo by nejprve nutné definovat konkrétní způsob, jakým bude tato ostraha zajištěna. Tento režim může být navržen individuálně – není nezbytné, aby byla ostraha přítomna nepřetržitě 24 hodin denně, 7 dní v týdnu. V mnoha případech postačí pravidelné kontrolní obchůzky v předem stanovených intervalech.

Z finančního hlediska však v této fázi není možné náklady přesně vyčíslit, protože budou závislé na konkrétním dodavateli bezpečnostních služeb, rozsahu poskytovaných služeb a jeho dojezdové vzdálenosti k objektu.

Pro ilustraci lze uvést orientační výpočet – při průměrné hodinové sazbě bezpečnostní služby ve výši přibližně 150 Kč (bez rozlišení pracovních dnů, víkendů a svátků) a zajištění kontroly po dobu 2 hodin denně [63], by celkové roční náklady činily přibližně:

- Dlouhodobá ostraha (déle než 3 měsíce) - 150,- Kč na hodinu – 2 hodiny denně – 365 dní v roce [63]

V celkové hodnotě bude započítána částka za rok, z důvodu lepší kalkulace výdajů

8.7 Vyčíslení nákladů

Vyčíslení nákladů v rámci optimální varianty zabezpečení odráží komfortní a ucelené řešení. Začlenění fyzické ostrahy sice zvyšuje finanční náročnost, ale zároveň významně posiluje celkovou efektivitu zabezpečení.

Tabulka 31 Náklady – varianta optimální požadavky

Produkt	Počet kusů	Cena za kus v Kč	Cena v Kč
Podhrabová deska betonová	127	399	50 673
VIVOTEK CC9380-HV	3	12 593	37 779
VIVOTEK FD9189-H-v2	1	8 390	8 390
Fyzická ostraha	300	365	109 500
Optimální varianta – rozšíření			206 342
Minimální varianta zabezpečení			478 824

Cena celkem		685 166
-------------	--	---------

(zdroj: vlastní)

Zhodnocení návrhu

Tato varianta představuje optimální návrh zabezpečení hlavní budovy i celého areálu a výrazně zvyšuje úroveň ochrany proti všem identifikovaným hrozbám. Použití podhrabových desek je velmi efektivní řešení pro zamezení neoprávněného vniknutí. Rozšíření kamerového systému umožní téměř úplný dohled nad celým areálem, čímž se zlepší kontrola pohybu osob v prostoru objektu. Doplnující fyzická ostraha by v tomto případě představovala vhodné rozšíření systému zabezpečení, které by přineslo další úroveň jistoty. Pro daný objekt by byla vhodná jakákoli forma monitorování, která přispěje k větší bezpečnosti.

8.8 Výstupní analýza

Ověření navržených opatření na základě metod analýzy rizik, které zde byly použity. Znovu provedu vyhodnocení kontrolním seznamem a analýzu rizik dle metody PNH.

vyhodnocení hrozeb dle kontrolního seznamu:

- Areál má nevyhovující oplocení
 - Opatření – plotový panel a sloupek
- Oplocení nemá další doplňkové zábrany
 - Opatření – podhrabová betonová deska
 - Opatření – bezpečnostní fólie
- Areál není monitorován dohledovým kamerovým systémem
 - Opatření – dohledový systém
- Hlavní vstupy do budovy nemají bezpečnostní certifikaci
 - Opatření zabezpečení oken a dveří
- Není zde použito přídatné bezpečnostní zařízení (mříže, bezpečnostní fólie)
 - Opatření – bezpečnostní fólie
- Systém PZS je nemoderní a opotřebovaný, neplní svoji funkci
 - Modernizace PZTS

- Systém PZS není instalován po celé budově, pouze v přízemí
 - Modernizace PZTS
- Ostraha objektu ani areálu není zajištěna bezpečnostní službou.
 - Opatření – připojení na systém PCO
 - Opatření – dohledový systém
- Ve vnitřních částech objektu není instalován kamerový dohled.
 - Opatření – dohledový systém

Po vložení bezpečnostních opatření nám výstupní Tabulka 32 metody PNH znovu vyhodnocuje hrozby, které byly zobrazeny v tabulce Tabulka 17 - PNH analýza rizikové stupně III. až I.

Tabulka 32 Výstupní analýza PNH

Aktivum	Hrozba	Období	P	N	H	Rizikovost	RS
Hlavní budova a areál objektu	Krádež	1	2	2	3	12	IV.
	Požár	1	1	3	3	9	IV.
		2	2	3	2	12	IV.
Majetek školy	Požár	1	2	3	2	12	IV.
		2	2	2	3	12	IV.
	Krádež	1	2	1	3	6	V.
Majetek zaměstnanců	Krádež	1	1	2	3	6	V.
Majetek žáků	Krádež	1	2	2	2	8	V.
	Zničení	1	2	3	1	6	V.
Lidé – zaměstnanci	Napadení	1	2	3	2	12	IV.
Lidé – žáci	Napadení	1	3	2	2	12	IV.
Peníze – hotovost u zaměstnanců	Krádež	1	2	3	3	12	IV.
Peníze – hotovost u žáků	Krádež	1	2	2	3	12	IV.
Kontinuita	Požár	1	2	2	3	12	IV.
		2	3	3	1	9	IV.
	Krádež	1	2	2	2	8	V.

(zdroj: vlastní)

Shrnutí osmé kapitoly

Osmá kapitola se věnuje návrhu řešení pro zvýšení úrovně zabezpečení základní školy na základě předchozí analýzy rizik a zjištěných hrozeb. Navrhovány jsou dvě varianty opatření – minimální a optimální. Minimální varianta se zaměřuje na klíčové prvky zabezpečení, jako je výměna nevyhovujícího oplocení, zabezpečení vstupních dveří a oken pomocí certifikovaných zámků a bezpečnostních fólií, instalace základního kamerového systému, modernizace stávajícího poplachového zabezpečovacího systému (PZTS) a zavedení jednoduchého systému elektrické požární signalizace (EPS). Dále počítá s napojením na pult centralizované ochrany. Optimální varianta rozšiřuje základní opatření o doplnění podhrabových desek k oplocení, rozšíření kamerového systému a zavedení fyzické ostrahy prostřednictvím externí bezpečnostní služby. Návrhy jsou zpracovány s ohledem na ekonomickou efektivitu a hodnotu chráněných aktiv. Výsledná výstupní analýza ukazuje, že navržená opatření vedou ke snížení rizik na přijatelnou úroveň a představují smysluplnou investici do bezpečnosti školy.

ZÁVĚR PRAKTICKÉ ČÁSTI

Praktická část diplomové práce se detailně zaměřila na zabezpečení konkrétní základní školy v Třebíči a jeho zhodnocení z hlediska bezpečnostních standardů. Úvodem byl podrobně popsán objekt školy včetně jeho areálu, technického vybavení a způsobu využití během školního dne i mimo něj. Na základě těchto informací byla provedena identifikace hlavních aktiv – budovy, majetku, osob i provozní kontinuity – a následně byla analyzována potenciální rizika, která by mohla tato aktiva ohrozit. Analýza byla zpracována pomocí metody PNH.

Součástí praktické části byla také analýza současného stavu zabezpečení objektu pomocí metody kontrolního seznamu, která poukázala na konkrétní nedostatky v jednotlivých oblastech ochrany – zejména na zastaralé či nefunkční technické prostředky, chybějící kamerový dohled, nedostatečné mechanické zabezpečení oken a dveří či absenci systému elektrické požární signalizace.

Na základě těchto zjištění byl navržen konkrétní soubor opatření rozdělený do dvou variant – minimální a optimální. Minimální varianta představuje základní úroveň zabezpečení, která reflektuje nejpalčivější nedostatky a navrhuje jejich efektivní, ale finančně šetrné řešení. Oproti tomu optimální varianta obsahuje rozšířená opatření včetně fyzické ostrahy, podhrabových desek a rozšíření kamerového systému, která dále zvyšují celkovou úroveň ochrany.

Výstupní analýza potvrdila, že navržené kroky vedou ke snížení identifikovaných rizik na akceptovatelnou úroveň a významně zvyšují celkovou úroveň ochrany osob, majetku i provozní kontinuity školy. Praktická část tak prokázala, že kombinace moderních technických a organizačních opatření může efektivně přispět k vytvoření bezpečného školního prostředí.

ZÁVĚR

Závěr diplomové práce shrnuje klíčové poznatky získané během teoretické i praktické části, které společně tvoří ucelený pohled na problematiku zabezpečení objektu základní školy s využitím integrovaného bezpečnostního systému. V teoretické části byly popsány základní pojmy z oblasti bezpečnosti, právní rámec a platné technické normy, které tvoří základ pro správné navrhování ochranných opatření. Dále byly rozpracovány jednotlivé typy ochran, specifika zabezpečení školních objektů a možnosti využití moderních technických systémů jako jsou PZTS, EPS, VSS a MZS. Teoretický základ poskytl nezbytné východisko pro praktickou část práce.

Praktická část se zaměřila na konkrétní objekt základní školy v Třebíči. Byla provedena analýza stávajícího stavu zabezpečení pomocí kontrolního seznamu a riziková analýza metodou PNH, která umožnila identifikovat kritické slabiny v ochraně areálu, budovy, majetku i osob. Následně byl navržen soubor bezpečnostních opatření ve dvou variantách – minimální a optimální – které reflektují nejen úroveň rizik, ale i ekonomickou přiměřenost navržených řešení. Závěrečná výstupní analýza potvrdila, že implementace těchto opatření významně snižuje úroveň rizik a zvyšuje celkovou bezpečnostní úroveň objektu.

Diplomová práce tak prokázala, že správně provedená analýza rizik a důsledně zpracovaný návrh opatření mohou zásadně přispět k ochraně školního prostředí. Výsledky této práce jsou aplikovatelné nejen na konkrétní objekt, ale mohou sloužit jako vzorový přístup i pro další školy a veřejné budovy, které hledají efektivní a realistické cesty ke zvýšení bezpečnosti.

SEZNAM POUŽITÉ LITERATURY

- [1] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management II. Zlín: Radim Bačuvčík – VeRBuM, 2012. ISBN 978-80-87500-19-4.
- [2] LUKÁŠ, Luděk. Teorie bezpečnosti I. Zlín: Radim Bačuvčík - VeRBuM, 2017. ISBN 978-80-87500-89-7.
- [3] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. Zlín: Radim Bačuvčík – VeRBuM, 2011. ISBN 978-80-87500-05-7.
- [4] VALOUCH, Jan. Projektování bezpečnostních systémů. 2. vydání. Zlín: Univerzita Tomáše Bati ve Zlíně, 2019. ISBN 978-80-7454-858-1.
- [5] ZEMAN, Petr. Česká bezpečnostní terminologie: výklad základních pojmů. Brno: Masarykova univerzita v Brně, Mezinárodní politologický ústav. Sborníky, sv. 11., 2002. ISBN 80-210-3037-2.
- [6] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management IV. Zlín: Radim Bačuvčík – VeRBuM, 2014. ISBN 978-80-87500-57-6.
- [7] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management III. Zlín: Radim Bačuvčík – VeRBuM, 2013. ISBN 978-80-87500-35-4.
- [8] KYSELOVÁ, Lucie. České technické normy, jejich závaznost a užitečnost. Online. VÝZKUMNÝ ÚSTAV BEZPEČNOSTI PRÁCE, V. V. I. ZNALOSTNÍ SYSTÉM PREVENCE RIZIK V BOZP. 2019. Dostupné z: <https://zsbozp.vubp.cz/ceske-technicke-normy-jejich-zavaznost-a-uzitecnost>. [cit. 2024-04-01].
- [9] MVČR. Stanovení úrovně zabezpečení objektů a provozoven proti vloupání podle evropských technických norem. Online. MVČR. Ministerstvo vnitra České republiky. 2018. Dostupné z: <https://www.mvcr.cz/clanek/stanoveni-urovne-zabezpeceni-objektu-a-provozoven-proti-vloupani-podle-evropskych-technickych-norem.aspx>. [cit. 2024-04-01].
- [10] Zákon č. 22/1997 Sb.: Zákon o technických požadavcích na výrobky a o změně a doplnění některých zákonů. Zákony pro lidi [online]. 1997. Dostupné z: <https://www.zakonyprolidi.cz/cs/1997-22>. [cit. 2024-03-29].
- [11] TECHNOR PRINT, S.R.O. 3345 - Elektrická řídicí zařízení. Online. TECHNOR PRINT, S.R.O., ČESKOSLOVENSKÉ ARMÁDY 216/41, 500 03 HRADEC

- KRÁLOVÉ. Technické normy ČSN. 2022. Dostupné z: <https://www.technicke-normy-csn.cz/technicke-normy-csn/33-elektrotechnika-elektrotechnicke-predpisy/3345-elektricka-ridici-zarizeni/>. [cit. 2024-04-01].
- [12] Zákon č. 89/2012 Sb.: Zákon občanský zákoník. Online. In: *Zákony pro lidi*. 2012. Dostupné z: <https://www.zakonyprolidi.cz/cs/2012-89>. [cit. 2024-04-04].
- [13] KOTKOVÁ, Dora; KOTEK, Lukáš; JENČKOVÁ, Klára; KALVACH, Zdeněk a ŠTERNOVÁ, Tereza. *Hromadné společenské a kulturní akce a jejich ochrana*. Online. Zlín: Univerzita Tomáše Bati ve Zlíně, 2021. ISBN 978-80-7678-058-3. Dostupné z: <https://digilib.k.utb.cz/handle/10563/50142>. [cit. 2024-04-04].
- [14] Zákon č. 273/2008 Sb.: Zákon o Policii České republiky. Online. In: *Zákony pro lidi*. 2008. Dostupné z: https://www.zakonyprolidi.cz/cs/2008-273#_. [cit. 2024-04-04].
- [15] Zákon č. 40/2009 Sb.: Zákon trestní zákoník. Online. In: *Zákony pro lidi*. 2009. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>. [cit. 2024-04-04].
- [16] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Co je GDPR. Online. MVCR. 2024. Dostupné z: <https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx>. [cit. 2024-04-05].
- [17] EUR-LEX. Nařízení - 2016/679 - EN – GDPR - EUR-Lex. Online. EUR-Lex Access to European Union law. 2024. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679>. [cit. 2024-04-05].
- [18] Zákon č. 110/2019 Sb.: Zákon o zpracování osobních údajů. Online. In: *Zákony pro lidi*. 2019. Dostupné z: <https://www.zakonyprolidi.cz/cs/2019-110>. [cit. 2024-04-05].
- [19] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.
- [20] ŠEFCÍK, Vladimír. *Analýza rizik*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-80-7318-696-8.
- [21] ČERMÁK, Miroslav. *Analýza rizik: Jemný úvod do analýzy rizik*. Online. In: *Clever and Smart*. 2010. Dostupné z: <https://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/>. [cit. 2024-04-15].

- [22] SMEJKAL, Vladimír a RAIS, Karel. Řízení rizik ve firmách a jiných organizacích. 3., rozš. a aktualiz. vyd. Expert (Grada). Praha: Grada, 2010. ISBN 978-80-247-3051-6.
- [23] Metody a způsoby hodnocení rizik na pracovišti. Online. In: CRDR SPOL. S R.O. Dokumentace BOZP. 2018. Dostupné z: https://www.dokumentacebozp.cz/aktuality/metody-hodnoceni-rizik-bozp/#kap_12. [cit. 2024-04-27].
- [24] SWOT Analysis A tool for making better business decisions. Online. Ucanr.edu. 2008. Dostupné z: <https://ucanr.edu/sites/nichemarketing/files/341914.pdf>. [cit. 2025-02-11].
- [25] SWOT analýza v Excelu. Online. In: Fotis Fotopulos, 2011. 2011. Dostupné z: http://excel-navod.fotopulos.net/swot-analyza.html#SWOT_analyza_-_teorie. [cit. 2024-04-27].
- [26] LÁŠVAY, Radek. FTA. Online. Ikvalita.cz. 2020. Dostupné z: <http://www.ikvalita.cz/tools.php?ID=52>. [cit. 2024-04-29].
- [27] KOUDELKA, Ctirad a VRÁNA, Václav. Rizika a jejich analýza. Online, skripta. Ostrava: VŠB – TU Ostrava, Fakulta elektrotechniky a informatiky, Katedra obecné elektrotechniky, 2006. Dostupné z: <https://docplayer.cz/421968-Rizika-a-jejich-analyza.html>. [cit. 2024-04-30].
- [28] VALOUCH, Jan a HROMADA, Martin. Bezpečnostní futurologie. Zlín: Univerzita Tomáše Bati ve Zlíně, 2016. ISBN 978-80-7454-621-1.
- [29] IVANKA, Ján a Fakulta aplikované informatiky. Mechanické zábranné systémy. Online. Druhé. Zlín: Univerzita Tomáše Bati ve Zlíně, 2014. ISBN 978-80-7454-427-9. Dostupné z: <https://digilib.k.utb.cz/handle/10563/18575>. [cit. 2025-02-25].
- [30] LENNART, Alexandrie a SÖDERLUND, Henrik. Things to consider when specifying lighting for perimeter security: Perimeter surveillance – Part 4 of 6. Online. In: The North America Security Market. 05/04/2022. Dostupné z: <https://www.securityworldmarket.com/na/News/Themes/things-to-consider-when-specifying-lighting-for-perimeter-security>. [cit. 2025-02-27].

- [31] WORBIS, Vít. Plášťová ochrana. Online. In: ChatGPT. 2025. Dostupné z: OpenAI, <https://chatgpt.com/share/67c05652-4078-8002-bec6-42a7a0ea1380>. [cit. 2025-02-27].
- [32] ČSN EN 50131-1 ED.2... Online. In: TECHNOR PRINT, S.R.O. TECHNOR Technické normy ČSN. 04/2007. Dostupné z: <https://www.technicke-normy-csn.cz/csn-en-50131-1-ed-2-334591-181882.html>. [cit. 2025-03-02].
- [33] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management V. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-67-5.
- [34] BROŽ, Radim. MZS – mechanické zábranné systémy. Online. Elektronická učebnice. 2025. Dostupné z: <https://eluc.ikap.cz/lekce/mechanicke-zabezpeceni>. [cit. 2025-03-11].
- [35] FRYČ, Zbyněk. Kamerové systémy. Online. In: Aret. 2024. Dostupné z: <https://www.aret.info/kamerove-systemy.html>. [cit. 2025-03-13].
- [36] ADÁMEK, Milan. Struktura kamerového systému: Kamerové systémy. Online, Prezentace. Zlín: Univerzita Tomáše Bati ve Zlíně, Ústav bezpečnostního inženýrství, Fakulta aplikované informatiky, 2023.
- [37] Kamerový systém. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2001-. Dostupné z: https://cs.wikipedia.org/wiki/Kamerov%C3%BD_syst%C3%A9m. [cit. 2025-03-13].
- [38] Elektronická požární signalizace (EPS): Co tvoří systém EPS? Online. In: VA-Elektronik – Zabezpečení objektů a slaboproudé rozvody. 2025. Dostupné z: <https://www.va-elektronik.cz/faq/co-tvori-system-eps>. [cit. 2025-03-17].
- [39] Elektronická zabezpečovací signalizace. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2024. Dostupné z: https://cs.wikipedia.org/wiki/Elektronick%C3%A1_zabezpe%C4%8Dovac%C3%A1_D_signalizace. [cit. 2025-03-18].
- [40] BÁRTL, Vítězslav. ZŠ a MŠ Třebíč, Na Kopcích 342: Výroční zpráva. Online. In: Zskopce. 28.září 2024. Dostupné z: https://www.zskopce.cz/data_6/soubory/159.pdf. [cit. 2025-04-08].

- [41] ZŠ Na Kopcích: Třebíč. Online. In: Mapy.cz. 2025. Dostupné z: <https://mapy.cz/letecka?source=firm&id=359744&gallery=1&sourcep=ffoto&idp=622293&x=15.9020583&y=49.2191296&z=17>. [cit. 2025-04-08].
- [42] Satelitní snímek Třebíč. Online. In: Mapy.cz. 2025. Dostupné z: <https://mapy.cz/letecka?x=15.9019399&y=49.2191161&z=18>. [cit. 2025-04-12].
- [43] Mapa kriminality. Online. In: © 2025 POLICIE ČR. Kriminalita.policie.cz. 2025. Dostupné z: <https://kriminalita.policie.gov.cz/>. [cit. 2025-04-13].
- [44] Plotový panel 2D DOUBLE LIGHT – 183 cm, drát 5/4/5 mm, antracit. Online. In: Levné-pletivo.cz. 2025. Dostupné z: <https://www.levne-pletivo.cz/plotovy-panel-2d-double-light-183-cm-drat-5-4-5-mm-antracit/>. [cit. 2025-05-14].
- [45] Sloupek 60x40mm PVC 200 cm. Online. In: Levné-pletivo.cz. 2025. Dostupné z: <https://www.levne-pletivo.cz/jekl-60-x-40-poplastovany-vyska-200-cm/>. [cit. 2025-05-14].
- [46] Třída bezpečnosti dveří: Co je třída bezpečnosti dveří? Online. In: Lomax.cz. 2025. Dostupné z: <https://www.lomax.cz/trida-bezpecnosti-dveri>. [cit. 2025-05-15].
- [47] Jednostranná cylindrická vložka FAB 2. Online. In: Fab-shop.cz. 2025. Dostupné z: <https://www.fab-shop.cz/jednostranna-cylindricka-vlozka-fab-2-1>. [cit. 2025-05-15].
- [48] Bezpečnostní kování - 802. Online. In: Eshop.rostex.cz. 2025. Dostupné z: <https://eshop.rostex.cz/eshop-bezpecnostni-kovani-802-29.html>. [cit. 2025-05-15].
- [49] Bezpečnostní folie SMC7. Online. In: Sklenarstvinonstop.cz. 2025. Dostupné z: <https://www.sklenarstvinonstop.cz/bezpecnostni-folie-smc7.htm>. [cit. 2025-05-15].
- [50] VIVOTEK FD9189-H-v2. Online. In: Kamery-vivotek.cz. 2025. Dostupné z: <https://www.kamery-vivotek.cz/vnitri-ip-kamery-vivotek-fixdome-dome/vivotek-fd9189-h-v2/>. [cit. 2025-05-15].
- [51] VIVOTEK ND9323P. Online. In: Kamery-vivotek.cz. 2025. Dostupné z: <https://www.kamery-vivotek.cz/zaznamova-zarizeni-vivotek/vivotek-nd9323p/>. [cit. 2025-05-15].
- [52] WD RED Plus 4 TB. Online. In: Kamery-vivotek.cz. 2025. Dostupné z: <https://www.kamery-vivotek.cz/pevne-disky/wd-red-plus-4-tb/>. [cit. 2025-05-15].

- [53] VIVOTEK CC9380-HV. Online. In: Kamery-vivotek.cz. 2025. Dostupné z: <https://www.kamery-vivotek.cz/venkovni-ip-kamery-180-panoramicke/vivotek-cc9380-hv/>. [cit. 2025-05-15].
- [54] VIVOTEK FD9383-HVF2. Online. In: Kamery-vivotek.cz. 2025. Dostupné z: <https://www.kamery-vivotek.cz/venkovni-ip-kamery-vivotek-fixdome/vivotek-fd9383-hvf2/>. [cit. 2025-05-15].
- [55] ALARMAX s.r.o.: Specializovaný e-shop se zabezpečovací technikou. Online. In: Alarmax.cz. 2025. Dostupné z: <https://www.alarmax.cz/>. [cit. 2025-05-16].
- [56] Euroalarm B01090-00 "APOLLO F2": 1-2 smyčková ústředna EPS. Online. In: Euroalarm.cz. 2025. Dostupné z: <https://www.euroalarm.cz/eshop-zabezpecovaci-technika/pozarni-signalizace/analogove-systemy/ustredny/apollo-f2/b01090-00-apollo-f2>. [cit. 2025-05-16].
- [57] Euroalarm AKU CJ-12/12Ah. Online. In: Euroalarm.cz. 2025. Dostupné z: <https://www.euroalarm.cz/eshop-zabezpecovaci-technika/zdroje-napajeni-a-zaloha/olovene-akumulatory/akumulatory-alarmguard/aku-cj-12-12ah>. [cit. 2025-05-16].
- [58] Euroalarm SA5900-908APO: SOTERIA tlačítkový hlásič s izolátorem. Online. In: Euroalarm.cz. 2025. Dostupné z: <https://www.euroalarm.cz/eshop-zabezpecovaci-technika/pozarni-signalizace/analogove-systemy/hlasice/tlacitka/sa5900-908apo>. [cit. 2025-05-16].
- [59] Euroalarm PSS-0020: Siréna, červená, 106 dB, 32 tónů. Online. In: Euroalarm.cz. 2025. Dostupné z: <https://www.euroalarm.cz/eshop-zabezpecovaci-technika/pozarni-signalizace/signalizace/sireny/pss-0020>. [cit. 2025-05-16].
- [60] Euroalarm TSD-1: Teplotní a kouřový detektor. Online. In: Euroalarm.cz. 2025. Dostupné z: <https://www.euroalarm.cz/eshop-zabezpecovaci-technika/zabezpeceni/detektory/pozarni-hlasice-pro-pzts/tsd-1>. [cit. 2025-05-16].
- [61] Cena za napojení objektu na PCO. Online. In: Pult-centralizovane-ochrany.cz. 2025. Dostupné z: <https://www.pult-centralizovane-ochrany.cz/cena-napojeni-pco/>. [cit. 2025-05-17].

- [62] Podhrabová deska betonová 2500 x 200 x 40 mm. Online. In: Nej-plot.cz. 2025. Dostupné z: <https://nej-plot.cz/produkt/podhrabova-deska-betonova-2500-x-20-x-40-mm/>. [cit. 2025-05-17].
- [63] Fyzická ostraha: Fyzická ostraha majetku a osob. Online. In: SOMAX SECURITY, s. r. o. 2025. Dostupné z: <https://www.somax.cz/cenik/fyzicka-ostraha/>. [cit. 2025-05-17].
- [64] NORMAN, Thomas P. Electronic access control. Amsterdam: Butterworth-Heinemann, 2012. ISBN 978-0-12-382028-0. Dostupné také z: <https://ebookcentral.proquest.com/lib/natl-ebooks/detail.action?docID=787245>.
- [65] LOVEČEK, Tomáš a REITŠPÍŠ, Josef. Projektovanie a hodnotenie systémov ochrany objektov. Vedecké monografie. V Žiline: Žilinská univerzita v Žiline, EDIS-vydavateľstvo Žilinskej univerzity, 2011. ISBN 978-80-554-0457-8.
- [66] PETRÁŠ, Dušan. Analýza rizik a návrh zabezpečení objektu autoservisu. Online, Diplomová práce, vedoucí Martin Hromada. Zlín: Univerzita Tomáše Bati ve Zlíně, 2024. Dostupné z: <http://195.178.95.140:8080/handle/10563/55548>. [cit. 2025-05-18].

SEZNAM OBRÁZKŮ

Obrázek 1 Analýza rizik [21].....	26
Obrázek 2 SWOT analýza rizik [25].....	28
Obrázek 3 Ukázka FTA analýzy [vlastní].....	33
Obrázek 4 Bezpečnostní opatření [vlastní]	40
Obrázek 5 Kategorie ochran [vlastní]	42
Obrázek 6 Perimetrická ochrana [30]	43
Obrázek 7 Plášťová ochrana – vytvořená podle AI [31]	44
Obrázek 8 Bezpečnost objektu podle stupně ochrany [vlastní]	45
Obrázek 9 Ukázka – schéma zapojení systému EPS [vlastní]	55
Obrázek 10 Ukázka – schéma zapojení systému PZTS [vlastní].....	59
Obrázek 11 Vchod do ZŠ Na Kopcích [41].....	65
Obrázek 12 Satelitní snímek Třebíč [42]	66
Obrázek 13 Půdorys hlavní budovy 1.podlaží [vlastní]	68
Obrázek 14 Půdorys hlavní budovy 2.podlaží [vlastní]	69
Obrázek 15 Půdorys hlavní budovy 3.podlaží [vlastní]	70
Obrázek 16 Mapa kriminality v Třebíči [43]	71
Obrázek 17 Plot okolo základní školy [vlastní]	81
Obrázek 18 Vstup do areálu – Hlavní brána [vlastní].....	81
Obrázek 19 Fotografie umístěného systému PZS [vlastní].....	85
Obrázek 20 Ústředna EPS [56]	93
Obrázek 21 Požární tlačítko [58]	93
Obrázek 22 Siréna [59]	94
Obrázek 23 Teplotní a kouřový detektor [60].....	94
Obrázek 24 Přízemí hlavní budovy s elektronickými zabezpečovacími systémy [vlastní].....	95
Obrázek 25 První patro hlavní budovy s elektronickými zabezpečovacími systémy [vlastní]	96
Obrázek 26 Druhé patro hlavní budovy s elektronickými zabezpečovacími systémy [vlastní]	97
Obrázek 27 Doplnění kamerového systému do přízemí hlavní budovy [vlastní].....	102

SEZNAM TABULEK

Tabulka 1 Příklad vyjádření hodnot při jednotlivých typech analýzy rizik [vlastní]	34
Tabulka 2 Pravděpodobnost vzniku rizika [27]	35
Tabulka 3 Možné následky ohrožení [27]	35
Tabulka 4 Názor hodnotitelů [27]	36
Tabulka 5 Celkové hodnocení rizika [27]	36
Tabulka 6 Úroveň rizika a stupeň zabezpečení [vlastní]	46
Tabulka 7 Rozdělení chráněných objektů z hlediska prostředí [vlastní]	47
Tabulka 8 Celková suma uvedených aktiv [vlastní]	73
Tabulka 9 Zvolená aktiva a hrozby [vlastní]	75
Tabulka 10 PNH analýza – Hlavní budova a areál objektu [vlastní]	75
Tabulka 11 PNH analýza – Majetek školy [vlastní]	76
Tabulka 12 PNH analýza – Majetek zaměstnanců [vlastní]	76
Tabulka 13 PNH analýza – Majetek žáků [vlastní]	76
Tabulka 14 PNH analýza – Lidé [vlastní]	77
Tabulka 15 PNH analýza – Peníze - hotovost [vlastní]	77
Tabulka 16 PNH analýza – Kontinuita [vlastní]	78
Tabulka 17 PNH analýza rizikové stupně III. až I. [vlastní]	78
Tabulka 18 Kontrolní seznam – Perimetrická ochrana [vlastní]	81
Tabulka 19 Kontrolní seznam – Plášťová ochrana [vlastní]	82
Tabulka 20 Kontrolní seznam – Prostorová ochrana [vlastní]	83
Tabulka 21 Kontrolní seznam – Předmětová ochrana a Fyzická ostraha [vlastní]	84
Tabulka 22 Hrozby související s výměnou plotových panelů [vlastní]	88
Tabulka 23 Hrozby související se zabezpečením oken a dveří [vlastní]	89
Tabulka 24 Hrozby související s kamerovým systémem – VSS [vlastní]	91
Tabulka 25 Hrozby související s ochranou PZTS [vlastní]	92
Tabulka 26 Hrozby související s požární ochranou [vlastní]	94
Tabulka 27 Hrozby související s bezpečnostní službou [vlastní]	98
Tabulka 28 Náklady – varianta minimální požadavky [vlastní]	99
Tabulka 29 Hrozby související s výměnou plotových panelů [vlastní]	100
Tabulka 30 Hrozby související s kamerovým systémem – VSS [vlastní]	101
Tabulka 31 Náklady – varianta optimální požadavky [vlastní]	103
Tabulka 32 Výstupní analýza PNH [vlastní]	105

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI	Artificial intelligence – umělá inteligence
AKU	Akumulátorový
CCTV	Closed-circuit television, uzavřený televizní okruh
ČR	Česká republika
ČSN	Česká technická norma
DV	Dohledový video systém
DVR	Digital Video Recorder – nahrávací zařízení
EN	Evropská norma
EPS	Elektronická požární signalizace
EU	Evropská unie
GDPR	General Data Protection Regulation
GSM	Groupe Spécial Mobile
HZS	Hasičský záchranný sbor
ICT	Information and Communication Technologies
LAN	Local Area Network
LCD	Liquid Crystal Display
MZS	Mechanické zábranné systémy
PCO	Pult centrální ochrany
PIR	Passive infra red - pasivní infračervené čidlo
PZS	Poplachový zabezpečovací systém
PZTS	Poplachový zabezpečovací a tísňový systém
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
VSS	Video Surveillance Systems
ZŠ	Základní škola

SEZNAM PŘÍLOH

Příloha P I: Název první přílohy

PŘÍLOHA P I: NÁZEV PRVNÍ PŘÍLOHY

Obsah první přílohy.