

Posouzení zabezpečení objektu z hlediska bezpečnostních rizik

Bc. David Rudý

Diplomová práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav krizového řízení

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. David Rudý
Osobní číslo:	L23345
Studijní program:	N1032A020002 Bezpečnost společnosti
Specializace:	Rizikové inženýrství
Forma studia:	Kombinovaná
Téma práce:	Posouzení zabezpečení objektu z hlediska bezpečnostních rizik

Zásady pro vypracování

- Zpracujte literární rešerši o zabezpečení objektů z hlediska bezpečnostních rizik.
- Posuďte současný stav ochrany řešeného objektu.
- Posuďte rizika, které ohrožují zkoumaný objekt.
- Navrhněte opatření zvyšující úroveň zabezpečení objektu.

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

Seznam doporučené literatury:

1. BURDA, Karel. *Základy elektronických zabezpečovacích systémů*. Brno: CERM, 2018. ISBN 978-80-7204-967-7.
2. HOFREITER, Ladislav. *Manažment ochrany objektov*. Žilina: EDIS – vydavateľstvo Žilinskej univerzity v Žiline, 2016. ISBN 978-80-554-1164-4.
3. KHAIRALLAH, Michael. *Physical Security Assessment Handbook: An Insider's Guide to Securing a Business*. 2. doplněné a upravené vydání. CRC Press, 2024. ISBN 9781032790800.
4. KRATOCHVÍL, Václav; KRATOCHVÍL, Michal a NAVAROVÁ, Šárka. *Požární bezpečnostní zařízení ve stavbách: Stručná encyklopedie pro jednotky PO, požární prevenci a odbornou veřejnost*. 2. doplněné a upravené vydání. Praha: Sdružení požárního a bezpečnostního inženýrství, 2021. ISBN 978-80-7385-238-2.
5. LOVEČEK, Tomáš; MARIŠ, Ladislav a ŠISER, Anton. *Plánovanie a projektovanie systémov ochrany objektov*. Žilina: EDIS – vydavateľstvo Žilinskej univerzity v Žiline, 2018. ISBN 978-80-554-1482-9.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **doc. Ing. Miroslav Tomek, PhD.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **2. prosince 2024**
Termín odevzdání diplomové práce: **25. dubna 2025**

L.S.

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

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 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.

V Uherském Hradišti, dne 25.04.2025

.....
podpis autora

ABSTRAKT

Diplomová práce se věnuje problematice zabezpečení objektů vůči potenciálním hrozbám. Cílem práce je posoudit zabezpečení zkoumaného objektu a navrhnout opatření, která zajistí vyšší úroveň jeho ochrany před identifikovanými hrozbami. Teoretická část práce se zaměřuje na právní prameny týkající se zabezpečení vybraných subjektů a dále specifikuje jednotlivé složky v rámci fyzické bezpečnosti. Praktická část práce obsahuje analýzu bezpečnostního prostředí zkoumaného objektu a následné hodnocení složek rizika, jako jsou pravděpodobnost výskytu události, zranitelnost objektu či potenciální negativní následky při narušení bezpečnosti vybraného objektu. Na základě výsledků analýzy jsou navržena doporučení a opatření zaměřená na zvýšení celkové úrovně ochrany objektu.

Klíčová slova: bezpečnost, dopad, objekt, ohrožení, riziko, zabezpečení, zranitelnost

ABSTRACT

The diploma thesis addresses the issue of object security against potential threats. Its aim is to assess the security of the studied object and propose measures to enhance its protection against identified threats. The theoretical part focuses on legal frameworks related to the security of selected entities and further specifies individual components of physical security. The practical part includes an analysis of the security environment of the studied object, followed by an assessment of risk components such as the likelihood of an event occurring, the vulnerability of the object, and the potential negative consequences of a security breach. Based on the analysis results, recommendations and measures to enhance the overall level of protection are proposed.

Keywords: safety, impact, object, threat, risk, security, vulnerability

Rád bych srdečně poděkoval doc. Ing. Miroslavu Tomkovi, PhD., za jeho profesionální přístup k vedení studentů a cenný čas, který mi věnoval při zpracování této práce.

Velké díky patří mé rodině a přátelům za veškerou podporu, které se mi od nich dostávalo.

Dále chci poděkovat představitelům Fakulty logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně za příležitost k osobnímu rozvoji, kterou mi během studia poskytli.

OBSAH

ÚVOD.....	11
CÍLE PRÁCE A POUŽITÉ METODY	12
I TEORETICKÁ ČÁST	14
1 TERMINOLOGIE A PRÁVNÍ NORMY ČESKÉ REPUBLIKY V OBLASTI ZABEZPEČENÍ OBJEKTU.....	15
1.1 VYMEZENÍ ZÁKLADNÍCH POJMŮ	16
1.2 PRÁVNÍ NORMY	17
1.3 PRÁVNÍ RÁMEC OCHRANY VYBRANÝCH SUBJEKTŮ.....	21
2 ZABEZPEČENÍ OCHRANY OBJEKTU.....	24
2.1 MECHANICKÝ ZÁBRANNÝ SYSTÉM	24
2.2 POPLACHOVÝ ZABEZPEČOVACÍ A TÍŠŇOVÝ SYSTÉM	27
2.3 ELEKTRONICKÝ SYSTÉM KONTROLY VSTUPU	28
2.4 DOHLEDOVÝ VIDEOSYSTÉM	31
3 ORGANIZAČNÍ PROSTŘEDKY OCHRANY OBJEKTU	37
3.1 REŽIMOVÁ OCHRANA OBJEKTU	37
3.2 FYZICKÁ OSTRaha OBJEKTU	38
DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI.....	40
II PRAKTICKÁ ČÁST	42
4 INFORMACE O OBJEKTU.....	43
4.1 KRIMINALITA V LOKALITĚ	44
4.2 NEBEZPEČNÉ LÁTKY NACHÁZEJÍCÍ SE V OBJEKTU	45
4.3 SPECIFIKACE CHRÁNĚNÝCH PROSTOR.....	48
5 SOUČASNÝ STAV ZABEZPEČENÍ OBJEKTU.....	52
5.1 SOUČASNÝ STAV ZABEZPEČENÍ PERIMETRU AREÁLU	52
5.2 SOUČASNÝ STAV ZABEZPEČENÍ PLÁŠŤŮ BUDOV	58
5.3 TECHNICKÉ ZABEZPEČENÍ PROSTOROVÉ OCHRANY	61
5.4 ZAJIŠTĚNÍ FYZICKÉ OSTRahY	61
5.5 VNITŘNÍ REŽIMOVÁ OPATŘENÍ	62
5.6 ZHODNOCENÍ SOUČASNÉHO STAVU ZABEZPEČENÍ	62
6 POSOUZENÍ BEZPEČNOSTNÍCH RIZIK	65
6.1 IDENTIFIKACE AKTIV A HROZEB	65
6.2 ANALÝZA A HODNOCENÍ BEZPEČNOSTNÍCH RIZIK	68
6.3 STANOVENÍ ZRANITELNOSTI CHRÁNĚNÝCH PROSTOR	73

7	NÁVRH OPATŘENÍ ZVYŠUJÍCÍCH CELKOVOU ÚROVEŇ OCHRANY OBJEKTU	78
8	SHRNUTÍ.....	83
	ZÁVĚR.....	84
	SEZNAM POUŽITÉ LITERATURY	85
	SEZNAM OBRÁZKŮ	90
	SEZNAM TABULEK.....	91
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	92
	SEZNAM PŘÍLOH.....	93

ÚVOD

Zabezpečení majetku není novodobý trend, ale jeho kořeny sahají hluboko do historie, kdy lidé čelili hrozbám ztráty nejen svého majetku, ale také svého života. Tento přirozený instinkt chránit to, co je pro jednotlivce nebo komunitu cenné, byl hnacím motorem pro vznik forem ochrany, jako byly opevnění, strážní věže nebo hradby, které chránily obyvatelstvo před nepřátelskými útoky zvenčí. S postupem času se tento instinkt měnil v organizovanější a sofistikovanější způsoby ochrany, včetně vytváření pravidel, zákonů a institucí, které zajišťovaly bezpečnost a stabilitu ve společnosti. Ochrana života a majetku se tak stala základním pilířem rozvoje civilizací, ať už prostřednictvím osobní ostrahy, státní moci nebo kolektivní obrany, což vedlo k posílení stability společnosti.

Dnes již zabezpečení majetku nespočívá pouze v mechanických zábranných prostředcích, ale stále více se opírá o moderní technologie, jako jsou umělá inteligence, kamerové systémy, chytré alarmy, biometrická autentizace uživatele a další pokročilé technologie. Tyto inovativní metody ochrany jsou běžnou součástí ochrany domovů, podniků i veřejných institucí, přičemž výrazně zvyšují úroveň bezpečnosti a efektivitu ochrany. Kombinace těchto moderních technologií představuje komplexní a efektivní způsob, jak chránit nejen majetek, ale i životy, zdraví, data a soukromí. Vzhledem k neustálému vývoji technologií je zřejmé, že budoucnost bude i nadále směřovat k ještě pokročilejším a inteligentnějším systémům, které budou reagovat autonomně na stále sofistikovanější hrozby.

V této práci je věnována pozornost fyzické bezpečnosti zkoumaného objektu, prostřednictvím identifikace a analýzy aktiv, potenciálních hrozeb, zranitelností, možných negativních dopadů a pravděpodobností výskytu mimořádné události. Během realizace praktické části se zaměříme na to, zdali je současná úroveň ochrany zkoumaného objektu dostatečná pro eliminaci nebo minimalizaci identifikovaných hrozeb.

CÍLE PRÁCE A POUŽITÉ METODY

Hlavním cílem této práce je vyhodnocení současné úrovně zabezpečení zkoumaného objektu a následné navržení bezpečnostních opatření, která povedou k posílení úrovně ochrany objektu s ohledem na identifikované potenciální hrozby.

Prvním dílčím cílem je provedení analýzy vnitřního a vnějšího bezpečnostního prostředí zkoumaného objektu.

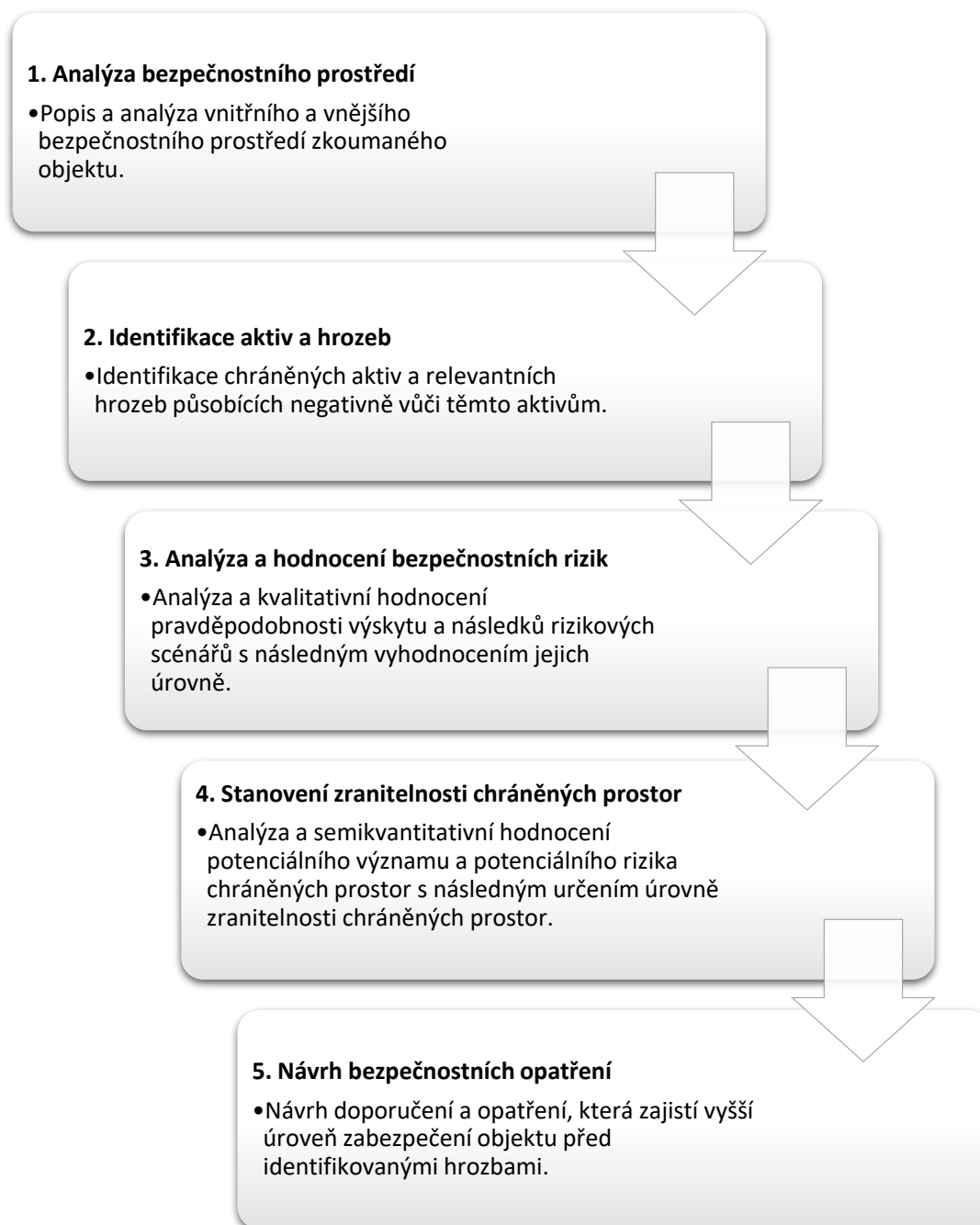
Druhým dílčím cílem je identifikace a vyhodnocení úrovně jednotlivých hrozeb s následným zaměřením na rizikové scénáře vyhodnocené s nepříjatelnou, nebo podmíněně přijatelnou úrovní rizika, při návrhu bezpečnostních opatření.

Třetím dílčím cílem je identifikace a vyhodnocení nejzranitelnějších chráněných prostor v rámci objektu, které mají pro podnik zvláštní význam.

Čtvrtým dílčím cílem je poskytnutí výsledků diplomové práce a relevantních informací příslušníkům soukromé bezpečnostní služby, které poslouží jako východisko pro provedení bezpečnostního auditu daného objektu.

Pro získání empirických dat jsou v práci využity jednoduché metody zahrnující kontrolní seznamy, pozorování a nestrukturované rozhovory s příslušníky soukromé bezpečnostní služby. Tyto metody poskytnou sběr relevantních informací pro hlubší porozumění konkrétním problémům a výzvám v rámci zabezpečení objektu, což bude nezbytné pro návrh efektivních opatření, která zajistí vyšší úroveň ochrany.

V další fázi diplomové práce jsou aplikovány kvalitativní a semikvantitativní metody pro hodnocení složek rizik, jako jsou úroveň zranitelnosti, pravděpodobnost výskytu události a možné negativní dopady. Touto kombinací metod bude umožněno provést analýzu bezpečnostní situace objektu a následné formulování návrhů opatření a doporučení, která povedou k účinnému zajištění vyšší úrovně ochrany před identifikovanými hrozbami. Podrobné informace a parametry jednotlivých metod jsou uvedeny v přílohách této práce. Postup zpracování praktické části práce je představen na Obrázku 1.



Obrázek 1 – Postup při zpracování praktické části diplomové práce

(zdroj: vlastní)

I. TEORETICKÁ ČÁST

1 TERMINOLOGIE A PRÁVNÍ NORMY ČESKÉ REPUBLIKY V OBLASTI ZABEZPEČENÍ OBJEKTU

Bezpečnost a zabezpečení představují dva úzce spjaté pojmy, které bývají v českém jazyce často zaměňovány, avšak jejich význam se může lišit v závislosti na kontextu. V německém jazyce jsou tyto dva pojmy dokonce překládány z angličtiny jako jeden termín „Sicherheit“. Co se dále jeví problematickým, v souvislosti s terminologií k tématu diplomové práce, jsou anglické pojmy „Safety Risk“ a „Security Risk“ pro které má český jazyk jediný termín „bezpečnostní riziko“. Je podstatné tyto pojmy jasně rozlišit, aby nedocházelo k omylům v rámci práce se zahraniční literaturou, jelikož každý z těchto termínů odkazuje na odlišnou oblast systému ochrany, které ohrožují různé druhy bezpečnostních rizik.

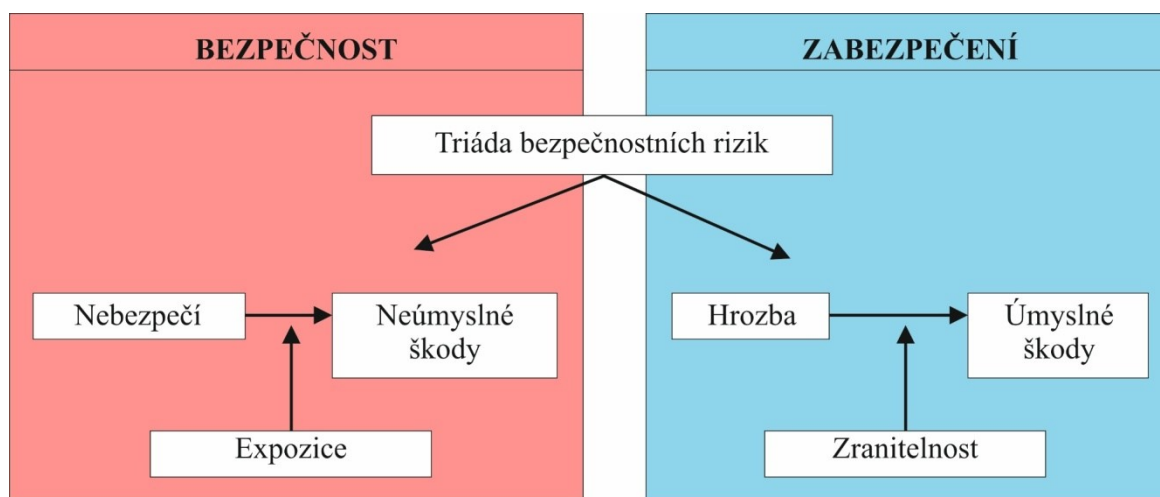
Podle Springera (2020) spočívá rozdíl mezi těmito pojmy v tom, že bezpečnost souvisí s předcházením vzniku nehod a zabezpečení souvisí s prevencí kriminality. Pro účely této práce vycházejme z následujícího vymezení zaměření těchto pojmů:

Bezpečnost (z angl. Safety) je stav, kdy je člověk chráněn před nebezpečím způsobeným přírodními silami nebo náhodnými lidskými chybami (Nas, 2015).

Zabezpečení (z angl. Security) je stav, kdy je člověk chráněn před hrozbami, které mají původ v úmyslném záměru způsobit škodu (Nas, 2015).

Rozlišení těchto pojmů je zcela zásadní, neboť i přesto, že oba termíny popisují stav, mohou také popisovat i formu ochrany - kroky nebo opatření přijatá ke zlepšení stavu bezpečnosti referenčního objektu (Hofreiter, 2015).

Předmětem výzkumu v oblasti bezpečnosti jsou nebezpečí, míra expozice vůči nebezpečí a možné ztráty, kdežto v oblasti zabezpečení jsou zkoumány hrozby, zranitelnost vůči těmto hrozbám a možné ztráty. Analogie bezpečnostních rizik v souvislosti s bezpečností a zabezpečením je zachycena na Obrázku 2.



Obrázek 2 – Analogie bezpečnostních rizik

(zdroj: vlastní zpracování dle Reniers et al., 2020)

Rozdíl je tedy určen především na základě specifického zdroje rizika, konkrétního rizikového faktoru a charakteru dopadu, který může mít různé projevy a intenzitu v závislosti na daných okolnostech.

1.1 Vymezení základních pojmů

Objasnění následujících termínů umožní čtenáři lépe porozumět problematice diplomové práce, která je projednávána v následujících kapitolách.

- **Aktivum** je všechno, co má pro subjekt hodnotu, která může být zmenšena působením hrozby. Dělíme je na hmotná a nehmotná (Tomek, 2018).
- **Dohledové centrum** (také monitorovací centrum nebo pult centralizované ochrany) je soukromé nebo veřejné personálem trvale obsazené centrum, přijímající ze vzdálených objektů poplachové signály, jako je vloupání, požár, informace o technických stavech (ČSN 14383-1, 2007).
- **Fyzická bezpečnost** je soubor opatření sloužících k ochraně a rozvoji lidského systému, kterou je možno rozdělit na fyzickou ostrahu, režimovou ochranu, klasickou ochranu prostřednictvím mechanického zábranného systému a technickou ochranu (Ščurek a Jarkuliš, 2021).
- **Objekt ochrany** je předmět, osoba nebo informace, které jsou v pozornosti subjektu s protispolečenskými cíli a na jejichž ochraně má společnost zájem (Hofreiter, 2015).

- **Hrozba** je konkrétní, fyzicky existující objekt, jev nebo událost, která má schopnost způsobit škodu nebo újmu (Hofreiter, 2015).
- **Perimetr** je souvislý soubor zábran, jako jsou zdi, dveře a přírodní prvky, které zcela obklopují chráněný objekt (Khairallah, 2017).
- **Riziko** je kombinace pravděpodobnosti vzniku negativního jevu a jeho následku (Ščurek a Jarkuliš, 2021).
- **Zranitelnost** znamená přirozenou vlastnost jakéhokoli hmotného objektu, technického prostředku nebo systému ochrany, že ztratí schopnost plnit svou přirozenou funkci nebo určenou funkci v důsledku působení vnějších nebo vnitřních hrozeb různé povahy a intenzity. Vyjadřuje stupeň nebo míru jeho schopnosti odolat vnějším a vnitřním hrozbám (Hofreiter, 2015).

1.2 Právní normy

Právní normy České republiky (dále jen „ČR“) neukládají právnickým osobám povinnost zabývat se zabezpečením objektu, respektive tuto povinnost ukládají pouze vybraným subjektům, které svou charakteristikou a činností představují zvýšenou míru rizika, a jejichž narušení bezpečnosti by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, ochranu života a zdraví osob, ochranu majetku a životního prostředí, popřípadě veřejný pořádek.

Cílem těchto právních předpisů je zejména zajištění požadované úrovně bezpečnosti, ochrana majetku před neoprávněným vniknutím, poškozením či zničením, ale rovněž i zajištění práv vlastníků a uživatelů těchto objektů v souladu s principy právního státu.

Zásadním právním předpisem pro účely praktické části diplomové práce je zákon č. 40/2009 Sb. trestní zákoník. Tento zákon představuje soubor právních norem, které vymezují trestné činy, jejich skutkové podstaty a sankce za jejich spáchání. Níže jsou uvedeny výňatky trestního zákoníku, které se přímo dotýkají problematiky diplomové práce:

- **Krádež:** Kdo si присvojí cizí věc tím, že se jí zmocní, a způsobí tak na cizím majetku škodu nikoliv nepatrnou, čin spáchá vloupáním, bezprostředně po činu se pokusí uchovat si věc násilím nebo pohrůžkou bezprostředního násilí, čin spáchá na věci, kterou má jiný na sobě nebo při sobě, nebo čin spáchá na území, na němž je prováděna nebo byla provedena evakuace osob, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci (§ 205 odst. 1 zákona č. 40/2009 Sb. trestní zákoník).
- **Krajní nouze:** Čin jinak trestný, kterým někdo odvrací nebezpečí přímo hrozící zájmu chráněnému trestním zákonem, není trestným činem (§ 28 odst. 1 zákon č. 40/2009 Sb. v platném znění).
- **Nutná obrana:** Čin jinak trestný, kterým někdo odvrací přímo hrozící nebo trvajícím útok na zájem chráněný trestním zákonem, není trestným činem (§ 29 odst. 1 zákona č. 40/2009 Sb. v platném znění).
- **Pachatel:** Pachatelem trestného činu je, kdo svým jednáním naplnil znaky skutkové podstaty trestného činu nebo jeho pokusu či přípravy, je-li trestná (§ 22 odst. 1 zákona č. 40/2009 Sb. v platném znění). Pachatelem se rozumí, nevyplyvá-li z jednotlivého ustanovení trestního zákona něco jiného, i spolupachatel a účastník (§ 113 zákona č. 40/2009 Sb. v platném znění).
- **Poškození cizí věci:** Kdo zničí, poškodí nebo učiní neupotřebitelnou cizí věc, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci (§ 228 odst. 1 zákona č. 40/2009 Sb. trestní zákoník).
- **Vloupání:** Vloupáním se rozumí vniknutí do uzavřeného prostoru lstí, nedovoleným překonáním uzamčení nebo překonáním jiné jistící překážky s použitím síly (§ 121 zákona č. 40/2009 Sb. trestní zákoník).
- **Zpronevěra:** Kdo si присvojí cizí věc, která mu byla svěřena, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci (§ 206 odst. 1 zákona č. 40/2009 Sb. trestní zákoník).

Dále představme subjekty, jejichž potřeba zabezpečení pramení ze zákona. Vybrané typy subjektů jsou uvedeny v Tabulce 1. Nutno dodat, že uvedené právní předpisy nejsou zdaleka jediným předpisem, který se zabývá ochranou před hrozbami pro danou oblast, jelikož konkrétní problematika může být upravena i dalšími zákony, vyhláškami či mezinárodními smlouvami, které je nutno zohlednit.

Tabulka 1 – Výběr subjektů, jejichž potřeba zabezpečení pramení ze zákona

Subjekt	Právní předpis	Znění právního předpisu
Civilní letiště	Zákon č. 49/1997 Sb. o civilním letectví	Provozovatel letiště dále zajistí provádění kontroly osob a vozidel vstupujících a vjíždějících do prostoru letiště; vydávání letištních identifikačních průkazů a povolení k vjezdu; provádění detekční kontroly osob jiných než cestujících a jimi vnášených věcí; ostrahu prostoru letiště (§ 85n odst. 2).
Chráněné objekty a prostory dle zákona č. 273/2008 Sb. v platném znění	Zákon č. 273/2008 Sb. o Policii České republiky	Policie zajišťuje bezpečnost chráněných objektů a prostorů. Rozsah zajišťování bezpečnosti stanoví na návrh policejního prezidenta ministr v závislosti na bezpečnostní situaci a možné míře ohrožení (§ 48 odst. 1).
Jaderná zařízení	Zákon č. 263/2016 Sb. atomový zákon	Pro účely fyzické ochrany musí být na jaderném zařízení na základě analýzy možných následků pro jadernou bezpečnost v případě neoprávněných činností vymezeny a fyzicky ohraničeny prostory, do nichž je omezen a kontrolován vstup a vjezd, a to střežený prostor; chráněný prostor; vnitřní prostor a životně důležitý prostor (§ 161 odst. 1).
Kulturní památky	Zákon č. 20/1987 Sb. o státní památkové péči	Vlastník kulturní památky je povinen na vlastní náklad pečovat o její zachování, udržovat ji v dobrém stavu a chránit ji před ohrožením, poškozením, znehodnocením nebo odcizením (§ 9 odst. 1).

(zdroj: vlastní)

Tabulka 1 – Výběr subjektů, jejichž potřeba zabezpečení pramení ze zákona (pokračování)

Subjekt	Právní předpis	Znění právního předpisu
Objekty důležité pro obranu státu	Zákon č. 222/1999 Sb. o zajišťování obrany ČR	Do objektů důležitých pro obranu státu z důvodu veřejného zájmu nebo z důvodu bezpečnosti fyzických osob může být statutárním orgánem, nebo jím pověřenou osobou, do jehož působnosti objekty důležité pro obranu státu náleží, vstup omezen nebo zakázán (§ 29 odst. 3).
Objekty sk. A, sk. B dle zákona č. 224/2015 Sb. v platném znění	Zákon č. 224/2015 Sb. o prevenci závažných havárií	Provozovatel nebo uživatel objektu přijme všechna opatření nezbytná k prevenci závažných havárií a omezení jejich následků na životy a zdraví lidí a zvířat, životní prostředí a majetek (§ 3 odst. 1).
Prvky kritické infrastruktury	Zákon č. 240/2000 Sb. o krizovém řízení	Subjekt kritické infrastruktury odpovídá za ochranu prvku kritické infrastruktury (§ 29a).
Utajované informace dle zákona č. 412/2005 Sb. v platném znění	Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti	Pro zabezpečení ochrany utajovaných informací v rámci fyzické bezpečnosti se určují objekty, zabezpečené oblasti a jednací oblasti (§ 24 odst. 1).
Zařízení sociálních služeb	Zákon č. 133/1985 Sb. o požární ochraně	Zařízení sociálních služeb, které poskytuje služby sociální péče formou pobytových služeb, musí být v části stavby, v níž je služba poskytována, vybaveno elektrickou požární signalizací, je-li ubytovací kapacita tohoto zařízení nad 50 osob, zařízením autonomní detekce a signalizace, je-li ubytovací kapacita tohoto zařízení 50 osob nebo nižší (§ 8 odst. 1).

(zdroj: vlastní)

Zabezpečení dalších subjektů, jako například obchodních a administrativních prostor či bytových prostor jsou předmětem technických norem. Vybrané subjekty a příslušné zákonné a podzákonné právní předpisy, ze kterých pramení potřeba zabezpečení těchto subjektů, jsou uvedeny v podkapitole níže.

1.3 Právní rámec ochrany vybraných subjektů

V rámci této podkapitoly bude věnována pozornost specifickým subjektům, jako jsou objekty s vysokým množstvím nebezpečných látek (objekty skupiny A a skupiny B dle zákona č. 224/2015 Sb. v platném znění), prvky kritické infrastruktury (dle zákona č. 240/2000 Sb. v platném znění) a subjekty nakládající s utajovanými informacemi (dle zákona č. 412/2005 Sb. v platném znění).

Objekty, ve kterých se nacházejí nebezpečné látky (dále jen „NL“) **dle zákona č. 224/2015 Sb. v platném znění** byly vymezeny na základě požadavků Směrnice Evropského parlamentu a Rady 2012/18/EU o kontrole nebezpečí závažných havárií s přítomností NL (Seveso III). Těto směrnici historicky předcházely Směrnice Rady 96/82/ES o kontrole nebezpečí závažných havárií s přítomností nebezpečných látek z roku 1996 (Seveso II) a Směrnice Rady 82/501/EHS o nebezpečí závažných havárií při vybraných průmyslových činnostech z roku 1982 (Seveso).

Název Seveso vychází z ikonické havárie chemické továrny Icmesa, která se odehrála 10. července 1976 v italském městě Meda, poblíž města Seveso, přibližně 25 km severně od Milána. V továrně explodoval chemický reaktor, což vedlo k uvolnění vysokých hladin 2,3,7,8-tetrachlordibenzo-p-dioxinu (označovaného jako TCDD nebo dioxin). Následkem prudké chemické reakce vznikl aerosolový oblak obsahující hydroxid sodný, ethylenglykol, trichlorfenát sodný a odhadem 15 až 30 kg dioxinu, který se rozšířil na ploše 18 km² (Eskenazi et al., 2018). Dopady havárií jako byla právě ta u Sevesa ukázala na zásadní význam regulace v oblasti nakládání s NL.

Na základě požadavků Seveso III vznikl v roce 2015 v ČR zákon, který stanovuje povinnosti provozovatelů objektů, jejichž činnost souvisí s nakládáním s nebezpečnými chemickými látkami. Provozovatelé těchto objektů jsou dle množství NL umístěné v objektu kategorizovány do skupiny A nebo skupiny B (§ 6 a § 7 zákona č. 224/2015 Sb. v platném znění), a podle výsledků zařazení se na ně vztahují povinnosti, které souvisí s fyzickou bezpečností samotného objektu. Jedná se o zpracování bezpečnostní dokumentace (§ 9 až § 20 zákona č. 224/2015 Sb. v platném znění) a havarijního plánování (§ 21 až § 30 zákona č. 224/2015 Sb. v platném znění), pojištění odpovědnosti za škody vzniklé v důsledku závažné havárie (§ 33 zákona č. 224/2015 Sb. v platném znění) a způsob informování veřejnosti při mimořádné události (dále jen „MU“) (§ 34 až § 38 zákona č. 224/2015 Sb. v platném znění). Mimo jiné jsou tyto provozovatelé povinni

spolupracovat se státními orgány, jako jsou krajské ředitelství Policie ČR (v souvislosti s § 21 odst. 3 zákona č. 224/2015 Sb. v platném znění) a hasičský záchranný sbor kraje (v souvislosti s § 23 odst. 6, § 25 odst. 3 a § 26 až § 30 zákona č. 224/2015 Sb. v platném znění). Zákon je doplněn o několik prováděcích vyhlášek, které stanovují podrobnosti konkrétních ustanovení zákona:

- Vyhláška č. 225/2015 Sb. o stanovení rozsahu bezpečnostních opatření fyzické ochrany objektu zařazeného do skupiny A nebo skupiny B.
- Vyhláška č. 226/2015 Sb. o zásadách pro vymezení zóny havarijního plánování a postupu při jejím vymezení a o náležitostech obsahu vnějšího havarijního plánu a jeho struktury.
- Vyhláška č. 227/2015 Sb. o náležitostech bezpečnostní dokumentace a rozsahu informací poskytovaných zpracovateli posudku.
- Vyhláška č. 228/2015 Sb. o rozsahu zpracování informace veřejnosti, hlášení o vzniku závažné havárie a konečné zprávy o vzniku a dopadech závažné havárie.
- Vyhláška č. 229/2015 Sb. o způsobu zpracování návrhu ročního plánu kontrol a náležitostech obsahu informace o výsledku kontroly a zprávy o kontrole.

Objekty nakládající s utajovanými informacemi dle zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti navazují na předchozí úpravu stanovenou vyhláškou Národního bezpečnostního úřadu č. 258/1998 Sb. o objektové bezpečnosti, kterou o rok později nahradila vyhláška Národního bezpečnostního úřadu č. 339/1999 Sb. o objektové bezpečnosti. Od roku 2006 je problematika těchto vyhlášek v působnosti zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Zákon č. 412/2005 stanoví právní rámec pro ochranu utajovaných informací a bezpečnostní způsobilost pro nakládání s utajovanými informacemi. Dále stanoví stupně utajení informací přísně tajné, tajné, důvěrné a vyhrazené (§ 4 zákona č. 412/2005 Sb. v platném znění), podmínky pro získání přístupu k utajované informaci (§ 6 až § 20 zákona č. 412/2005 Sb. v platném znění), požadavky na fyzickou bezpečnost (§ 24 až § 33 zákona č. 412/2005 Sb. v platném znění), požadavky na kryptografickou ochranu (§ 36a až § 45 zákona č. 412/2005 Sb. v platném znění), povinnosti při ochraně utajovaných informací (§ 65 až § 72 zákona č. 412/2005 Sb. v platném znění), požadavky

pro získání dokladu bezpečnostní způsobilosti (§ 80 až § 88 zákona č. 412/2005 Sb. v platném znění).

Bližší požadavky pro opatření fyzické bezpečnosti, zabezpečené oblasti a jednacích oblastí jsou popsány ve vyhlášce č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků. Dalším prováděcím právním předpisem, který souvisí s ochranou utajovaných informací je vyhláška č. 275/2022 Sb. o administrativní bezpečnosti a o registrech utajovaných informací.

Prvky kritické infrastruktury ČR dle zákona č. 240/2000 Sb. o krizovém řízení zahrnují stavby, zařízení nebo veřejnou infrastrukturu určené podle průřezových a odvětvových kritérií (§ 2 zákona č. 240/2000 Sb. v platném znění). Průřezová a odvětvová kritéria jsou specifikována v nařízení vlády č. 432/2010 Sb. v platném znění.

Za ochranu prvků kritické infrastruktury je zodpovědný subjekt, který ji provozuje a za tímto účelem zpracovává plán krizové připravenosti subjektu kritické infrastruktury. Náležitosti a způsob zpracování plánu krizové připravenosti jsou obsaženy v § 17 a § 18 nařízení vlády č. 462/2000 Sb. v platném znění. Plán se skládá ze základní, operativní a pomocné části. Součástí plánu je mimo jiné i přehled a hodnocení možných zdrojů rizik a analýzy ohrožení a jejich možný dopad, jakož i přehled opatření vyplývajících z krizového plánu (§ 15 nařízení vlády č. 462/2000 Sb. v platném znění).

Ochrana prvků kritické infrastruktury je dále předmětem strategických dokumentů ČR jako například Metodika zajištění ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie (2012), Komplexní strategie ČR k řešení problematiky kritické infrastruktury (2010), Národní program ochrany kritické infrastruktury (2010), Strategie ČR pro boj proti terorismu (2013) a Audit národní bezpečnosti (2016). Ochrana prvků kritické infrastruktury probíhá ze strany státu ve spolupráci se subjekty kritické infrastruktury formou nastavení bezpečnostních standardů nebo vzájemné včasné komunikace v případě výskytu nestandardní situace včetně stanovení spolupráce se složkami bezpečnostního systému státu (Ministerstvo vnitra, ©2025).

2 ZABEZPEČENÍ OCHRANY OBJEKTU

Následující podkapitoly popisují specifika subsystémů v rámci technické ochrany objektu. V textu je objasněna funkce jednotlivých subsystémů a relevantní technické normy, které definují požadavky na jejich funkčnost, spolehlivost a úroveň zabezpečení.

2.1 Mechanický zábranný systém

Mechanické zábranné prostředky (dále jen „MZP“) jsou charakterizované mechanickými bariérami, které svými vlastnostmi stěžují nebo zabraňují protiprávnímu přístupu potenciálnímu útočníkovi do chráněného objektu. (Tomek, 2018). Mezi tyto prostředky můžeme řadit například brány, dveře, okna, trezory, turnikety, závory apod.

Kombinace těchto bariér tvoří tzv. mechanický zábranný systém (dále jen „MZS“). Ten představuje základ v oblasti zabezpečení objektu a ochrany majetku, jak ukazuje pyramidové schéma na Obrázku 3. Bez jeho implementace by bylo nasazení dalších ochranných opatření neefektivní, jelikož by mohlo dojít k výraznému zvýšení jejich zranitelnosti.



Obrázek 3 – Pozice MZS v rámci zabezpečení objektu

(zdroj: vlastní zpracování dle Ivanka, 2014)

Různé zdroje uvádí odlišné třídy MZS na základě ochranné zóny, kterou zajišťují. Mach (2014) rozlišuje čtyři kategorie ochranných zón:

- **Obvodová ochrana** zabezpečuje bezpečnost v okolí chráněného objektu, jeho obvod, který může být vymezený přírodní hranicí (vodní tok) nebo umělou hranicí (plot, stěna a další). Může se jednat o různé druhy oplocení, vjezdy a vstupy do chráněného prostoru – brány, branky, turnikety, bezpečnostní propusti, závory apod. (Mach, 2014).
- **Plášťová ochrana** zabráňuje narušení pláště objektu a všech jeho otvorových výplní. Tvoří především ochranu stavebních otvorů budovy (dveře, okna atd.) před vniknutím pachatele. Je však potřeba brát v úvahu i samotné stěny, podlahy, stropy a střechy budov (Mach, 2014).
- **Prostorová ochrana** je vnímána jako vnitřní ochrana objektů, která zabezpečuje vnitřní prostory chráněného zájmu v objektu. Z hlediska MZP jde především o vnitřní stavební otvory (Mach, 2014), ale i detektory pohybu, požární hlásiče, sprinklery a další.
- **Předmětová ochrana** zabezpečuje ochranu předmětů v chráněném objektu. Jedná se především o zařízení, jejichž cílem je chránit cenné předměty, dokumenty, finanční hotovost a jiné důležité listiny (Mach, 2014).

Ivanka (2014) k výše uvedeným třídám MZS doplňuje navíc dvě kategorie:

- **Speciální ochrana** je chemická ochrana předmětů, cenin apod. Do této kategorie patří taky ochrana, do které řadíme plomby, pečete, hologramy a další. Jde o zdravotně nezávadné chemické prostředky, které lze využít jako nástrahový prostředek před pachatelem, jako například prášky, pasty, inkousty, barvy, laky, aerosoly, lepidla, roztoky, vosky, fixy. Dále plomby, pečete, vodoznak, hologram, chemická nástraha apod. (Ivanka, 2014).
- **Prostředky individuální ochrany** jsou přenosné i nepřenosné technické prostředky používané ve speciální a předmětové ochraně, ale i vlastní zámky, trezory a další (Ivanka, 2014).

Efektivita mechanické bariéry se odvíjí od její schopnosti prodloužit časový interval útočníka nutný k překonání dané bariéry. Čím je tento časový interval delší,

tím vyšší je i pravděpodobnost, že útočník bude odrazen, zadržen nebo odhalen, což zajišťuje celkovou vyšší úroveň zabezpečení chráněného objektu.

Doba, kterou musí pachatel vynaložit na překonání mechanické pevnosti MZS, se nazývá průlomová odolnost. Tu lze vyjádřit matematickou rovnicí (1):

$$\Delta t = t_2 - t_1 [\text{min}] \quad (1)$$

Kde:

- Δt je časový interval potřebný k překonání překážky,
- t_1 je čas zahájení útoku na překážku,
- t_2 je čas konečného překonání překážky (Ivanka, 2014).

Jednotka měření průlomové odolnosti je obvykle uváděna v minutách popř. sekundách. Cílem efektivního MZS je tedy maximalizace doby, kterou pachatel potřebuje k překonání jednotlivých mechanických bariér až po dosažení cíle, včetně útěku. V rámci návrhu MZS se zaměříme na to, aby jednotlivé mechanické bariéry splňovaly požadavky na mechanickou odolnost (pevnost), proto aby byla maximalizovaná doba jejich překonání pachatelem.

Každá mechanická bariéra je dle hodnoty průlomové odolnosti klasifikována do příslušné bezpečnostní třídy, která vychází z technických norem pro daný typ mechanické bariéry. Existují různé škály bezpečnostních tříd, které jsou určeny na základě standardizovaných testů, jež hodnotí dobu, po kterou bariéra odolává pokusům o její překonání. Níže jsou uvedeny rozdíly mezi bezpečnostními třídami vybraných mechanických bariér a technické normy, které danou bezpečnostní třídu definují:

- **Dveře, okna, lehké obvodové pláště, mříže a okenice** se klasifikují dle ČSN EN 1627:2022 do šesti bezpečnostních tříd: 1, 2, 3, 4, 5 a 6.
- **Skříňové trezory (kromě ATM trezorů)** se klasifikují dle ČSN EN 1143-1:2020 do jedenácti bezpečnostních tříd: 0, I, II, III, IV, V, VI, VII, VIII, IX a X.
- **ATM trezory** se klasifikují dle ČSN EN 1143-1:2020 do devíti bezpečnostních tříd: L, I, II, III, IV, V, VI, VII a VIII.
- **Trezorové dveře a komorové trezory** se klasifikují dle ČSN EN 1143-1:2020 do čtrnácti bezpečnostních tříd: 0, I, II, III, IV, V, VI, VII, VIII, IX, X, XI, XII a XIII.

- **Zámky s vysokou bezpečností** se klasifikují dle ČSN EN 1300:2024 do čtyř bezpečnostních tříd: A, B, C a D.
- **Bezpečnostní schránky** se klasifikují dle ČSN EN 14450+A1:2024 do dvou bezpečnostních tříd: S1 a S2 (Ivanka, 2014).

2.2 Poplachový zabezpečovací a tísňový systém

Poplachový zabezpečovací a tísňový systém (dále jen „PZTS“) je kombinovaný systém určený k detekci poplachu vniknutí a tísňového poplachu (ČSN EN 50131-1 ed. 2, 2007). Jedná se o systém, kterému náleží dva subsystémy:

- **Poplachový zabezpečovací systém**, který slouží k detekování a indikaci přítomnosti, vniknutí nebo pokusu o vniknutí vetřelce do střeženého prostoru (ČSN EN 50131-1 ed. 2, 2007).
- **Poplachový tísňový systém** poskytuje uživateli možnost úmyslného vyvolání poplachového stavu (ČSN EN 50131-1 ed. 2, 2007).

Tyto systémy slouží k ochraně majetku i osob a umožňují přivolání pomoci při narušení bezpečnosti chráněného objektu. Zároveň zajišťují přenos poplachových signálů na stanoviště s nepřetržitým dohledem. Bývají využívány nejen v komerčních a průmyslových objektech, ale i v domácnostech, školách, zdravotnických zařízeních a dalších veřejných prostorech, kde je třeba zajistit bezpečnost osob a majetku.

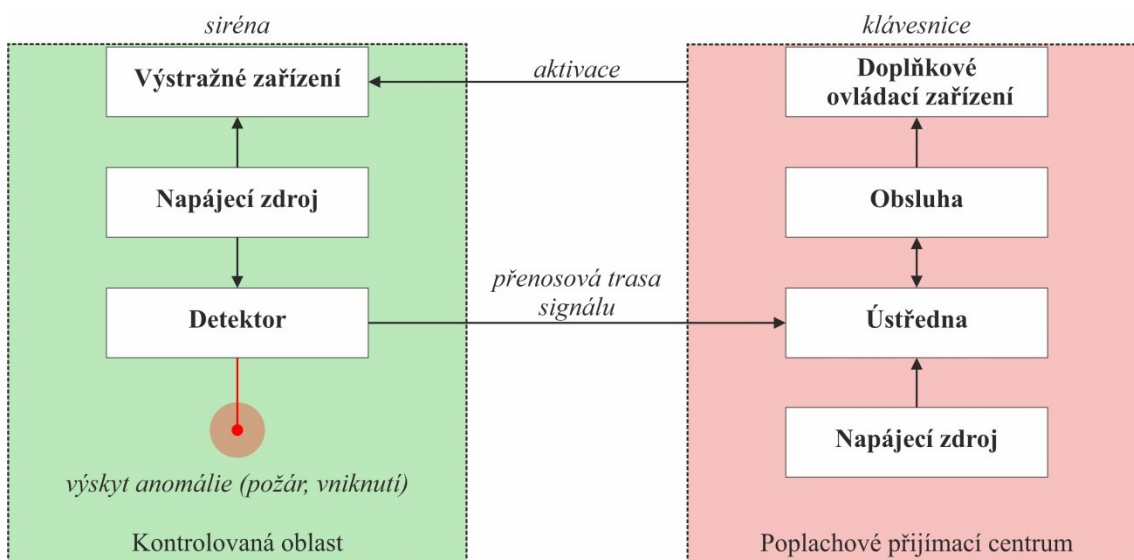
Poplachový zabezpečovací a tísňový systém se obecně skládá z těchto komponent:

- **Detektory** jsou elektrická zařízení určená k detekci incidentů. Incident je přitom doprovázen specifickými fyzikálními ději, které se nazývají příznaky. Detekční logika je pak taková, že pokud detektor zjistí výskyt příznaků, tak se předpokládá, že došlo k incidentu a detektor proto vyhlásí stav poplachu. Detektory se v kontrolované oblasti rozmisťují systematicky s cílem detekovat incident co nejdříve. Rozlišujeme detektory předmětové (tíhový závěsový detektor, tíhový podložkový detektor), překážkové (otřesový detektor, detektor tříštění skla, magnetický kontakt), objemové (infračervené detektory, mikrovlnné detektory, duální detektory), hraniční (úsekový detektor se štěrbinovými kabely) (Burda, 2017).
- **Napájecí zdroj** zajišťuje energii pro napájení PZTS (ČSN EN 50131-1 ed. 2, 2007).

- **Doplňkové ovládací zařízení** je například klávesnice, která umožňuje uživateli aktivovat nebo deaktivovat zařízení.
- **Výstražné zařízení** je akustické zařízení, které produkuje zvukový poplachový signál v odezvě na hlášení poplachu (ČSN EN 50131-1 ed. 2, 2007).
- **Ústředna** je zařízení pro příjem, zpracování, ovládání, indikaci a iniciaci následného přenosu informace (ČSN EN 50131-1 ed. 2, 2007).

Poplachové zabezpečovací a tísňové systémy jsou předmětem řady technických norem ČSN EN 50131.

Na Obrázku 4 je zachyceno obecné schéma přenosu signálu do poplachového přijímacího centra a následné vyhlášení poplachu v kontrolované oblast.



Obrázek 4 – Schéma PZTS

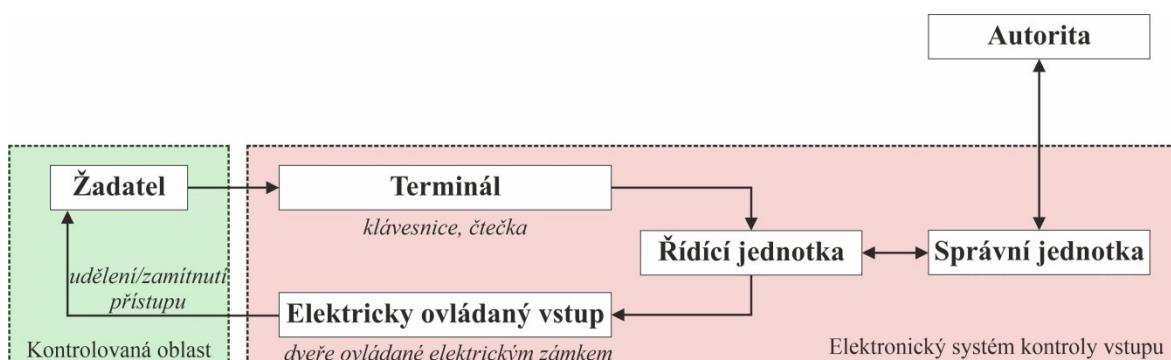
(zdroj: vlastní)

2.3 Elektronický systém kontroly vstupu

Elektronický systém kontroly vstupu (dále jen „ESKV“), označovaný také jako systém kontroly vstupu, je elektronický systém poskytující oprávněným osobám, nebo entitám, vstup do a/nebo opuštění zabezpečeného prostoru, a zamítající vstup a/nebo odchod neoprávněným jedincům, nebo entitám (ČSN EN 60839-11-1, 2014).

Účelem těchto moderních systémů je zajištění kontroly nad osobami, které vstupují do chráněné oblasti a eliminace rizika vniknutí neautorizovaných osob (Obrázek 5). Elektronický systém kontroly vstupu umožňuje rozlišení jednotlivých vstupujících osob a sledování jejich pohybu v definovaných zónách. Princip přístupových systémů spočívá

ve schopnosti přečíst pomocí speciálních zařízení (čteček) zakódované údaje/oprávnění a vyhodnotit je podle přidělených oprávnění (TZB-info, 2017).



Obrázek 5 – Schéma ESKV

(zdroj: vlastní zpracování dle Burda, 2017)

V rámci tohoto systému je mozkiem řídicí jednotka (kontrolér), který na základě požadavku o vstup ověřuje totožnost žadatele na základě uživatelského seznamu, který obsahuje identifikační údaje a přístupová oprávnění všech uživatelů. Tento seznam je definován autoritou, což zpravidla bývá správce systému. Na základě výsledků autentizace řídicí jednotka udělí nebo zamítne přístup žadatele do chráněné oblasti. V případě udělení přístupu řídicí jednotka zajistí odemknutí elektricky ovládaného vstupu (například dveře vybavené mechatronickým kováním).

Ověření identity (totožnosti) uživatele s cílem zamezit udělení autorizace neoprávněným osobám se nazývá autentizace. Každý uživatel, který je autoritou definován v uživatelském seznamu, disponuje unikátním dokazovacím faktorem (například osoba má na prstu svůj unikátní tvar papilárních linií), kterým autentizátoru (terminálu nebo řídicí jednotce) dokazuje svou identitu (Burda, 2017).

Autentizace uživatele, který žádá o přístup, se provádí několika způsoby. Uvedme následující třídy autentizace:

- **Autentizace pomocí biometriky** využívá charakteristiky morfologického typu (vnější stavba organismu) nebo behaviorálního typu (souvisí s chováním organismu). Autentizace pomocí biometriky může zahrnovat například charakteristický tón hlasu, tvar papilárních linií na prstech, skvrny na oční duhovce apod. (Burda, 2017).

- **Autentizace pomocí hardwaru** je uskutečňována prostřednictvím fyzického zařízení, jako jsou například čipové karty, které umožňují žadateli vstup do chráněného prostoru. (Burda, 2017).
- **Autentizace pomocí hesla** zahrnuje znalost tajné, uživatelem zapamatovatelné informace (hesla). Žadatel vloží do systému například svůj PIN (z angl. Personal Identification Number) prostřednictvím klávesnice terminálu. Terminál tuto hodnotu předá kontroléru, který ji pak vyhledá v přístupovém seznamu. V řádku, který přísluší hodnotě PIN, pak nalezne práva uživatele (Burda, 2017).
- **Vícefaktorová autentizace** představuje kombinaci více způsobů ověření identity (Blue Partners, 2025) uvedených výše.

Klasifikace systému kontroly vstupu musí být určena jedním ze čtyř stupňů, kde stupeň 1 značí nejnižší úroveň rizika a stupeň 4 nejvyšší (Tabulka 2). Klasifikace zabezpečení musí být definována individuálně pro každé místo přístupu pro vstup a opuštění (ČSN 60839-11-1, 2014).

Tabulka 2 – Klasifikace úrovně ochrany ESKV

Stupeň	1	2	3	4
Úroveň rizika	Nízké	Nízké až střední	Střední až vysoké	Vysoké
Aplikace	organizační prostředky, ochrana majetku nízké hodnoty	organizační prostředky, ochrana prostředků nízké až střední hodnoty	méně organizačních prostředků, ochrana komerčních prostředků střední až vysoké hodnoty	zejména ochrana komerčních prostředků velmi vysoké hodnoty nebo kritické infrastruktury

(zdroj: ČSN EN 60839-11-1, 2014)

Tabulka 2 – Klasifikace úrovně ochrany ESKV (pokračování)

Stupeň	1	2	3	4
Úroveň rizika	Nízké	Nízké až střední	Střední až vysoké	Vysoké
Dovednosti/ znalosti pachatelů/ útočníků	malá dovednost, malá znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií malé finanční prostředky pro napadení	střední dovednost a znalosti systémů kontroly vstupu, identifikačních prostředků a IT technologií malé až střední finanční prostředky pro napadení	velká dovednost a znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií střední finanční prostředky pro napadení	velmi vysoká dovednost a znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií velké finanční prostředky pro napadení
Typické příklady	hotel	obchodní kanceláře, malé firmy	průmysl, administrativní prostory, finanční instituce	vysoce citlivé prostory (vojenská zařízení, vládní budovy, výzkum a vývoj, kritická infrastruktura)

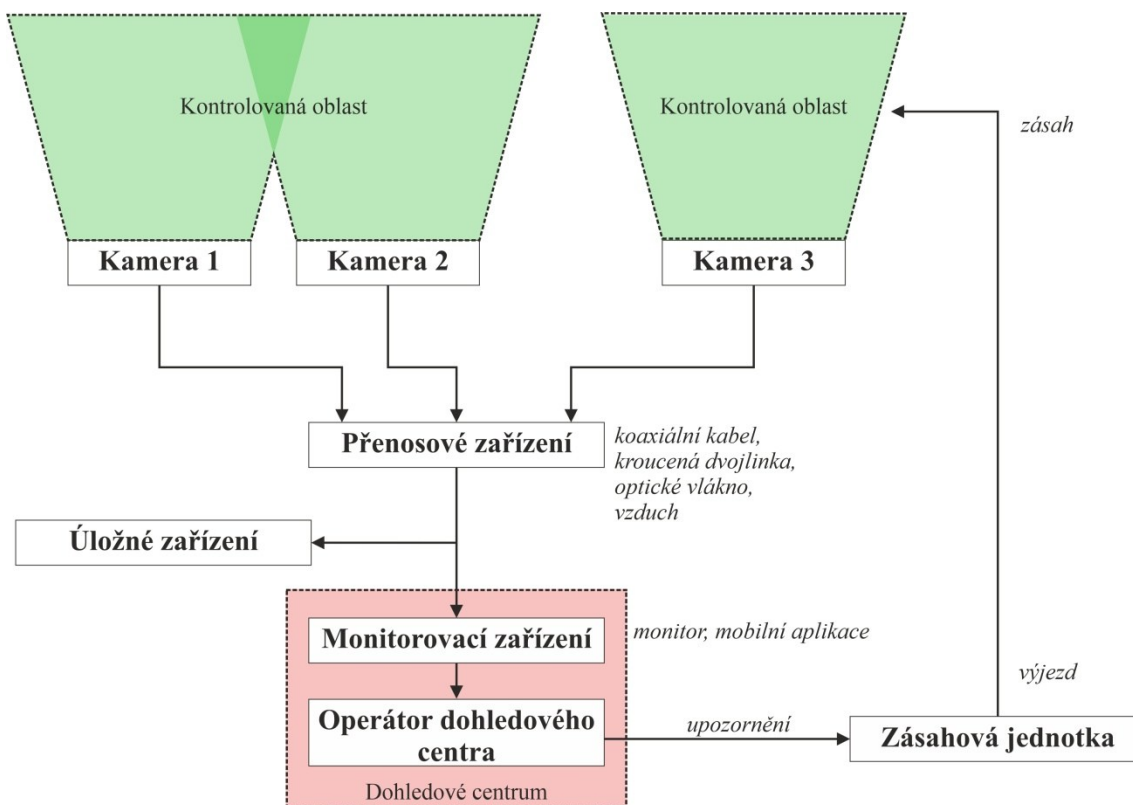
(zdroj: ČSN EN 60839-11-1, 2014)

Elektronický systém kontroly vstupu je předmětem řady technických norem ČSN EN 60839.

2.4 Dohledový videosystém

Dohledový videosystém (dále jen „DVS“) je systém, který se skládá z kamerového vybavení, úložiště, monitorovacího zařízení a souvisejících zařízení pro účely přenosu obrazu a ovládání (ČSN 62676-1-1, 2014). Burda (2017) popisuje DVS jako elektronický systém, který oprávněné osobě umožňuje vizuálně a na dálku sledovat dění v kontrolované oblasti. Oprávněnou osobou může být například pracovník ostrahy, který se nachází na pracovišti dohledového centra, na kterém monitoruje a vyhodnocuje obrazové, popř. zvukové záznamy z kamer. Dění ve vybraných částech kontrolované oblasti se pomocí vhodných zařízení (obvykle kamer) snímá a následně převádí na elektrický

signál, který je pak přenášén do dohledového centra (Burda, 2017). Pojem dohledový videosystém nahradil dříve užívané termín CCTV – z angl. Closed Circuit Television (ČSN EN 62676-1-1, 2014). Schéma DVS je zachyceno na Obrázku 6.



Obrázek 6 – Schéma DVS

(zdroj: vlastní)

Dohledové videosystémy mohou být také využity v oblasti bezpečnosti. Mohou například sloužit k monitorování zaměstnanců v rámci využívání osobních ochranných pracovních prostředků při vstupu na pracoviště, kde je jejich použití vyžadováno příslušnými předpisy. Nebo také při kontrole dodržování stanovených pravidel chování osob ve vymezených prostorech, ovšem za podmínek § 316 odst. 2 a odst. 3 zákona č. 262/2006 Sb. zákoník práce, při existenci závažného důvodu k pochybnostem o pracovních výkonech zaměstnance a za předpokladu, že o tom byl zaměstnanec řádně informován.

Jak bylo uvedeno výše, snímacím zařízením je zpravidla kamera. V rámci technologie přenosu informací rozlišujeme dva druhy kamerových systémů:

- **analogové kamerové systémy,**
- **digitální kamerové systémy** (Burda, 2017).

Analogové systémy využívají analogový přenos signálu, digitální systémy přenášejí obraz prostřednictvím běžné počítačové sítě. Analogové kamerové systémy jsou historicky starší a svůj vývoj zahájily v 50. letech 20. století (Nejkam, ©2023). Tyto systémy jsou obvykle cenově dostupnější a jednodušší na instalaci, avšak vykazují i několik nevýhod, například omezenou vzdálenost přenosu signálu, která je dána délkou kabelového propojení. Naproti tomu digitální kamerové systémy disponují řadou inteligentních funkcionalit, jako například rozpoznávání obličejů, detekce vozidel a další (ZEPCAM, 2023). Kromě toho umožňují flexibilní možnosti připojení, včetně bezdrátových variant.

Zatímco v analogových systémech musí být každá kamera propojena kabelem k nahrávacímu zařízení, u digitálních kamerových systémů jsou možnosti uspořádání a propojení komponentů prakticky neomezené. Analogové systémy postupně ustupují do pozadí s příchodem digitálních IP technologií. Digitální kamerové systémy postupně nahrazují analogové systémy a stávají se novým standardem pro zabezpečovací a dohledové aplikace (Nejkam, ©2023).

Dohledové videosystémy jsou předmětem řady technických norem ČSN EN 62676.

Norma ČSN EN 62676-1-1 za účelem poskytnutí požadované úrovně zabezpečení definuje čtyři stupně zabezpečení DVS:

- **Stupeň 1 (nízké riziko):** nemá žádnou ochranu a žádná omezení přístupu.
- **Stupeň 2 (nízké až střední riziko):** má nízkou úroveň ochrany a nízká omezení přístupu.
- **Stupeň 3 (střední až vysoké riziko):** má vysokou úroveň ochrany a vysoká omezení přístupu.
- **Stupeň 4 (vysoké riziko):** má velmi vysokou úroveň ochrany a velmi vysoká omezení přístupu (ČSN EN 62676-1-1, 2014).

Každý stupeň zabezpečení má specifické požadavky, kterým musí daný DVS vyhovovat. Norma stanovuje požadavky například pro ukládání snímků, archivaci a zálohování dat apod. Uvedme rozdíl mezi jednotlivými stupni zabezpečení dohledových videosystémů, a to jaké události narušení musí být systém schopen detekovat (Tabulka 3).

Tabulka 3 – Detekce narušení pro daný stupeň zabezpečení DVS

Systém musí detekovat tyto události	Stupeň zabezpečení			
	1	2	3	4
Ztráta videa		X	X	X
Pokud zařízení snímající obraz s trvale nastaveným úhlem pohledu přestane zobrazovat specifikovanou oblast			X	X
Úmyslné zakrytí nebo oslepení snímacího zařízení			X	X
Nahrazení jakýchkoliv video dat ve zdroji obrazu, během propojení nebo při zpracování				X
Významné snížení kontrastu obrazu				X

(zdroj: ČSN EN 62676-1-1, 2014)

Výběr konkrétního typu bezpečnostní kamery závisí na účelu použití a povahy hrozeb zabezpečovaného objektu. Pokud budeme chtít zabezpečit kamerovým systémem domácnost, budeme mít zcela odlišná výběrová kritéria než v případě zabezpečení podniku. Khairallah (2024) tvrdí, abychom při výběru kamery zvažili především úroveň osvětlení a požadovaný výhled kamery. Při výběru bezpečnostní kamery můžeme použít rozhodovací kritéria uvedená v Tabulce 4.

Tabulka 4 – Kritéria pro výběr bezpečnostní kamery

Kritérium	Možnosti
Mobilita kamery	statické, otočné
Prostředí využití	venkovní, vnitřní
Tvar a konstrukce	válcové, kupolové, věžové, s rybím okem
Úroveň rozlišení	1 Mpx (1280 x 720); 1,3 Mpx (1280 x 1024); 2 Mpx (1920 x 1080); 3 Mpx (2048 x 1536); 4 Mpx (2688 x 1520); 5 Mpx (2560 x 1920); 8 Mpx (3480 x 2160); 12 Mpx (4000 x 3000)

(zdroj: vlastní)

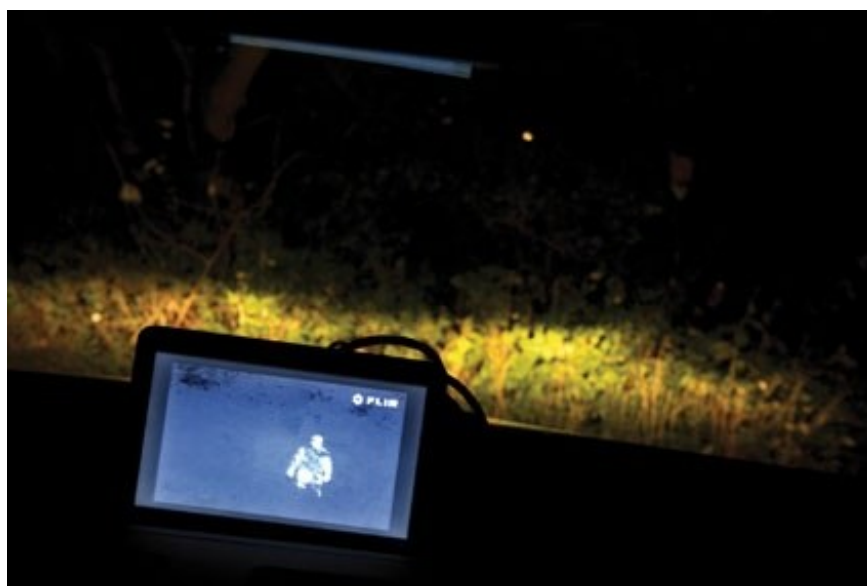
Tabulka 4 – Kritéria pro výběr bezpečnostní kamery (pokračování)

Kritérium	Možnosti
Způsob zapojení	bezdrátové, drátové
Způsob uložení záznamu	interní úložiště, cloudové úložiště

(zdroj: vlastní)

Mimo standardní bezpečnostní kamery se v praxi můžeme setkat s využitím dalších pokročilých technologií, jako jsou termovizní kamery, kamery s umělou inteligencí a drony. Tyto moderní technologie rozšiřují nejen možnosti monitorování, ale také zvyšují účinnost detekce narušitelů v různých podmínkách.

Termovizní kamery umožňují identifikaci objektů na základě detekce a měření dlouhovlnného infračerveného záření, které tyto objekty emitují v závislosti na jejich povrchové teplotě. Tyto kamery zvládnou vytvořit obraz na základě teplotních rozdílů v prostředí bez ohledu na dostupnosti viditelného světla. Infračervené záření je pro lidské oko a tedy i pro klasické kamery neviditelné, což činí termovizní kamery zvláště efektivní při monitorování ochranných zón za nepříznivých podmínek, jako jsou tma, mlha, kouř apod. Mimo to dokáží rozeznat osoby či vozidla na větší vzdálenost než klasické kamery, a odhalí i zamaskovaného pachatele (Burda, 2017). Ukázka funkcionality termovizní kamery za tmy je zachycena na Obrázku 7.



Obrázek 7 – Ukázka funkcionality termovizní kamery za tmy

(zdroj: GIT Sicherheit, 2011)

Kamery s umělou inteligencí představují vysoce pokročilou technologii, která rozšiřuje možnosti monitorování a analýzy videozáznamů. Tato zařízení využívají algoritmy strojového učení a hlubokého učení k automatické analýze obrazového materiálu v reálném čase, čímž eliminují potřebu lidského dohledu při běžné detekci hrozeb, jako jsou neoprávněný vstup, podezřelé chování, nebo jiná bezpečnostní rizika. Kromě samotného záznamu, uchovávání a zobrazování videa jsou kamery s umělou inteligencí schopny přesně rozpoznávat a klasifikovat osoby, obličeje, vozidla (včetně jejich typů) a registrační značky. Dále dokáží rozlišovat mezi objekty zájmu a irelevantním pohybem, jako jsou divoká zvěř, zvířata, stíny nebo pohybující se stromy (Hanwha Vision Europe, 2024).

Významnou výhodou kamer s umělou inteligencí je jejich schopnost minimalizovat falešné poplachy, což je kritický aspekt pro efektivní správu zabezpečovacích systémů. Tradiční systémy, které zajišťují detekci pomocí senzorů, mohou často reagovat na neškodné podněty, jako jsou vítr v korunách stromů nebo zvířata, což vede k zatížení operátorů dohledového centra a jejich kapacit na události, které nevyžadují okamžitou reakci. Kromě času a nákladů spojených s řešením těchto falešných poplachů mohou být také hlavní příčinou frustrace operátorů dohledového centra (Thorpe, 2020).

V neposlední řadě lze jako doplněk zabezpečení objektu využít dron, neboli bezpilotní letecký prostředek. Jedná se o typ letadla, které může být ovládáno na dálku nebo letět autonomně bez přímého lidského řízení (DronPro, 2024). Díky pohledu z ptačí perspektivy a vysoké mobilitě dronu lze efektivně monitorovat rozsáhlé oblasti a včas odhalit potenciální bezpečnostní hrozby. Drony mohou být vybaveny různými technologiemi, včetně navigačních systémů, senzorů pro sběr dat, kamer a dalšího vybavení přizpůsobeného specifickým účelům (DronPro, 2024). U rozsáhlých areálů lze využít drony s termokamerami, které umožňují detekci pohybu a odhalení narušení perimetru i za snížené viditelnosti nebo v noci (TZB-info, 2017). To výrazně zefektivňuje bezpečnostní dohled a snižuje reakční dobu při identifikaci podezřelých aktivit.

V současnosti jsou drony dostupné široké veřejnosti, což s sebou přináší rizika spojená s jejich neodborným používáním. Nezodpovědné nebo nelegální využití dronů může vést k narušení soukromí, bezpečnostním incidentům nebo kolizím s jinými objekty ve vzdušném prostoru. Proto je důležité dbát na odpovídající právní normy a regulace týkající se jejich provozu.

3 ORGANIZAČNÍ PROSTŘEDKY OCHRANY OBJEKTU

Následující podkapitoly se zaměřují na organizační prostředky ochrany objektu, které představují nezbytnou součást komplexní ochrany. V textu jsou objasněny aspekty režimové ochrany a fyzické ostrahy, včetně jejich funkcí a významu v rámci ochrany objektu.

3.1 Režimová ochrana objektu

Pojem režimová ochrana označuje soubor organizačně administrativních opatření a postupů směřujících k zajištění požadovaných podmínek pro řádnou funkci zabezpečovacího systému a jeho sladění s provozem chráněného objektu (Lichorobiec et al., 2010). Zabývá se tedy, v souladu se zákony a potřebami podniku, jakým způsobem budou lidé při ochraně podniku postupovat. Tento pojem je mnohdy nahrazován názvem organizační nebo administrativní ochrana, podle toho, které pojetí převládá (Tomek, 2018).

Tento způsob ochrany je neoddělitelnou součástí celkového zabezpečení objektu spolu s fyzickou ostrahou a technickými prostředky ochrany objektu. Zahrnuje pravidla, postupy, pokyny, směrnice a jiná opatření, kterými se řídí zaměstnanci, ale i ostatní osoby, které hodlají vykonávat určitou činnost uvnitř objektu, nebo ho jen navštěvují. Veškeré tyto zásady by měly být zakotveny v odpovídajících interních dokumentech daného podniku, a příslušní zaměstnanci i ostatní osoby musí být o těchto zásadách informováni. Hlavní oblasti řešené v rámci režimové ochrany podniku zahrnují:

- klíčový režim provozu,
- materiálový a expediční režim,
- provozní režim,
- režim pohybu zaměstnanců v objektu,
- vstupní a výstupní režim osob a dopravních prostředků (Tomek, 2018).

Režimová opatření lze dělit na vnitřní a vnější opatření (Uhlář, 2005). Vnitřní režimová opatření souvisí zejména s činností zaměstnanců podniku. Jedná se o dodržování pravidel, postupů, pokynů, směrnic, definované entitou, která zodpovídá za bezpečnost podniku. Vnější režimová opatření zahrnují zejména kontrolu osob (klientů, dodavatelů, návštěv, cizinců), které vstupují do objektu, nebo z něj vystupují.

V rámci režimové ochrany je zásadní, aby nastavená opatření byla efektivní a současně nenarušovala provozní procesy organizace. Nadměrná omezení mohou představovat překážku nejen pro zaměstnance, ale i pro efektivní fungování samotného podniku.

3.2 Fyzická ostraha objektu

Fyzická ostraha je bezpečnostní služba vykonávaná bezpečnostními pracovníky. Bezpečnostní pracovník (strážný) je osoba, které je vyplácena odměna, mzda nebo plat, je vyškolená a prověřena a vykonává funkci soukromé bezpečnostní služby (ČSN EN 15602, 2022).

Pro účely diplomové práce se budeme zabývat především soukromou bezpečnostní službou (dále jen „SBS“). Ta nemá oporu v zákoně, ani v jiném právním předpise, který by se zabýval udělováním zvláštních pravomocí pracovníkům SBS. Česká republika je posledním státem Evropské unie, kterému doposud chybí speciální zákon o SBS (Securitas ČR, 2024), a to i přes fakt, že je tento zákon schvalován a slibován vládními představiteli formou programových vyhlášení vlády již přes 30 let.

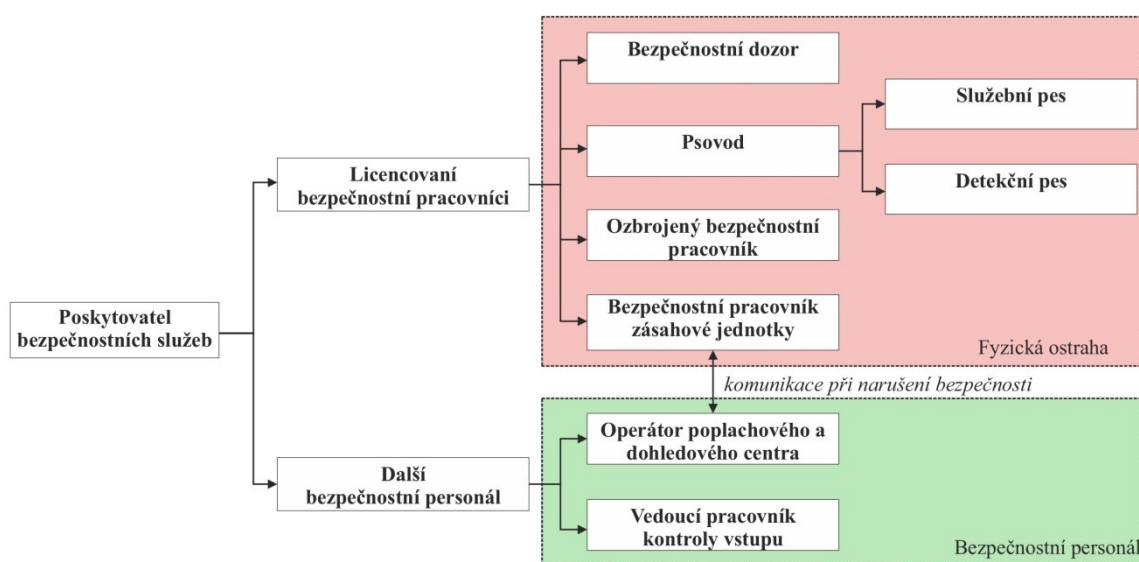
Cílem této služby je zajistit bezpečnost a ochranu osob, majetku a prostor proti hrozbám jako jsou krádeže, vandalismus, ale i požáry. Tato služba je nedílnou součástí fyzické bezpečnosti objektu, společně s technickými prostředky zabezpečení objektu a režimovými opatřeními.

Konkrétní náplň práce bezpečnostního pracovníka může zahrnovat různorodé pracovní činnosti jako například kontrolu dodržování režimových opatření, kontrolu vstupu a pohybu osob, vjezdu a výjezdu vozidel, pochůzkové a kontrolní činnosti ve střeženém objektu, provádění základních činností při součinnosti s Policií ČR, obecní policií, jednotkami hasičského záchranného sboru, zdravotnické záchranné služby a ostatními složkami integrovaného záchranného systému a určenými osobami, vedení dokumentace

o průběhu služby, pořizování záznamů o provedených úkolech (Ministerstvo práce a sociálních věcí, ©2025).

Pracovník ostrahy by měl disponovat určitými fyzickými i psychickými vlastnostmi, které mu umožní efektivně vykonávat svou práci a reagovat na MU. Mezi základní fyzické požadavky patří zejména dobrá kondice, síla, obratnost a vytrvalost. Pracovník ostrahy by měl být schopen zvládnout případný fyzický konflikt, aniž by způsobil zbytečné škody nebo ohrozil sám sebe. Z psychického hlediska je podstatná odolnost vůči stresu, rozvaha a schopnost rychlého vyhodnocení situace. Pracovník soukromé bezpečnostní služby se může v rámci výkonu své činnosti ocitnout v situaci, kdy je nucen použít přiměřenou sílu. V takovýchto situacích je oprávněn využít ustanovení § 28 a § 29 zákona č. 40/2009 Sb. trestní zákoník, které definují krajní nouzi a nutnou obranu (Bezpečnostní agentury, 2020).

Fyzická ostraha zahrnuje několik pracovních pozic, jejichž kvalifikace a výkon se mohou výrazně lišit v závislosti na specifických požadavcích a povaze vykonávané činnosti. Každá pozice vyžaduje odlišné dovednosti a úroveň odbornosti. Norma ČSN 15602:2022 poskytuje přehled a definice v oblasti soukromých bezpečnostních služeb. V rámci této normy bylo zpracováno schéma zachycené na Obrázku 8, které poskytuje obecný přehled o pracovních pozicích soukromých bezpečnostních služeb.



Obrázek 8 – Schéma vybraných pracovníků SBS

(zdroj: vlastní)

DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

Zabezpečení vybraných subjektů je v ČR upraveno řadou právních předpisů, které stanovují specifické požadavky na jejich ochranu. U některých subjektů existuje potřeba jejich zabezpečení již ve fázi projektového návrhu, aby bylo dosaženo požadovaných bezpečnostních standardů a byla minimalizována potenciální rizika. Potřeba zabezpečení dalších subjektů může vyplývat v závislosti na splnění určitých kritérií, například pokud podnik převyší určitý limit NL umístěné v objektu. Rozsah zabezpečení ostatních subjektů, jejichž potřeba zabezpečení nevyplývá z žádného právního předpisu, technických norem ani smluvních závazků, zůstává na individuálním rozhodnutí majitele nebo provozovatele objektu.

Vyšší úroveň ochrany vyžaduje odpovídající úroveň spolehlivosti jednotlivých technických prvků zabezpečovacího systému, které jsou určeny k efektivní minimalizaci potenciálních rizik. Spolehlivost zahrnuje odolné a dobře udržované MZP, účinné detekční a výstražné prvky PZTS, prvky DVS pokrývající veškeré chráněné zóny a zabezpečovaný majetek, a ESKV umožňující autentizaci a autorizaci uživatele žádajícího o udělení přístupu do chráněné zóny. Důležitou součástí efektivního zabezpečení je rovněž integrace jednotlivých systémů do jednotné platformy pro centralizovaný dohled a řízení bezpečnosti. Správu a údržbu těchto systémů je nezbytné provádět pravidelně v souladu s platnými normami a legislativními požadavky. To zahrnuje nejen periodické testování funkčnosti jednotlivých prvků zabezpečovacího systému, ale i jejich včasnou modernizaci s cílem eliminovat potenciální zranitelnosti starších systémů.

V současnosti lze pozorovat významný vývoj v oblasti zabezpečení objektů, kde se stále více uplatňují moderní technologie, především kamerové systémy využívající prvky umělé inteligence a bezpilotní systémy určené pro monitoring rozsáhlých nebo těžko přístupných oblastí. Tyto systémy jsou schopny autonomně detekovat bezpečnostní incidenty s výrazně nižší chybovostí ve srovnání s tradičními metodami, což může vést ke snížení výskytu falešných poplachů v budoucnosti. Kamery s umělou inteligencí nejen zlepšují přesnost detekce, ale také umožňují efektivnější a rychlejší reakci na potenciální hrozby. Tato technologie má potenciál výrazně zvýšit úroveň ochrany a zároveň snížit zátěž pro lidský personál. Dalším trendem v oblasti bezpečnostních technologií je implementace dronů pro monitoring rozsáhlých areálů nebo těžko přístupných míst. Drony poskytují flexibilitu při monitorování velkých prostor, kde je tradiční dozor omezený.

V kontextu fyzické bezpečnosti jsou důležitá nastavená režimová opatření a pracovní fyzické ostrahy, jakožto dvě klíčové komponenty zajišťující ochranu lidí a majetku. Podstatné je, aby režimová ochrana byla nastavena tak, aby pravidla nebyla příliš restriktivní, protože by mohly zpomalit pracovní tok a negativně ovlivnit běžné pracovní procesy a každodenní činnost podniku.

II. PRAKTICKÁ ČÁST

4 INFORMACE O OBJEKTU

Aby tato práce nemohla sloužit potenciálnímu útočníkovi, jako návod k identifikaci zranitelných míst v rámci ochrany podniku, jsou veškeré identifikační údaje o společnosti utajeny a vybrané skutečnosti jsou upraveny tak, aby neodhalily detaily týkající se konkrétních zranitelností.

Jako objekt zkoumání v rámci této práce byl zvolen areál stavebního podniku o přibližné rozloze 44 713 m². Objekt se nachází v zastavěném území místní průmyslové zóny na okraji obce. V areálu se nachází dvanáct objektů, které zahrnují sklady, dílny, administrativní prostory, čerpací stanici, mycí linku a garáže. Dvě budovy jsou spravovány nájemci, a protože odpovědnost za ně nespadá pod správu provozovatele areálu, nebudou předmětem této diplomové práce. Jedna budova, ve vlastnictví provozovatele, je rozdělena na dva funkční celky, čili budeme zkoumat celkově jedenáct objektů.

Areál podniku je situován v prostředí s různorodými přírodními a urbanistickými prvky. Podél severní hranice areálu vede silnice I. třídy, která představuje jedinou pozemní komunikaci umožňující vjezd do podniku. Na jižní straně areálu se rozkládají pozemky s ornou půdou a trvalým travním porostem, který působí jako přírodní bariéra zajišťující ochranu areálu ještě před samotným oplocením perimetru. Východní část areálu tvoří zástavba rodinných domů a zahrady těchto domů. Na západní straně areálu se nachází několik pozemků zahrad, které od perimetru odděluje drobný vodní tok zarostlý trvalým travním porostem. Za zahradami vede železnice. Pozemek areálu se nachází na rovinatém terénu, který není součástí chráněného ani záplavového území.

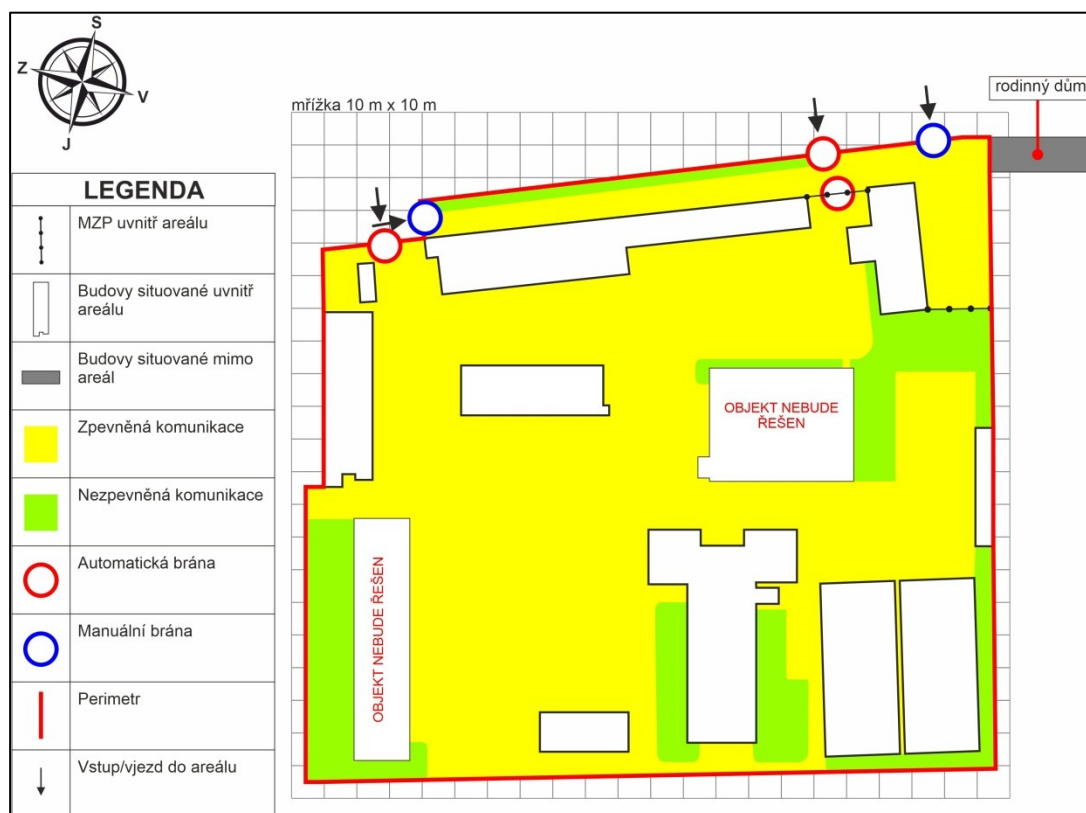
Tři úseky perimetru tvoří oplocení, ale budovy situované uvnitř či vně areálu. První úsek tvoří budova situovaná uvnitř areálu (přibližně 55 m perimetru), stejně jako druhý úsek (přibližně 40 m perimetru). Třetí úsek tvoří rodinný dům situovaný mimo areál (přibližně 12 m perimetru).

Přístup do areálu je zajištěn ze severní strany areálu prostřednictvím automatických vjezdových bran integrovaných s ESKV a manuálních vjezdových bran. Hlavní vjezdová brána je plně automatická a je navíc vybavena vjezdovou závorou. Ostatní automatické brány nejsou vybaveny vjezdovou závorou. Zbylé dva vjezdy jsou uzamykány mechanicky. Mimo provozní dobu areálu jsou brány uzamčeny. Automatické brány

se otevírají každý pracovní den v 4:30 hodin a uzavírají v 19:00 hodin. Během víkendů a svátků zůstává areál trvale uzavřen.

Areál využívá přibližně 50 zaměstnanců podniku, návštěvníci podniku a návštěvníci veřejné jídelny situované uvnitř jedné z budov.

Pro vizualizaci výše uvedených skutečností byla vytvořena mapa zkoumaného objektu (Obrázek 9). Mapa poskytuje přehled o prostorovém uspořádání jednotlivých budov v rámci areálu, přístupových bodech a perimetru objektu.



Obrázek 9 – Schéma vybraných pracovníků SBS

(zdroj: vlastní)

4.1 Kriminalita v lokalitě

Pomocí dat a informací poskytovaných Policií ČR byla analyzována kriminální situace za rok 2024 na území obce, ve které je podnik situován. V daném období bylo dle mapy kriminality na území obce uskutečněno celkem 75 trestných činů proti majetku, z toho 22 zahrnovalo krádež vloupáním (Policie ČR, ©2025). Pro porovnání vývoje trendu kriminality na území dané obce slouží Tabulka 5. Hodnoty uvedené v závorkách představují meziroční nárůst.

Tabulka 5 – Vývoj trendu majetkové trestné činnosti na území obce zkoumaného objektu

Rok	Krádeže vloupáním	Krádeže	Podvody	Jiná majetková	Majetková trestná činnost celkem
2020	17	11	6	18	43
2021	6 (- 11)	23 (+ 12)	8 (+ 2)	30 (+ 12)	58 (+ 15)
2022	10 (+ 4)	30 (+ 7)	13 (+ 5)	38 (+ 8)	73 (+ 15)
2023	11 (+ 1)	25 (- 5)	9 (- 4)	31 (- 7)	59 (- 14)
2024	22 (+ 11)	26 (+ 1)	10 (+ 1)	35 (+ 4)	75 (+ 16)

(zdroj: Policie ČR, ©2025)

Z těchto dat vyplývá, že roste trend celkové majetkové trestné činnosti na území dané obce s výjimkou v roce 2023. Meziroční nárůst krádeží vloupáním vykazoval v posledním sledovaném období vůbec nejhorší výsledky, které dokonce dvakrát převýšily počet krádeží vloupáním předchozího roku. Krádeže, podvody a jiná majetková trestná činnost vykazují v porovnání s prvním sledovaným období značně horší výsledky. Celkově lze tvrdit, že kriminalita v oblasti majetkové trestné činnosti na území dané obce ve sledovaném období značně vzrostla.

4.2 Nebezpečné látky nacházející se v objektu

V areálu podniku se nachází široká škála NL, které mohou představovat nebezpečí pro zdraví pracovníků, životní prostředí a bezpečnost celkového provozu. Formou fyzické kontroly byla provedena identifikace NL v objektu společně s jejich množstvím a bylo ověřeno, zda není překročeno maximální povolené množství dané NL v podniku.

Byly identifikovány NL, jako jsou motorová nafta, motorový olej, hydraulický olej, odpadní olej, tlakové lahve obsahující kyslík, acetylen a argon určených pro svařování, a tlakové lahve obsahující propan-butan používaných jako pohonná hmota vysokozdvížných vozíků. Tyto látky představují nebezpečí, jelikož při nedodržení postupů pro vhodnou manipulaci, skladování a používání těchto látek se zvyšuje riziko vzniku MU a snižuje se míra bezpečnosti objektu. Identifikace NL, které jsou umístěny v objektu, včetně jejich množství jsou uvedeny v Tabulce 6.

Tabulka 6 – Informace o NL v objektu

Nebezpečná látka	Číslo CAS	H-věty	Skupenství	Množství celkem
Acetylen	74-86-2	– H220 Extrémně hořlavý plyn. – H280 Obsahuje plyn pod tlakem; při zahřívání může vybuchnout.	plynné	200 litrů
Argon	7440-37-1	– H281 Obsahuje zchlazený plyn; může způsobit omrzliny nebo poškození chladem.	plynné	250 litrů
Hydraulická kapalina	125643-61-0	– H413 Může vyvolat dlouhodobé škodlivé účinky pro vodní organismy.	kapalné	300 litrů
Hydroxid sodný 20%	1310-73-2	– H302 Zdraví škodlivý při požití. – H314 Způsobuje těžké poleptání kůže a poškození očí.	kapalné	220 litrů
Kyslík	7782-44-7	– H270 Může způsobit nebo zesílit požár, oxidant. – H280 Obsahuje plyn pod tlakem, při zahřívání může vybuchnout.	plynné	250 litrů
LPG (zkapalněný propan-butan)	68476-40-4	– H220 Extrémně hořlavý plyn. – H280 Obsahuje plyn pod tlakem, při zahřívání může vybuchnout.	plynné	200 kg

(zdroj: vlastní zpracování dle krizport.cz, ©2023)

Tabulka 6 – Informace o NL v objektu (pokračování)

Nebezpečná látka	Číslo CAS	H-věty	Skupenství	Množství celkem
Motorová nafta	68334-30-5	– H226 Hořlavá kapalina a páry. – H304 Při použití a vniknutí do dýchacích cest může způsobit smrt. – H315 Dráždí kůži. – H351 Podezření na vyvolání rakoviny. – H373 Může způsobit poškození orgánů při prodloužené nebo opakované expozici. – H411 Toxický pro vodní organismy, s dlouhodobými účinky.	kapalné	max. 10 000 litrů
Motorový olej	-	– H317 Může vyvolat alergickou kožní reakci. – H413 Může vyvolat dlouhodobé škodlivé účinky pro vodní organismy.	kapalné	800 litrů
Odpadní olej	-	-	kapalné	max. 3000 litrů

(zdroj: vlastní zpracování dle krizport.cz, ©2023)

Všechny uvedené NL jsou řádně skladovány ve skladech k tomu určených a v žádném z pozorovaných případů nebylo zjištěno překročení maximálního povoleného množství NL ve skladě. Současně bylo ověřeno, zda se v objektu nevyskytuje dostatečné množství uvedených látek, aby bylo objekt možné kategorizovat do příslušné skupiny dle zákona č. 224/2015 Sb. o prevenci závažných havárií, resp. Směrnice Evropského parlamentu a Rady 2012/18/EU o kontrole nebezpečí závažných havárií s přítomností NL.

Nejvyšší množství NL bylo identifikováno u motorové nafty (max. 10 000 litrů), která je uložena v podzemních nádržích čerpací stanice uvnitř podniku, a odpadního oleje (max. 3 000 litrů), který je uložen v podzemní nádrži ve skladě hořlavých kapalin. Žádná z uvedených NL nesplňuje kritéria proto, aby mohl být objekt zařazen do skupiny A dle zákona č. 224/2015 Sb. o prevenci závažných havárií.

4.3 Specifikace chráněných prostor

Na základě informací o dispozičním uspořádání budov v rámci zkoumaného objektu přistoupíme k určení jejich specifického využití a provozních účelů. Jak bylo uvedeno výše, budeme zkoumat pouze budovy ve správě provozovatel areálu. Jedná se o deset budov, z nichž jedna je členěna na dva funkční celky:

- administrativní budova,
- dílna,
- garáže,
- mycí linka,
- podniková čerpací stanice motorové nafty,
- sklad č. 1,
- sklad č. 2,
- sklad č. 3,
- sklad č. 4,
- sklad hořlavých kapalin,
- uvažované nájemní prostory.

Administrativní budova je dvoupodlažní, podsklepená budova určená pro správní a provozní účely podniku. Součástí administrativní budovy je i jídelna, kterou kromě zaměstnanců využívají také další návštěvníci. Jídelna je provozována každý pracovní den od 9:00 do 13:00 hodin. Budova má celkem šest vstupů. Hlavní vstup tvoří posuvné, skleněné dveře, které jsou integrovány s ESKV. Další vstup, který je rovněž napojen na ESKV, tvoří dřevěné, prosklené dveře vedoucí do prostor 1. podzemního podlaží (dále jen „PP“). Forma uživatelské autentizace těchto vstupů je zajištěna pomocí hardwaru (čipové karty). Ostatní vstupy do budovy nejsou integrovány s ESKV. Jedná se o plastové,

prosklené dveře vedoucí do 2. nadzemního podlaží (dále jen „NP“), které jsou přístupné přes venkovní ocelové schodiště. Další plastové, prosklené dveře vedou do jídelny. Dále dvojce ocelové, plné dveře, které slouží jako vstup do technických prostor kotelny v 1. PP. Na plášti budovy se nachází několik stavebních otvorů osazených plastovými okny. Většina oken je umístěna v dostatečné výšce a bez použití zařízení, jako je žebřík či lešení, nejsou přístupná. Dalších čtrnáct stavebních otvorů vyplněných plastovými okny vedou do prostor 1. PP. Tato okna jsou v porovnání s ostatními snadno přístupná. Střecha má rovinatý povrch a je přístupná prostřednictvím ocelového žebříku, který je ve spodní části chráněn bezpečnostními dvířky pro zamezení vstupu nepovolaných osob. Vstup do budovy přes střechu je vyloučený, neboť na střeše nejsou žádné stavební otvory, jako střešní světlíky apod. Technické zabezpečení budovy zahrnuje pohybová čidla, signalizační zařízení (sirénu) a kamerový systém instalovaný uvnitř budovy. Na stav těchto zařízení dohlíží pracovník dohledového centra. Dále budova zahrnuje kamerový systém instalovaný na vnějším plášti, ESKV integrovaný s elektronicky řízenými vstupy vybavenými mechatronickými vložkami. V rámci požární ochrany jsou zajištěny pouze hasicí přístroje. V budově se nachází archiv s interními dokumenty, četná výpočetní technika, ceniny, ale i firemní know-how ve formě strategických plánů apod.

Dílna je jednopodlažní, nepodsklepená budova, která slouží jako specializované pracoviště určené k opravám a údržbě stavebních a zemědělských strojů, stejně jako osobních automobilů. Provádí se zde diagnostiky poruch, opravy mechanických, hydraulických a elektrických systémů a výměny součástí. Pro vstup do budovy slouží hlavní vchod, který je osazen plastovými, prosklenými dveřmi. Pro vjezd vozidel slouží tři sekční, garážová vrata. Uvnitř budovy je instalován kamerový systém.

Garáže zahrnují celkem dvanáct samostatných garáží, které jsou určeny pro parkování osobních vozidel. V praxi ovšem nejsou primárně využívány k parkování, ale slouží spíše jako skladovací prostory, například pro přívěsy a jiné vybavení.

Mycí linka je jednopodlažní nepodsklepená budova, která slouží jako zařízení pro čištění vozidel pomocí rotačních kartáčů a vysokotlakých trysek. Pro vstup osob slouží plastové dveře a pro vjezd vozidel sekční garážová vrata. V budově se nachází přibližně 220 litrů hydroxidu sodného, který se používá jako součást čisticích prostředků k odstraňování silných nečistot.

Podniková čerpací stanice motorové nafty slouží k čerpání motorové nafty pro vozidla a stroje podniku. Motorová nafta je skladována v podzemních nádržích

s kapacitou 10 000 litrů. Čerpání paliva je možné výhradně pomocí čipové karty, která zajišťuje kontrolu osob a evidenci spotřeby motorové nafty z podzemních nádrží. Podzemní nádrže jsou uzamčeny visacím zámekem. Čerpací stanice je kompletně monitorována kamerovým systémem a disponuje ochranným zařízením, které slouží pro detekci netěsnosti plášťů podzemních nádrží, pro zamezení úniku plynů a kapalin.

Sklad č. 1 je ocelová, oblouková hala, jejíž konstrukce je tvořena ocelovými vazníky. Hala je opláštěná trapézovým plechem, který kromě pláště plní funkci střešní konstrukce. Podlaha je betonová. Sklad disponuje dvěma vstupy, které jsou zajištěny posuvnými ocelovými vraty. Hala je určena pro skladování stavebního materiálu, především potrubí určené pro rozvody vody a kanalizace.

Sklad č. 2 má stejné konstrukční řešení jako Sklad č. 1. Je zde skladována nepoužívaná zemědělská a stavební technika.

Sklad č. 3 je jednopodlažní, nepodsklepená budova sloužící jako skladovací prostor pro instalátorský materiál a pneumatiky, zároveň jako klempířská dílna. Vstup do budovy je umožněn ze všech stran budovy. Na jižní straně se nachází dvě posuvná, dřevěná vrata zabezpečená visacím zámekem a kamerovým systémem. Ze severní strany vede vstup prostřednictvím dvou posuvných, ocelových vrat. Na východní i západní straně budovy jsou dvoukřídlé, ocelové dveře. Okna budovy jsou ve špatném technickém stavu.

Sklad č. 4 je ocelová, oblouková hala opláštěná textilní plachtovinou. Tento sklad slouží především pro uskladnění stavebního materiálu a vybavení stavebního podniku, jako jsou lešení, bednění, žebříky a další technické prostředky. Vstup do skladu je umožněn dvěma vstupy prostřednictvím dvoukřídlých, ocelových vrat, která jsou opatřena visacím zámekem.

Sklad hořlavých kapalin je jednopodlažní nepodsklepená budova, která dříve sloužila pro opravu zemědělských strojů, dřevo výrobu a sklad. Pro vstup do skladu slouží odolné, ocelové, dvoukřídlé dveře. Střecha budovy je přístupná pomocí žebříku. Na střeše se nachází střešní světlíky. V budově jsou skladovány NL jako motorový, hydraulický a převodový olej (hořlavé kapaliny IV. třídy) v celkovém množství přibližně 1 500 litrů. Pod zemí jsou umístěny podzemní nádrže s celkovým objemem 3 000 litrů, které slouží ukládání vyjetého oleje (hořlavá kapalina I. třídy). Nádrže jsou vyrobeny z odolného materiálu s dvojitým pláštěm, aby se minimalizovalo riziko úniku a kontaminace půdy. Sklad je stejně jako čerpací stanice motorové nafty podniku vybavena

zařízením pro detekci netěsnosti plášťů podzemních nádrží, pro zamezení úniku plynů a kapalin.

Uvažované nájemní prostory jsou jednopodlažní, nepodsklepená budova, která není v současné době nijak využívána. V minulosti sloužila jako sklad materiálu. Budova má potenciál pro využití jako nájemní prostor. Vstup do budovy je umožněn prostřednictvím ocelových vrat. Budova disponuje celkem čtyřmi těmito vraty, nicméně tři z nich jsou opatřeny proti nepovolanému vniknutí (odstraněné dvevní kování, přivařená ocel s visacím zámkem).

5 SOUČASNÝ STAV ZABEZPEČENÍ OBJEKTU

Ověření současného stavu zabezpečení areálu je rozděleno do pěti částí. První část se zaměřuje na úroveň zabezpečení perimetru, který chrání přístup na soukromý pozemek podniku. Ve druhé části je prověřeno zabezpečení plášťů jedenácti objektů v areálu, které brání neoprávněnému vniknutí do vnitřních prostor. Třetí a čtvrtá část poskytují informace o technickém zabezpečení prostorové ochrany a výkonů pracovníků SBS, kteří zajišťují ostrahu objektu. V páté části jsou uvedena konkrétní režimová opatření, která upravují denní provoz a bezpečnostní postupy uvnitř areálu. Na závěr je provedeno zhodnocení současného stavu zabezpečení objektu s popisem identifikovaným nedostatků.

5.1 Současný stav zabezpečení perimetru areálu

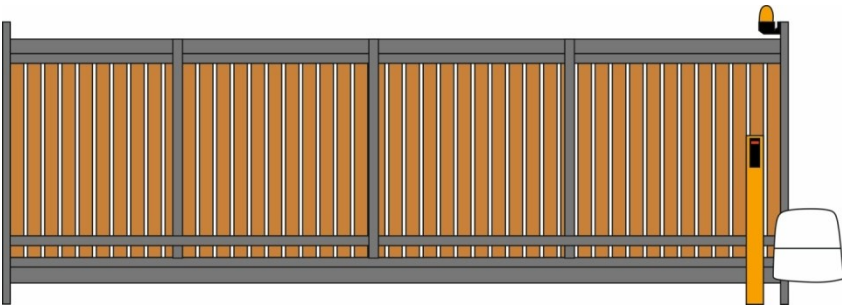
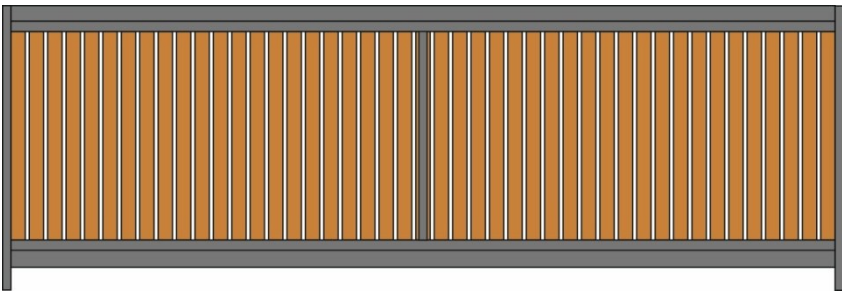
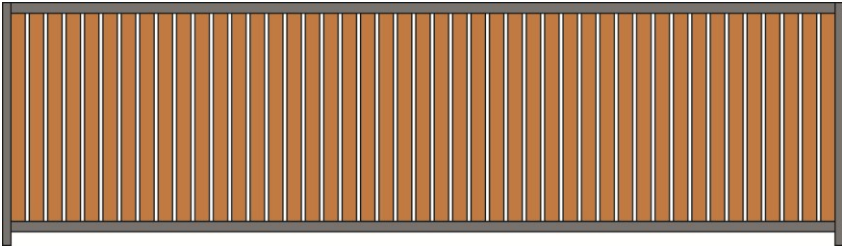
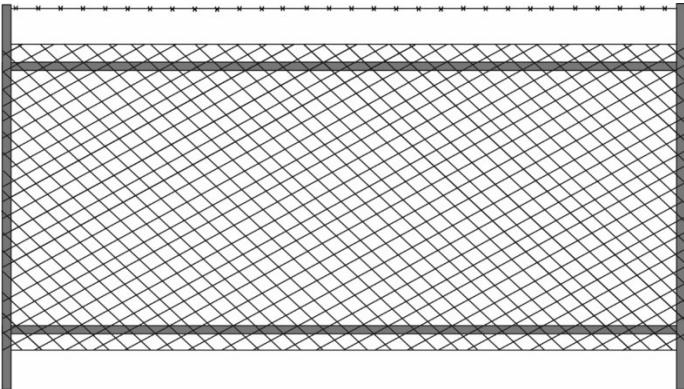
V této podkapitole je představen současný stav zabezpečení perimetru zkoumaného objektu. Cílem je identifikace zranitelných oblastí, které mohou umožnit pachateli neautorizovaný vstup do areálu.

Perimetr zkoumaného objektu tvoří brány, oplocení a pláště budov. Celkově lze perimetr rozčlenit na tyto prvky:

- automatické brány ($h = 1,8 \text{ m}$),
- manuální brány ($h = 1,8 \text{ m}$),
- oplocení z profilovaného plechu ($h = 2,0 \text{ m}$),
- oplocení z profilovaného plechu skryté v živém plotě z tují ($h = 2,0 \text{ m} + \text{túje}$),
- drátěný plot s ostnatým drátem ($h = 2,0 \text{ m}$),
- drátěný plot s ostnatým drátem skrytý v živém plotě z tují ($h = 2,0 \text{ m} + \text{túje}$),
- oplocení z betonových tvarovek ($h = 1,8 \text{ m}$),
- oplocení s kovovou nosnou konstrukcí a výplní z dřevěných latí ($h = 1,8 \text{ m}$),
- pláště budov ($h_1 = 7,0 \text{ m}$; $h_2 = 4,0 \text{ m}$; $h_3 = 2,1 \text{ m}$).

Přehled prvků, které tvoří perimetr zkoumaného objektu, mimo plášťů budov, je uveden v Tabulce 7.

Tabulka 7 – Prvky perimetru zkoumaného objektu

Mechanická bariéra	Schéma/Fotografie
Automatická brána	
Manuální brána	
Oplocení s kovovou nosnou konstrukcí a výplní z dřevěných latí	
Drátěný plot s ostnatým drátem	

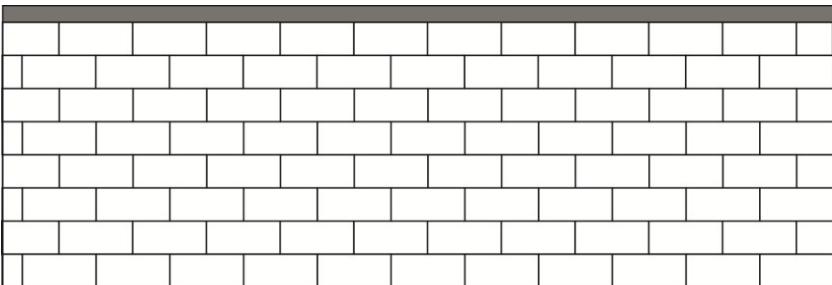
(zdroj: vlastní)

Tabulka 7 – Prvky perimetru zkoumaného objektu (pokračování)

Mechanická bariéra	Schéma/Fotografie
Oplocení z profilovaného plechu	
Oplocení z profilovaného plechu skryté v živém plotě z tújí	

(zdroj: vlastní)

Tabulka 7 – Prvky perimetru zkoumaného objektu (pokračování)

Mechanická bariéra	Schéma/Fotografie
Oplocení z betonových tvarovek	
Drátěný plot s ostnatým drátem skrytý v živém plotě z tújí	

(zdroj: vlastní)

Pro ověření současného stavu zabezpečení perimetru byl vytvořen kontrolní seznam, který je obsažen v Tabulce 8. Tento seznam slouží k systematickému posouzení aspektů týkajících se ochrany vnější hranice podniku. Vyhodnocení otázek kontrolního seznamu je obsaženo v Tabulce 9 a identifikované zranitelnosti jsou popsány v komentáři pod tabulkou.

Tabulka 8 – Kontrolní seznam současného stavu zabezpečení perimetru objektu

N	Otázka	Ano	Ne
1	Je oplocení či jiná fyzická bariéra perimetru dostatečně vysoká, aby zpomalila dobu překonání této bariéry?	Ano	
2	Je oplocení či jiná fyzická bariéra v dobrém technickém stavu?		Ne
3	Je oplocení odolné vůči pokusům o podhrabání?		Ne
4	Jsou v blízkosti perimetru odstraněny nebo zabezpečeny všechny objekty (stromy apod.), které by mohly umožnit jeho překonání?		Ne
5	Nachází se v okolí perimetru přírodní bariéry?	Ano	
6	Je zajištěno dostatečné osvětlení perimetru v celém jeho průběhu v nočních hodinách?		Ne
7	Pokrývá oplocení areálu celou plochu katastrální hranice areálu?		Ne
8	Jsou všechny přístupové body zabezpečeny vhodnou fyzickou bariérou?	Ano	
9	Jsou brány uzamykány mimo provozní dobu areálu?		Ne
10	Jsou všechny přístupové body do areálu monitorovány kamerovým systémem?	Ano	
11	Je na perimetru instalováno značení upozorňující na monitorování areálu kamerovým systémem?	Ano	
12	Je kamerový systém vybaven termovizí, nebo nočním viděním?	Ano	
13	Jsou zaměstnanci obeznámeni s postupy při identifikaci podezřelých aktivit?	Ano	
14	Je v objektu přítomna fyzická ostraha?		Ne

(zdroj: vlastní)

Vytvořený kontrolní seznam byl hodnocen pomocí vztahů (2 a 3):

$$S_{KO}(\%) = \left(\frac{\sum S_{KO}}{\sum C_N} \right) * 100 \quad (2)$$

$$S_{ZO}(\%) = \left(\frac{\sum S_{ZO}}{\sum C_N} \right) * 100 \quad (3)$$

Kde:

- S_{KO} je součet kladných odpovědí,
- S_{ZO} je součet záporných odpovědí,
- C_N je součet celkového počtu otázek (Fojtík, 2024).

Tabulka 9 – Vyhodnocení kontrolního seznamu současného stavu zabezpečení perimetru

Proměnná	Počet	Procentuální vyjádření
S_{KO}	7	50
S_{ZO}	7	50
C_N	14	100

(zdroj: vlastní)

Komentář

Otázky kontrolního seznamu byly ověřeny formou fyzické kontroly perimetru z jeho vnitřní i vnější části za účasti pracovníka SBS a byly identifikovány následující nedostatky.

- **N2:** Při kontrole vnějšího oplocení areálu bylo zjištěno, že jeho technický stav není v některých úsecích dostačující. Byly identifikovány průlezné mezery v oplocení z profilovaného plechu, které představují zranitelné místo perimetru. Dále bylo zjištěno, že žiletkové oplocení nebylo v některých místech řádně nataženo, což snižuje jeho účinnost jakožto fyzické bariéry.
- **N3:** V jedné části perimetru existuje reálná hrozba podhrabání. Tato část perimetru má specifické terénní vlastnosti, které umožňují snadnější přístup pod plot. Tato skutečnost činí část perimetru zranitelnou vůči nelegálnímu vniknutí.
- **N4:** Byly identifikovány části perimetru, ve kterých se nachází objekty usnadňující jeho překonání. V prvním případě se jednalo o stromy vyšší než samotné oplocení perimetru. Ve druhém případě šlo o terénní úpravy situované mimo areál, které poskytovaly snadný přístup na střechu jedné z budov v rámci podniku.
- **N6:** Úroveň osvětlení vnější hranice areálu není v nočních hodinách na všech úsecích dostatečná. Částečné osvětlení perimetru je dostupné pouze ze severní strany podniku, kde je perimetr osvětlen veřejným pouličním osvětlením podél silnice I. třídy. Kritickým nedostatkem je absence jakékoli formy osvětlení na jižní a západní straně, což činí tyto části perimetru zranitelné.

- **N7:** Přibližně 275 m² plochy, která je ve vlastnictví provozovatele areálu, se nachází v blízkosti jedné z budov. V této části má potenciální pachatel přímý přístup k plášti budovy.
- **N9:** Manuální brána nebyla v době mimo provoz areálu uzamčena, což umožnilo neoprávněný vstup do části areálu. Dále bylo zjištěno, že jsou mechanické bariéry uzamykány prostřednictvím lanového zámku. Tento typ zámku není vhodný pro zabezpečení přístupových bodů vzhledem ke své nízké průlomové odolnosti.
- **N14:** Fyzická ostraha není trvale přítomná v areálu. Ostraha je zajišťována externí firmou poskytující SBS. V případě potřeby vyslání zásahové jednotky je třeba vzít v úvahu, že tento fakt ovlivňuje dobu dojezdu zásahové jednotky na místo zásahu, což může mít vliv na rychlost reakce a účinnost zásahu.

5.2 Současný stav zabezpečení plášťů budov

Tato podkapitola se zaměřuje na popsání současného stavu zabezpečení plášťů budov v rámci zkoumaného areálu. Cílem je analyzovat úroveň ochrany vstupních bodů, výplní stavebních otvorů a dalších konstrukčních prvků, které mohou představovat zranitelná místa umožňující neoprávněný přístup do vnitřních prostor budov.

Kontrolní seznam uvedený v Tabulce 10 se zaměřuje na otázky týkající se zabezpečení plášťů budov. Prověřeno bylo zabezpečení plášťů u jedenácti objektů v areálu. Vyhodnocení kontrolního seznamu je obsaženo v Tabulce 11 a zjištěné nedostatky jsou popsány v komentáři pod tabulkou. Kontrolní seznam byl hodnocen pomocí vztahů (2 a 3) definovaných v kapitole 5.1.

Tabulka 10 – Kontrolní seznam současného stavu zabezpečení plášťů budov

N	Otázka	Ano	Ne
1	Jsou všechny vstupy do budov zabezpečeny proti neoprávněnému vniknutí?		Ne
2	Jsou vnější dveře a okna v dobrém technickém stavu?		Ne
3	Jsou okna podzemního podlaží vybavena bezpečnostními fóliemi či jinou vhodnou mechanickou bariérou?	Ano	

(zdroj: vlastní)

Tabulka 10 – Kontrolní seznam současného stavu zabezpečení plášťů budov (pokračování)

N	Otázka	Ano	Ne
4	Jsou v blízkosti budovy odstraněny všechny objekty, které mohou umožnit přístup osoby do budovy nebo na střechu?		Ne
5	Jsou všechna okna chráněna bezpečnostní fólií, mřížemi nebo jinými MZP?		Ne
6	Jsou všechny vnější dveře vyrobeny z odolných materiálů, které ztěžují jejich překonání?		Ne
7	Je zajištěno dostatečné osvětlení všech vstupních bodů budovy v nočních hodinách?		Ne
8	Jsou hlavní vstupy do budovy opatřeny kamerou?		Ne
9	Jsou všechny vstupy pro zaměstnance odděleny od vstupů pro návštěvníky?		Ne
10	Je znemožněn přístup na střechu pomocí žebříku?		Ne
11	Je plášť budovy vyroben z materiálů odolných proti mechanickému poškození (např. ocel, beton)?	Ano	
12	Bylo v době kontroly zamezeno vstupu do budov?		Ne

(zdroj: vlastní)

Tabulka 11 – Vyhodnocení kontrolního seznamu současného stavu zabezpečení plášťů budov

Proměnná	Počet	Procentuální vyjádření
S_{KO}	2	16,7
S_{ZO}	10	83,3
C_N	12	100

(zdroj: vlastní)

Komentář

Otázky kontrolního seznamu byly ověřeny formou fyzické kontroly plášťů jednotlivých budov situovaných v areálu za účasti pracovníka SBS a byly identifikovány významné nedostatky popsány níže.

- **N1:** Bylo zjištěno, že v době kontroly, mimo provozní dobu areálu, zůstaly dva vstupy do budov odemknuté a byl tak umožněn neautorizovaný přístup do budov. První případ se týkal hlavního vstupu do jednoho ze skladů, který měl být zajištěn visacím zámekem, který však zůstal odemknutý a pouze zavěšen. Druhý problém vykazovaly dřevěné dveře napojené

na ESKV, přičemž zřejmě nebylo zajištěno jejich řádné dovření. Tyto dveře vykazují mimo jiné známky opotřebování.

- **N2:** V areálu byla identifikována dřevěná, posuvná vrata, která jsou na hranici životnosti, jelikož jejich posuvná konstrukce je značně opotřebovaná a dochází k jejich prohýbání. Další problém vykazují dřevěné dveře napojené na ESKV, které nedovírají.
- **N4:** V blízkosti jedné z budov jsou skladovány kontejnery, které při jejich výstupu umožňují přístup na střechu budovy. Další budova má na plášti instalován nezabezpečený žebřík umožňující přístup na střechu.
- **N5:** Zabezpečení oken v rámci areálu je v dobrém stavu, nicméně jedna budova zahrnuje několik rozbitých oken v úrovni přízemí a 1. NP.
- **N6:** Problematické se jeví zejména vstupy, které tvoří dveře nebo vrata konstruované ze dřeva. Tyto vstupy jeví ztráty pevnosti materiálu a těsnosti, opotřebované kování a celkově by se dalo tvrdit, že jsou na hranici životnosti.
- **N7:** V nočních hodinách není zajištěno dostatečné osvětlení vstupních bodů téměř všech budov v areálu. Část plášťů budov, které přiléhají k silnici, je osvětlena pouličním osvětlením. Ostatní objekty, které nepřiléhají k silnici, nejsou osvětleny vůbec.
- **N8:** Většina budov v areálu nemá hlavní vstup do budovy zabezpečen kamerovým systémem.
- **N9:** Pro vstup zaměstnanců slouží automatická brána a pro vstup návštěvníků jídelny slouží manuální brána, které jsou od sebe vzdáleny přibližně 28 m. Mezi vstupy neexistuje žádná hranice, která by oddělovala prostor pro zaměstnance a prostor pro návštěvníky. Tyto dva vstupy odděluje pouze bariéra z betonových květináčů o výšce 80 cm, což nijak neprodlužuje dobu překonání této bariéry, a tedy neplní svou funkci efektivně.
- **N10:** Na plášti jedné z budov v rámci areálu je instalován nezabezpečený žebřík, který umožňuje přístup na střechu. Na střeše se navíc nachází nezabezpečené polykarbonátové střešní světlíky.

- **N12:** V době kontroly byl získán neautorizovaný přístup do tří z deseti kontrolovaných budov (podniková čerpací stanice motorové nafty nebyla předmětem kontroly). Detail je uveden v komentáři N1.

5.3 Technické zabezpečení prostorové ochrany

Technické zabezpečení prostorové ochrany objektu tvoří poplachový zabezpečovací systém, kamerový systém a věcné prostředky požární ochrany.

Pouze administrativní budova je integrována s poplachovým zabezpečovacím systémem, ostatní objekty v areálu do tohoto systému integrovány nejsou. Poplachový zabezpečovací systém zahrnuje pohybové detektory, které monitorují neoprávněný vstup do budovy. V případě detekce narušení systém odesílá signál do poplachového přijímacího centra a zároveň informuje provozovatele podniku prostřednictvím telefonního oznámení. Po aktivaci poplachu dochází k automatickému spuštění sirén.

Kamerový systém objektu zahrnuje celkem 22 kamer, jejichž záznamy jsou nepřetržitě přenášeny do dohledového centra. Používané kamery jsou válcového nebo půlkulatého tvaru, zahrnují venkovní i vnitřní prostory. Operátor dohledového centra monitoruje veškeré vizuální informace a v případě identifikace bezpečnostního incidentu má možnost rozhodnout o vyslání pracovníka zásahové jednotky na místo události. Současná konfigurace kamerového systému zahrnuje zařízení s podporou nočního vidění, což rozšiřuje možnosti monitorování v podmínkách snížené viditelnosti.

Elektronický systém kontroly vstupu zahrnuje tři automatické vjezdové brány, z nichž dvě tvoří perimetru areálu, a jedna z nich je navíc doplněna automatickou závorou. Administrativní budova zahrnuje dva vstupy do budovy a jedny vnitřní dveře integrované s ESKV. Ostatní vstupy do budov v areálu nejsou integrovány s ESKV.

V rámci zdolávání požáru jsou zajištěny pouze věcné prostředky požární ochrany, jako jsou přenosné hasicí přístroje a dále sorbenty určené k absorpci uniklých nebezpečných kapalin. Tato forma požární ochrany platí pro celý areál.

5.4 Zajištění fyzické ostrahy

Ostraha objektu je zajišťována formou outsourcingu společnosti, která poskytuje SBS. Fyzická ostraha není v areálu trvale přítomna, ovšem nepřetržitý dohled nad detekčními prvky v objektu zajišťuje operátor dohledového centra. V případě narušení bezpečnosti

či jiných incidentů má operátor dohledového centra možnost k objektu vyslat pracovníka zásahové jednotky nebo spustit výstražné zařízení v podobě sirény.

5.5 Vnitřní režimová opatření

Pro zajištění adekvátní úrovně bezpečnosti uvnitř objektu definuje podnik konkrétní režimová opatření, která jsou zaměstnanci povinni dodržovat.

Autentizace osob je zajišťována prostřednictvím čipových karet, které jsou zaměstnancům vydávány při nástupu do pracovní pozice. Správa přístupů je v kompetenci místního oddělení informačních technologií, které zajišťuje správu čipových karet a jejich deaktivaci při ukončení pracovního poměru, kdy jsou karty vydány zpět zaměstnavateli.

Klíčový režim je ve správě pověřeného zaměstnance, který klíče distribuuje, rovněž vede přehled o jejich vydání a zajišťuje, že klíče jsou poskytovány pouze oprávněným osobám.

Kontrola vozidel probíhá prostřednictvím elektronického zvonku umístěného u automatické brány, který umožňuje řidiči navázat spojení s operátorem dohledového centra. Operátor následně provádí vzdálenou verifikaci oprávnění k přístupu a na základě ověření rozhoduje o udělení nebo zamítnutí přístupu. Při výjezdu z areálu podniku se tento proces opakuje.

Pohyb vozidel je regulován maximální povolenou rychlostí 20 km/h v celém areálu.

Provozní režim je nastaven každý pracovní den od 4:30 do 19:00 hodin. Během víkendů a svátků je areál trvale uzavřen. Pro práci mimo provozní dobu podniku je nutné hlásit se pracovníkovi SBS.

Uzamykání vstupních bodů je zajišťováno kombinovaně (automaticky i manuálně). Automatické brány se každý pracovní den v 19:00 hodin automaticky uzamknou a zůstanou uzamčené do 4:30 hodin ráno následujícího dne. Uzamykání manuálních bran je v kompetenci pověřeného pracovníka.

5.6 Zhodnocení současného stavu zabezpečení

Na základě provedené kontroly zabezpečení objektu byly identifikovány následující nedostatky, které mohou představovat ohrožení.

Ochrana perimetru vykazuje určité nedostatky, jejichž odstranění by bylo vhodné zvážit pro zamezení neoprávněného přístupu do prostor areálu. Některé úseky oplocení jsou v nevyhovujícím technickém stavu, což usnadňuje jejich překonání. Mezi zranitelná místa patří neuzamčené manuální brány, které umožňují neoprávněným osobám přímý přístup k plášťům budov, čímž se zvyšuje riziko vzniku vandalismu (například sprejování graffiti na plášť budovy). Další slabinou je absence osvětlení v jižní a západní části perimetru, což usnadňuje nekontrolovaný pohyb v této oblasti. Na druhou stranu významnou výhodou lokality je přirozená ochrana v podobě obtížně překonatelných přírodních bariér, které omezují možnosti neoprávněného vstupu na pozemek.

Ochrana plášťů budov byla pro většinu zkoumaných objektů posouzena jako nedostačující. V době kontroly bylo možné získat neoprávněný přístup do dvou z deseti zkoumaných budov. Tato skutečnost naznačuje, že některé pláště budov nejsou dostatečně chráněny proti vniknutí neoprávněných osob. Pláště budov, které tvoří perimetr areálu, ohrožuje vandalismus a rizika jako jsou, poškození fasády, sprejování graffiti, či rozbití oken, což povede k finančním ztrátám vynaložených na opravy. Některé vstupy do budov jsou ve špatném technickém stavu (opotřebené kování) a to dokonce i dveře integrované s ESKV (nedovírají). Existuje tak opět riziko umožnění nežádoucího přístupu do budovy. Přístup prostřednictvím oken je nepravděpodobný, jelikož většina budov tato okna nemají (obloukové haly), nebo okna nejsou přístupná bez využití zařízení jako žebřík či lešení. Výjimku tvoří jeden objekt, který zahrnuje několik rozbitých oken v úrovni 1. NP. Dalším zjištěným nedostatkem je nezabezpečený žebřík poskytující přístupovou cestu na střechu budovy.

Technické zabezpečení prostorové ochrany zahrnuje poplachový zabezpečovací systém tvořený pohybovými detektory a sirénami instalovaný uvnitř jediné budovy. Tato forma zabezpečení před vloupáním je vhodná a má schopnost odradit útočníka před dokončením vloupání. Jako silný nedostatek v rámci technického zabezpečení je nutné zmínit absenci prostředků pro zajištění požární ochrany, neboť v budovách nejsou instalovány žádné požární hlásiče, požární tlačítka, sprinklery, ale pouze přenosné hasicí přístroje. Detekce požáru je v celém areálu zajištěna pouze prostřednictvím kamerového systému, který je monitorován operátorem dohledového centra. Tento způsob ochrany před požárem není dostatečný pro včasné odhalení požárního nebezpečí. Kamery navíc nepokrývají mnoho vnitřních prostor, kde by mohlo dojít ke vzniku požáru. Forma ESKV je pro podnik vhodná, vjezd do areálu podniku není možný bez dálkového ověření

od operátora dohledového centra. Tento způsob autentizace má své jisté zranitelnosti (omezené možnosti identifikace uživatele na dálku, z dlouhodobého hlediska není spolehlivý).

Ostraha objektu vykazuje trvalou absenci přítomnosti fyzické ostrahy v areálu. Pokud není strážný přítomný v areálu, může se doba reakce na bezpečnostní incident zbytečně prodloužit, což zvyšuje riziko úspěšného útoku na objekt. Jedinou okamžitou reakci, kterou operátor dohledového centra disponuje kromě přivolání zásahové jednotky, je spuštění výstražného zařízení (sirény). Vzdálený dohled prostřednictvím kamer navíc není z pohledu bezpečnosti optimálním řešením, neboť zahrnuje slepá místa, může selhávat a mít technické problémy. Pokud dojde k selhání v momentě, kdy je objekt ohrožen, řešení této situace bez fyzické přítomnosti ostrahy není efektivní. Dohledové centrum může vyslat pracovníka zásahové jednotky na místo incidentu, ale není zaručeno, že tato jednotka bude k dispozici v daný okamžik. V souhrnu lze konstatovat, že model ochrany založený na absenci trvalé fyzické ostrahy může představovat riziko pro bezpečnost objektu, zejména při MU, kdy je nezbytná rychlá a efektivní reakce.

6 POSOUZENÍ BEZPEČNOSTNÍCH RIZIK

Tato část práce se zabývá identifikací, analýzou a hodnocením bezpečnostních rizik a zranitelností v rámci zkoumaného objektu. Na základě zjištění budou navržena bezpečnostní opatření, která povedou ke zmírnění nebo odstranění identifikovaných rizik. Obecný postup je popsán na Obrázku 1 a bližší informace o postupu jsou uvedeny v jednotlivých podkapitolách.

6.1 Identifikace aktiv a hrozeb

Prvním krokem v procesu posuzování bezpečnostních rizik je identifikace aktiv podniku, neboli stanovení prvků, které mají pro organizaci významnou hodnotu a vyžadují adekvátní úroveň zabezpečení před potenciálním ohrožením. Identifikace těchto aktiv je klíčová pro další části diplomové práce. Dle charakteristik objektu byla společně s pracovníkem SBS konzultována tato aktiva:

- bezpečnost osob (dále jen „A₁“),
- finanční hotovost a ceniny (dále jen „A₂“),
- majetek podniku (dále jen „A₃“),
- chráněné prostory (dále jen „A₄“),
- reputace podniku (dále jen „A₅“).

Na základě identifikovaných aktiv je možné přistoupit k procesu identifikace hrozeb (Tabulka 12). Hrozby představují události nebo činnosti, které by mohly způsobit škodu nebo ohrozit hodnotu těchto aktiv. Pro každé z uvedených aktiv je třeba zvážit možné scénáře ohrožení na základě současného stavu zabezpečení, které by mohly nastat. K tomu je nezbytné definovat možné zdroje (nositele) ohrožení. Vzhledem ke zkoumanému objektu rozlišme čtyři druhy útočníků, jakožto zdrojů ohrožení, které jsou relevantní ve vztahu k definovaným aktivům:

- **Náhodný pachatel** (dále jen „P₁“) má minimálními znalosti, dovednosti a zkušenosti v oblasti protiprávního jednání. Jedná bez konkrétního úmyslu a relevantních informací o cíli. Používá nástroje, které má po ruce, jako jsou kámen, kus dřeva, cihla a jedná bez předem stanoveného plánu.
- **Vědomý pachatel** (dále jen „P₂“) má základní až pokročilé znalosti a dovednosti v oblasti protiprávního jednání. Jedná s konkrétním motivem způsobit škodu,

má základní informace o cíli a jeho zranitelnostech. Používá nástroje jako klíče nebo páčidla. Jedná spíše intuitivně a bez detailního plánu.

- **Profesionální pachatel** (dále jen „P₃“) disponuje rozsáhlými znalostmi a dovednostmi v oblasti protiprávního jednání. Jedná podle předem stanoveného, promyšleného plánu s cílem dosáhnout maximálního zisku. Má detailní informace o zranitelnostech objektu, formě zabezpečení a režimu provozu. Používá specializované zlodějské náčiní, jako jsou paklíč, lupa nebo univerzální klíč.
- **Vnitřní hrozba** (dále jen „P₄“) je osoba, která má přístup do chráněných oblastí díky svému pracovnímu nebo organizačnímu postavení. Má znalosti o vnitřních procesech, strukturách a zranitelnostech podniku. Jedná s konkrétním úmyslem a plánem, který vychází z osobní motivace (finanční zisk, pomsta apod.). Využívá přitom praktik sociálního inženýrství a základních nástrojů pro vloupání.

Tabulka 12 – Identifikace potenciálních hrozeb

Hrozba	Zdroj hrozby	Scénář	Ohrožená aktiva
Krádež	P ₁	Pachatel při návštěvě podniku využije příležitost a odcizí drobné předměty, ke kterým má přístup.	A ₃
	P ₄	Má oprávněný přístup do chráněných prostor a v průběhu dnů, měsíců nebo let se obohacuje odcizenými předměty.	A ₂ , A ₃
Kybernetický útok	P ₃	Hacker prostřednictvím malwaru pronikne do firemní sítě a zašifruje důležitá data podniku.	A ₁ , A ₃
Loupež	P ₃	Ozbrojený útok s cílem získat finanční hotovost nebo cennosti s vysokou hodnotou.	A ₁ , A ₂ , A ₃ , A ₄ , A ₅
Násilí	P ₁ , P ₂	Fyzické napadnutí zaměstnance nebo návštěvníka jídelny.	A ₁
	P ₄	Fyzická potyčka při sporu zaměstnanců nebo návštěvníků jídelny.	A ₁
Neoprávněný vstup	P ₁ , P ₂ , P ₃	Pachatel překoná perimetr a získá přístup do areálu (chráněné oblasti).	A ₃ , A ₄
	P ₂ , P ₃	Pachatel překoná perimetr a plášť budovy a získá přístup do budovy (chráněné oblasti).	A ₂ , A ₃ , A ₄
	P ₃	Pachatel překoná perimetr, plášť budovy, prvky prostorové a předmětové ochrany.	A ₂ , A ₃ , A ₄ , A ₅

(zdroj: vlastní)

Tabulka 12 – Identifikace potenciálních hrozeb (pokračování)

Hrozba	Zdroj hrozby	Scénář	Ohrožená aktiva
Sabotáž	P ₄	Fyzické poškození strojů a materiálu.	A ₃ , A ₅
	P ₄	Odstranění důležitých podnikových dat.	A ₃
	P ₄	Rozesílání falešných informací obchodním partnerům.	A ₃ , A ₅
	P ₄	Úmyslné založení požáru.	A ₁ , A ₃ , A ₅
Sociální inženýrství	P ₃ , P ₄	Pachatel oklame zaměstnance lstí a získá přístup ke klíčům, chráněným prostorům a chráněným předmětům v podniku.	A ₂ , A ₃ , A ₄
Únik citlivých informací	P ₃	Pachatel získá neoprávněný přístup k fyzickým či digitálním dokumentům podniku a podnik vydírá (požaduje výkupné).	A ₁ , A ₂ , A ₄ , A ₅
	P ₄	Pachatel získá oprávněný přístup k fyzickým či digitálním dokumentům podniku a zpřístupní je třetím stranám.	A ₄ , A ₅
Únik NL	P ₃ , P ₄	Únik NL z technologického zařízení nebo skladovacích prostor a kontaminace půdy.	A ₁ , A ₃
Vandalismus	P ₁ , P ₂	Sprejování graffiti na oplocení nebo plášť budovy.	A ₃ , A ₅
	P ₂ , P ₃	Poškození vozidel (poškrábání laku, proříznutí pneumatiky) a jiných zařízení v areálu.	A ₃ , A ₄
Vloupání	P ₂	Pachatel překoná perimetr, pomocí páčidla vypáchá dveře a získá neoprávněný přístup do budovy, kde následně odcizí předměty v hodnotě několika tisíc korun.	A ₂ , A ₃ , A ₄
	P ₃	Pachatel úspěšně překoná veškeré vrstvy ochrany, aniž by byl detekován. Následně získá neoprávněný přístup do trezoru, odkud odcizí finanční hotovost v hodnotě několika stovek tisíc korun.	A ₂ , A ₃ , A ₄
Zpronevěra	P ₄	Pachatel s oprávněným přístupem k financím a majetku podniku tyto prostředky zneužije pro osobní prospěch.	A ₂ , A ₃
Žhářství	P ₂ , P ₄	Pachatel úmyslně založí požár vznícením hořlavé kapaliny.	A ₁ , A ₃ , A ₄ , A ₅

(zdroj: vlastní)

6.2 Analýza a hodnocení bezpečnostních rizik

Na základě identifikovaných hrozeb lze provést analýzu a hodnocení bezpečnostních rizik. Riziko se posuzuje jako kombinace pravděpodobnosti jeho výskytu a možných negativních následků. Kritéria pro hodnocení pravděpodobnosti jsou uvedena v Tabulce 13 a kritéria pro hodnocení následků v Tabulce 14.

Tabulka 13 – Kritéria pro určení pravděpodobnosti vzniku rizika

Početnost	Frekvence vzniku	Časové působení
Velmi vysoká	Vzniká velmi často	Nepřetržité
Vysoká	Několikrát	Časté
Střední	Občas	Vzácné
Nízká	Málo možná	Velmi vzácné
Velmi nízká	Vyloučená	Skoro nemožné

(zdroj: Hofreiter, 2015)

Tabulka 14 – Kritéria pro určení následků při působení rizika

Následek	Popis
Zanedbatelný	Dopad na podnik je minimální, bez významných finančních ztrát, narušení provozu nebo poškození reputace. Incident nevyžaduje okamžitou reakci a lze jej snadno zvládnout běžnými postupy.
Málo významný	Mírný dopad na podnikové procesy, menší finanční ztráty nebo dočasné narušení provozu. Organizace se snadno zotaví bez dlouhodobých následků.
Významný	Událost způsobuje znatelné narušení provozu, značné finanční ztráty nebo ohrožení citlivých dat. Vyžaduje aktivní zásah a může ovlivnit důvěru zákazníků či obchodních partnerů.
Kritický	Závažné narušení chodu podniku, značné finanční škody, únik citlivých informací nebo významné ohrožení bezpečnosti. Vyžaduje okamžitou reakci vedení a rozsáhlá nápravná opatření.
Katastrofický	Fatální dopad na podnik, dlouhodobá nebo nevratná ztráta dat, úplná paralýza provozu, zásadní finanční ztráty nebo právní důsledky. Může vést k ukončení činnosti organizace.

(zdroj: vlastní)

Výstup těchto dvou kvalitativních metod se následně dosadí do matice rizik (Tabulka 15) a na základě výsledku je určena úroveň daného rizika na stupnici – nepřijatelné riziko, podmíněně přijatelné riziko, přijatelné riziko.

Tabulka 15 – Kritéria pro určení míry rizika

		Pravděpodobnost				
		Velmi nízká	Nízká	Střední	Vysoká	Velmi vysoká
Následek	Zanedbatelný	Přijatelné riziko	Přijatelné riziko	Přijatelné riziko	Přijatelné riziko	Podmíněně přijatelné riziko
	Málo významný	Přijatelné riziko	Přijatelné riziko	Podmíněně přijatelné riziko	Podmíněně přijatelné riziko	Podmíněně přijatelné riziko
	Významný	Přijatelné riziko	Podmíněně přijatelné riziko	Podmíněně přijatelné riziko	Nepřijatelné riziko	Nepřijatelné riziko
	Kritický	Přijatelné riziko	Podmíněně přijatelné riziko	Nepřijatelné riziko	Nepřijatelné riziko	Nepřijatelné riziko
	Katastrofický	Podmíněně přijatelné riziko	Podmíněně přijatelné riziko	Nepřijatelné riziko	Nepřijatelné riziko	Nepřijatelné riziko

(zdroj: vlastní)

Výsledky analýzy a hodnocení bezpečnostních rizik pro zkoumaný objekt jsou uvedeny v Tabulce 16. Hrozby vyhodnocené s nepřijatelnou nebo podmíněně přijatelnou mírou rizika budou předmětem v rámci návrhu doporučení a bezpečnostních opatření.

Tabulka 16 – Analýza a hodnocení bezpečnostních rizik

Identifikace rizik				Analýza rizik		
Hrozba	Zdroj hrozby	Scénář	Ohrožená aktiva	Pravděpodobnost	Následky	Úroveň rizika
Krádež	P ₁	Pachatel při návštěvě podniku využije příležitost a odcizí drobné předměty, ke kterým má přístup.	A ₃ , A ₄	střední	málo významné	Podmíněně přijatelné riziko
	P ₄	Má oprávněný přístup do chráněných prostor a v průběhu dnů, měsíců nebo let se obohacuje odcizenými předměty.	A ₂ , A ₃	vysoká	významné	Nepřijatelné riziko
Kybernetický útok	P ₃	Hacker prostřednictvím malwaru pronikne do firemní sítě a zašifruje důležitá data podniku.	A ₁ , A ₃	střední	významný	Podmíněně přijatelné riziko
Loupež	P ₃	Ozbrojený útok s cílem získat finanční hotovost nebo cennosti s vysokou hodnotou.	A ₁ , A ₂ , A ₃ , A ₄ , A ₅	nízká	kritické	Podmíněně přijatelné riziko
Násilí	P ₁ , P ₂	Fyzické napadnutí zaměstnance nebo návštěvníka jídelny.	A ₁	nízká	významné	Podmíněně přijatelné riziko
	P ₄	Fyzická potyčka při sporu zaměstnanců nebo návštěvníků jídelny.	A ₁	střední	málo významné	Podmíněně přijatelné riziko
Neoprávněný vstup	P ₁ , P ₂ , P ₃	Pachatel překoná perimetr a získá přístup do areálu (chráněné oblasti).	A ₃ , A ₄	vysoká	málo významné	Podmíněně přijatelné riziko
	P ₂ , P ₃	Pachatel překoná perimetr a plášť budovy a získá přístup do budovy (chráněné oblasti).	A ₂ , A ₃ , A ₄	vysoká	významné	Nepřijatelné riziko
	P ₃	Pachatel překoná perimetr, plášť budovy, prvky prostorové a předmětové ochrany.	A ₂ , A ₃ , A ₄ , A ₅	nízká	významné	Podmíněně přijatelné riziko

(zdroj: vlastní zpracování dle Hofreiter, 2015)

Tabulka 16 – Analýza a hodnocení bezpečnostních rizik (pokračování)

Identifikace rizik				Analýza rizik		
Hrozba	Zdroj hrozby	Scénář	Ohrožená aktiva	Pravděpodobnost	Následky	Úroveň rizika
Sabotáž	P ₄	Fyzické poškození materiálu, strojů nebo serverů.	A ₃ , A ₅	nízká	kritické	Podmíněně přijatelné riziko
	P ₄	Odstranění důležitých podnikových dat.	A ₃	nízká	kritické	Podmíněně přijatelné riziko
	P ₄	Rozesílání falešných informací obchodním partnerům.	A ₃ , A ₅	nízká	kritické	Podmíněně přijatelné riziko
	P ₄	Úmyslné založení požáru.	A ₁ , A ₃ , A ₅	velmi nízká	katastrofické	Podmíněně přijatelné riziko
Sociální inženýrství	P ₃ , P ₄	Pachatel oklame zaměstnance listí a získá přístup ke klíčům, chráněným prostorům a chráněným předmětům v podniku.	A ₂ , A ₃ , A ₄	střední	významné	Podmíněně přijatelné riziko
Únik citlivých informací	P ₃	Pachatel získá neoprávněný přístup k fyzickým či digitálním dokumentům podniku a podnik vydírá (požaduje výkupné).	A ₁ , A ₂ , A ₄ , A ₅	nízká	významné	Podmíněně přijatelné riziko
	P ₄	Pachatel získá oprávněný přístup k fyzickým či digitálním dokumentům podniku a zpřístupní je třetím stranám.	A ₄ , A ₅	střední	významné	Podmíněně přijatelné riziko
Únik NL	P ₃ , P ₄	Úmyslné poškození nádrže a následný únik NL z technologického zařízení nebo skladovacích prostor.	A ₁ , A ₃	nízká	kritický	Podmíněně přijatelné riziko
Vandalismus	P ₁ , P ₂	Sprejování graffiti na oplocení nebo plášť budovy.	A ₃ , A ₅	vysoká	významné	Nepřijatelné riziko
	P ₂ , P ₃	Poškození vozidel (poškrábání laku, proříznutí pneumatiky) a jiných zařízení v areálu.	A ₃ , A ₄	střední	významné	Podmíněně přijatelné riziko

(zdroj: vlastní zpracování dle Hofreiter, 2015)

Tabulka 16 – Analýza a hodnocení bezpečnostních rizik (pokračování)

Identifikace rizik			Analýza rizik			
Hrozba	Zdroj hrozby	Scénář	Ohrožená aktiva	Pravděpodobnost	Následky	Úroveň rizika
Vloupání	P ₂	Pachatel překoná perimetr, pomocí páčidla vypáčí dveře a získá neoprávněný přístup do budovy, kde následně odcizí předměty v hodnotě několika tisíc korun.	A ₂ , A ₃ , A ₄	nízká	významný	Podmíněně přijatelné riziko
	P ₃	Pachatel úspěšně překoná veškeré vrstvy ochrany, aniž by byl detekován. Následně získá neoprávněný přístup do trezoru, odkud odcizí finanční hotovost v hodnotě několika desítek tisíc korun.	A ₂ , A ₃ , A ₄	velmi nízká	kritický	Přijatelné riziko
Zpronevěra	P ₄	Pachatel s oprávněným přístupem k financím a majetku podniku tyto prostředky zneužije pro osobní prospěch.	A ₂ , A ₃	střední	významný	Podmíněně přijatelné riziko
Žhárství	P ₂ , P ₄	Pachatel úmyslně založí požár vznícením hořlavé kapaliny.	A ₁ , A ₃ , A ₄ , A ₅	nízká	katastrofické	Podmíněně přijatelné riziko

(zdroj: vlastní zpracování dle Hofreiter, 2015)

6.3 Stanovení zranitelnosti chráněných prostor

Aby bylo možné určit, které chráněné prostory nejsou adekvátně zabezpečeny proti identifikovaným hrozbám, je nezbytné analyzovat jejich zranitelnost. K tomuto účelu je využita semikvantitativní bodová metoda, která hodnotí dvě složky zranitelnosti – potenciální význam chráněného prostoru a potenciální riziko chráněného prostoru. Podrobnosti o hodnocených položkách jsou uvedeny v Příloze P I (pro určení potenciálního významu) a Příloze P II (pro určení potenciálního rizika).

Obě složky zranitelnosti jsou bodově ohodnoceny, přičemž součet získaných bodů je následně porovnán s maximální možnou hodnotou pro danou složku a je vyjádřen v procentech. Na základě procentuálního vyjádření jsou složky zranitelnosti kategorizovány v matici rizik do jedné ze tří úrovní – vysoká zranitelnost, střední zranitelnost, nízká zranitelnost (Tabulka 17).

Tabulka 17 – Matice rizik pro určení zranitelnosti chráněných prostor

		Úroveň potenciálního významu		
		< 30 %	30 % až 50 %	> 50 %
Úroveň potenciálního rizika	< 35 %	nízká zranitelnost	nízká zranitelnost	střední zranitelnost
	35 % až 65 %	nízká zranitelnost	střední zranitelnost	vysoká zranitelnost
	> 65 %	střední zranitelnost	vysoká zranitelnost	vysoká zranitelnost

(zdroj: vlastní zpracování dle ČSN P CEN/TS 14383-3, 2006)

V rámci provedené analýzy jsou chráněné prostory anonymizovány, při použití formátu „CHP_x“ označujícího konkrétní chráněný prostor. Díky tomuto přístupu bude zajištěno, že zranitelnosti analyzovaných prostorů zůstanou pro čtenáře skryté, což přispěje k prevenci rizik.

Podrobnosti hodnocení jsou zachyceny v Tabulce 18 a Tabulce 19, výsledky hodnocení jsou zachyceny v Tabulce 20.

Tabulka 18 – Vyhodnocení potenciálního významu chráněných prostor

Potenciální význam											
Položka	CHP ₁	CHP ₂	CHP ₃	CHP ₄	CHP ₅	CHP ₆	CHP ₇	CHP ₈	CHP ₉	CHP ₁₀	CHP ₁₁
1.1	3	3	15	3	3	6	1	1	3	6	3
1.2	9	0	11	0	4	0	0	4	4	4	0
1.3	0	0	16	0	0	0	0	0	0	0	0
2.1	5	3	9	1	1	5	1	1	5	9	1
2.2	5	8	11	5	5	8	5	5	8	13	5
2.3	8	10	15	8	8	10	8	8	13	10	8
Celkem	30 b.	24 b.	77 b.	17 b.	21 b.	29 b.	15 b.	19 b.	33 b.	42 b.	17 b.
Výsledek v %	36,6 %	29,3 %	93,9 %	20,7 %	25,6 %	35,4 %	18,3 %	23,2 %	40,2 %	51,2 %	20,7 %

(zdroj: vlastní)

Tabulka 19 – Vyhodnocení potenciálního rizika chráněných prostor

Položka	CHP ₁	CHP ₂	CHP ₃	CHP ₄	CHP ₅	CHP ₆	CHP ₇	CHP ₈	CHP ₉	CHP ₁₀	CHP ₁₁
1.1	12	2	12	2	2	2	2	7	2	2	2
1.2	5	10	5	10	10	10	10	12	5	5	10
1.3	7	0	2	0	4	3	7	0	2	2	0
2.1	5	5	7	5	5	5	5	5	5	5	5
2.2	7	13	2	13	10	13	13	13	7	2	13
2.3	3	7	1	7	3	3	7	3	3	0	7
2.4	5	1	3	1	8	8	8	8	8	0	1
2.5	3	3	7	3	3	12	7	12	3	0	3
2.6	12	0	7	0	3	12	0	12	3	0	0
2.7	7	0	2	0	2	15	0	12	1	0	0
2.8	0	0	1	0	0	0	0	0	0	0	0

(zdroj: vlastní)

Tabulka 19 – Vyhodnocení potenciálního rizika chráněných prostor (pokračování)

Položka	CHP ₁	CHP ₂	CHP ₃	CHP ₄	CHP ₅	CHP ₆	CHP ₇	CHP ₈	CHP ₉	CHP ₁₀	CHP ₁₁
3.1	12	14	12	14	12	14	14	12	12	12	14
3.2	14	14	3	3	3	3	3	14	3	3	3
3.3	13	13	5	13	13	13	13	13	3	3	13
3.4	7	7	0	7	7	7	7	7	7	0	7
3.5	8	10	1	10	10	3	10	10	8	1	10
3.6	3	15	1	10	15	13	15	15	10	1	10
3.7	8	10	1	8	8	10	10	0	8	1	8
Celkem	131 b.	124 b.	72 b.	106 b.	118 b.	146 b.	131 b.	155 b.	90 b.	37 b.	106 b.
Výsledek v %	60,4 %	57,1 %	33,2 %	48,9 %	54,4 %	67,3 %	60,4 %	71,4 %	41,5 %	17,0 %	48,9 %

(zdroj: vlastní)

Tabulka 20 – Určení míry zranitelnosti chráněných prostor

Chráněný prostor	Potenciální význam	Potenciální riziko	Úroveň zranitelnosti
CHP ₂	29,3 %	57,1 %	Nízká zranitelnost
CHP ₄ a CHP ₁₁	20,7 %	48,9 %	Nízká zranitelnost
CHP ₅	25,6 %	54,4 %	Nízká zranitelnost
CHP ₇	18,3 %	60,4 %	Nízká zranitelnost
CHP ₁	36,6 %	60,4 %	Střední zranitelnost
CHP ₃	93,9 %	33,2 %	Střední zranitelnost
CHP ₈	23,2 %	71,4 %	Střední zranitelnost
CHP ₉	40,2 %	41,5 %	Střední zranitelnost
CHP ₁₀	51,2 %	17,0 %	Střední zranitelnost
CHP ₆	35,4 %	67,3 %	Vysoká zranitelnost

(zdroj: vlastní)

Hodnocení zranitelnosti chráněných prostor ukázalo, že jeden posuzovaný prostor je vysoce zranitelný, pět středně zranitelných a pět málo zranitelných. Výsledky naznačují, že současná úroveň zranitelnosti objektů v areálu umožňuje existenci vzniku ohrožení, a proto by měla být zvážena vhodná opatření ke zvýšení ochrany chráněných prostor vyhodnocených se střední a vysokou zranitelností. U málo zranitelných prostor lze stávající opatření považovat za dostatečná, ale i v těchto oblastech je doporučeno provádět periodické kontroly, aby se předešlo možným budoucím ohrožením.

7 NÁVRH OPATŘENÍ ZVYŠUJÍCÍCH CELKOVOU ÚROVEŇ OCHRANY OBJEKTU

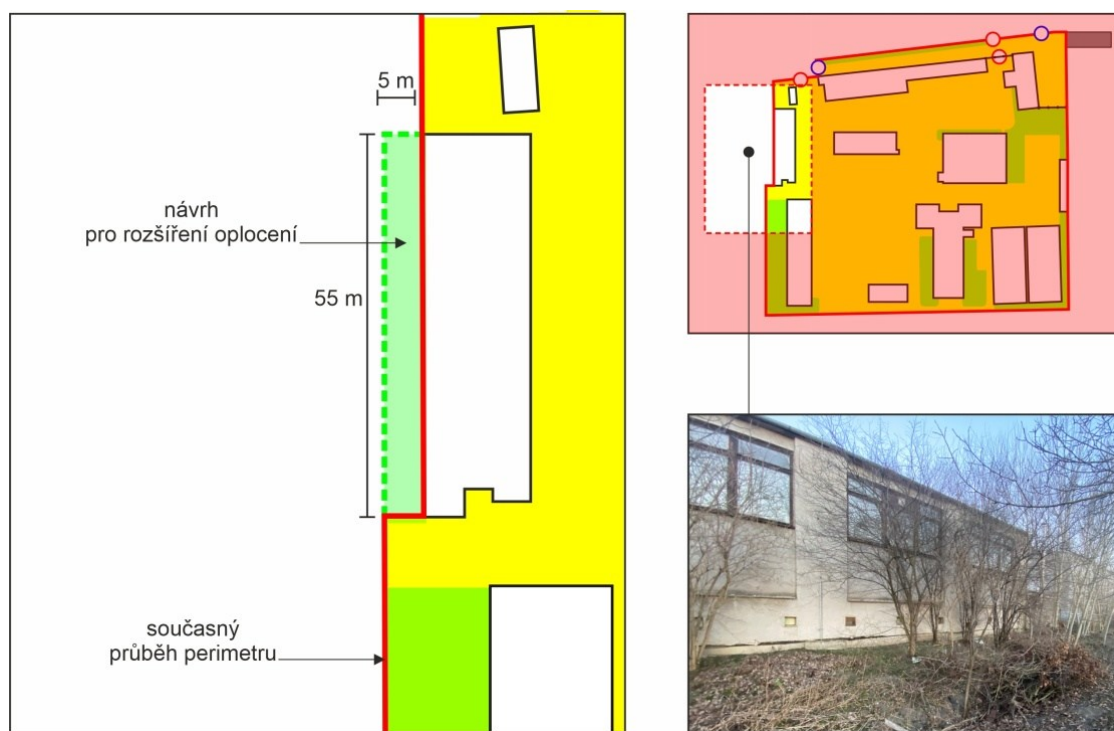
Na základě výsledků analýzy a hodnocení bezpečnostních rizik v rámci zkoumaného objektu lze přistoupit k návrhu bezpečnostních opatření, která si budou klást za cíl posílit ochranu objektů, které byly vyhodnoceny s vysokou nebo střední úrovní zranitelnosti. Při implementaci níže uvedených opatření dojde ke snížení pravděpodobnosti výskytu rizika nebo ke zvýšení odolnosti objektu vůči identifikovaným hrozbám, což posílí celkovou úroveň zabezpečení objektu. Popis doporučení a bezpečnostních opatření je obsažen v následujících bodech.

1. Zavedení preventivní údržby. Analýza současného stavu zabezpečení objektu odhalila, že mnoho technických nedostatků má společnou kořenovou příčinu – absenci systematické údržby. V současnosti řeší podnik otázky údržby zabezpečovacích prvků formou reaktivní údržby, kdy k opravám a odstranění závad dochází až po jejich vzniku. Kontrola stavu perimetru a plášťů budov je sice v kompetenci pracovníků SBS, avšak tato činnost není prováděna dle žádného harmonogramu, plánu či definovaného rozsahu kontrol. Tento přístup zvyšuje pravděpodobnost výskytu rizika, jako je opožděná detekce technických závad, nebo potenciálního neoprávněného vniknutí do chráněného prostoru. Z tohoto důvodu doporučuji zavedení systematického programu preventivní údržby, který bude zahrnovat:

- Vypracování harmonogramu pravidelných kontrol prvků v rámci zabezpečovacího systému podniku (mechanické bariéry, kamery, detektory pohybu, sirény apod.).
- Zajištění specializovaného pracovníka, který bude odpovědný za pravidelnou kontrolu a údržbu těchto komponent.
- Vedení dokumentace o provedených kontrolách a zjištěných závadách, což umožní sledovat dlouhodobé trendy a plánovat potřebné investice do modernizace zabezpečení.
- Zavedení softwarového řešení pro správu údržby, které umožní efektivní evidenci, plánování a vyhodnocování údržbářských zásahů.

Implementací preventivní údržby lze předejít technickým selháním, zvýšit provozní spolehlivost prvků zabezpečovacího systému a snížit riziko neoprávněného vniknutí do chráněného prostoru.

2. Zamezení přístupu k plášťům budov. Přístup k plášti budovy rozšiřuje pachatele jeho možnosti napadení objektu, a proto je zapotřebí přístup k plášti eliminovat. Součástí perimetru jsou pláště dvou budov. První plášť navrhuji opatřit následovně. Za hranicí areálu se nachází plocha o velikosti přibližně 275 m², která je ve vlastnictví provozovatele (majitele) areálu. Navrhuji provést oplocení dané plochy (viz. Obrázek 10) vhodným typem oplocení (například drátěný plot s ostnatým drátem) o výšce alespoň 1,8 m. Oplocení zamezí přímému přístupu pachatele k plášti budovy, což povede ke snížení pravděpodobnosti vzniku ohrožení, jako jsou sprejování graffiti, poškození fasády apod. Druhou budovu, jejíž plášť je součástí perimetru, navrhuji zabezpečit v úrovni střechy budovy (2,1 m ve výšce) vhodnou mechanickou bariérou (například žiletkovým drátem).



Obrázek 10 – Návrh na rozšíření perimetru

(zdroj: vlastní)

nebo výměně nelze přistoupit, bylo by vhodné tyto vstupy zajistit kamerovým systémem či jiným vhodným detekčním zařízením. Mimo zmíněné nedostatky doporučuji provádět pravidelnou kontrolu uzamykání vstupů do objektů, které nebyly řádně uzamčeny a byly vyhodnoceny se střední až vysokou zranitelností, popř. tyto vstupy zajistit kamerovým systémem.

5. Zamezení přístupu na střechu budov. Na plášti jedné z budov je instalován žebřík, který umožňuje přístup na střechu, na které se nacházejí střešní světlíky. Pro zamezení neoprávněného přístupu na střechu, popř. dovnitř budovy, navrhuji stávající žebřík doplnit o uzamykatelná bezpečnostní dvířka, která budou vyrobena z odolného materiálu. Konstrukce dvířek bude navržena tak, aby byla kompatibilní s typem pevného žebříku, který je instalován na budově. Dvířka budou vybavena zámkovým mechanismem, který zajistí ochranu před vniknutím nepovolaných osob. Zavedením tohoto opatření se sníží riziko neoprávněného vstupu na střechu popř. dovnitř budovy, což přispěje k ochraně majetku i bezpečnosti osob. Obrázek 12 představuje současný stav žebříku. Obrázek 13 a Obrázek 14 představují vhodnou variantu řešení.



Obrázek 12 – Současný stav žebříku

(zdroj: vlastní)



Obrázek 13 – Žebřík zabezpečený bezpečnostními dvířky a ostnatým drátem



Obrázek 14 – Žebřík zabezpečený bezpečnostními dvířky a pletivem

(zdroj: vlastní)

6. Posílení požární ochrany v objektu. Současná úroveň požární ochrany v objektu není dostatečná, jelikož mnoho vnitřních prostor, ve kterých by mohlo dojít ke vzniku požárního nebezpečí (sklad hořlavých kapalin, kanceláře, dílna) nejsou nepřetržitě monitorovány. Detekce požáru a vyhlášení poplachu je zajišťována vzdáleně operátorem dohledového centra prostřednictvím kamerového systému, který nepokrývá tyto vnitřní prostory. Vznik požáru v těchto místech by mohl mít katastrofální dopad na životy a zdraví lidí, životní prostředí a majetek podniku. Z tohoto důvodu doporučuji opatřit prostory, ve kterých dochází k manipulaci nebo skladování hořlavých kapalin, vhodným zařízením pro detekci kouře nebo požáru, jako je například autonomní požární hlásič, popř. rozšířit kamerový systém o tyto vnitřní prostory. Autonomní požární hlásiče je vhodné instalovat do prostor kanceláří.

8 SHRNUTÍ

Předmětem zkoumání byla úroveň zabezpečení areálu stavební společnosti, včetně zabezpečení budov, situovaných uvnitř tohoto areálu, které jsou ve správě majitele. Bezpečnostní prostředí podniku vykazuje rostoucí trend majetkové kriminality na území obce, ve které je podnik situován. Z tohoto důvodu je na místě položit otázku, zdali je podnik připraven na potenciální MU, a jestli jsou implementovaná opatření vhodná pro efektivní redukci nebo eliminaci bezpečnostních rizik. Analýza současného stavu zabezpečení odhalila, že zkoumaný objekt vykazuje několik zranitelných oblastí, zejména v rámci plášťové ochrany a technického zabezpečení prostorové ochrany. Vzhledem k tomu, že více než polovina budov v areálu (šest z jedenácti) byla vyhodnocena s vysokou a střední mírou zranitelnosti byl objekt vyhodnocen jako neadekvátně zabezpečený vůči identifikovaným hrozbám. Z tohoto důvodu jsem přistoupil k návrhu bezpečnostních opatření se zaměřením na identifikované hrozby a zranitelné oblasti. Navržená opatření mají za cíl posílit celkovou úroveň ochrany objektu. Implementace opatření je v kompetenci vedení podniku, které by mělo doporučení zvážit a rozhodnout o jejich realizaci.

Při zpracování této práce se jevilo problematické stanovit, kdy je úroveň zabezpečení dostačující a kdy ne, neboť definice dostatečné ochrany může být vysoce subjektivní a liší se podle specifických podmínek a aktuálních hrozeb. Obzvláště u objektu, který nevykazuje požadavky na minimální úroveň ochrany z žádného právního předpisu, technických norem ani smluvních závazků.

Další výzvou byla dynamika rizik, která se mění v průběhu času. Bezpečnostní opatření, která byla efektivní před několika lety, mohou být dnes již zastaralá, protože se hrozby vyvíjejí a adaptují. S tímto vývojem se pojí i problém neustálé potřeby aktualizace a modernizace systémů, které se stávají zranitelnými vůči novým metodám útoků.

V neposlední řadě je zde problém neochoty organizací investovat do bezpečnostních opatření, dokud nedojde k mimořádné události nebo bezpečnostnímu incidentu. V mnoha případech je zajištění bezpečnosti podceňováno, dokud není pozdě a podnik čelí skutečné hrozbě. Tato reakční mentalita může být nebezpečná, protože proaktivní investice do prevence a modernizace zabezpečovacích systémů jsou nezbytné pro dlouhodobou stabilitu a ochranu.

ZÁVĚR

Tato diplomová práce se zaměřila na problematiku zabezpečení objektů vůči relevantním hrozbám. V teoretické části byla představena příslušná terminologie a výběr právních předpisů, jejichž znalost umožní pochopit komplexnost problematiky, jak se požadavky na zabezpečení mohou lišit v závislosti na způsobu užívání nebo typu objektu. Dále byly objasněny principy technických a organizačních prostředků ochrany objektu, jež tvoří nedílnou součást fyzické bezpečnosti.

Praktická část se zaměřila na analýzu vnitřního a vnějšího bezpečnostního prostředí zkoumaného objektu, jímž byl areál stavební společnosti, včetně budov uvnitř areálu, spravovaných majitelem. Analýza poukázala na rostoucí trend majetkové trestné činnosti na území obce, ve které je podnik situován. Tento pesimistický fakt umocňuje potřebu přijetí adekvátních opatření pro zajištění připravenosti na potenciální hrozby. Proto, aby bylo zřejmé, které hrozby jsou relevantní vzhledem ke zkoumanému objektu, byla definována aktiva podniku a možné zdroje hrozeb působících proti těmto chráněným aktivům. Jednotlivé rizikové scénáře byly ohodnoceny z hlediska pravděpodobnosti výskytu a možných dopadů, proto, aby byla jednoznačně stanovena jejich úroveň rizika. Rizika vyhodnocená s nepřijatelnou nebo podmíněně přijatelnou mírou rizika byla předmětem uvažování při návrhu bezpečnostních opatření. Dále byla vyhodnocena zranitelnost chráněných prostorů, která odhalila, že polovina budov v objektu je středně zranitelná a jedna budova vysoce zranitelná. Na základě zjištění byla současná úroveň zabezpečení objektu vyhodnocena jako nedostatečná. Implementace navržených opatření a doporučení povede ke zvýšení úrovně ochrany objektu před identifikovanými hrozbami.

Práce poukázala na konkrétní nedostatky a nabídla návrhy na jejich odstranění. Výsledky této práce a budou poskytnuty příslušníkům soukromé bezpečnostní služby, kteří se zabývají ochranou zkoumaného objektu. Vytyčené cíle diplomové práce byly splněny.

SEZNAM POUŽITÉ LITERATURY

BEZPEČNOSTNÍ AGENTURY, 2020. *Jaké pravomoci a oprávnění mají pracovníci bezpečnostních služeb?* Online. Dostupné z: <https://www.securityagencies.cz/clanek/jake-pravomoci-a-opravneni-maji-pracovnici-bezpecnostnich-sluzeb>. [cit. 2025-04-01].

BURDA, Karel, 2017. *Základy elektronických zabezpečovacích systémů*. Brno: Akademické nakladatelství CERM. ISBN 978-80-7204-967-7.

ČESKO. Nařízení vlády č. 462 ze dne 22. listopadu 2000 k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb. krizový zákon. In: *Sbírka zákonů České republiky*. ISSN 1211-1244.

ČESKO. Zákon č. 133 ze dne 17. prosince 1985 o požární ochraně. In: *Sbírka zákonů České republiky*. ISSN 1211-1244.

ČESKO. Zákon č. 20 ze dne 30. března 1987 o státní památkové péči. In: *Sbírka zákonů České republiky*. ISSN 1211-1244.

ČESKO. Zákon č. 222 ze dne 14. září 1999 o zajišťování obrany České republiky. In: *Sbírka zákonů České republiky*. ISSN 1211-1244.

ČESKO. Zákon č. 224 ze dne 12. srpna 2015 o prevenci závažných havárií. In: *Sbírka zákonů České republiky*. ISSN 1211-1244.

ČESKO. Zákon č. 226 ze dne 21. dubna 2006 zákoník práce. In: *Sbírka zákonů České republiky*. ISSN 1211-1244.

ČESKO. Zákon č. 240 ze dne 28. června 2000 krizový zákon. In: *Sbírka zákonů České republiky*. ISSN 1211-1244.

ČESKO. Zákon č. 262 ze dne 21. dubna 2006 zákoník práce. In: *Sbírka zákonů České republiky*. ISSN 1211-1244.

ČESKO. Zákon č. 263 ze dne 14. července 2016 atomový zákon. In: *Sbírka zákonů České republiky*. ISSN 1211-1244.

ČESKO. Zákon č. 273 ze dne 17. července 2008 o Policii České republiky. In: *Sbírka zákonů České republiky*. ISSN 1211-1244.

ČESKO. Zákon č. 40 ze dne 8. ledna 2009 trestní zákoník. In: *Sbírka zákonů České republiky*. ISSN 1211-1244.

ČESKO. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. ISSN 1211-1244.

ČESKO. Zákon č. 49 ze dne 6. března 1997 o civilním letectví. In: *Sbírka zákonů České republiky*. ISSN 1211-1244.

ČSN 60839-11-1, 2014. *Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN 62676-1-1, 2014. *Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 1-1: Systémové požadavky – Obecně*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN 14383-1, 2007. *Prevence kriminality – Plánování městské výstavby a navrhování budov – Část 1: Definice specifických termínů*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN 15602, 2022. *Soukromé bezpečnostní služby – Terminologie*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN 50131-1 ed. 2, 2007. *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN P CEN/TS 14383-3, 2006. *Prevence kriminality – Plánování městské výstavby a navrhování budov – Část 3: Obydlí*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

DRONPRO, 2024. *Co je to Bezpilotní letecký prostředek - UAV?* Online. Dostupné z: <https://dronpro.cz/co-je-to-bezpilotni-letecky-prostredek-uav>. [cit. 2025-03-25].

ESKENAZI, Brenda; WARNER, Marcella; BRAMBILLA, Paolo; SIGNORINI, Stefano; AMES, Jennifer et al., 2018. *The Seveso accident: A look at 40 years of health research and beyond*. Online. Environment International. Vol 121, s. 71-84. ISSN: 0160-4120. Dostupné z: <https://doi.org/10.1016/j.envint.2018.08.051>. [cit. 2025-03-25].

FOJTÍK, Jakub, 2024. *Řešení radiační události z pohledu Hasičského záchranného sboru České republiky*. Diplomová práce. Uherské Hradiště: Univerzita Tomáše Bati ve Zlíně.

GIT SICHERHEIT, 2011. *Thermal Imaging to Spot Criminals*. Online. Dostupné z: <https://git-sicherheit.de/en/topstories/thermal-imaging-to-spot-criminals>. [cit. 2025-03-26].

Hanwha Vision Europe, 2024. *Multi-directional AI cameras offer cost-effective and intelligent surveillance coverage*. Online. Dostupné z: <https://hanwhavision.eu/multi-directional-ai-cameras-offer-cost-effective-and-intelligent-surveillance-coverage/>. [cit. 2025-03-31].

HOFREITER, Ladislav, 2015. *Manažment ochrany objektov*. Žilina: Žilinská univerzita v Žiline. ISBN 978-80-554-1164-4.

IVANKA, Ján, 2014. *Mechanické zábranné systémy*. 2. vydání. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 978-80-7454-427-9.

KHAIRALLAH, Michael, 2017. *Are Your Perimeters Secure*. Online. Security Design Solutions LLC. Dostupné z: <http://sds-web.net/are-your-perimeters-secure/>. [cit. 2025-03-25].

KHAIRALLAH, Michael, 2024. *Physical Security Assessment Handbook: An Insider's Guide to Securing a Business*. 2. vydání. CRC Press, Taylor & Francis Group. ISBN 978-1032790800.

LICHOROBIEC, Stanislav; HOLUBOVÁ, Věra a VESELÝ, Václav, 2010. *Pojmy bezpečnosti osob a majetku*. Online. Ostrava: Vysoká škola báňská - Technická univerzita Ostrava - Fakulta bezpečnostního inženýrství. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/TBOM_POJMY.pdf. [cit. 2025-03-25].

MACH, Vlastimil, 2015. *Testovanie prielomovej odolnosti mechanických zábranných prostriedkov*. In: 20. medzinárodná vedecká konferencia - Riešenie krízových situácií v špecifickom prostredí. Online. Žilina: Fakulta bezpečnostného inžinierstva Žilinskej univerzity v Žiline. ISBN 978-80-554-1024-1. Dostupné z: <https://www.fbi.uniza.sk/uploads/Dokumenty/weby/rks-archiv/2015/prispevky.html>. [cit. 2025-03-26].

MINISTERSTVO PRÁCE A SOCIÁLNÍCH VĚCÍ ČR, ©2025. *Strážný*. Online. Národní soustava povolání. Dostupné z: <https://nsp.cz/jednotka-prace/strazny>. [cit. 2025-03-31].

MINISTERSTVO VNITRA ČR, ©2025. *Ochrana kritické infrastruktury*. Online. Dostupné z: <https://mv.gov.cz/clanek/ochrana-kriticke-infrastruktury-ochrana-kriticke-infrastruktury.aspx>. [cit. 2025-03-25].

NAS, Selçuk, 2015. *The Definitions of Safety and Security*. Online. Journal of ETA Maritime Science. Vol. 3, s. 53-54. ISSN: 2148-9386. Dostupné z: <https://doi.org/10.5505/jems.2015.42713>. [cit. 2025-03-25].

NEJKAM, ©2023. *AHD vs. IP: Jakou technologii vybrat?* Online. Dostupné z: https://www.nejkam.cz/advisor/ahd-vs-ip-jakou-technologie-vybrat?srsId=AfmBOob_DByFzQ-O5uk5DQONxx1MmxchCJ-D_1dQPi6OpT2PXsp7Stp. [cit. 2025-03-25].

POLICIE ČR, ©2025. *Mapa kriminality*. Online. Dostupné z: <https://kriminalita.policie.gov.cz/>. [cit. 2025-03-26].

PORTÁL KRIZOVÉHO ŘÍZENÍ JIHOMORAVSKÉHO KRAJE, ©2023. *Nebezpečné látky*. Online. Dostupné z: <https://www.krizport.cz/ohrozeni/nebezpecne-latky>. [cit. 2025-03-26].

RENIERS, Gensarik; LANDUCCI, Gabriele a KHAKZAD, Nima, 2020. *What safety models and principles can be adapted and used in security science*. Online. Journal of Loss Prevention in the Process Industries. Vol. 64. ISSN: 0950-4230. Dostupné z: <https://doi.org/10.1016/j.jlp.2020.104068>. [cit. 2025-03-26].

SECURITAS ČR, 2020. *Jak správně vybrat kamerový systém?* Online. Dostupné z: <https://www.securitas.cz/novinky--blog/blog/jak-spravne-vybrat-kamerovy-system/>. [cit. 2025-03-25].

SPRINGER, Matthias, 2020. *Difference between safety and security*. Online. Hannover: TÜV NORD GROUP. Dostupné z: <https://www.tuev-nord.de/explore/en/explains/whats-the-difference-between-safety-and-security/>. [cit. 2025-03-25].

ŠČUREK, Radomír a JARKULIŠ, Vojtěch, 2021. *Studijní opora do předmětu: Metodologie fyzické bezpečnosti podniku*. Online. Ostrava: Vysoká škola báňská - Technická univerzita Ostrava - Fakulta bezpečnostního inženýrství. Dostupné z: <https://www.fbi.vsb.cz/060/cs/studium/studijni-materialy/>. [cit. 2025-03-25].

THORPE, James, 2020. *Can the pain of false alarms become a thing of the past?* Online. International Security Journal. Dostupné z: <https://internationalsecurityjournal.com/can-the-pain-of-false-alarms-become-a-thing-of-the-past/>. [cit. 2025-03-26].

TOMEK, Miroslav, 2018. *Studijní opora do předmětu: Bezpečnost a ochrana objektů a osob*. Uherské Hradiště: Univerzita Tomáše Bati ve Zlíně – Fakulta logistiky a krizového řízení.

TZB-info, 2017. *Drony jsou skvělou pomůckou v oblasti bezpečnosti*. Online. ISSN 1801-4399. Dostupné z: <https://www.tzb-info.cz/fm-sluzby/15523-drony-jsou-skvelou-pomuckou-v-oblasti-bezpecnosti>. [cit. 2025-03-26].

TZB-info, 2017. *Přístupové systémy*. Online. ISSN 1801-4399. Dostupné z: <https://www.tzb-info.cz/pristupove-systemy>. [cit. 2025-03-26].

UHLÁŘ, Jan, 2005. *Technická ochrana objektů II. díl: Elektrické zabezpečovací systémy II*. Praha: Policejní akademie České republiky. ISBN 80-725-1189-0.

ZEPCAM, 2023. *The Impact of AI on Bodycams and Video Surveillance*. Online. Dostupné z: <https://zepcam.com/the-impact-of-ai-on-bodycams-and-video-surveillance/>. [cit. 2025-03-31].

SEZNAM OBRÁZKŮ

Obrázek 1 – Postup při zpracování praktické části diplomové práce	13
Obrázek 2 – Analogie bezpečnostních rizik	16
Obrázek 3 – Pozice MZS v rámci zabezpečení objektu.....	24
Obrázek 4 – Schéma PZTS	28
Obrázek 5 – Schéma ESKV	29
Obrázek 6 – Schéma DVS	32
Obrázek 7 – Ukázka funkcionality termovizní kamery za tmy	35
Obrázek 8 – Schéma vybraných pracovníků SBS	39
Obrázek 9 – Schéma vybraných pracovníků SBS	44
Obrázek 10 – Návrh na rozšíření perimetru	79
Obrázek 11 – Návrh na instalaci oplocení	80
Obrázek 12 – Současný stav žebříku	81
Obrázek 13 – Žebřík zabezpečený bezpečnostními dvířky a ostnatým drátem	82
Obrázek 14 – Žebřík zabezpečený bezpečnostními dvířky a pletivem.....	82

SEZNAM TABULEK

Tabulka 1 – Výběr subjektů, jejichž potřeba zabezpečení pramení ze zákona.....	19
Tabulka 2 – Klasifikace úrovně ochrany ESKV	30
Tabulka 3 – Detekce narušení pro daný stupeň zabezpečení DVS.....	34
Tabulka 4 – Kritéria pro výběr bezpečnostní kamery.....	34
Tabulka 5 – Vývoj trendu majetkové trestné činnosti na území obce zkoumaného objektu	45
Tabulka 6 – Informace o NL v objektu.....	46
Tabulka 7 – Prvky perimetru zkoumaného objektu.....	53
Tabulka 8 – Kontrolní seznam současného stavu zabezpečení perimetru objektu.....	56
Tabulka 9 – Vyhodnocení kontrolního seznamu současného stavu zabezpečení perimetru	57
Tabulka 10 – Kontrolní seznam současného stavu zabezpečení plášťů budov	58
Tabulka 11 – Vyhodnocení kontrolního seznamu současného stavu zabezpečení plášťů budov	59
Tabulka 12 – Identifikace potenciálních hrozeb	66
Tabulka 13 – Kritéria pro určení pravděpodobnosti vzniku rizika	68
Tabulka 14 – Kritéria pro určení následků při působení rizika	68
Tabulka 15 – Kritéria pro určení míry rizika	69
Tabulka 16 – Analýza a hodnocení bezpečnostních rizik.....	70
Tabulka 17 – Matice rizik pro určení zranitelnosti chráněných prostor	73
Tabulka 18 – Vyhodnocení potenciálního významu chráněných prostor.....	74
Tabulka 19 – Vyhodnocení potenciálního rizika chráněných prostor	75
Tabulka 20 – Určení míry zranitelnosti chráněných prostor	77

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

A_x	Aktivum
C_N	Součet celkového počtu otázek
ČR	Česká republika
DVS	Dohledový videosystém
ESKV	Elektronický systém kontroly vstupu
h	Výška
CHP_x	Chráněný prostor
IP	Internet Protocol
MU	Mimořádná událost
MZP	Mechanický zábranný prostředek
MZS	Mechanický zábranný systém
NL	Nebezpečná látka
NP	Nadzemní podlaží
PIN	Personal Identification Number
PP	Podzemní podlaží
P_x	Zdroj hrozby
PZTS	Poplachový zabezpečovací a tísňový systém
Sb.	Sbírka zákonů a mezinárodních smluv
SBS	Soukromá bezpečnostní služba
sk.	Skupina
S_{KO}	Součet kladný odpovědí
S_{ZO}	Součet záporných odpovědí
t_1	Čas zahájení útoku na překážku
t_2	Čas konečného překonání překážky
Δt	Časový interval potřebný k překonání překážky

SEZNAM PŘÍLOH

Příloha P I: Hodnocení potenciálního významu pro určení zranitelnosti chráněných prostor

Příloha P II: Hodnocení potenciálních rizik pro určení zranitelnosti chráněných prostor

PŘÍLOHA P I: HODNOCENÍ POTENCIÁLNÍHO VÝZNAMU OBJEKTU PRO URČENÍ ZRANITELNOSTI

Skupina	Položka	Parametr	Varianty výstupu	Bodové ohodnocení
Objektivní význam majetku	1.1	Tržní hodnota předmětů	Více než 1 milion Kč	15
			Do 1 milionu Kč	12
			Do 500 000 Kč	6
			Do 250 000 Kč	3
			Zanedbatelná	1
	1.2	Typ dokumentů	Úřední dokumenty vyhrazené	14
			Úřední dokumenty obchodního charakteru, důvěrné dokumenty	11
			Soukromé, dokumenty důvěrného charakteru	9
			Běžné dokumenty	4
	1.3	Nenahraditelné dokumenty	Sbírky	16
			Současná přítomnost několika z uvedených hodnot	16
			Umělecké předměty, historické archivy	13
			Vzácný, případně starožitný nábytek	13
			Prototypy	12
			Nenachází se	0
Subjektivní význam majetku	2.1	Odhadnutá hodnota předmětů nacházejících se v objektu	Vysoká	9
			Střední	5
			Nulová/nízká	1

(pokračování Přílohy P I)

Skupina	Položka	Parametr	Varianty výstupu	Bodové ohodnocení
	2.2	Vážnost vloupání, při němž nedojde ke krádeži nebo jakékoli další újmě	Vždy vysoká	13
			Vysoká je-li někdo přítomen	11
			Vysoká není-li někdo přítomen	8
			Střední v každém případě	5
	2.3	Nejvíce obávaný způsob napadení	Vandalismus	8
			Krádež	10
			Fyzické násilí	13
			Krádež s fyzickým násilím	15

(zdroj: vlastní zpracování dle ČSN P CEN/TS 14383-3, 2006)

PŘÍLOHA P II: HODNOCENÍ POTENCIÁLNÍCH RIZIK OBJEKTU PRO URČENÍ ZRANITELNOSTI

Skupina	Položka	Parametr	Varianty výstupu	Bodové ohodnocení
Lokalita	1.1	Přístupové komunikace	Přístup k objektu z více veřejných komunikací	15
			Přístup k objektu jednou veřejnou komunikací	12
			Přístup k objektu soukromou komunikací	7
			Přístup k objektu přes kontrolovaný vstup	2
	1.2	Užívání objektu	Trvale opuštěný	12
			Často opuštěný	10
			Osoby často přítomné	5
			Osoby trvale přítomné	1
	1.3	Vysoká úroveň hluku	Ano	9
			Ne	0
Fyzické charakteristiky	2.1	Vzhled působící na zvýšení zranitelnosti	Nádherný	11
			Bohatý	8
			Skromný	5
	2.2	Úroveň obecné údržby vstupů (brány, dveře, okna)	Špatná	13
			Průměrná	7
			Dobrá	2
	2.3	Konstrukce	Lehká, montovaná	10
			Lehká, stabilní	7
			Plná cihla	3
			Beton, železobeton	1

(pokračování Přílohy P II)

Skupina	Položka	Parametr	Varianty výstupu	Bodové ohodnocení
	2.4	Střecha	Sedlová, lehce přístupná, průlezná střešní okna	10
			Plochá, lehce přístupná	8
			Sedlová, lehce přístupná, neprůlezná střešní okna	5
			Plochá, těžce přístupná	3
			Sedlová, těžce přístupná, průlezná střešní okna	2
			Sedlová, bez oken	1
	2.5	Dveře venkovní	Nízká odolnost	12
			Střední odolnost	7
			Vysoká odolnost	3
	2.6	Dveře vnitřní	Nízká odolnost	12
			Střední odolnost	7
			Vysoká odolnost	3
	2.7	Okna	Lehce dostupné, nezabezpečené	15
			Lehce dostupné, málo odolné	12
			Lehce dostupné, zabezpečené, dostatečné odolné	7
			Těžko dostupné, nezabezpečené	2
			Těžko dostupné, zabezpečené	1

(pokračování Přílohy P II)

Skupina	Položka	Parametr	Varianty výstupu	Bodové ohodnocení
Forma zabezpečení	2.8	Sklep, suterén nebo přiléhající garáž	Průlezné nezabezpečené otvory	10
			Průlezné zabezpečené otvory, málo odolné	7
			Průlezné zabezpečené otvory, dostatečně odolné	1
			Bez průlezných otvorů	0
	3.1	Osvětlení přístupů	Žádné	14
			Pouze pouliční osvětlení	12
			Bezpečnostní osvětlení na fasádách	8
			Bezpečnostní osvětlení na všech přístupech	4
	3.2	Kontrola vstupu	Neexistuje	14
			Existuje	3
	3.3	Poplachové zařízení	Žádné	13
			Necertifikovaný poplachový systém bez dálkového přenosu	11
			Necertifikovaný poplachový systém s dálkovým přenosem	5
			Certifikované poplachové zařízení	3
	3.4	Trezor pro cennosti	Ne	7
			Ano	0

(pokračování Přílohy P II)

Skupina	Položka	Parametr	Varianty výstupu	Bodové ohodnocení
	3.5	Ochrana pláště budovy	Neexistuje	15
			Vstupy uzamykatelné, nemonitorované	10
			Vstupy uzamykatelné, monitorované	8
			Bezpečnostní osvětlení na plášti	7
			Kamerový systém na plášti	3
			Detektory otevření (prolomení) dveří	2
			Detektory otevření (rozbití) oken	2
			Kombinace	1
	3.6	Vnitřní (prostorová) ochrana budovy	Neexistuje	15
			Pouze MZP	10
			Kamerový systém	3
			ESKV	1
	3.7	Předmětová ochrana	Žádná, přestože je potřebná	10
			Minimální (uzamykatelná skříň)	8
			Bezpečnostní úschovný objekt (trezor)	1

(zdroj: vlastní zpracování dle Hofreiter, 2015 a ČSN P CEN/TS 14383-3)