# Systém řízení bezpečnosti informací vybraného subjektu

Bc. Kristýna Benešová

Diplomová práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva
akademický rok: 2018/2019

# ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Bc. Kristýna Benešová** |
| Osobní číslo: | **L17084** |
| Studijní program: | **N3953 Bezpečnost společnosti** |
| Studijní obor: | **Bezpečnost společnosti** |
| Forma studia: | **prezenční** |

Téma práce: **Systém řízení bezpečnosti informací vybraného subjektu**

Zásady pro vypracování:

1. **Zpracujte literární rešerši vztahující se k dané problematice s důrazem na monografie a analytické materiály.**
2. **Proveďte analýzu úrovně zabezpečení zvolené oblasti systému řízení bezpečnosti informací vybraného subjektu.**
3. **Na základě předchozí analýzy navrhněte případná opatření ke zkvalitnění stávajícího stavu.**
4. **Sumarizujte získané výstupy diplomové práce.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

**[1] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-05-7.**

**[2] IVANKA, Ján. Systemizace bezpečnostního průmyslu. Vyd. 5. Zlín: Univerzita Tomáše Bati ve Zlíně, 2014. ISBN 978-80-7454-410-1.**

**[3] VALOUCH, Jan. Projektování integrovaných systémů. Zlín: UTB, 2013. ISBN 978-80-7454-296-1.**

**[4] VALOUCH, Jan. Projektování bezpečnostních systémů. Zlín: UTB, 2012. ISBN 978-80-7454-230-5.**

**Další odborná literatura dle doporučení vedoucího diplomové práce.**

Vedoucí diplomové práce: **Ing. Petr Svoboda**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **30. listopadu 2018**

Termín odevzdání diplomové práce: **15. května 2019**

V Uherském Hradišti dne 30. listopadu 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení
L.S.
③

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

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

# PROHLÁŠENÍ AUTORA
# DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- 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 UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu 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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 15.5.2019

Jméno a příjmení studenta: Bc. Michaela Zelená

.....
podpis studenta

## ABSTRAKT

Diplomová práce je věnována problematice systému řízení bezpečnosti informací ve vybraném objektu. Cílem práce je analýza stávajícího stavu bezpečnosti informací z hlediska fyzické bezpečnosti ve vybraném objektu. Je rozdělena do dvou částí, teoretickou s praktickou. Teoretická část je zaměřena na rešerši problematiky, což poskytuje teoretický základ nezbytný pro pochopení systému řízení bezpečnosti informací. Praktická část obsahuje charakteristiku vybraného objektu, zhodnocení stávajícího stavu rizik s následnou analýzou s využitím analytických metod KARS a SWOT. Dále obsahuje projekt realizace zabezpečení vybraného objektu, jeho součástí je metoda RIPRAN a v neposlední řadě obsahuje i návrhové opatření, které povede ke zlepšení stávajícího stavu zabezpečení ve vybraném objektu.



Klíčová slova: bezpečnost, detektor, ISMS, informace, systém



## ABSTRACT

The thesis is devoted to the issue of information security management system in the selected object. The aim of this work is to analyze the current state of information security in terms of physical security in the selected object. It is divided into two parts, theoretical and practical. The theoretical part is focused on research of the issue, which provides the theoretical basis necessary for understanding the information security management system. The practical part contains the characteristics of the selected object, the assessment of the current state of risks with subsequent analysis using analytical methods KARS and SWOT. It also includes the project of realization of the security of the selected object, its part is the RIPRAN method and it also includes a design measure that will lead to the improvement of the current security status in the selected object.



Keywords: Information, ISMS, Detector, Security, System

Ráda bych poděkovala vedoucímu diplomové práce panu Ing. Petru Svobodovi., který mi poskytl velké množství informací, cenných rad a zejména odborné vedení. Dále děkuji vedení a všem zaměstnancům daného objektu za poskytnutí informací, odborných konzultací a cenných materiálů.

V neposlední řadě bych ráda poděkovala také své rodině a přátelům za podporu během studia.

*„ Bezpečnost je tak účinná, jak je silný její nejslabší článek“*

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

# OBSAH

# ÚVOD

Žijeme v době, kdy se vyspělé národy vydávají na cestu ke znalostní společnosti. Probíhají změny v ekonomice, došlo k transformaci na ekonomiku znalostí. Přičemž se pozornost obrací k informačním systémům, informačním a komunikačním technologiím, jako významnému zdroji konkurenční výhody.

Položme si otázku, co znamená onen systém řízení bezpečnosti informací. Systém řízení informací není nic jiného než jedna z problémově orientovaných složek managementu, proto i úvahy o účelnosti tohoto systému a její ověřování patří mezi manažerské funkce.

Cílem diplomové práce je analýza stávajícího stavu bezpečnosti informací z hlediska fyzické bezpečnosti ve vybraném objektu. Vedlejším cílem práce je stanovení návrhových opatření, která povedou ke zlepšení stávajícího stavu. Tím dojde k posílení systému a lepší odolnosti objektu.

V teoretické části bude věnována pozornost především rešerši vztažných materiálů. Dále bude objasněn systém řízení bezpečnosti informací a jednotlivé oblasti. Přičemž důraz bude kladen na fyzickou bezpečnost. Pozornost bude věnována i normativnímu rámci, jakožto základnímu atributu dané problematiky.

V praktické části bude použito hned několik metod. V první řadě se bude jednat o metodu sběru dat a informací, řízené rozhovory s vedením vybraného objektu. Další metodou bude určení zdrojů ohrožení pomocí metod analýzy rizik. Prvotně bude provedena kvalitativní metoda s využitím jejich souvztažností (KARS). Vyplynulá rizika stanoví, jaký druh ochrany je nejvíce zranitelný. Pro podrobnější analýzu zranitelnosti druhů ochrany bude využita SWOT analýza, protože komplexně vyhodnotí všechny stránky fungování. Dalším krokem bude vytvoření samotného projektu realizování návrhových opatření. Bude představen sled činností doprovázející projekt, metoda RIPRAN, která vyhodnotí riziková místa projektu. Součástí návrhu projektu bude i ukázka controllingu a návrhová opatření s konkrétními komponenty, které zabezpečí vybraný objekt a zvýší tím jeho odolnost.

# I. TEORETICKÁ ČÁST

# 1 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Pro pochopení problematiky systému řízení bezpečnosti informací je důležité definovat, co je to bezpečnost informací – jedná se o ochranu důvěrnosti, integrity a dostupnosti informací, kromě toho, že může také zahrnovat další vlastnosti (autenticitu, odpovědnost, nepopiratelnost a spolehlivost). V souvislosti s bezpečností informací je důležité zmínit také bezpečnost organizace a bezpečnost IS/ICT. Nejvyšší kategorií je bezpečnost organizace. Cílem bezpečnosti informací je shrnout v sobě zásady bezpečné práce s informacemi všeho druhu i všech typů. [1]

Prakticky není možné, aby se jakákoliv firma obešla bez řízení bezpečnosti informací. Jedná se o nedílnou součást každodenního řízení organizace. Pro efektivní řízení bezpečnosti informací je potřebné se na tento prvek řízení pohlížet jako na ucelený systém řízení bezpečnosti informací. Systém řízení v sobě zahrnuje organizační strukturu, politiky, plánovací činnosti, odpovědnosti, mechanismy, postupy, procesy a zdroje. [1]

Systém řízení bezpečnosti informací, neboli ISMS (Information Security Management System), část celkového systému řízení organizace, je založen na posuzování rizikovosti činností které jsou zaměřeny na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací. ISMS je definován následujícími čtyřmi etapami:

- Ustanovení – cílem je upřesnit rozsah a hranice, kterých se řízení bezpečnosti týká, stanovit manažerská zadání a na základě ohodnocení rizik vybrat bezpečnostní opatření.
- Zavádění a provoz – systematické a účelné prosazení vybraných bezpečnostních opatření.
- Monitorování a přezkoumání – v této etapě je důležitá zpětná vazba a pravidelné sledování všech stránek systému řízení bezpečnosti informací.
- Údržba a zlepšení – poslední etapa slouží k realizaci možných zlepšení systému a to tak, že odstraníme slabiny a nedostatky, nebo pomocí soustavného zlepšování systému. [1]

## 1.1 Oblasti bezpečnosti informací

Soubor postupů pro řízení bezpečnosti informací je zachycen v normě ISO/IECM 27002:2005. Obsahuje tzv. nejlepší zkušenosti řízení bezpečnosti informací. Doporučení

normy obsahuje 133 bezpečnostních opatření, která jsou rozdělena do jedenácti oblastí, což je znázorněno na obrázku 1.


Obr. 1 Oblasti bezpečnosti informací. Zdroj:[1]

Jednotlivé oblasti:

- Bezpečnostní politika – jedná se o pravidla, směrnice a zvyklosti, které určují způsoby, pomocí kterých jsou v dané organizaci a jejích systémech řízena, chráněna a distribuována aktiva, včetně citlivých informací.
- Organizace bezpečnosti – definuje požadavky na organizaci bezpečnosti informací, je rozdělena na dva bloky: interní organizace a externí subjekty.
- Řízení aktiv – cílem je nalezení a udržování přiměřené ochrany aktiv, která jsou součástí ISMS.
- Bezpečnost z hlediska lidských zdrojů – jedná se o velmi důležitou oblast, sleduje životní cyklus pracovníků,
- Fyzická bezpečnost a bezpečnost prostředí – tvoří ho dvě související skupiny: zabezpečené oblasti (chrání prostředí organizace jako celek) a bezpečnost zařízení (opatření, která chrání jednotlivé prvky infrastruktury ICT).
- Řízení komunikací a řízení provozu – skládá se z celkem deseti skupin bezpečnostních opatření, které se věnují různým aspektům bezpečnostního provozu

IS/ICT, východiskem je stanovení rozumných provozních procesů, postupů, odpovědností a pravomocí.

- Řízení přístupu – základem je sledování požadavků na řízení přístupů a stanovení takové politiky, která se bude promítat do všech informačních systémů a aplikací.
- Akvizice, vývoj a údržba informačních systémů – zahrnuje bezpečnostní opatření, která jsou účelná při prosazování bezpečnosti související s rozvojem informačních systémů – zahrnuje různorodá bezpečnostní opatření.
- Zvládání bezpečnostních incidentů – oblast je rozdělena do dvou částí: první se soustředí na uživatelskou komunitu (ta je motivována k hlášení bezpečnostních událostí, slabin, popřípadě podezřelých situací), druhá je určena pro bezpečnostní odborníky (měla by postihnout zvládání bezpečnostních incidentů a upřesnit kroky k nápravě).
- Řízení kontinuity činností organizace – jedná se o postupy prevence a minimalizace škod plynoucích pro organizaci z havárií, živelných pohrom či jiných mimořádných událostí.
- Soulad s požadavky – organizace dokladuje naplnění požadavků vyplývajících z právních, smluvních a jiných závazků. [1]

Vzhledem k tomu, že diplomová práce se zaobírá problematikou fyzické bezpečnosti, jak bylo avizováno v úvodu, tak další kapitoly budou věnovány právě této problematice.

## 1.2 Normativní rámec

K problematice systému řízení bezpečnosti informací existuje celá řada norem, a to i z pohledu fyzické bezpečnosti. Nejdůležitější technická norma týkající se bezpečnosti informací obecně je International Organization for Standardization (dále jen „ISO“) 27000. Významnou normou je však i Česká technická norma ISO/IEC 27001, která poskytuje požadavky na ustanovení, implementaci, udržení a neustálé zlepšování systému řízení bezpečnosti informací. Práce se zaměřuje především na jednu část ISMS, a to na fyzickou bezpečnost k ní se vztahují následující normy. [2]

Elektromagnetickou kompatibilitu zahrnuje ČSN EN 50130-4 ed. 2 – obsahuje požadavky na odolnost komponentů požárních systémů, poplachových zabezpečovacích a tísňových systémů a systémů CCTV, kontroly vstupu a přivolání pomoci.

Poplachové systémy upravují následující normy:ČSN CLC/TS 50131-2-10 obsahuje detektory narušení (magnetické kontakty), ČSN CLC/TS 50131-2-11obsahuje detektory narušení ALDDR, ČSN EN 50131-2-2 obsahuje detektory narušení – pasivní infračervené detektory.

Poplachové zabezpečovací a tísňové systémy popisují následující normy: ČSN EN 50131-2-7-1 zahrnuje detektory narušení, a to detektory rozbití skla (akustické), ČSN EN 50131-2-7-2 obsahuje detektory narušení, a to detektory rozbití skla (pasivní), ČSN EN 50131-5-3 zahrnuje požadavky na zařízení využívající bezdrátové propojení (EZS), TNI 33 4591-2 obsahuje montáž PZTS.

Dohledových videosystémů se týká norma ČSN EN 62676-1-1, která vyjadřuje obecné systémové požadavky.

Poplachové systémy a EPS řeší norma TNI 33 4592 obsahující požadavky na přenos zpráv ze střežených objektů pomocí internet protokolu. [2]

Poplachové a elektronické bezpečnostní systémy jsou zachyceny v normách: ČSN EN 60839-11-1 obsahuje elektronické systémy kontroly vstupu – požadavky na systém a komponenty, ČSN EN 60839-11-31 mapuje základní specifikaci implementace IP interoperability na základě webových služeb.[2]

Problematiku dohledových a poplachových přijímacích centr řeší normy: ČSN EN 50518-1 ed. 2 obsahuje umístění a konstrukční požadavky, ČSN EN 50518-2 ed. 2 zahrnuje technické požadavky, ČSN EN 50518-3 ed. 2 obsahuje postupy a požadavky na provoz. [2]

# 2 OCHRANA A FYZICKÁ BEZPEČNOST OBJEKTU

Ochrana a bezpečnost objektů je složitou a v současném bezpečnostním prostředí obzvláště významnou oblastí. Potřeba chránit objekty vedla postupem času k vypracování celkem čtyř forem ochrany objektů. Právě ochrana objektů a fyzická bezpečnost jsou jednou z významných oblastí. Základním opatřením se zde jeví klasická ochrana, dále se pak jedná o režimovou, fyzickou a technickou ochranu. Je důležité si uvědomit, že pokud chceme vybudovat kvalitní zabezpečení, je nejlepším řešením pojmout zabezpečení objektu komplexně a neopomenout kombinaci jednotlivých druhů ochrany. [3]

## 2.1 Klasická ochrana

I přesto, že patří mezi nejstarší způsob ochrany objektů, je hodně rozšířená a používána jako základní forma ochrany objektu. Klasická ochrana je realizována pomocí přírodních překážek, staveb, mechanických zábranných systémů, které znemožňují odcizení nebo poškození objektů, jejich částí nebo cenných předmětů uvnitř objektů. [3]

**Mechanické zábranné systémy**

Jedná se o historicky nejstarší typ bezpečnostních systémů. Slouží jako základní prvek v oblasti ochrany majetku a osob. Prakticky každý bezpečnostní prvek lze překonat, proto hlavním úkolem MZS je především vytvořit pachateli překážku, jejíž překonání je pro něj z hlediska časové náročnosti, použitých prostředků a vynaložené energie neúnosné. Slouží obecně jako ochrana proti neoprávněnému vniknutí do střeženého prostoru, odcizení, znehodnocení nebo poškození chráněných aktiv ve střeženém prostoru, manipulaci s nebezpečnými látkami či předměty.

Mechanické zábranné systémy tedy musí být mechanicky odolné – což prvky charakterizuje a vzájemně odlišuje. Čas potřebný k překonání mechanické odolnosti je nazýván průlomovou odolností – určuje výslednou úroveň zabezpečení při použití daného prvku MZS. S ohledem na průlomovou odolnost jsou prvky členěny do několika bezpečnostních tříd – tím se ve výsledku liší jejich provedení, kvalita a cena. [4], [5], [6]

V současnosti bývá kombinována s ostatními druhy ochrany – vzájemně se doplňují, což je nejúčinnější a nejspolehlivější metoda zabezpečení objektu. Soudobý systém fyzické bezpečnosti zahrnuje režimová opatření, fyzickou ochranu a technickou ochranu.

## 2.2 Režimová opatření

Jedná se o organizačně - administrativní opatření a postupy, které vedou k zabezpečení správných funkcí ochranných systémů a jejich sladění s provozem chráněných objektů. Cílem je stanovit zásady, pravidla, oprávnění při pohybu zaměstnanců a dalších osob v prostorách subjektu, způsob nakládaní s důležitými aktivy a pravidla pro bezpečnostní kontrolu vnášeného a především vynášeného materiálu. Opatření by neměla omezovat pohyb osob v objektu, ale zároveň musí zajistit dostatečný stupeň bezpečnosti. Významnou roli hraje především systém kontroly vstupu. [7]

**Jsou rozlišována:**

- **Vnější režimová opatření** - týkají se vstupních a výstupních podmínek u chráněných objektů, konkrétně u kontroly vozidel a osob při vstupu a výstupu z chráněných prostorů.
- **Vnitřní režimová opatření** – týkají se pohybu uvnitř chráněného objektu (omezení pohybu vozidel a osob na určitém úseku chráněných prostor, monitoring materiálu a výrobků v objektu).

**Systémy kontroly vstupu**

Přístupové systémy, také nazývané jako systém kontroly vstupu, můžeme chápat jako soubor opatření pro vstup do hlídaného objektu pomocí jednotlivých opatření (systémová, fyzická, mechanická, nebo elektronická), avšak nejlepší je jejich kombinace. Mezi základní funkce patří identifikace, zpracování dat, ovládání přístupového místa, programovatelnost, stavová hlášení, komunikace, styk s uživatelem, napájení, samoochrana. [8], [9]

Přístupový bod

Jedná se o všechny prvky, které umožňují kontrolovaný přístup. Přístupový bod je tvořen především místem přístupu, rozhraním místa přístupu, snímačem místa přístupu a APAS (ovládací prvky přístupového místa). Struktura celého přístupového systému se skládá z jednoho nebo více přístupových bodů, hlavní řídící jednotky, napájení, komunikační sítě a řídícího obslužného pracoviště. [8], [9]

Identifikace

Objekt se může identifikovat třemi způsoby, a to něčím, co subjekt zná, popřípadě něčím, co má subjekt fyzicky u sebe, a v neposlední řadě sám sebou – typickými rysy.

Identifikační prvky jsou manuální, čipové, magnetické, optické, radiofrekvenční nebo biometrické. [8], [9]

Ovládaná zařízení

Ve většině případů se snažíme elektronicky řídit od dveří, přes turnikety, závory, rámy, až po detekční rámy. Aby mohlo dojít k odblokování takového řídícího mechanismu, jsou zapotřebí akční prvky, mezi něž patří elektromagnety, elektromagnetické otvírače, elektromechanické/elektromotorické zámky, elektromotorické/elektrohydraulické otvírače, motory, přídržné elektromagnety, vstupní/výstupní moduly. [8], [9]

Integrace SKV s jinými systémy

Systém kontroly vstupu je vhodné provázat i s jinými systémy, například s docházkovým systémem, poplachovým zabezpečovacím systémem, elektrickou požární signalizací, kamerovým systémem, IT systémy a v neposlední řadě se systémem měření a regulace. [8], [9]

Jedná se o soubor technických zařízení, konstrukčních a organizačních opatření, která zajišťují řízení a evidenci přístupu do zabezpečených prostor objektu, a to na základě přístupových práv. Jedná se o jeden z typů poplachových systémů. Cílem tohoto systému je především zvýšení úrovně bezpečnosti objektu. Základním přínosem, který systém kontroly vstupu přináší, je řízení přístupu z hlediska rozhodování o tom komu, kde a kdy bude umožněn vstup do zabezpečeného prostoru, s ohledem na minimalizování rizika vstupu nepovolaných osob.

Architektura systému kontroly vstupu vychází z jeho základních funkcí, které se vztahují k uživatelům systému, managementu systému, místům přístupu a k ostatním systémům. Systém kontroly vstupu se skládá z následujících prvků:

- místo přístupu,
- zařízení pro vyžádání odchodu,
- rozhraní místa přístupu,
- rozhraní uživatele,
- řídící jednotka kontroly vstupu,
- napájení,
- komunikační síť,
- management systému. [8], [9]

Podle rozsahu a typologie můžeme systém kontroly vstupu kvalifikovat do dvou typů:

- Autonomní – zabezpečuje pouze jedno přístupové místo v rámci vstupu/výstupu, obsahuje dvě snímací zařízení a jednu řídící jednotku, je vhodný pro nižší počet zaměstnanců a nízký počet samostatných míst přístupu.
- Modulární – uplatnění především u rozsáhlých objektů s velkým počtem přístupových míst a velkým počtem uživatelů.

Dveře v systému kontroly vstupu

Patří k základním komponentům systému kontroly vstupu, jejich vzhled je v zásadě stejný u různých výrobců, odlišná může být pouze terminologie. Ve většině případů se používají dveře s elektrickým zámkem. Mohou obsahovat tísňové tlačítko, což umožňuje vstup z vnější strany. Magnetické zámky se používají například v laboratořích, energetice, kasinech, věznicích a podobně. [8], [9]

Komponenty kontroly vstupu

V zásadě se jedná o tyto komponenty:

- dveře,
- elektrické zámky na dveřích,
- klasické čtečky karet,
- biometrické čtečky,
- klávesnice,
- docházkové terminály,
- řadiče,
- hostitelské PC v roli,
- kabeláž,
- sirény a jiné signalizační zařízení. [8], [9]

Softwarová řešení kontroly vstupu

- uživatelské rozhraní,
- komunikační server,
- databázový server.

Pro správné fungování uživatelského rozhraní je důležité, aby proběhlo správné přihlášení do databázového serveru a spojení s komunikačním serverem. Pokud vše proběhne bez

obtíží, je možné se do serveru přihlásit a pracovat v něm. Jedná se o multiuživatelský program. [8], [9]

## 2.3 Fyzická ochrana

Patří mezi základní pilíře v poskytování ochrany majetku a osob. Ve většině případů bývá doplněna o technické prostředky, protože ani sebelepší technologie plně nenahradí lidský faktor. Úkolem je odhalení a zadržení narušitele systému, realizace protipožárních a havarijních opatření. Realizována bývá strážnými, hlídači, hlídací službou či policisty. Subjekty pro tento druh ochrany využívají soukromé bezpečnostní služby, což je nejnákladnější způsob zajištění bezpečnosti. Fyzickou ostrahu lze dělit z několika hledisek. Nejčastější je časové hledisko:

- Vázaná na pracovní dobu – pracovník bezpečnostní agentury provádí ostrahu objektu jen v pracovní době podniku.
- Nepřetržitá – objekt je hlídán pracovníkem bezpečnostní agentury nepřetržitě celých 24 hodin.
- Nárazová – je prováděna pouze dle potřeb podniku, určená spíše k zajištění přepravy hotovosti a cenností. [9], [10]

Požadavky na pracovníka fyzické ostrahy jsou odlišné – podle konkrétní pracovní pozice. Obecné požadavky:

- věk nad 18 let,
- trestní bezúhonnost,
- oprávnění k právním úkonům,
- výborný zdravotní stav a dobrá fyzická kondice,
- dobré psychické předpoklady,
- důstojné chování a schopnost komunikace,
- schopnost přesvědčování,
- odborné znalosti,
- vhodné osobnostní charakteristiky.

Vše začíná výběrem ideálního pracovníka, u kterého chceme, aby disponoval určitými osobními charakteristikami, dovednostmi a znalostmi. [3], [9], [10]

## 2.4 Technická ochrana

Je tvořena technickými prostředky, které zajišťují automatické střežení chráněného objektu. Cílem je podpora realizace režimových opatření, zkvalitnění činnosti fyzické ochrany a v neposlední řadě odrazení narušitele od jeho počínaní. Technickou podporu zabezpečují hlavně mechanické zábranné systémy (dveře, zámky, ploty, mříže, ostnaté dráty) a elektronické bezpečnostní systémy (kontrola vstupu, kamerové systémy, elektrická požární signalizace a poplachový zabezpečovací systém).

Důležitým prvkem systému fyzické ochrany je optimalizace, mezi jejíž výsledky patří vymezení principů uplatněných při jeho návrhu a realizaci. Jedním z nich je princip vícestupňové ochrany kombinace mechanických zábranných systémů a elektronických bezpečnostních systémů. [11]

Technická ochrana má mít na pachatele především odstrašující účinek. V kombinaci s klasickou a fyzickou ochranou je považována za nejúčinnější a nejhůře překonatelnou ochranu. [9]

## 2.5 Fyzická bezpečnost z hlediska utajovaných informací

Problematiku utajovaných informací z hlediska fyzické bezpečnosti upravuje zákon č. 412/2005 Sb. O ochraně utajovaných informací a o bezpečnostní způsobilosti. Prováděcí vyhláškou k tomuto zákonu je vyhláška č. 528/2005 Sb. – obsahuje přílohu pojednávající o způsobech aplikace opatření fyzické bezpečnosti. Pojem utajovaná informace je dle zákona definován jako: „informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označována v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmům České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací. [12], [13], [14]

**Stupně utajení:**

- Přísně tajné – vyzrazení neoprávněné osobě či zneužití může způsobit mimořádně vážnou újmu zájmům ČR.
- Tajné – vyzrazení neoprávněné osobě či zneužití může způsobit vážnou újmu zájmům ČR.
- Důvěrné – vyzrazení neoprávněné osobě či zneužití může způsobit prostou újmu zájmům ČR.

- Vyhrazené – vyzrazení neoprávněné osobě či zneužití může být nevýhodné pro zájmy ČR. [3]

Podle zákona o utajovaných informacích se opatření fyzické bezpečnosti rozdělují do tří základních částí:

- Ostraha - zabezpečují zaměstnanci státu, právnické nebo podnikající fyzické osoby – vztažené k danému objektu. Dále pak příslušníci ozbrojených sil nebo ozbrojených sborů anebo zaměstnanci bezpečnostní ochranné služby.
- Režimová opatření - stanovuje oprávnění osob a dopravních prostředků pro vstup a vjezd do objektu, oprávnění osob pro vstup do zabezpečené oblasti, zahrnuje i způsob kontroly těchto oprávnění. Stanoví i způsob manipulace s klíči a identifikačními prostředky, které používají pro elektrická zámková zařízení a systémy kontroly vstupů, v neposlední řadě i způsob práce s technickými prostředky a jejich používání.
- Technické prostředky – jedná se o bezpečnostní prvek, který použitím zabraňuje, ztěžuje nebo oznamuje narušení ochrany objektu. [3]

Zabezpečení jednotlivých stupňů utajení se stanovuje v závislosti na kategorii a třídě dané zabezpečené oblasti následovně:

- kategorie vyhrazené – mechanické zábranné systémy,
- kategorie důvěrné – mechanické zábranné prostředky a zařízení elektrické zabezpečovací signalizace,
- kategorie tajné a přísně tajné – mechanické zabezpečovací prostředky, systémy pro kontroly vstupů, zařízení elektrické zabezpečovací signalizace, speciální televizní systémy, elektrické požární signalizace. [3]

# 3 SYSTÉM FYZICKÉ BEZPEČNOSTI

Jedním z výsledků optimalizace bezpečnostního systému objektu je vymezení principů, uplatněných při jeho návrhu a realizaci. Jedním z principů je vícestupňová ochrana, podstatou je vymezení základních stupňů při zajištění fyzické bezpečnosti, které představují hranice, oblasti nebo domény, které musí narušitel překonat. [3]
Základní stupně ochrany:

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

Výše zmíněné stupně ochrany mají svá specifika, vycházející z určení, pořadí a prostorových dispozic dané ochrany.

**Perimetrická ochrana**

Představuje souhrn bezpečnostních opatření uplatněných na obvodu pozemku chráněného objektu a v prostoru mezi jeho hranicí a chráněným objektem. Perimetr je jeho katastrální hranicí, vymezenou přírodními či umělými bariérami. Cílem je především odstranění, odhalení a zpoždění narušitele. Měla by signalizovat narušení obvodu objektu. Prvky musí splňovat vysokou klimatickou odolnost a odolnost vůči planým poplachům. [3], [6]

**Plášťová ochrana**

Je realizována na plášti chráněného objektu, zpravidla budovy - tvoří ji stěny, dveře, okna, zámky, zámkové systémy, mříže, bezpečnostní folie, kamerové systémy a detektory narušení. Cílem plášťové ochrany je odstrašení, znemožnění průchodu zpoždění a odhalení narušitele. Signalizuje narušení pláště budovy. Detekční prvky se umisťují zpravidla vně budovy a musí též splňovat vyšší klimatickou odolnost. [3], [6]

**Prostorová ochrana**

Cílem je zpoždění a odhalení pohybu narušitele. Realizována je zpravidla na chodbách, schodištích a v místnostech, tvoří jí dveře, zámky, zámkové systémy, kamerové systémy, systémy kontroly vstupu, PZTS a detektory narušení. [3], [6]

**Předmětová ochrana**

Chrání ve většině případů cenné předměty (patenty, umělecká díla). Předmětovou ochranu tvoří vitríny, skleněné tabule, kamerové systémy, PZTS. Detektory narušení by měly identifikovat bezprostřední přítomnost narušitele. [3], [6]

**Stupně zabezpečení:**

**Stupeň 1: Nízké riziko** – je zde předpoklad, že narušitel má malou znalost PZTS a má malý sortiment nástrojů.

**Stupeň 2: Nízké až střední riziko** – narušitel má omezené znalosti PZTS a používá běžné vybavení.

**Stupeň 3: Střední až vysoké riziko** – narušitel je obeznámen s PZTS a má rozsáhlý sortiment nástrojů, i těch elektronických.

**Stupeň 4: Vysoké riziko** – využívá se, pokud má zabezpečení nejvyšší prioritu. Předpokládá se, že narušitel může zpracovat podrobný plán vniknutí a má veškeré vybavení k jeho provedení. [3]

# 4 ZABEZPEČENÍ OBJEKTŮ

Okamžik, kdy riziko plynoucí z hrozby je eliminováno na akceptovatelnou úroveň, můžeme považovat za stav bezpečnosti subjektu. Pokud chceme zajistit bezpečnost subjektu, musíme znát hrozby, které by mohly ovlivnit jeho chod. Hlavní hrozbou v dnešní době je kriminální činnost, jejímž cílem je především zcizení, neoprávněné nakládání či poškození chráněných zájmů.

## 4.1 Poplachové zabezpečovací a tísňové systémy

Poplachové zabezpečovací a tísňové systémy - informují o nežádoucím vniknutí do objektu. Tato zařízení jsou sama o sobě neúčinná, pokud tedy informace nejsou včasně předány určeným osobám. V této oblasti dochází k neustálé inovaci v rámci komunikátorů, ovládací periferie, využívá se i inteligentní elektroinstalace a v neposlední řadě pozorujeme posun vpřed i v oblasti aktivní ochrany.

Hodnota chráněných aktiv je rozdílná a tomu by měla odpovídat i úroveň jednotlivých ochran. Bezpečnostní opatření by měla odpovídat předpokládaným schopnostem narušitele, k čemuž se využívají jednotlivé stupně zabezpečení. [15]

**Detektory narušení**

Detektory narušení můžeme dělit podle několika kritérií, dělí se například podle způsobu napájení:

- Napájené – ke své činnosti vyžadují napájecí zdroj, napájení může být zajištěno lokálním zdrojem či dálkovým připojením na ústředny poplachového zabezpečovacího systému. Dále je dělíme:
    - Aktivní- výhodou je jednoznačné snímání fyzikálních projevů narušení, naopak jejich nevýhodou je jejich vyšší energetická spotřeba, nezbytná koordinace činností a v neposlední řadě i snadná lokalizace narušitelem.
    - Pasivní – výhodou je nižší energetická náročnost, obtížná lokalizace narušitelem, též velmi snadná koexistence více detektorů, nevýhodou je však náchylnost k častým poplachům, kterou způsobí nejednoznačné fyzikální projevy.

  - Napájené detektory můžeme dělit i podle střežené oblasti na prostorové, směrové, bariérové, polohové. Také podle tvaru detekční charakteristiky rozdělujeme detektory narušení se/s standardním rozsahem, širokoúhlým rozsahem, kruhovým rozsahem, svislou bariérou, vodorovnou bariérou, dlouhým rozsahem. [9]
- Nenapájené – vyžadují zdroj napájení ke své činnosti. Dělíme je podle schopnosti obnovy:
  - Destrukční – plní pouze jednorázovou funkci, po detekci narušení dojde k jejich destrukci.
  - Nedestrukční – prostřednictvím vratných změn po narušení dochází k aktivaci.
  - Dále detektory dělíme podle druhu ochrany v rámci umístění a směřování detektorů na perimetrickou, plášťovou, prostorovou a předmětovou. Podle fyzikálního signálu, který je použit: elektromechanické, elektromagnetické a elektroakustické. Bližší informace o těchto detektorech obsahují následující kapitoly.[3], [15]

Vlastnosti detektorů narušení hrají velkou roli při jejich výběru. Je důležité, aby kromě klasických vlastností disponovaly i doplňkovými funkcemi. Ty totiž zlepšují jejich technickou spolehlivost a ochranu vůči jejich vyřazení z funkce narušitelem - mezi tyto funkce patří kontrola autotestem. Testování lze iniciovat **lokálně** (automatické testování alespoň jednou za 24 hodin, provozní funkci lze omezit maximálně na 30 s během 2 hodin) či **dálkově** (zpravidla kontrolu provádí ústředna, vrácení do původního stavu je potřeba do 30 s od iniciace testu). Detektor musí být odolný i vůči chybné funkci. Detektor narušení by měl být odolný vůči projevům narušitele především proti neoprávněnému přístupu k součástkám a nastavovacím prvkům detektoru, proti odejmutí z montážního úchytu, dále by měl být odolný vůči nastavení orientace. [3], [15]

**Elektromechanické detektory narušení**

Elektromechanické detektory se řadí k nejstarším detekčním prvkům. I přesto v dnešní době mají své uplatnění ve všech vrstvách ochrany. Obecně se jedná o zařízení, která reagují na mechanické změny. Fungují na jednoduchém principu – nejprve přijde podnět z vnějšího prostředí, zde přichází fyzikální změna, kterou zachytí senzor. Ten následně

naměřenou hodnotu posílá do obvodu zpracování signálu, zpracovaná hodnota pokračuje do obvodu prahové komparace, kde plní detekční funkci a hlásí buď poplach, nebo je v klidovém režimu. [3], [15]

Fyzikální změny, které mohou vést ke spuštění poplachu:

- sepnutí nebo rozepnutí spínače,
- přerušení spojení elektrického obvodu,
- změna elektrického parametru,
- změna frekvence nebo signálu v důsledku mechanických vibrací.

Mezi nejčastější detektory tohoto typu patří:

- Mechanické detektory (spínače) – konstrukčně přizpůsobené pro zabudování např. do rámu proti západce dveří, střeží tak uzamčený stav prostupů a při otevření dveří nebo okna se obvod přeruší a v tu chvíli se spustí poplach. Nevýhodou je náročná montáž, častá údržba a krátká životnost. Dnes se skoro nepoužívají.
- Magnetické detektory – slouží k bezdotykové realizaci detekce polohy. Jsou v převážné míře využívané v plášťové ochraně, samozřejmě jsou využívané i v předmětové ochraně.
- Tenzometrické detektory – jedná se o pasivní kontaktní detektory, využívané předmětové ochraně pro ochranu vzácných předmětů.
- Kontaktní detektory destrukce skleněných ploch – řadíme je mezi prvky plášťové ochrany. Patří sem poplachové folie, tapety a skla, foliové polepy a pasivní kontaktní detektory rozbití skla.
- Nášlapné detektory – jedná se o speciální druh elektromechanických kontaktních detektorů. Jednou z nevýhod je, že jsou citlivé na trvalá a častá zatížení, dále jsou náchylná na poškození a v neposlední řadě musí být umístěny skrytě. Jsou vyráběny ve dvou provedeních – foliové a páskové.
- Diferenciální tlakové detektory – jsou určeny pro perimetrickou ochranu střeženého prostoru, detektor je schopen snímat podněty až do 100 m. Lze je využít i ve velmi členitém terénu. Vzhledem k tomu, že jsou ukryté pod zemí, je pro narušitele složité je odhalit. Nevýhodou je však citlivost na kořeny stromů a keřů. [3], [15]

**Elektromagnetické detektory narušení**

Z širokého spektra elektromagnetického záření jsou využitelná všechna spektra v detektorech narušení, přitom se zohledňuje chování elektromagnetického pole po narušení narušitelem. Tento princip je využíván u následujících typů detektorů narušení:

- Pasivní infračervené detektory (PIR – Passive Infared Receiver) – pasivní detektor, který vyhodnocuje změny v infračerveném pásmu spektra elektromagnetického vlnění. Jedná se o nejrozšířenější druh detektorů pohybu, určený k perimetrické ochraně. Výhodami je zcela nepochybně jeho nenáročná konstrukce a nízká spotřeba energie. Nevýhodou je možnost rušení například osvětlením automobilu, popřípadě přímým slunečním zářením. Skládá se z těchto základních částí:
  - detektor infračerveného záření,
  - optický systém,
  - elektronika na zpracování snímaného signálu,
  - zajišťovací kontakt na signalizaci manipulace s detektorem,
  - indikační prvky LED pro indikaci stavu detektoru,
  - doplňkové obvody.
- Infračervené bariéry a závory – nejrozšířenější druh venkovních detektorů narušení. V současné době jsou trendem bezdrátové přenosy informací o narušení. Důležitou funkcí se jeví odolnost vůči falešným poplachům způsobených například sněžením, přeběhnutí zvěře.
- Mikrovlnné detektory (MW – microwave detectors) – aktivní prvky, které se pohybují v odlišném frekvenčním pásmu než ostatní detektory. Základním principem, který se používá v těchto detektorech, je Dopplerův jev (změna vlnové délky elektromagnetických či akustických vln vyvolaná relativním pohybem zdroje pozorovatele). Jsou z velké části podobné PIR, ale obsahují vysílač i přijímač v jednom.
- Rádiové bariéry a detektory – pracují na bázi velmi krátkých vln spektra. Tento druh je velmi zřídka používaný.
- Štěrbinové kabely – jde o koaxiální kabely uložené v zemi zpravidla v páru v přibližné hloubce cca 30cm a přibližně dva metry od sebe. Existuje i mobilní verze.
- Kapacitní detektory – pracují na principu kondenzátoru, kde mezi dvěma elektrodami vzniká elektrostatické pole. Systém vyvolá poplach ve chvíli, kdy

narušitel změní kapacitu pole tím, že se přiblíží nebo dotkne. Systém vyhodnocení může být umístění ne jen nad, ale i v okolí plotu. Tento systém je charakteristický vysokým počtem poplašných hlášení, proto je vhodné zkombinovat ho s kamerovým systémem.

- Laserové radary – jedná se atypické a málo používané systémy ochrany civilních objektů, i tento typ využívá Dopplerův jev. Kromě laserových radarů se v současné době využívají i laserové bariéry, jediný rozdíl je ve zdroji záření. [3]

Tento typ detektoru narušení můžeme dělit na pasivní (snímá fyzikální změny ve svém okolí) a aktivní (vytváří vlastní pracovní prostřední a poté snímá změnu v daném prostředí).

**Elektroakustické detektory narušení**

Pokud se útočník pohybuje v chráněném prostoru a překonává různé bariéry, je typické, že jeho činnost je doprovázena akustickými tlakovými vlnami, které se šíří prostorem.

Akustické detektory lze dělit hned z několika hledisek:

- Podle zdroje akustického signálu:
  - pasivní,
  - aktivní.
- Podle použitého frekvenčního pásma:
  - detektory pracující v akustickém pásmu 16 Hz – 20 kHz,
  - detektory pracující v ultrazvukovém pásmu víc jak 20 kHz.
- Podle určení z hlediska prostorového působení:
  - perimetrická ochrana,
  - prostorová ochrana,
  - plášťová ochrana,
  - předmětová ochrana. [3]

Ultrazvukové detektory

Jsou to detektory určené pro prostorovou ochranu objektů, jejich princip lze však využívat i v plášťové nebo předmětové ochraně. Tvoří je dvě části – vysílač a přijímač. Nevýhodou těchto detektorů je nestabilita vysílané frekvence, která může způsobit falešné poplachy nebo malou citlivost na pohyb nízkou rychlostí. Typický dosah detektorů je 10m. Pokud k detektoru umístíme předměty absorbující zvuk, snížíme tím výrazně jeho dosah. [3], [15]

Detektory rozbití skla

Lze je charakterizovat jako významnou skupinu detektorů spadajících do plášťové ochrany. Slouží k ochraně větších skleněných ploch. Pasivní detektor vyhodnocuje lámání a tříštění skla, tlakovou vlnu šířící se po povrchu skleněné tabule a akustickou tlakovou vlnu šířící se v prostoru při rozbíjení skleněné tabule. Naopak aktivní detektor vyhodnocuje akustické ultrazvukové vlny a elektromagnetické infračervené vlny. [3], [15]

Mikrofonický kabel

Patří mezi detekční kabely, které se budují přímo na obvodovém oplocení. Je charakteristický svými odlišnými detekčními systémy. Tím, že jeho výstupní signál se pohybuje nízkofrekvenčně, umožňuje tak po zesílení připojit k vyhodnocovací jednotce reproduktor. Umožňuje obsluze rozlišit falešné poplachy od těch skutečných. [3]

## 4.2 Kamerové systémy

Jedná se o systém zahrnující kamerovou soustavu, zobrazovací a další přídavná zařízení důležitá pro přenos signálu. Nejčastěji používanou zkratkou je CCTV. Systém primárně slouží k identifikaci, rekognoskaci a detekci osob tedy k monitorování osob, kromě toho má širokospektrální využití. V dnešní době se přechází právě k digitálnímu zpracování videosignálu, což je způsobené především doplňkovými funkcemi kamer, ve kterých se využívá číslicového zpravování signálu procesorem v kameře. [8]

Jednotlivé funkce kamerových systémů

- Gama korekce – umožňuje lepší podání jednotlivých stupňů šedi a tím se zlepší i rozlišení detailů.
- Funkce elektronické uzávěrky (Electronic Shutter Control - ESC) – umožňuje při omezených světelných podmínkách použít i levnější objektiv se clonou.
- Funkce obrazové paměti – tato funkce je zabudována v kamerovém procesoru a umožňuje i při slabých světelných podmínkách dodat kvalitní obraz. Funkce bývá též označována jako tzv. Pomalá uzávěrka.
- Obvod eliminace protisvětla (Black Light Compensation – BLC) – Částečně vylučuje důsledky nesprávného umístění kamery při silném zdroji světla.
- Bodová kompenzace protisvětla – pracuje tak, že nahradí obraz s vysokým jasem tmavým obrazem.

- Funkce Auto Black – automaticky zvyšuje kontury, zvyšuje se kontrast a dynamický rozsah.
- Široký dynamický rozsah (Wild Dynamic Range – WDR) – umožňuje získat detailní informace z tmavých částí obrazu bez saturace světlých částí.
- Den a noc (Day-night) – přizpůsobuje se zhoršeným světelným podmínkám.
- Odstranění infračerveného filtru – umožňuje mnohem větší citlivost v černobílém režimu.
- Automatické vyvážení bílé (Automatic White Balance – AWB) – nastaví teplotu barev rozdílně pro venkovní a vnitřní prostředí.
- Detekce pohybu (Motion Detection – MD) – uplatňuje se především při větším počtu sledovaných monitorů, automaticky při detekci pohybu odešle zprávu.
- Maskování privátních zón (Privacy Zone Masking – PZM) – překryje část snímaného obrazu, který není součástí účelu snímání a mohlo by tak dojít k narušení soukromí nezúčastněných osob.
- Inteligentní analýza obrazu (Intelligent Video Content Analysi – IVA) – funkce pro analýzu obsahu videa.
- Digitální redukce šumu (Digital Noise Reduction – DNR) – při nízké světelnosti se samozřejmě snižuje i kvalita, a to z důvodu přibývajícího šumu. Tato funkce šum dokáže z velké části eliminovat. Existuje i 3D verze tohoto programu.
- Stabilizace obrazu (Digital Image Stabilization – DIS) – eliminuje nežádoucí vibrace způsobené například silným větrem.
- Automatické sledování (Autotracking) – poskytuje velmi přesnou detekci pohybu v monitorované oblasti. Automaticky otáčí nebo naklání kameru. [8]

## 4.3 Elektrická požární signalizace

Pro splnění základních funkcí elektrické požární signalizace je nezbytná ústředna EPS a hlásič požáru. Propojení mezi těmito komponenty se nazývá požární smyčka, přičemž požadavky pro jednotlivé komponenty lze nalézt v normě, která specifikuje technické požadavky.

Podle identifikace místa požáru dělíme EPS:

- Systémy s kolektivní adresací - ústředna je schopna rozlišit pouze z jaké požární smyčky signál o požáru přišel, nemůžeme tedy použít ani hlásiče s přenosem naměřených hodnot, protože je ústředna vůbec nezaznamená.
- Systémy s individuální adresací – jsou založeny na datové komunikaci mezi hlásičem požáru a ústřednou EPS. Požární smyčka slouží v tomto případě jako datová sběrnice, která umožňuje tuto komunikaci. [15], [17]

**Hlásiče požáru**

Slouží k identifikaci a lokalizaci požáru při jeho vzniku a rozvoji. Hlásiče můžeme na základním stupni dělit na dva druhy, a to na tlačítkové (je zapotřebí osoba, která je přítomna v místě požáru a aktivuje hlásič požáru) a samočinné (detektor se sám spustí na základě vyhodnocení výskytu nebo změny fyzikálních parametrů, a to bez lidského činitele). Nejužívanějším způsobem klasifikace patří klasifikace podle vyhodnocovaného jevu - podle tohoto kritéria můžeme dělit samočinné hlásiče na:

- Hlásiče kouře:
    - Ionizační - detekuje změnu (pokles) vodivosti vzduchu, ke které dojde úbytkem ionizovaných částí vzduchu v měřící komůrce.
    - Optické - detekuje pevné částice kouře generované během požáru - ovlivňují šíření světelného paprsku emitovaného skrz vrstvu vzduchu kontaminovaného kouřem.
- Hlásiče teplot – jde o historicky nejstarší detekční prvky, princip detekce je založen na vyhodnocování teplotních změn v místě instalace vyvolaných uvolněným teplem v důsledku exotermické reakce hoření.
- Hlásiče plamene – detekují požár na základě vyhodnocení specifických vlastností sálání plamene při požáru.
- Hlásiče plynu.
- Hlásiče multisenzorové. [15], [17]

**Ústředny EPS**

Představují klíčový komponent systému elektrické požární signalizace. Všechny prvky systému závisí na bezchybné a nepřetržité funkci ústředny.

V rámci bezchybnosti musí ústředna plnit základní funkce:

- Nepřetržité napájení komponentů systému EPS elektrickou energií – napájení musí být vždy ze dvou na sobě nezávislých zdrojů, v případě výpadku musí dojít k okamžitému samočinnému přechodu na náhradní zdroj napájení. Využívané napájecí zdroje:
    - hlavní,
    - náhradní,
    - záložní.
- Akustickou a optickou indikaci funkčních stavů systému EPS obsluze.
- Příjem a vyhodnocování signálů z připojených hlásičů – jsou závislé na druhu použitého systému:
    - Neadresovatelné (s kolektivní adresací) – vyhodnocuje proudové a napěťové změny v požární smyčce.
    - Adresovatelné (s individuální adresací) – vyhodnocuje proudové impulzy generované v hlásiči nebo vyhodnocuje datovou komunikaci mezi ústřednou a jednotlivými komponenty.
- Ovládání zařízení připojených do systémů EPS – realizuje se prostřednictvím ovládacích jednotek zapojených do hlásící linky. Mají charakter vstupně/výstupní nebo jen výstupní. Další alternativou mohou být potenciálové a bezpotenciálové výstupy. [15]
- Kontrola provozuschopnosti celého systému – provádí se automaticky tak manuálně a v neposlední řadě i samočinně za běžného provozu.

**Doplňující a ovládaná zařízení EPS**

Tato zařízení významně rozšiřují funkce systému elektrické požární signalizace v protipožárním systému budov. Mezi nejpoužívanější doplňující zařízení EPS patří:

- Obslužné pole požární ochrany – doplňuje zařízení systému, které je určené pro požární zásah. Musí jednotkám a servisním technikům umožnit jednoduchou obsluhu a ovládání určitých funkcí systému EPS a zařízení dálkového přenosu.
- Klíčový trezor požární ochrany – úschovný objekt, ve kterém je uschovaný objektový klíč. Ten umožňuje nenásilný vstup do všech střežených prostor objektu. Umístěn je z vnější strany objektu a je odemykatelný pouze při aktivaci systému EPS.

- Zařízení dálkového přenosu – slouží k provedení, zrychlení a zefektivnění požárního zásahu. Jedná se o spojení mezi signalizujícím a vyhodnocujícím místem. Tato činnost musí být proveden samočinně a nezávisle na obsluze.

Ovládaná a pomocná zařízení:

- Stabilní hasicí zařízení – hrají důležitou roli v rámci požární bezpečnosti, slouží k zamezení vzniku výbuchu či požáru, k likvidaci požáru hasebními látkami, popřípadě k přerušení hoření, zabránění šíření požáru a k jeho kontrole a v neposlední řadě k ochlazování.
- Zařízení pro odvod kouře a tepla – cílem těchto zařízení je především zajištění únikové cesty, minimalizace použitých hasicích přístrojů, ochrana majetku, evakuace bez cizí pomoci a ochrana před vzplanutím hořlavých plynů. K tomuto cíli nám dopomáhají kouřová ventilační okna, kouřovody a další systémy. [15]

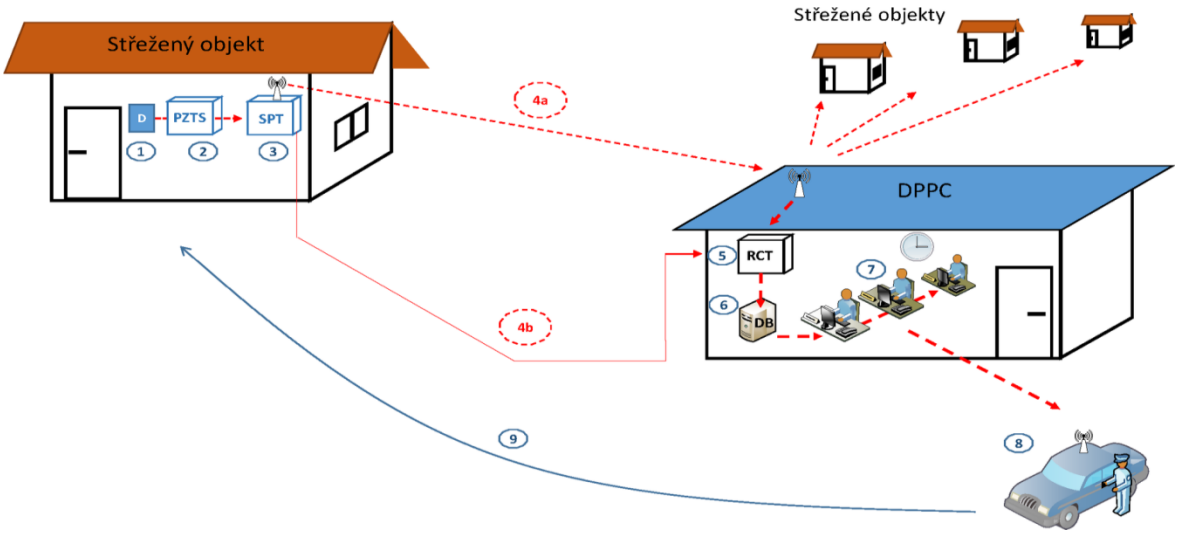
## 4.4 Dohledová a poplachová přijímací centra

Dříve nazývaný pult centrální ochrany slouží k potřebě ochrany nejen zdraví či majetku, ale slouží i k minimalizaci škod. V roce 2011 vstoupilo v platnost nové označení - dohledová a poplachová přijímací centra. V dnešní době jsou tato centra velmi moderní a v dalších letech budou nepochybně směřovat k oblasti internetu. [15], [17]
Centrum přijímá signály z připojených objektů, a tím zajišťuje s vysokou účinností, nepřetržitě 24 hodin denně, jejich bezpečnost. Bezpečnostní služba, která nabízí služby DPPC, v optimální variantě disponuje precizně vycvičeným a školeným personálem. V případě nestandardní situace na připojeném objektu, popřípadě v jeho perimetru, reaguje řízeným zásahem, v některých případech s koordinací s PČR. Jejich rozsah a možnosti střežení konkrétního objektu právě moderním DPPC jsou široké a variabilní – právě proto, že skutečné plnění se odvíjí od individuálních potřeb zákazníka, což je také předmětem smlouvy a konkrétních podmínek mezi majitelem objektu a společností, která provozuje DPPC.

Jak funguje centrum, popisuje obrázek níže. Číselné označení modulů je seřazeno vzestupně, jak postupně v čase vzniká posloupnost jednotlivých fází.

1. Detektor – modul snímá a měří určitou veličinu, která může znamenat narušení objektu. Zařízení byla blíže specifikována výše.

2. PZTS – jedná se o vyhrnovací ústřednu, na kterou je připojena soustava detektorů. Rozhoduje o tom, zda je objekt hlídán nebo jsou zabezpečeny pouze některé jeho části. Je ovládám buď uživatelem (lze ovládat i pomocí dálkových ovladačů, telefonů či dotykových karet) nebo automaticky podle časového rozvrhu.
3. SPT – přenosové zařízení střeženého prostoru má za úkol předávat poplachové zprávy z objektu do DPPC. Informace jsou předávány různou cestou.
4. Poplachová přenosová trasa – jedná se o trasu, kterou jsou předávány informace z objektu do DPPC. Na obrázku jsou trasa 4a, která značí bezdrátové spojení, a trasa 4b znázorňující kabelové spojení. Tras může být hned několik pro zvýšení spolehlivosti a bezpečnosti.
5. RCT – komunikátor přijímacího centra komunikuje s přenosovými zařízeními a přijatá data předává do centra. Zde jsou data zpracována a zobrazena operátorovi.
6. Vyhodnocovací jednotka – data, která přijme RCT jsou zpravidla předány do vyhodnocovací jednotky, kterou je obvykle nějaký server s aplikací DPPC a databází. Zde dochází k archivaci dat, předávání potřebných dat operátorům, signalizaci poplachů, evidenci instrukcí, mapové podklady.
7. Operátor – osoba vyhodnocující informace přijímané na DPPC ze střežených objektů.
8. Zásahová jednotka – obvykle se jedná o vozidlo s osobou/osobami, které v případě narušení objektu vyjíždí k objektu za účelem zajištění pachatele. V některých případech může zásah provádět i pěší hlídka. [18]




Obr. 2 Dohledová a poplachová přijímací centra. Zdroj:[18]

# 5 CÍLE A METODY ZPRACOVÁNÍ DIPLOMOVÉ PRÁCE

Cílem diplomové práce je analýza stavu bezpečnosti informací z hlediska fyzické bezpečnosti ve vybraném objektu. Vedlejším cílem je návrh vhodných prostředků pro zlepšení stavu, a tím posílit systém a samotnou odolnost objektu. Dalším dílčím cílem je vytvoření literární rešerše obsahující problematiku systému řízení bezpečnosti informací a fyzické bezpečnosti.

Prvotním krokem bylo shromáždění odborných zdrojů a zahájení rešeršní činnosti. Následovalo zpracování poznatků a objasnění systému řízení bezpečnosti informací. Velký důraz byl kladen na jednotlivé komponenty fyzické bezpečnosti. Podstatným krokem bylo zpracování veškerých získaných informací od nejobecnějších až po konkrétní.

Druhotným krokem bylo seznámení se s vybraným objektem. Podrobnou analýzu umožnila metoda sběru dat a řízené rozhovory s vedením daného subjektu. Další použitou metodou je určení zdrojů ohrožení pro celý systém. K tomu byla využita analýza rizik s využitím jejich souvztažností (KARS). Poté, co byla definována rizika, bylo nutné provést SWOT analýzu.

Pro specifičtější analýzu rizik je využita SWOT analýza. Jedná se o komplexní metodu kvalitativního hodnocení všech stránek fungování – v tomto případě se bude jednat o plášťovou a prostorovou ochranu objektu ochrany obyvatelstva, vzhledem k výsledkům KARS metody. Jedná se o silný nástroj pro celkovou analýzu vnitřních i vnějších činitelů. SWOT je anglická zkratka pro: Strengths (silné stránky), Weaknesses (slabé stránky), Opportunities (příležitosti), Threats (hrozby). Spočívá v klasifikaci a ohodnocení jednotlivých faktorů, které jsou rozděleny do čtyř základních skupin. Vztahovala na jednotlivé druhy ochrany, na které se vztahují daná rizika vyplývající z KARS metody. Po určení kritických míst systému bylo na místě provést samotný projekt zabezpečení vybraného objektu.

Pomocí projektu byl sestaven sled činností, na tu navazující Ganttův diagram. Součástí je i metoda analýzy rizik RIPRAN - představuje empirickou metodu pro analýzu rizik projektů (se zaměřením na střední a velké projekty). Vychází z procesního pojení analýzy rizik, analýzu jednotlivých rizik tedy chápe jako posloupnost procesů, přičemž každý proces má jasně definovány vstupy, výstupy a činnosti procesů, transformující vstupy na výstupy s určitým cílem. Slouží k prvotnímu zkoumání, která stanovila hrozby pro daný projekt.

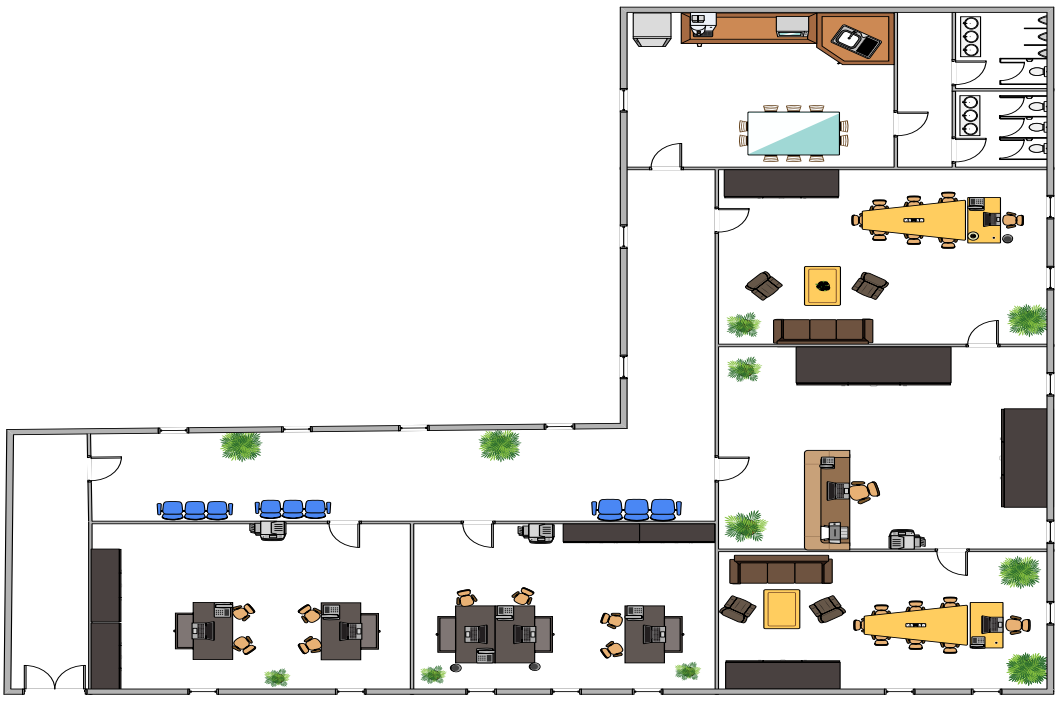
# II. PRAKTICKÁ ČÁST

# 6 CHARAKTERISTIKA VYBRANÉHO OBJEKTU

Kapitola je věnována charakteristice vybraného objektu vztaženého k ochraně obyvatelstva. Subjekt si nepřeje být jmenován, proto tomu celá praktická část bude přizpůsobena.

Obec, ve které se nachází objekt, je situována ve Zlínském kraji s přibližným počtem 2 000 obyvatel a katastrální výměrou 7 $km^2$. Člení se na dva celky, lokalitou též protéká potok. Svou polohou tvoří přirozené centrum pro okolní obce. Významným prvkem je ideální silniční propojení. V obci se nachází základní škola, jejíž součástí je mateřská škola a školní jídelna, obecní knihovna, tělocvičná jednota a v neposlední řadě i sbor dobrovolných hasičů.

Vybraným objektem se stal obecní úřad obce. Jeho součástí je kancelář starosty, matrika, stavební úřad, ekonomický úsek. Celkový prostor se skládá z pěti kancelářských místností, kuchyňky, toalet a dvou oddělených chodeb situovaných v přízemí budovy. V prostoru se pohybuje hned několik pracovníků, vzhledem k tomu, že se v budově konají i pravidelná zasedání zastupitelstva a rady obce. V rámci zastupitelstva se jedná o 15 členů. Radu obce tvoří 5 členů a stálých pracovníků obce se samostatnou působností je celkem dvacet přičemž je nutné zahrnout čtyři zaměstnance s přenesenou působností.



Obr. 3 Orientační plánek budovy. Zdroj:[vlastní]

# 7 ANALÝZA RIZIK

Kapitola představí výstupy z několika analýz. V první řadě bude využita analýza rizik s využitím jejich souvztažností (KARS). Využijeme ji pro analýzu rizik celého objektu. Tím zjistíme, jaká oblast objektu je nejvíce zranitelná a na tu následně provedeme SWOT analýzu. Provedena bude tedy pouze na kritickou část objektu. V další kapitole bude vytvořen projekt pro zavedení navržených opatření, vztažený k těmto analýzám.

## 7.1 KARS

Tato kapitola je věnována analýze rizik vybraného objektu, provedené pomocí kvalitativní metody s využitím souvztažností jednotlivých rizik (KARS). Pomocí této metody získáme hodnotu nejvyššího hrozícího rizika, což povede k návrhům opatření pro daný subjekt. V tomto případě hovoříme o objektu ochrany obyvatelstva.

### 7.1.1 Soupis rizik

Ke správnému fungování metody KARS je důležité sestavit seznam rizik, který obsahuje možné zdroje rizika pro daný objekt. Pomocí literární rešerše bylo vybráno deset možných rizik v rámci pravděpodobnosti vzniku ohrožení. [19], [20], [21]

Jedná se o následující rizika:

1. rozbití okna,
2. vloupání,
3. požár,
4. selhání mechanických systémů,
5. výpadek elektrické energie,
6. poškození fasády,
7. kybernetický útok,
8. výbuch,
9. povodeň,
10. selhání EPS. [21]

### 7.1.2 Sestavení a vytvoření tabulky souvztažnosti rizik

Sestavení tabulky rizik je dalším důležitým aspektem k provedení analýzy KARS. V prvním sloupci jsou vypsána vybraná rizika pro objekt a označena pořadovými čísly 1 – 10. V prvním řádku tabulky jsou pak napsána jednotlivá čísla rizik. [19], [20], [21] Metoda se zakládá na vzájemném působení a souvztažnosti jednotlivých rizik. Pro správné dodržení postupu musí být tabulka vyplněna následovně:

- 1 – je vyplněna pokud $R_i$ může vyvolat riziko $R_j$.
- 0 – je vyplněna pokud $R_i$ nemůže vyvolat riziko $R_j$. [19], [20], [21]

Tab. 1Vytvoření tabulky souvztažnosti rizik.

| **Riziko** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **Součet** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. Rozbití okna | **0** | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | **2** |
| 2. Vloupání | 1 | **0** | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | **8** |
| 3. Požár | 1 | 0 | **0** | 1 | 1 | 1 | 0 | 1 | 0 | 1 | **6** |
| 4. Selhání mechanických systémů | 0 | 1 | 0 | **0** | 1 | 0 | 0 | 0 | 0 | 1 | **3** |
| 5. Výpadek el. energie | 0 | 1 | 0 | 1 | **0** | 0 | 0 | 0 | 0 | 1 | **3** |
| 6. Poškození fasády | 0 | 0 | 0 | 0 | 0 | **0** | 0 | 0 | 0 | 0 | **0** |
| 7. Kybernetický útok | 0 | 1 | 0 | 1 | 1 | 0 | **0** | 0 | 0 | 1 | **4** |
| 8. Výbuch | 1 | 0 | 1 | 1 | 1 | 1 | 0 | **0** | 0 | 1 | **6** |
| 9. Povodeň | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | **0** | 1 | **5** |
| 10. Selhání EPS | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | **0** | **2** |
| **Součet** | **3** | **6** | **2** | **8** | **6** | **4** | **1** | **2** | **0** | **7** | |

Zdroj:[21]

### 7.1.3 Výpočet koeficientů aktivity a pasivity

Pro kvantifikaci rizik pro vybraný objekt bylo využito koeficientů aktivity a pasivity. Za pomoci těchto koeficientů byla převedena výsledná tabulka souvztažnosti do matematické a následně také grafické podoby.

- $K_{ARi}$ – koeficient aktivity – představuje procentuální vyjádření počtu vybraných rizik, která jsou návazná na riziko označené $R_i$. V případě, že riziko $R_i$ nastane, tak tato návazná rizika mohou být vyvolána.
- $K_{PRi}$ – koeficient pasivity – představuje procentuální vyjádření počtu vybraných rizik, která jsou návazná na riziko označené $R_i$ a která mohou riziko $R_i$ následně vyvolat. [19], [20], [21]

Pro vyjádření koeficientu aktivity a pasivity bylo nutné sestavit počet kombinací. Jedním z předpokladů je, že riziko $R_i$ nemůže vyvolat samo sebe, dále může nastat situace, kdy riziko $R_i$ vyvolá další rizika, případně může být vyvoláno jimi samotnými. V tomto případě se počet rizik rovná x = 10, v tom případě tedy platí, že počet možných kombinací je x – 1. [19], [20], [21]

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

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

1. $K_{ARi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{2}{10-1} . 100 = \frac{2}{9} . 100 = 22{,}22\%$
2. $K_{ARi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{8}{10-1} . 100 = \frac{8}{9} . 100 = 88{,}88\%$
3. $K_{ARi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{6}{10-1} . 100 = \frac{6}{9} . 100 = 66{,}66\%$
4. $K_{ARi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{3}{10-1} . 100 = \frac{3}{9} . 100 = 33{,}33\%$
5. $K_{ARi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{3}{10-1} . 100 = \frac{3}{9} . 100 = 33{,}33\%$
6. $K_{ARi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{0}{10-1} . 100 = \frac{0}{9} . 100 = 0\%$
7. $K_{ARi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{4}{10-1} . 100 = \frac{4}{9} . 100 = 44{,}44\%$
8. $K_{ARi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{6}{10-1} . 100 = \frac{6}{9} . 100 = 66{,}66\%$
9. $K_{ARi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{5}{10-1} . 100 = \frac{5}{9} . 100 = 55{,}55\%$

10. $K_{ARi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{2}{10-1} . 100 = \frac{2}{9} . 100 = 22{,}22\%$

**Výpočet koeficientů pasivity $K_{PRi}$ pro jednotlivá rizika $R_i$:**

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

1. $K_{PRi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{3}{10-1} . 100 = \frac{3}{9} . 100 = 33{,}33\%$
2. $K_{PRi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{6}{10-1} . 100 = \frac{6}{9} . 100 = 66{,}66\%$
3. $K_{PRi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{2}{10-1} . 100 = \frac{2}{9} . 100 = 22{,}22\%$
4. $K_{PRi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{8}{10-1} . 100 = \frac{8}{9} . 100 = 88{,}88\%$
5. $K_{PRi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{6}{10-1} . 100 = \frac{6}{9} . 100 = 66{,}66\%$
6. $K_{PRi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{4}{10-1} . 100 = \frac{4}{9} . 100 = 44{,}44\%$
7. $K_{PRi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{1}{10-1} . 100 = \frac{1}{9} . 100 = 11{,}11\%$
8. $K_{PRi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{2}{10-1} . 100 = \frac{2}{9} . 100 = 22{,}22\%$
9. $K_{PRi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{0}{10-1} . 100 = \frac{0}{9} . 100 = 0\%$
10. $K_{PRi} = \frac{\sum Ri}{x-1} . 100\ [\%] = \frac{7}{10-1} . 100 = \frac{7}{9} . 100 = 77{,}77\%$

Tab. 2 Koeficienty aktivity a pasivity

| **$K_{ARi}$ [%]** | 22,22 | 88,88 | 66,66 | 33,33 | 33,33 | 0 | 44,44 | 66,66 | 55,55 | 22,22 |
|---|---|---|---|---|---|---|---|---|---|---|
| **$K_{PRi}$ [%]** | 33,33 | 66,66 | 22,22 | 88,88 | 66,66 | 44,44 | 11,11 | 22,22 | 0 | 77,77 |

Zdroj:[21]

Tabulka obsahuje hodnoty koeficientů aktivity a pasivity, které jsou důležité, pro výsledný graf. Hodnoty budou doplněny do tabulky v programu Excel, kdy po zadání hodnot program vytvoří výsledný graf.

### 7.1.4 Výsledný graf souvztažností

Účelem vytvoření grafu je stanovení významnosti všech rizik a jejich souvztažnosti v systému. Graf je rozdělen dvěma osami $O_1$ a $O_2$ na 4 kategorie:

I. Primárně a sekundárně nebezpečná rizika.

II. Sekundárně nebezpečná rizika.

III. Primárně nebezpečná rizika.

IV. Oblast relativně bezpečná. [19], [20], [21]

Oblast I ve výsledném grafu pokrývá 80 % z celkové oblasti, kde se nachází posuzovaná rizika. Pro osu $O_1$ platí:

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

V případě konstrukce osy $O_1$ za splnění 80% podmínky to bude rovnoběžka s osou y ve vzdálenosti: [7]

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

$$O_1 = 88{,}88 - \frac{88{,}88 - 0}{100}.80 = 88{,}88 - 71{,}04 = 17{,}84$$

**Výsledek pro $O_1$ = 17,84 %**

Pro osu $O_2$ za splnění 80% podmínky je rovnoběžka s osou x ve vzdálenosti:

$$O_2 = K_{Pmax} - \frac{K_{Pmax} - K_{Pmin}}{100}.80$$

$$O_2 = 88{,}8 - \frac{88{,}8 - 0}{100}.80 = 88{,}8 - 71{,}04 = 17{,}84$$

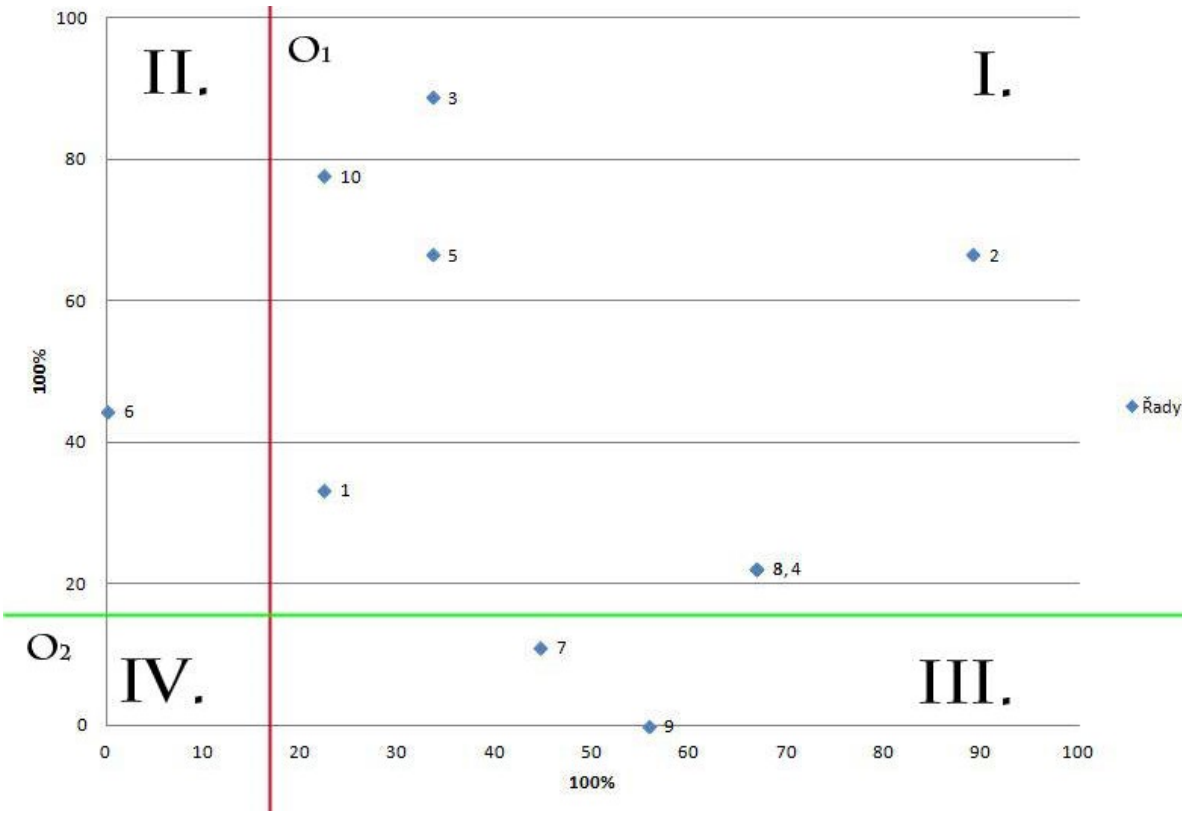
**Výsledek pro $O_2$ = 17,84 %**

### 7.1.5 Vyhodnocení metody KARS

Oblast I. Primárně a sekundárně nebezpečná rizika – rizika – 1 (rozbití okna), 2 (vloupání), 3 (požár), 4 (selhání mechanických zařízení), 5 (výpadek elektrické energie), 8 (výbuch), 10 (selhání EPS).

Oblast II. a III. Primárně a sekundárně nebezpečná rizika – rizika – 6 (poškození fasády objektu), 7 (kybernetický útok), 9 (povodeň).

Oblast IV. Relativně bezpečná - bez zjištěných rizik. [21]




Obr. 4 Vyhodnocení metody KARS. Zdroj:[21]

## 7.2 SWOT ANALÝZA

Pro specifičtější analýzu rizik je využita SWOT analýza. Jedná se o komplexní metodu kvalitativního hodnocení všech stránek fungování – v tomto případě se bude jednat o plášťovou a prostorovou ochranu objektu ochrany obyvatelstva, vzhledem k výsledkům KARS metody. Jedná se o silný nástroj pro celkovou analýzu vnitřních i vnějších činitelů.

SWOT je anglická zkratka pro: Strengths (silné stránky), Weaknesses (slabé stránky), Opportunities (příležitosti), Threats (hrozby). Spočívá v klasifikaci a ohodnocení jednotlivých faktorů, které jsou rozděleny do čtyř základních skupin.

Prvotním krokem této analýzy je sestavení jednotlivých složek. Obsahuje posouzení silných a slabých stránek současného zabezpečení objektu ochrany obyvatelstva, nalezení příležitostí ke zlepšení stavu bezpečnosti a odhalení hrozeb, jež by se mohly negativně projevit. Vnitřním prostředím se rozumí prostředí, kde může systém ovlivnit sám sebe. Vnější naopak představuje prostředí, jehož chování subjekt nemůže ovlivnit. [21]

V další fázi jsou jednotlivé části opatřeny váhami důležitosti, tedy jak důležitá je tato silná nebo slabá stránka. Pro silné stránky a příležitosti je použita kladná stupnice od 1 do 5, přičemž 5 znamená nejvyšší spokojenost a 1 nejnižší spokojenost. Slabé stránky a hrozby využívají zase zápornou stupnici od -1 nejnižší spokojenost až -5 nejvyšší nespokojenost. Následuje bodové hodnocení jednotlivých složek SWOT analýzy pomocí přiřazovaných čísel. Pro všechny skupiny je však stanoven součet vah roven 1. Čím vyšší číslo, tím je větší důležitost položky v dané kategorii a naopak. [22], [23]

Konečnou fází je graf, který vychází z předešlých výpočtů. Z nich vyplynou jednotlivé strategie, které pomohu zvolit vhodný druh postupu za účelem zlepšení stávajícího stavu. Ve výsledku by měla být vybrána jedna z následujících strategií – ofenzivní strategie (využívá silné stránky na získání výhody), strategie spojenectví (překonává slabiny využitím příležitostí), defenzivní strategie (využívá silné stránky na čelení hrozbám) a strategie likvidace (minimalizuje náklady a čelí hrozbám). [22], [23]

### 7.2.1 Plášťová ochrana

Tab. 3 SWOT analýza - soupis jednotlivých složek

| | | |
|---|---|---|
| **Vnitřní prostředí** | **Silné stránky** | **Slabé stránky** |
| | Mříže v přízemní části budovy | Absence venkovních kamer |
| | Finanční prostředky | Stáří komponentů |
| | Výběr objektu v klidné lokalitě | Výběr komponentů omezen cenou |
| | Detektory narušení | Horší technický stav oken |
| | Tloušťka zdi | Nutnost výběrového řízení pro bezpečnostní komponenty |
| **Vnější prostředí** | **Příležitosti** | **Hrozby** |
| | Vybavit objekt kamerovým systémem | Vloupání |
| | Spolupráce | Vandalismus |
| | Modernizace oken | Požár |
| | Modernizace vstupních dveří | Živelní pohromy |
| | Aktivní přístup zaměstnanců | Terorismus |

Zdroj: [21]

K silným stránkám v rámci zabezpečení objektu ochrany obyvatelstva z hlediska plášťové ochrany prvotně řadíme mříže v přízemní části budovy, což perfektně doplňují venkovní detektory narušení a tloušťka zdí – která je díky tomu, že se jedná o historickou budovu, nadstandardně silná. Ke všem těmto druhům zabezpečení přispívá i fakt, že se objekt nachází v klidné lokalitě. Důležitým aspektem je zcela nepochybně i finanční rovina, kterou řadím k silným stránkám, neboť majitelovo finanční zázemí umožňuje (v případě urgentní potřeby)vynaložení finančních prostředků.

Mezi slabé stránky byla zařazena absence kamerového systému a stáří komponentů, což by mohlo být velmi podstatné při vniknutí do objektu. Problematickým prvkem se dále jeví být systém vybavování objektu bezpečnostními prvky, ale vzhledem k tomu, že se jedná o objekt ochrany obyvatelstva, musí se zde postupovat podle předpisů. Musí tedy být vypsáno výběrové řízení a poté se rozhoduje podle nejlepší nabídky. Další zásadní slabou stránkou je technický stav oken. Vzhledem k tomu, že kanceláře pracovníků jsou již v přízemí.

Příležitostí se nabízí hned několik. Rozhodně se jedná o nainstalování kamerového systému – to je bohužel dosti problematická záležitost, vzhledem k tomu, že se jedná o historickou budovu. Veškeré venkovní zařízení tedy podléhá schválení Národnímu památkovému úřadu památkové péči. Taktéž je na tom i modernizace oken či modernizace vstupních dveří, praktická aplikace obou těchto příležitostí je více než nutná. Jako velká příležitost se jeví nejen spolupráce ze strany vedení objektu, ale především velmi aktivní přístup zaměstnanců k nastoleným opatřením. Všechny příležitosti jsou podstatné a důležité pro plášťovou ochranu objetu.

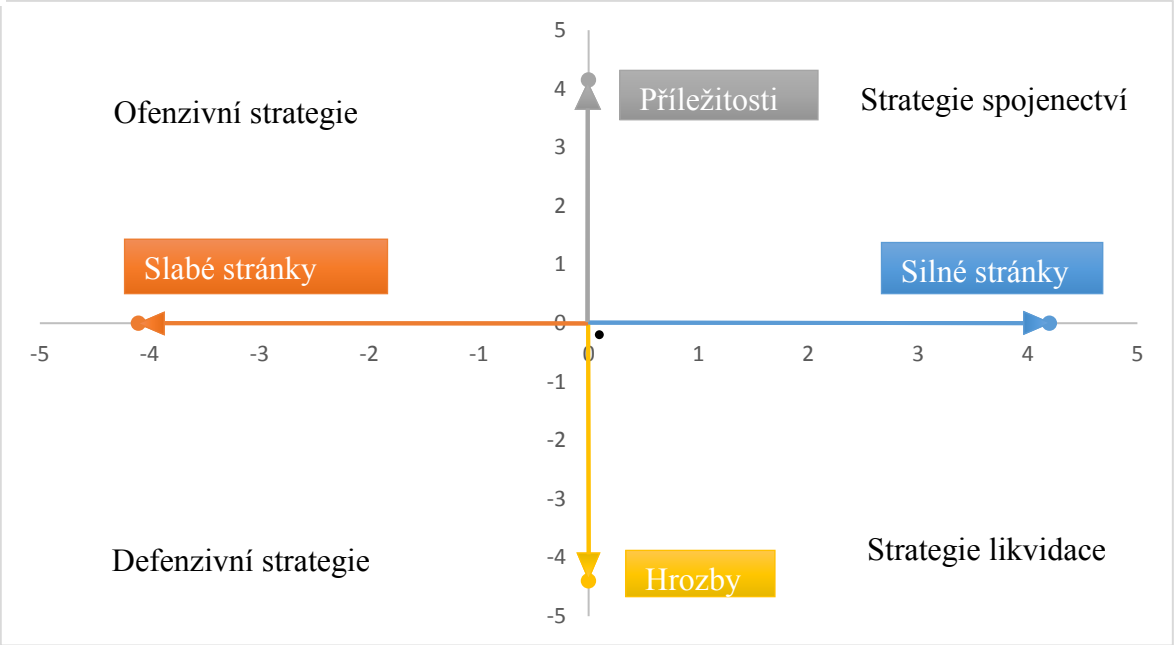
Nejvýznamnější hrozbou je riziko vloupání. I přesto, že se jedná o klidnou lokalitu, lze tuto hrozbu považovat za nejpravděpodobnější, když přihlédneme ke slabým stránkám. I přes již nainstalované systémy, by pachateli nečinilo příliš velké obtíže do objektu vniknout. Další hrozbou se jeví být požár, a to jak úmyslný, tak neúmyslný. Kriminalita v dnešní době neustále stoupá, proto nelze opomenout ani vandalismus, který je viditelný nejen ve větších městech, ale i v menších obcích. Dnešní doba je plná rizik, čímž se nijak neliší od dob dřívějších, jen zábrany některých obyvatel se bohužel dále posouvají. Do hrozeb musíme zcela nepochybně zahrnout i živelní pohromy, které sužují obyvatelstvo, nehledě na roční období. Na posledním místě, ale rozhodně ne z hlediska významnosti, byl do hrozeb zařazen terorismus.

V následující tabulce jsou shrnuty veškeré výpočty, s jednotlivými váhami a hodnocením, které jsou podstatné pro výsledný graf SWOT analýzy.

Tab. 4 SWOT analýza – složky s váhami a hodnocením

| Typ | Složka | Váha | Hodnocení | Součin | Součet |
|---|---|---|---|---|---|
| **Silné stránky** | Mříže v přízemní části budovy | 0.15 | 5 | 0,75 | 4,2 |
| | Finanční prostředky | 0,20 | 4 | 0.8 | |
| | Klidná lokalita | 0.30 | 3 | 0,9 | |
| | Detektory narušení | 0.25 | 5 | 1.25 | |
| | Tloušťka zdi | 0.10 | 5 | 0,5 | |
| **Slabé stránky** | Absence venkovních kamer | 0.25 | -4 | -1 | -4, 1 |
| | Stáří komponentů | 0.25 | -4 | -1 | |
| | Výběr komponentů omezen cenou | 0.10 | -3 | -0,3 | |
| | Horší technický stav oken | 0.30 | -5 | -1,5 | |
| | Nutnost výběrového řízení pro bezpečností komponenty | 0.10 | -3 | -0,3 | |
| **Příležitosti** | Vybavit objekt kamerovým systémem | 0.20 | 4 | 0,8 | 4,2 |
| | Spolupráce | 0.15 | 3 | 0,45 | |
| | Modernizace oken | 0.25 | 5 | 1,25 | |
| | Modernizace vstupních dveří | 0.25 | 5 | 1,25 | |
| | Aktivní přístup zaměstnanců | 0.15 | 3 | 0,45 | |
| **Hrozby** | Vloupání | 0.25 | -5 | -1,25 | -4,4 |
| | Vandalismus | 0.25 | -5 | -1,25 | |
| | Požár | 0.20 | -4 | -0,8 | |
| | Živelní pohromy | 0.20 | -4 | -0,8 | |
| | Terorismus | 0.10 | -3 | -0,3 | |
| **Součet za vnitřní prostředí** | | **0,1** | | | |
| **Součet za vnější prostředí** | | -0,2 | | | |
| **Celkem** | | 0,35 | | | |

Zdroj: [21]




Obr. 5 Vyhodnocení SWOT analýzy pro plášťovou ochranu. Zdroj:[vlastní]

Zhodnocení SWOT analýzy vychází ze strategií, které vznikají spojením vybraných kvadrantů. Z grafu SWOT analýzy pro plášťovou ochranu objektu, můžeme vyčíst, že výsledkem je strategie likvidace.

Strategie řeší kumulaci nepříznivých předpokladů a zaměřuje se na minimalizaci negativních efektů. Vzhledem k tomu, že finanční prostředky nejsou překážkou, může dojít k modernizaci starších komponentů, v rámci plášťové ochrany se tedy bude jednat především o novější detektory.

Neopomeneme v rámci projektové části této práce navrhnout adekvátní kamerový systém, který dopomůže k lepší orientaci, jaké osoby se zdržují v blízkých prostorách objektu, což dopomůže k odrazení pachatele jak při vloupání, tak i v případě vandalismu.

Jedinou překážku vidím v systému, který nařizuje výběrová řízení. Díky tomu se nemusí podařit, vše, co bude v projektu naplánováno.

### 7.2.2 Prostorová ochrana

V následující tabulce je SWOT analýza rozvržena stejně tak, jako v předchozí podkapitole.

Tab. 5 SWOT analýza - soupis jednotlivých složek

| | Silné stránky | Slabé stránky |
|---|---|---|
| Vnitřní prostředí | Finanční prostředky | Absence systému kontroly vstupu |
| | Střežení objektu pomocí agentury | Stáří komponentů |
| | Dveřní systém | Výběr komponentů omezen cenou |
| | Detektory narušení | Absence EPS |
| | EZS | Nutnost výběrového řízení pro bezpečností komponenty |
| | **Příležitosti** | **Hrozby** |
| Vnější prostředí | Vybavit objekt PZS | Krádež |
| | Spolupráce | Vandalismus |
| | Modernizace detektorů | Požár |
| | Modernizace dveří | Živelní pohromy |
| | Aktivní přístup zaměstnanců | Terorismus |

Zdroj: [21]

K silným stránkám pro prostorovou ochranu přispívá dveřní systém v kombinaci s vnitřními detektory narušení, které sice nejsou nejnovější, ale i přesto můžou dobře posloužit jako překážka pro případného pachatele. Za velmi významný považuji elektronický zabezpečovací systém propojený s ústřednou agentury GAN, což funguje následujícím způsobem. S vedením objektu je agentura smluvně domluvena na večerním střežení budovy – to znamená, že od osmé hodiny večerní do sedmé hodiny ráno agentura hlásí vedení objektu jakýkoliv pohyb v objektu. I přes toto opatření by byl vhodný systém

kontroly vstupu, jehož nepřítomnost je řazena k slabým stránkám systému. Další silnou stránkou se jeví být i finanční prostředky, které se vedení nebrání vynaložit pro zdokonalení stávajícího systému. Problém nastává v systému státní správy, kdy je vedení nuceno pro vynaložení vyšších výdajů vypsat výběrové řízení a v něm zvolit nejnižší cenovou nabídkou. Velmi podstatnou slabou stránkou je absence elektrické požární signalizace. V tak staré budově je tento systém více než žádaný, nemusí se přitom jednat ani o úmyslný požár.

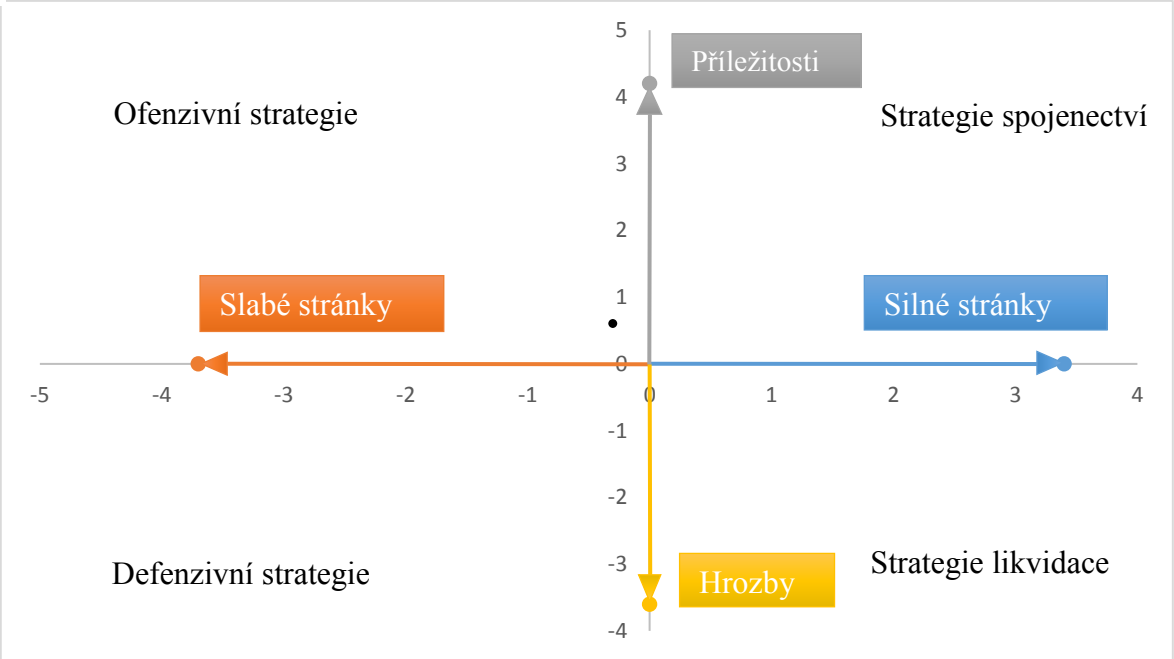
Jako zásadní příležitost se zde zcela nepochybně jeví vybavení objektu elektrickou požární signalizací. Do příležitostí lze zařadit i modernizaci detektorů narušení a dveřního systému. Je potřeba si uvědomit, že tyto příležitosti svým způsobem zasahují do slabých stránek, protože je potřeba vypsat výběrové řízení pro tyto komponenty. I přesto není důvod k obavám. Velkou příležitostí je i spolupráce vedení, bez kterého by projekt nemohl vůbec začít. Nelze opomenout ani aktivní přístup zaměstnanců.

Nejvýznamnějšími hrozbami se zde jeví být krádež a požár. Krádež by mohla vyústit v odcizení materiálů, které by mohly být následně zneužity, obzvláště v době rostoucí kybernetické kriminality. Citlivost materiálů v objektu je poměrně vysoká, tomu musí odpovídat i navržené opatření. Naproti tomu požár, ať už úmyslný nebo neúmyslný, je velmi pravděpodobnou záležitostí. Jedná se o starší budovu, v objektu nejsou vytvořené nové rozvody elektřiny, takže z tohoto hlediska může dojít k požáru opravdu lehce. Úmyslný požár pravděpodobně nehrozí ze strany zaměstnanců, ale je to reálná hrozba, došlo by k úplné ztrátě materiálů, ale i technologiím. Z hlediska vandalismu by mohlo dojít k poškození materiálů s vratnými či nevratnými materiálními změnami. Živelné pohromy jsou rizikem vždy, může dojít k velkému dešti, střecha bude prosakovat vodu do objektu. To zapříčiní zničení materiálů, popřípadě technologií, nebo také požár. Na posledním místě, ale opět nikoliv z hlediska významnosti dopadů, byl uveden terorismus.

Tab. 6 SWOT analýza – složky s váhami a hodnocením

| Typ | Složka | Váha | Hodnocení | Součin | Součet |
|---|---|---|---|---|---|
| **Silné stránky** | Finanční prostředky | 0.20 | 4 | 0,8 | 3,4 |
| | Střežení objektu agenturou | 0.10 | 5 | 0,5 | |
| | Dveřní systém | 0.25 | 3 | 0,75 | |
| | Detektory narušení | 0.25 | 3 | 0,75 | |
| | EZS | 0.20 | 3 | 0,60 | |
| **Slabé stránky** | Absence systému kontroly vstupu | 0,15 | -3 | -0,45 | -3,7 |
| | Stáří komponentů | 0,25 | -4 | -1 | |
| | Výběr komponentů omezen cenou | 0,15 | -3 | -0,45 | |
| | Absence PZS | 0,30 | -5 | -1,5 | |
| | Nutnost výběrového řízení pro bezpečnostní komponenty | 0,15 | -2 | 0,3 | |
| **Příležitosti** | Vybavit objekt PZS | 0,20 | 5 | 1 | 4,2 |
| | Spolupráce | 0,20 | 3 | 0,6 | |
| | Modernizace detektorů | 0,20 | 5 | 1 | |
| | Modernizace dveří | 0,20 | 5 | 1 | |
| | Aktivní přístup zaměstnanců | 0,20 | 3 | 0,6 | |
| **Hrozby** | Krádež | 0,30 | -5 | -1,5 | -3,6 |
| | Vandalismus | 0,25 | -2 | -0,5 | |
| | Požár | 0,25 | -5 | -1,25 | |
| | Živelní pohromy | 0,15 | -2 | -0,3 | |
| | Terorismus | 0,05 | -1 | -0,05 | |
| **Součet za vnitřní prostředí** | | -0,3 | | | |
| **Součet za vnější prostředí** | | 0,6 | | | |
| **Celkem** | | **-0,9** | | | |

Zdroj: [21]




Obr. 6 SWOT analýzy pro prostorou ochranu. Zdroj:[vlastní]

Jak bylo avizováno v kapitole 7.1.1., zhodnocení analýzy vychází ze čtyř strategií, které vznikají spojením vybraných kvadrantů. Z grafu SWOT analýzy pro prostorovou ochranu lze vyčíst, že výsledkem je ofenzivní strategie.

Strategie využívá silné stránky na získání výhod. Což znamená, že můžeme využít finančních prostředků, jakožto jednu z hlavních silných stránek. Pomohou modernizovat stávající prostředky zabezpečení. Dalším krokem může být nákup nových komponent, které budou dále rozváděny v kapitole samotného projektu. Tyto komponenty nejen, že zdrží pachatele, ale mohou ho i zastavit v páchání činnosti, čímž eliminují dané hrozby.

# 8 PROJEKT ZABEZPEČENÍ VYBRANNÉHO OBJEKTU

Kapitola je věnována samotnému projektování zabezpečení vybraného objektu. Poslouží ke zmapování jednotlivých činností, které jsou spjaté s realizací projektu, posléze bude provedena analýza RIPRAN, pomocí které dojdeme ke kritickým místům projektu. Závěrem bude sestavena kompletní sestava komponentů, která by měla napomoci zlepšení stávajícího stavu.

Cílem projektu je navrhnout optimální sestavu zabezpečující vybraný objekt. Jedním ze základních úkolů bude komplexní prostudování vybrané problematiky, ze které bude plynout celý kontext řešeného projektu. Následně v rámci procesu řízení rizik identifikujeme možná hlavní nebezpečí, které podrobíme analýze rizik. Výstupem projektu bude navržení konkrétních komponent dle požadavků zadavatele, pro jejichž výběr bude brát zřetel na finanční stránku, požadavky zadavatele, snadnou instalaci, provoz a údržbu.

Provozovatel vybraného objektu si nepřeje být jmenován. Jedná se o objekt ochrany obyvatelstva, a tak by jeho zmíněním mohla být negativně ovlivněna zranitelnost tohoto objektu.

Projekt bude zabezpečovat celkem sedm zaměstnanců - manažer a dalších šest specializovaných pracovníků. Z hlediska technických prostředků zahrnuje čtyři mobilní telefony, čtyři notebooky, katalogy dodavatelů, kancelářské potřeby, automobil, projektovou dokumentaci budovy, softwarové vybavení, kontaktní osobu vybraného subjektu, přístup do objektu a technické vybavení.

Doba realizace je rozdělena celkem do tří fází- předprojektová fáze v délce trvání tři týdny, projektová fáze by měla zabrat rovněž tři týdny a poprojektová fáze v délce trvání dva týdny. Celková předpokládaná doba trvání projektu byla datována na 13. 2. – 17. 4. 2019.

Rizikem projektu se jeví být zejména jeho nákladová stránka v úvaze k úrovni nutného zabezpečení. Dalším rizikem je nedostatečné souznění mezi zpracovatelem a zadavatelem po stránce vhodnosti jednotlivých zařízení pro daný subjekt a z hlediska představy zadavatele. V neposlední řadě lze zmínit riziko nepřipravení dokumentace k realizaci projektu dle potřebných náležitostí.

Celkové předpokládané náklady činí cca 289 000 Kč. Zatímco přímé náklady tvoří 220 000 Kč, nepřímé náklady 60 000 Kč a ostatní náklady 9 000 Kč.

## 8.1 Přehled činností v projektu

Níže uvedený obrázek vyobrazuje všechny činnosti, které je zapotřebí realizovat pro naplnění cíle projektu. Dále zahrnuje délku jejich trvání v jednotkách dnů a začátek konkrétních činnosti i jejich konec.

| | Jméno | Trvání | Začátek | Konec | Předchůdci |
|---|---|---|---|---|---|
| 1 | Studium zakázky | 2 dní | 20.2.19 8:00 | 21.2.19 17:00 | |
| 2 | Cenový odhad | 1 den | 22.2.19 8:00 | 22.2.19 17:00 | 1 |
| 3 | Získání podkladů a nutné dok | 1 den | 25.2.19 8:00 | 25.2.19 17:00 | 1 |
| 4 | Studium podkladů a dokumer | 2 dní | 26.2.19 8:00 | 27.2.19 17:00 | 1 |
| 5 | Analýza rizik | 2 dní | 28.2.19 8:00 | 1.3.19 17:00 | 2;3;4 |
| 6 | Vytvoření prvotního návrhu | 3 dní | 4.3.19 8:00 | 6.3.19 17:00 | 5 |
| 7 | Konzultace návrhu | 1 den | 7.3.19 8:00 | 7.3.19 17:00 | 5 |
| 8 | Nezbytné úpravy dle návrhu | 1 den | 8.3.19 8:00 | 8.3.19 17:00 | 5 |
| 9 | Konzultace úprav | 1 den | 11.3.19 8:00 | 11.3.19 17:00 | 8 |
| 10 | Schválení návrhu | 1 den | 12.3.19 8:00 | 12.3.19 17:00 | 9 |
| 11 | Nákup vybavení | 2 dní | 13.3.19 8:00 | 14.3.19 17:00 | 10 |
| 12 | Montáž | 5 dní | 15.3.19 8:00 | 21.3.19 17:00 | 11 |
| 13 | Proškolení obsluhy | 1 den | 22.3.19 8:00 | 22.3.19 17:00 | 12 |
| 14 | Zkušební provoz | 6 dní | 25.3.19 8:00 | 1.4.19 17:00 | 10 |
| 15 | Předání zakázky | 1 den | 2.4.19 8:00 | 2.4.19 17:00 | 13;14 |
| 16 | Ostrý provoz | 10 dní | 3.4.19 8:00 | 16.4.19 17:00 | 15 |
| 17 | Revize zařízení | 1 den | 17.4.19 8:00 | 17.4.19 17:00 | 16 |
| 18 | Servis zařízení | 1 den | 17.4.19 8:00 | 17.4.19 17:00 | 16 |
| | | | | | |

Obr. 7 Přehled činností v projektu. Zdroj:[vlastní]

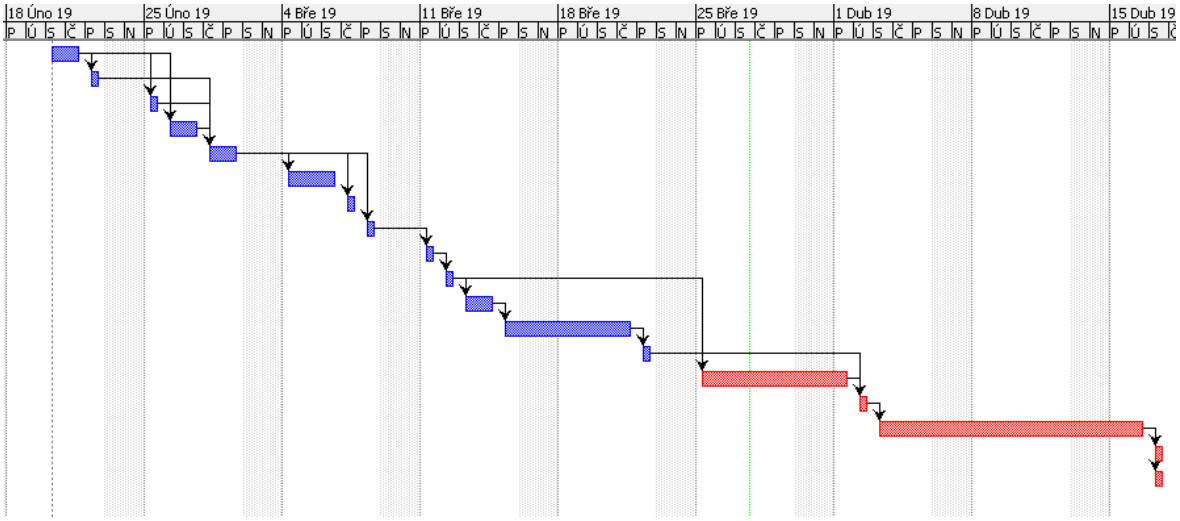
Z obrázku lze také vyčíst, jaké činnosti jsou na sobě závislé v rámci jejich uskutečnění (sloupec Předchůdci). Pro projekt bylo vytyčeno celkem 18 činností, které musejí být provedeny ve stanovené lhůtě, a to během 57 dnů (zhruba 8 týdnů). K jednotlivým činnostem byl vyhrazen potřebný čas ve formě dnů pro jejich splnění. Stanovená doba plnění konkrétní činnosti se odvíjí od vymezeného času pro celkový projekt a od minimálního potřebného reálného času provedení konkrétní činnosti. Většina uvedených činností potřebuje pro své uskutečnění jeden, případně dva dny. Avšak existují čtyři výjimky, kdy je na splnění činnosti zapotřebí věnovat větší časový interval, např. na činnost „Ostrý provoz“ bylo vymezeno až 10 dnů nebo na „Montáž“ 5 dní. Začátek projektu je datován k 20. únoru 2019 a konec je naplánován na 17. dubna 2019.

## 8.2 Ganttův diagram

Tento druh pruhového diagramu je využíván v řízení a při plánování projektů ke grafickému znázornění naplánování posloupnosti po sobě jdoucích činností v čase.

Na horizontální ose Ganttova diagramu je časové období trvání projektu rozdělené do stejně dlouhých časových jednotek (dny a týdny/měsíce). Projekt je vymezen v časovém období od 20. 2. 2019 do 17. 4. 2019. Na vertikální ose jsou pak uvedeny jednotlivé činnosti, na které se projekt člení. Jeden řádek je určen k fungování vždy jedné činnosti.

Plocha diagramu nám zobrazuje (viz následující obrázek) jednotlivé činnosti, které jsou označeny různě dlouhými obdélníky, kde levá strana poukazuje na plánovaný začátek činnosti a pravá strana určuje plánované ukončení. Různorodá délka obdélníkových pruhů označuje předpokládanou dobu trvání činnosti. Zobrazené čáry s šipkami v obrázku vedou vždy od začátku či konce činnosti jedné k činnosti druhé. Diagram dále může zobrazit data a délku konání jednotlivých činností a jména zdrojů (v tomto případě je to manažer, analytik, nákupčí, projektant, technici a servis), kteří na činnostech pracovali nebo se na práci nějak podíleli (z důvodu obsáhlého textu, který by působil zmatečně, proto v následujícím obrázku nejsou zobrazeny termíny a délka konání). [23]




Obr. 8 Ganttův diagram. Zdroj:[vlastní]

Diagram nám dále může zobrazovat kritickou cestu realizovaného projektu. Červená barva vyznačuje tzv. kritické činnosti projektu. Pod kritickou činností si lze představit činnost, která nemá žádnou časovou rezervu, a pokud se prodlouží délka jejího trvání, zpozdí se celý projekt. Modrá barva vyznačuje činnosti, které jsou vybaveny dostatečně velkou

časovou rezervou, tzn., že se činnosti mohou opozdit. Mezi činnosti, které mají zajištěnou dostatečnou časovou rezervu, patří studium zakázky, cenový odhad, získání podkladů a potřebných dokumentů, studium podkladů a dokumentů, analýza rizik, vytvoření prvotního návrhu, konzultace návrhu, nezbytné úpravy dle návrhu zadavatele, konzultace úprav, schválení návrhu, nákup vybavení, montáž a proškolení obsluhy.

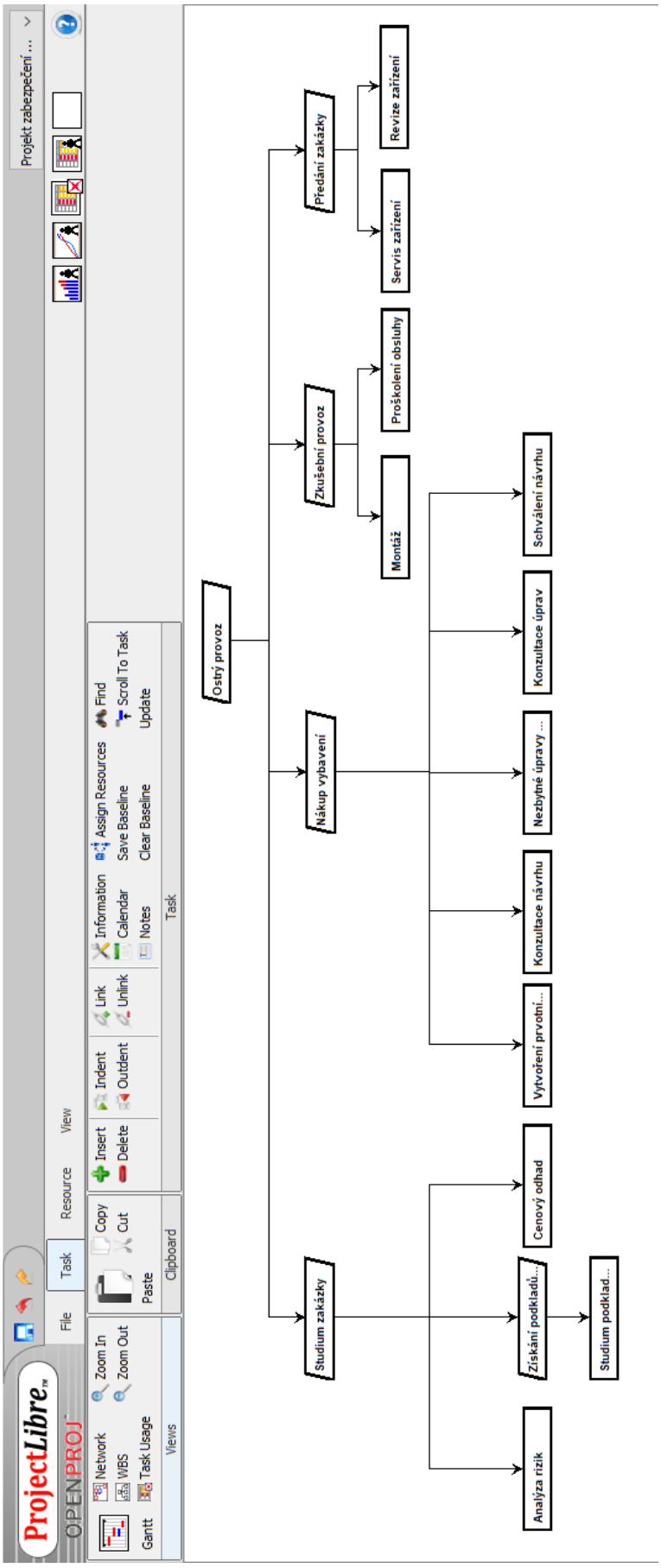
## 8.3 Work Breakdown Structure (WBS)

WBS je dokument, který se snaží vyobrazit postupně rozložené cíle projektu, které jsou rozděleny na jednotlivé výsledky, produkty a podprodukty směřující až k finální pracovní činnosti, které se při plánování projektu vytvoří.

Projekt WBS je realizován na zabezpečení vybraného objektu, který je následně rozdělován v důsledku navazování činností. Postupuje se z levé strany - od první k poslední činnosti. Jako start realizace je považován ostrý provoz, u kterého je potřebné studium zakázky. To je dále rozděleno na analýzu rizik, cenový odhad a získání podkladů, u kterých je třebařádné prostudování.

Následnoufází projektu je nákup vybavení, u kterého musí být prokonzultován jak jejich návrh, tak případné úpravy. V případě nejasností budou probíhat nezbytné úpravy dle návrhu a poté následuje jeho schválení.

Dalším bodem je zkušební provoz, v průběhu kterého probíhá montáž zakázky a následné proškolení obsluhy.V poslední části dochází ke konečnému předání zakázky. Do této fáze patří iservis zařízení a v určitých intervalech i k jeho revizi.




Obr. 9 Hierarchizace činností v projektu Zdroj:[vlastní]

## 8.4 RIPRAN

RIPRAN představuje empirickou metodu pro analýzu rizik projektů (se zaměřením na střední a velké projekty). Vychází z procesního pojení analýzy rizik, analýzu jednotlivých rizik tedy chápe jako posloupnost procesů, přičemž každý proces má jasně definovány vstupy, výstupy a činnosti procesů, transformující vstupy na výstupy s určitým cílem. Slouží k prvotnímu zkoumání, což samozřejmě neznamená, že bychom neměli s riziky pracovat v průběhu celého projektování. [24]

Celá analýza je rozdělena do následujících fází:

- příprava,
- identifikace,
- kvantifikace,
- návrh opatření snižující nebo eliminující vliv rizik na projekt,
- celkové zhodnocení rizikovosti projektu,
- sledování a vyhodnocování rizik v průběhu projektu. [24]


Obr. 10 Jednotlivé fáze metody RIPRAN. Zdroj:[24]

V tomto projektu byly využity pouze čtyři základní kroky a to:

1. Identifikace nebezpečí projektu.
2. Kvantifikace rizik projektu.
3. Reakce na rizika projektu.
4. Celkové posouzení rizik.

**Krok 1**

V tomto kroku jsou identifikována nebezpečí za pomoci sestavení seznamu. Text v řádku získáme buď tím, že k hrozbě hledáme možné následky nebo ke scénáři hledáme jeho příčinu. Hrozbou se rozumí konkrétní projev nebezpečí. Scénářem je pak myšlen děj, který nastane v důsledku výskytu hrozby. Je důležité si uvědomit, že hrozba je příčinou scénáře. [23],[24]

Tab. 7 První krok metody RIPRAN

| P. č. | Hrozba | Scénář | Poznámka |
|---|---|---|---|
| 1. | Nedostatečné informace | Špatný cenový odhad | Nedostatečná komunikace |
| 2 | Chybná analýza rizik | Zpoždění projektu, ztráta projektu | Špatná volba vybavení |
| 3. | Ztráta dokumentů | Zpoždění projektu, ztráta projektu | Ztráta důvěry |
| 4. | Průtahy při konzultaci projektu | Zpoždění projektu | Neustálé změny zadavatele, nedostatečná komunikace |
| 5. | Zpoždění dodávky materiálu | Zpoždění projektu | |
| 6. | Odcizení dodávky materiálu | Zpoždění projektu | |
| 7. | Špatná instalace vybavení | Přesčas, popřípadě zpoždění projektu | |
| 8. | Zvýšená nemocnost | Psychická a fyzická náročnost ostatních zaměstnanců | |
| 9. | Ukončení projektu ze strany zadavatele | Ztráta finančních prostředků, dluhová tíseň | |
| 10. | Nedostatek finančních zdrojů | Dluhová tíseň a ztráta projektu | |

Zdroj: [vlastní]

**Krok 2**

Při druhém kroku se provádí kvantifikace rizika. Tabulka, která byla vytvořena v prvním kroku, se nyní rozšíří o pravděpodobnost výskytu scénáře, hodnotu dopadu scénáře na projekt a výslednou hodnotu rizika, která je dána výpočtem:

*Hodnota rizika = pravděpodobnost scénáře x hodnota scénáře*

Metoda umožňuje jak číselnou kvantifikaci, tak i takzvanou verbální kvantifikace, při níž se využívá slovního hodnocení. Pro tuto analýzu byla využita číselná kvantifikace. [24], [25]

Tab. 8 Druhý krok metody RIPRAN

| P. č. | Hrozba | Scénář | Poznámka | Pravděpodobnost | Dopad (Kč) | Hodnota rizika (Kč) |
|---|---|---|---|---|---|---|
| 1. | Nedostatečné informace | Špatný cenový odhad | Nedostatečná komunikace | 50 % | 300 000 | 150 000 |
| 2 | Chybná analýza rizik | Zpoždění projektu, ztráta projektu | Špatná volba vybavení | 40% | 150 000 | 60 000 |
| 3. | Ztráta dokumentů | Zpoždění projektu, ztráta projektu | Ztráta důvěry | 30% | 400 000 | 120 000 |
| 4. | Průtahy při konzultaci projektu | Zpoždění projektu | Neustálé změny zadavatele, nedostatečná komunikace | 50% | 150 000 | 75 000 |
| 5. | Zpoždění dodávky materiálu | Zpoždění projektu | x | 70% | 100 000 | 70 000 |
| 6. | Odcizení dodávky materiálu | Zpoždění projektu | x | 20% | 300 000 | 60 000 |
| 7. | Špatná instalace vybavení | Přesčas, popřípadě zpoždění projektu | x | 40% | 250 000 | 100 000 |

| P. č. | Hrozba | Scénář | Poznámka | Pravděpodobnost | Dopad (Kč) | Hodnota rizika (Kč) |
|---|---|---|---|---|---|---|
| 8. | Zvýšená nemocnost | Psychická a fyzická náročnost ostatních zaměstnanců | x | 30% | 200 000 | 60 000 |
| 9. | Ukončení projektu ze strany zadavatele | Ztráta finančních prostředků, dluhová tíseň | x | 40% | 400 000 | 160 000 |
| 10. | Nedostatek finančních zdrojů | Dluhová tíseň a ztráta projektu | x | 25% | 350 000 | 87 500 |

Zdroj: [vlastní]

**Krok3**

Třetí krok složí k sestavení opatření, která mají snížit hodnotu rizika na akceptovatelnou úroveň. [24], [25]

Tab. 9 Třetí krok metody RIPRAN

| P. č. | Návrh opatření | Předpokládané náklady (Kč) | Termín | Odpovědná osoba | Nová hodnota rizika |
|---|---|---|---|---|---|
| 1. | Propracované vstupní šetření | 10 000 | 20. 2. | Michaela Zelená | 0 |
| 2. | Neustálé prověřování odbornosti | 11 000 | měsíčně | Lucie Jurasová | 5 000 |
| 3. | Řízení bezpečnosti informací | 30 000 | 2x ročně | Lucie Jurasová | 5 000 |
| 4. | Striktní dodržení časového plánu | 0 | 20. 2. | Alexandra Vicjanová | 0 |
| 5. | Včasná objednávka materiálu, zvolení ověřeného dodavatele | 0 | 13. 3. | Michaela Zelená | 0 |
| 6. | Dostatečné zabezpečení dodávky materiály | 2 500 | 13. 3. | Kristýna Benešová | 0 |
| 7. | Neustálé zvyšování kvalifikace zaměstnanců | 10 000 | 2x ročně | Alexandra Vicjanová | 2 000 |

| P. č. | Návrh opatření | Předpokládané náklady (Kč) | Termín | Odpovědná osoba | Nová hodnota rizika |
|---|---|---|---|---|---|
| 8. | Povinné lékařské prohlídky, doplňky stravy | 500 | 1x ročně | Kristýna Benešová | 100 |
| 9. | Prověření zadavatele | 0 | 20. 2. | Kristýna Benešová | 0 |
| 10. | Finanční rezervy | 500 000 | celoročně | Michaela Zelená | 0 |

Zdroj:[vlastní]

**Krok 4**

V tomto kroku je posuzována celková hodnota rizika. Dochází k vyhodnocení, jaká je míra rizika a zda je možné pokračovat v realizaci projektu i bez zvláštních opatření. V okamžiku, kdy tým shledá celkovou úroveň rizika za velmi vysokou, problém je postoupen k řešení na vyšší úroveň řízení. Z této skutečnosti vyplývá, že metoda vyžaduje práci s podrobným rozborem hrozeb, scénářů, hodnot pravděpodobností a hodnot dopadů. Proto je složitější, pracnější a vyžaduje určité znalosti v dané oblasti. Na druhou stranu přináší pro projekt mnohem přesnější výsledky analýzy rizik. [23]

Projekt lze na základě výsledků považovat za mírně rizikový, tudíž nejsou identifikovány překážky k další realizaci projektu.

## 8.5 Návrhová opatření

Návrhová opatření vyplývají z předcházející analýzy rizik, která zjistila riziková místa vybraného objetu. Pro tato místa bude rozpracován podrobný popis zavedených komponentů.

Po dlouhodobém mapování firem, které se věnují oblasti zabezpečovacích komponentů, bylo vyhodnoceno, že firem, jež by z hlediska zaměření své činnosti připadaly v úvahu, je hned několik. Předmětem zkoumání byl především přístup k zákazníkovi, sortiment – kvalita i četnost komponentů, historie firmy, ohlasy předešlých zákazníků a v neposlední řadě propojenost jednotlivých komponentů. Proto byla vybrána firma, jejíž pověst jí přechází. Firma Jablotron má svou dlouhou historii, na českém trh působí od roku 1990, tedy 29 let. Na počátku disponovala pouze čtyřmi zaměstnanci (zakladateli), kteří vyvíjeli elektroniku. V dnešní době se jedná o firmu s celosvětovou působností, vzhledem k tomu, že

své výrobky vyváží do 73 zemí po celém světě. Každoročně jsou komponenty a systémy firmy oceňovány na prestižních veletrzích po celém světě. [26]


Obr. 11 Bezpečnost ve čtyřech krocích. Zdroj:[26]

Bezpečnost ve čtyřech krocích

Základem je kvalitní český alarm, který se snadno ovládá. Následující krok představuje montáž certifikovaným technikem, který je firmou v pravidelných intervalech školen, tedy je zde jistota, že vše bude fungovat na 100 %, již od počátku. Pokračuje připojením alarmu na firemní pult centrální ochrany, vyškolení pracovníci nepřetržitě střeží objekt. Pokud alarm spustí poplach, ihned vysílají zásahovou jednotku ke střeženému objektu, což je poslední krok. [26]

Firma Jablotron dále nabízí vlastní webovou aplikaci – lze jí ovládat pomocí klávesnice se segmenty, mobilní aplikací, počítačovou aplikací nebo klíčenkou. Díky ní lze ovládat zabezpečovací systém na dálku, kromě toho lze:

- mít přehled o všech zařízeních,

- ovládat alarm stejně, jako pomocí klávesnice,
- zobrazit foto z detektorů v jednotlivých místnostech,
- sledovat teplotu nebo spotřebu energie. [26]

Firma nabízí v rámci kamerových systémů momentálně hned dvě nejmodernější provedení, a to buď JI – 111C nebo JI – 112C. Přičemž oba komponenty jsou si velmi podobné, liší se pouze úhlem záběru a dosahem IR přísvitu. Záleží na preferencích, vzhledem k tomu, že JI-111C má větší úhel záběru, a to 115°, ale s dosahem IR přísvitu 30m. Zatímco JI – 112C má úhel záběru 90°a dosah IR přísvitu 50m. [27], [28]


Obr. 12 JI – 111C. Zdroj:[27]


Obr. 13 JI – 112C. Zdroj:[28]

Základní funkcí těchto kamer je videosekvence – automatický záznam 30s před poplachem a 30s po poplachu. Nabízí zpětný záznam na tři až sedm dní s přehledem poplachů. Dále živé video z kamery, které lze spustit kdykoliv, a tím i ověřit nastalou situaci. Disponují barevným videem s rozlišením Full HD. Dalším kladem je velmi snadná instalace, která trvá jen několik minut - umístit je lze jak ve venkovních, tak i ve vnitřních prostorách. Kamerový systém je propojený s alarmem, takže reaguje na jeho stav, ať už v případě poplachu, zajištění nebo odjištění objektu. Uživatel obdrží z každé události minutový záznam, dostupný i v aplikaci. Pokud je objekt připojen k bezpečnostnímu centru, což se doporučuje, operátoři se o vše postarají. [27], [28]

Pokud jde o alarmy, existuje široká škála zařízení. Jako jedno z nejlepších variant se jeví JA – 114E neboli sběrnicový přístupový modul s displejem, klávesnicí a RFID. Jedná se o přístupový modul s LCD displejem, ovládacími klávesami a čtečkou RFID, pro ovládání zabezpečovacího systému. Obsahuje jeden ovládací segment, je však možné rozšíření až na dvacet ovládacích segmentů. Umožňuje jednoduché ovládání zabezpečovacího systému,

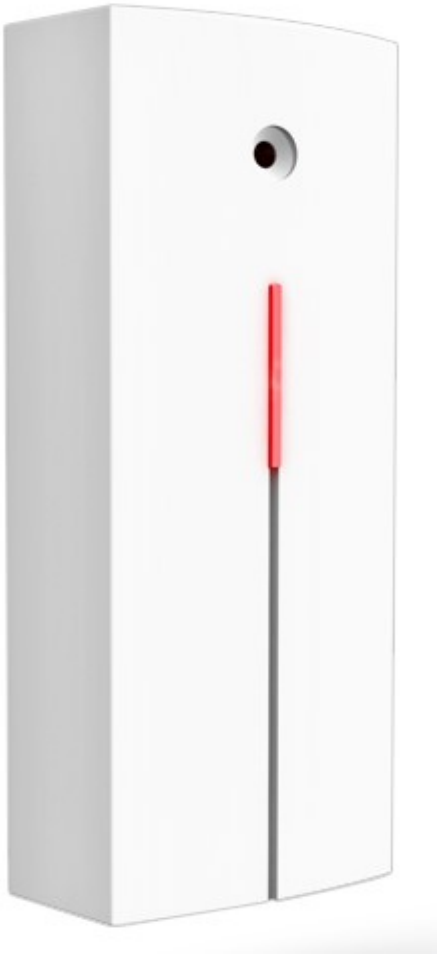
komunikuje prostřednictvím sběrnice a je z ní též napájen. Modul disponuje funkcí úspory energie i během výpadku napájení. Modul je adresovatelný a obsahuje jednu pozici v zabezpečovacím systému, nabídka menu umožňuje pohodlné ovládání a správu jednotlivých sekcí, zón a v neposlední řadě i zprávy o událostech. Napájen je ze sběrnice ústředny v rozsahu od 9 do 15V. Proudová spotřeba při záloze (klidová) je 15mA, přičemž proudová spotřeba pro volbu kabelu je 50 mA, frekvence RFID je 125 kHz. [29]


Obr. 14 alarm JA – 114E. Zdroj:[29]

Dále bude využita kombinace pohybového detektoru a detektoru rozbití skla. JA – 111P – WW sběrnicový PIR detektor pohybu slouží k detekci pohybu osob v interiérových prostorách budov. Garantované detekční pokrytí je 90°/12m. Detektor je výsledkem velmi vysokých kvalitativních cílů. Kromě standardního rohového umístění je možné provést montáž na plochu stěny do estetického rámečku. Částečně je tedy zapuštěn a splývá se stěnou. Pro speciální aplikace, jako je třeba montáž na strop, je detektor vybaven kloubovým držákem. Disponuje pulzní aktivací, kterou lze ovládat programovatelné výstupy. Odolnost vůči falešným poplachům je nastavitelná ve dvou úrovních. Přístroj je napájen ze sběrnice ústředny 12 V, doporučená instalační výška je 2,5m nad úrovní podlahy, detekční okrytí je 90°/12m s teplotním rozsahem -10 °C až +40 °C. [30]

Sběrnicový akustický detektor rozbití skla JA – 110B rozpozná rozbíjení skleněných výplní, a to nejen oken, ale i dveří. Detekce je založena na duální technologii, což znamená, že detekuje změny tlaku ve vzduchu provázené charakteristickým zvukem rozbíjení skla.

Obr. 15 detektor pohybu. Zdroj:[30]



Obr. 16 Detektor rozbití skla. Zdroj:[31]

Citlivost je samozřejmě nastavitelná. Komunikuje se sběrnicí ústředny a je z ní také napájen. Detektor je adresovatelný a obsahuje v zabezpečovacím systému jednu pozici. Poskytuje vizuální ověření spuštěného detektoru přes LED kontrolku. Doporučená instalační výška je 2,5m nad úrovní podlahy s detekční vzdáleností do 9m. Napájení je realizováno ze sběrnice ústředny 12 V. [31]

Dalším komponentem pro zabezpečení je bezdrátový kombinovaný detektor kouře a teploty se sirénou JA – 151ST. Slouží k detekci požárního nebezpečí v interiéru. Detektor je napájen ze tří baterií AA, k montáži je potřeba proškolený technik. Vznik nebezpečí detektoru indikuje opticky zabudovanou signálkou a akustickým signálem. Výrobek obsahuje dva samostatné detektory (kouře a teploty). Detektor kouře pracuje na principu

rozptýlení světla, je velmi citlivý, detekuje i nejmenší částice, které jsou obsaženy především v hustých dýmech. Méně citlivý je na malé částice, které vznikají hořením kapalin. Proto se společně s ním instaluje i detektor teplot, který má sice pomalejší reakci, ale na požár vyvíjející rychle teplo s malým množstvím kouře je ideální. Poplachová teplota je +60 °C až +65 °C, komunikační dosah je cca 300 m, typická životnost jsou 3 roky. [32]

Obr. 17 Detektor kouře a teploty. Zdroj:[32]


Obr. 18 Záplavový detektor. Zdroj:[33]

Záplavový detektor JA – 110F slouží k indikaci zaplavení prostor vodou. Informaci přenáší do zabezpečovací ústředny po sběrnici. Ve chvíli, kdy je elektroda zaplavena vodou, vyšle signál aktivace, přičemž signál zklidnění je vyslán, pokud skončí zaplavení elektrod. Napájení je řešeno prostřednictvím sběrnice ústředny 12 V, detektor reaguje na zaplavení vodou, jeho rozsah pracovních teplot je -10 °C až + 40 °C. [33]

Ústředna JA – 101KR – LAN je základním prvkem zabezpečovacího systému. Umožňuje flexibilní nastavení a snadnou ochranu nejen kancelářských prostor ve sběrnicovém provedení, ale i v bezdrátovém, popřípadě kombinovaném provedení. Ústředna nabízí až 50bezdrátových nebo sběrnicových zón, až 50 uživatelských kódů, až 8 sekvencí, 16 programových výstupů, 20vzájemně nezávislých kalendářů, SMS a hlasové reporty ze systému až osmi uživatelům, umožňuje vzdálené ovládání přes SMS, hlasové menu a aplikaci. Ústředna má vestavěné GSM/GPRS a LAN komunikátory, které umožňují

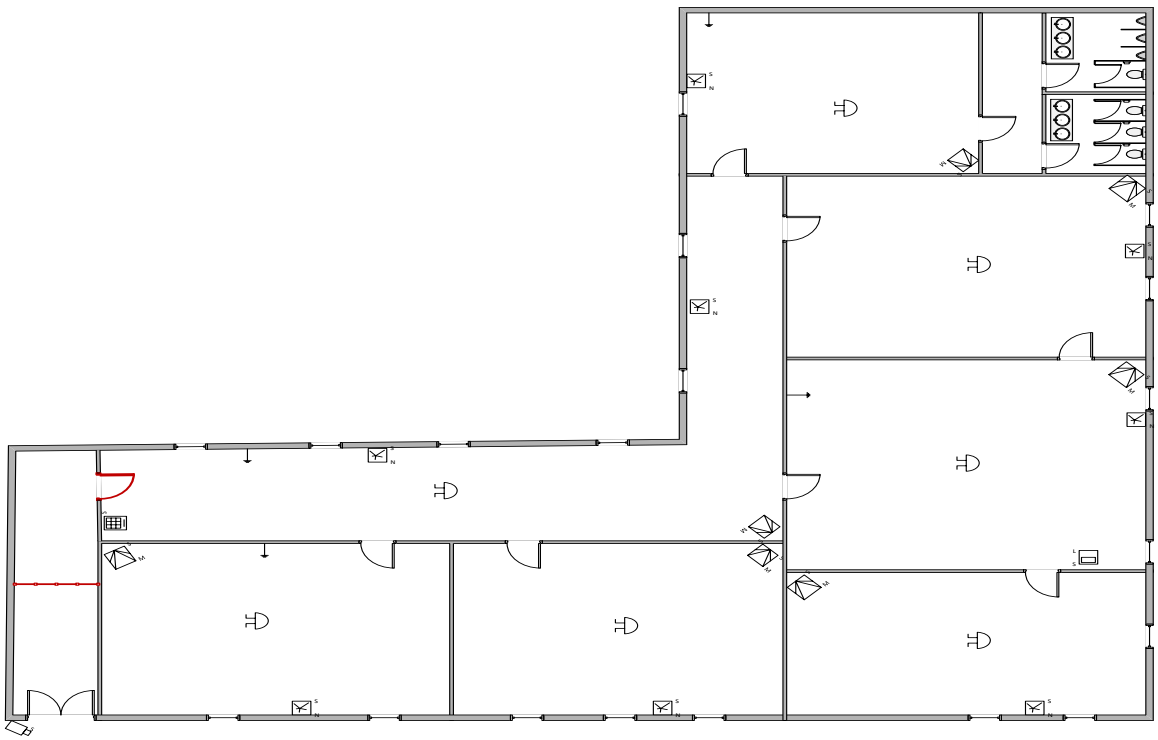
hlasovou komunikaci s koncovými uživateli nebo středisky PCO. Vybavena je i 4 GB paměťovou kartou pro uchování dat událostí, hlasových zpráv a snímků. [34]

Obr. 19 Ústředna JA – 101KR – LAN. Zdroj:[34]

V neposlední řadě je důležité zařadit i bezpečnostní dveře SHERLOCK. Disponují vnitřní výztuhou k ocelové konstrukci s rámem a svařovanou ocelovou dvouplášťovou konstrukcí. Přední i zadní ocelová deska je vybavena tepelně – zvukově- izolační protipožární výplní. Aktivní jistící body jsou ovládané zámkem, zdvojené, navařené do rozvorového mechanismu, kde znásobují nejen bezpečnost, ale i odolnost dveří proti jejich vysazení, páčení, popřípadě vytlačení ze zárubně. Součástí jsou i jistící body - zdvojené a pevně uchycené k ocelové konstrukci. Závěs dveří disponuje vnitřním pouzdrem bez mazání. Certifikované bezpečností kování s překrytím chrání vložku proti odvrtání a vylomení. Bezpečnostní zámek ovládá celý rozvorový mechanismu - je chráněn krytem a štítkem proti odvrtání, páčení a jiným způsobem překonání. Důležitým prvkem dveří je i zamykací systém. Ideální je využití systému, který nepodporuje sériové vyrábění klíčů, nýbrž výrobce vytvoří přesný počet klíčů, se kterými zákazník obdrží jednu bezpečnostní kartu, bez níž nelze vyrobit kopii klíče pro dané dveře. [35]

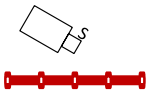
Obr. 20 Dveře Sherlock. Zdroj:[35]

Na dalším obrázku můžete vidět výsledné schéma, půdorysu vybraného objetu již s navrženými komponenty.



Obr. 21 Schéma rozložení navržených bezpečnostních opatření. Zdroj:[vlastní]

**Legenda:**

| Symbol | Komponent |
|---|---|
|  | Kamerový systém JI – 111C nebo JI – 112C |
| | mříž |
|  | Bezpečnostní dveře Sherlock |
|  | JA – 114E sběrnicový přístupový modul |
|  | Detektor pohybu JA – 111P – WW |
|  | Detektor rozbití skla JA – 110B |
|  | Detektor kouře a teploty JA – 151ST |
|  | Záplavový detektor JA – 110F |
|  | Ústředna JA – 101KR – LAN |

Z obrázku je patrné, že přístup do budovy je chráněn kamerovým systémem. Dalším prvkem jsou mříže. Červeně zbarvené dveře vyobrazují bezpečnostní dveře. Jde vidět, že každá místnost v objektu je vybavena detektorem pohybu, detektorem rozbití skla a detektorem kouře a teploty. Ve stěžejních místnostech je umístěn záplavový detektor. Celý prostor je střežen sběrnicovým přístupovým modulem. Celé to zastřešuje ústředna, která nejen, že ukládá, ale i sdílí všechny informace s dohledovým poplachovým a přijímacím centrem.

Na začátku projektu byla cena stanovena na 289 000 Kč, přičemž cena navržených komponentů se vyšplhá na 70 000 Kč, připočítat samozřejmě musíme, finanční ohodnocení pracovníků, kteří se podílejí nejen na montáži, ale i servisu. Mezi ostatní poplatky je důležité zahrnout i případné menší stavební práce. Vyčíslená hodnota projektu se tedy jeví, jako dostačující.

# ZÁVĚR

Na informační bezpečnost se dá nahlížet hned z několika různých pohledů, obecně však tento pojem zahrnuje řadu problémů a jejich řešení. Jedná se o zabezpečení sítě, fyzických spojů a serveru, kódování datových přenosů, dodržování interních směrnic, hodnocení, hodnotu a způsob ochrany firemních aktiv a mnoho dalších. Systém řízení bezpečnosti informací se netýká pouze průmyslových podniků a privátních organizací, týká se všech organizací včetně veřejných institucí a orgánů státu. Důkazem je existence mnoha národních, vládních a resortních usnesení doporučujících, popřípadě i vyžadujících zavedení systému řízení bezpečnosti informací v organizacích řízených a zřízených státem.

V teoretické části byla věnována pozornost především rešerši vztažných materiálů. Dále byl objasněn systém řízení bezpečnosti informací a dílčí jednotlivé oblasti, přičemž důraz byl kladen na fyzickou bezpečnost. Pozornost byla věnována i normativnímu rámci, jakožto základnímu atributu dané problematiky.

V praktické části bylo použito hned několik metod. V první řadě se jednalo o metodu sběru dat a informací, dále řízené rozhovory s vedením vybraného objektu. Další metodou bylo určení zdrojů ohrožení pomocí metod analýzy rizik. Prvotně byla provedena kvalitativní metoda s využitím jejich souvztažností (KARS). Z identifikovaných rizik (konkrétně z identifikovaných hrozeb) vyplynulo, jaký druh ochrany je nejvíce zranitelný - jednalo se o plášťovou a prostorovou ochranu. Pro podrobnější analýzu nejzranitelnějších druhů ochrany byla využita SWOT analýza, protože komplexně vyhodnotila všechny stránky fungování dvou kritických druhů ochran. Výstupem analýzy se stala ofenzivní strategie vztažená k prostorové ochraně a strategie likvidace týkající se plášťové ochrany. Dalším krokem bylo vytvoření samotného projektu realizování návrhových opatření. Byl představen sled činností potřebných k realizaci projektu a dále byla vypracována analýza RIPRAN, která vyhodnotila riziková místa projektu. Součástí projektu bylo stanovení návrhových opatření s konkrétními komponenty, které zabezpečí vybraný objekt a zvýší tím jeho odolnost. Jedná se o prvky, které lze mezi sebou propojit, tedy integrovat, což přispěje k efektivnějšímu zásahu proti jednotlivým druhům ohrožení. Jedná se o následující komponenty:

- Kamery JI - 111C, popřípadě JI - 112C - kamery se příliš neliší, proto záleží jen na výběru daného subjektu.

- Alarm JA - 114E, což je sběrnicový přístupný modul s LCD displejem, klávesnicí a RFID, z důvodu rozšíření až na dvacet ovládacích segmentů a jednoduchého ovládání.
- Dále byla využita kombinace detektorů rozbití skla JA - 110B (rozpozná rozbití skleněných tabulových výplní nejen oken, ale i dveří, což je důležité vzhledem k faktu, že vstupní dveře do objektu jsou skleněné) a detektor pohybu JA - 111P - WW (jeho výhodou je nejen rohová instalace s pokrytím 90°/12m, ale i zapuštění do estetického rámečku, který lze instalovat na plochu stěny, tím se z něj stává nenápadné zabezpečení). Citlivost obou zařízení je samozřejmě nastavitelná.
- Dalším komponentem je kombinovaný detektor kouře a teploty se sirénou JA - 151ST, který slouží k detekci požárního nebezpečí v interiéru. Záplavový detektor JA - 110F slouží k indikaci zaplavení prostor vodou, všechny informace přenáší do zabezpečovací ústředny po sběrnici. Celou sestavu zabezpečuje ústředna JA - 101KR - LAN, což je základní prvek zabezpečovacího systému, který umožňuje flexibilní nastavení a snadnou ochranu nejen kancelářských prostor ve sběrnicovém provedení. Firma, která byla vybrána, provádí zabezpečovací systém ve čtyřech krocích.
- Posledním krokem je napojení na ústřednu centrální ochrany.

Cílem diplomové práce bylo provedení analýzy stávajícího stavu bezpečnosti informací z hlediska fyzické bezpečnosti ve vybraném objektu a navržení opatření, která povedou ke zlepšení stávajícího stavu. Na základě výše uvedených výstupů z praktické části se lze domnívat, že cíl diplomové práce byl naplněn.

# SEZNAM POUŽITÉ LITERATURY

[1] DOUCEK, Petr, 2011. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing. ISBN 978-80-7431-050-8.

[2] *Technické normy ČSN* [online]. 2018 [cit. 2019-04-29]. Dostupné z: http://www.technicke-normy-csn.cz/.

[3] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-05-7.

[4] IVANKA, Ján. *Systematizace bezpečnostního průmyslu* [online]. Zlín, 2014 [cit. 2019-03-22]. ISBN 978-80-7454-410-1. Dostupné z: http://hdl.handle.net/10563/27488.

[5] Mechanické zábranné systémy. *Bezpečnostní poradce* [online]. Přerov, 2019 [cit. 2019-03-15]. Dostupné z: http://www.bepo.eu/shortcode/mzs.

[6] IVANKA, Ján. *Mechanické zábranné systémy*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 151 s. ISBN 978-80-7318-910-5.

[7] KINDL, Jiří. *Projektování bezpečnostních systémů*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007. ISBN 978-80-7318-554-1.

[8] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-57-6.

[9] UHLÁŘ, Jan, 2009. *Technická ochrana objektů*. 2. vyd. Praha: Policejní akademie České republiky v Praze. ISBN 978-80-7251-313-0.

[10] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-67-5.

[11] ČANDÍK, Marek. *Objektová bezpečnost II*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-731-8217-3.

[12] ČESKO. Nařízení vlády č. 522/2005 Sb. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2019 [cit. 21. 3. 2019]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-522.

[13] ČESKO. Zákon č. 412/2005 Sb. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2019 [cit. 21. 3. 2019]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412.

[14] ČESKO. Vyhláška č. 528/2005 Sb. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2019 [cit. 21. 3. 2019]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528.

[15] VALOUCH, Jan. [online]. Zlín, 2015 [cit. 2019-03-22]. ISBN 978-80-7454-557-3. Dostupné z: http://hdl.handle.net/10563/18616.

[16] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-19-4.

[17] LOVEČEK, Tomáš, Andrej VEĽAS a Martin ĎUROVEC. *Bezpečnostné systémy: poplachové systémy*. V Žiline: Žilinská univerzita, EDIS-vydavatel'ské centrum ŽU, 2015, 230 s. Vysokoškolské učebnice. ISBN 978-80-554-1144-6.

[18] URBAN, Miroslav. *Moderní dohledová poplachová a přijímací centra* [online]. 2019, 27.11.2017 [cit. 2019-04-12]. Dostupné z: https://www.tzb-info.cz/poplachove-a-zabezpecovaci-systemy/16607-moderni-dohledova-poplachova-a-prijimaci-centra-reprezentuji-vic-nez-jen-terminologickou-zmenu.

[19] *SÍŤOVÁ ANALÝZA A METODA KARS* [online], 2010. (1) [cit. 2018-04-08]. Dostupné z: http://www.population-protection.eu/prilohy/casopis/8/56.pdf.

[20] JELŠOVÁ, Katarína a Andrea PETERKOVÁ, 2013. *Řešení krizových situací - metody a jejich aplikace*. Opava. Projektu OPVK. Slezská univerzita v Opavě.

[21] *Applied Physics, System Science and Computers III: Proceedings of the 3nd International Conference on Applied Physics, Systém Science and Computers (APSAC2018), September 25-28, 2018, Dubrovnik, Croatia,* 2018. Springer. ISSN 978-3-319-75605-9.

[22] *SWOT analýza v Excelu* [online]. 2011 [cit. 2019-03-31]. Dostupné z: http://excel-navod.fotopulos.net/swot-analyza.html#SWOT_analyza_v_prakticke_ukazce.

[23] DOLEŽAL, Jan, Pavel MÁCHAL a Branislav LACKO. *Projektový management podle IPMA*. 2., aktualiz. a dopl. vyd. Praha: Grada, 2012. Expert (Grada). ISBN 978-80-247-4275-5.

[24] James Cadle a Donald Yeates, *Project Management forInformation Systems, pátá edice*, PearsEducation Limited, 2008, ISBN 978-0-13-206858-1.

[25] *RIPRAN: Metoda pro analýzu projektových rizik* [online]. [cit. 2019-03-31]. Dostupné z: https://ripran.cz/popis2.html.

[26] Bezpečí pro vaši firmu. *Jablotron* [online]. 2019 [cit. 2019-04-23]. Dostupné z: https://www.jablotron.com/cz/produkty/alarmy/alarm-do-kancelare/.

[27] JI-111C IP kamera vnitřní/venkovní 2MP - DOME. *Jablotron* [online]. 2019 [cit. 2019-04-23]. Dostupné z: https://www.jablotron.com/cz/produkt/ip-kamera-vnitrni-venkovni-2mp-dome-777/.

[28] JI-112C IP kamera vnitřní/venkovní 2MP - BULLET. *Jablotron* [online]. 2019 [cit. 2019-04-23]. Dostupné z: https://www.jablotron.com/cz/produkt/ip-kamera-vnitrni-venkovni-2mp-bullet-778/.

[29] JA-114E Sběrnicový přístupový modul s displejem, klávesnicí a RFID. *Jablotron* [online]. 2019 [cit. 2019-04-23]. Dostupné z: https://www.jablotron.com/cz/produkt/sbernicovy-pristupovy-modul-s-displejem-klavesnici-a-rfid-211/.

[30] JA-111P-WW Sběrnicový PIR detektor pohybu. *Jablotron* [online]. 2019 [cit. 2019-04-23]. Dostupné z: https://www.jablotron.com/cz/produkt/sbernicovy-pir-detektor-pohybu-604/.

[31] Detektor rozbití skla. *Jablotron* [online]. Praha [cit. 2019-04-07]. Dostupné z: https://www.jabloshop.cz/gbs-210-vivo-detektor-rozbiti-skla?gclid=Cj0KCQjwnKHlBRDLARIsAMtMHDFMg-Q64tKWLPNbaHZZOrBCowo1SCx2SQxHz_3xMYdoWJh9pvbN4xUaAlPVEALw_wcB#176.

[32] JA-151ST Bezdrátový kombinovaný detektor kouře a teploty se sirénkou. *Jablotron* [online]. 2019 [cit. 2019-04-23]. Dostupné z: https://www.jablotron.com/cz/produkt/bezdratovy-kombinovany-detektor-koure-a-teploty-se-sirenkou-400/.

[33] JA-110F Sběrnicový záplavový detektor. *Jablotron* [online]. 2019 [cit. 2019-04-23]. Dostupné z: https://www.jablotron.com/cz/produkt/sbernicovy-zaplavovy-detektor-295/.

[34] JA-101KR-LAN Ústředna s vestavěnými GSM/GPRS, LAN komunikátory a rádiovým modulem. *Jablotron*[online]. 2019 [cit. 2019-04-23]. Dostupné z:

https://www.jablotron.com/cz/produkt/ustredna-s-vestavenymi-gsm-gprs-lan-komunikatory-a-radiovym-modulem-436/.

[35] *SHERLOCK ASSA ABLOY* [online]. Praha, 2017 [cit. 2019-04-23]. Dostupné z: http://sherlock.cz/.

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|---|---|
| AWB | Automatic White Balance |
| BLC | Black Light Compensation |
| CCTV | Closed - Circuit Television |
| ČSN | České technické normy |
| ČSN EN | Evropské normy |
| ČR | Česká Republika |
| DIS | Digital Image Stabilization |
| DNR | Digital Noise Reduction |
| DPPC | Dohledová a Poplachová Přijímací Centrum |
| EPS | Elektrická Požární Signalizace |
| ESC | Electronic Shutter Control |
| EZS | Elektronické Zabezpečovací Systémy |
| GSM/GPRS | Groupe Spécial Mobile/General Packet Radio Service |
| IS/ICT | Information System/Information and Communication Technologies |
| ISMS | Information Security Management Systém |
| ISO | International Organization for Standardization |
| IT | Informační Technologie |
| IVA | Intelligent Video Content Analysi |
| LAN | Local Area Network |
| LCD | Liquid Crystal Display |
| LED | Light-emitting Diode |
| MD | Motion Detection |
| MW | Microwave Detectors |
| MZS | Mechanický Zábranný Systém |

| | |
|---|---|
| PCO | Pult Centralizované ochrany |
| PČR | Policie České Republiky |
| PIR | Passive Infared Receiver |
| PZM | Privacy Zone Masking |
| PZTS | Poplachové Zabezpečovací a Tísňové Systémy |
| RFID | Radio Frequency Identification |
| SKV | Systém Kontroly Vstupu |
| SMS | Short Message Service |
| WBS | Work Breakdown Structure |
| WDR | Wild Dynamic Range |

# SEZNAM OBRÁZKŮ

# SEZNAM TABULEK