Zabezpečení společenských akcí

Bc. Martin Džermanský

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. Martin Džermanský**
Osobní číslo:	**L17088**
Studijní program:	**N3953 Bezpečnost společnosti**
Studijní obor:	**Bezpečnost společnosti**
Forma studia:	**prezenční**
Téma práce:	**Zabezpečení společenských akcí**

Zásady pro vypracování:

1. **Seznamte se s teoretickými základy zabezpečovacích systémů.**
2. **Zaměřte se na problematiku jednotlivých bezpečnostních systémů.**
3. **Konkretizujte zvolenou společenskou akci/akce.**
4. **Navrhněte opatření pro zabezpečení společenských akcí.**
5. **Diskutujte získané výsledky.**

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

[3] IVANKA, J. Systemizace bezpečnostního průmyslu. [skriptum]. Zlín: UTB, 2014. ISBN 978-80-7454-410-1.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Jakub Rak, Ph.D.**
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.

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. Martin Džermanský

.....
podpis studenta

ABSTRAKT

Tato diplomová práce se zaměřuje na problematiku zabezpečení společenských akcí. V teoretické části této práce je uvedena základní problematika bezpečnostních prvků, informace o společenských akcích a základní pojmy. V praktické části je popsán objekt XY, na který je aplikována praktická část. Jsou zde uvedeny vytvořené analýzy a metody, mezi které patří analýza SWOT a KARS. Praktická část je ukončena kapitolou možných opatření, která obsahuje možnosti zlepšení systému a celého zabezpečení společenských akcí v objektu XY.

Klíčová slova: společenské akce, zabezpečení, analýza, KARS, SWOT

ABSTRACT

This thesis focuses on the issue of securing social events. In the theoretical part of this work there are introduced basic issues of security elements, in-formation about social events and basic concepts. The practical part describes the XY object, to which the practical part is applied. There are created analyzes and methods including SWOT and KARS analysis. The practical part is finished with a chapter of possible measures, which contains the possibilities of improving the system and the whole provision of social events in the XY building.

Keywords: social, events, safety, analysis, KARS, SWOT

Chtěl bych poděkovat mé rodině, přátelům a spolužákům za podporu při zpracování mé diplomové práce a při celé době studia a především mému vedoucímu diplomové práce panu Ing. Jakubu Rakovi, Ph.D. za celé vedení této práce a rady, které mi při psaní této diplomové práce pomohly.

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

OBSAH

ÚVOD

V dnešní době, kdy dochází k čím dál častějším útokům na skupiny lidí, je zapotřebí dbát na ochranu a zvýšenou bezpečnost. Oblíbenými cíli jsou v poslední době například vánoční trhy nebo hudební koncerty, kde se právě sdružuje velké množství lidí, a tak jsou jednoduchým terčem pro útočníky.

Tato diplomová práce se zabývá problematikou zabezpečení společenských akcí. Společenské akce patří mezi hojně navštěvované akce a může se jednat například o sportovní akce, hudební koncerty, divadla, plesy, představení ale i například také o folklorní akce.

Každá taková akce musí být patřičně zabezpečena. Zabezpečení začíná u samotných pořadatelů, až po jednotlivé bezpečnostní prvky, mezi které lze zařadit elektrickou požární signalizaci, uzavřené kamerové okruhy, mechanické zábranné systémy, poplachové zabezpečovací a tísňové systémy a další.

Nikdy není zřejmé, kdo se vyskytuje na dané akci a jaké jsou jeho myšlenky nebo úmysly. Tato osoba nebo skupina mohou napadnout nevinné účastníky nebo organizátory a ohrozit je na životě. Je zapotřebí proto dbát zvýšené opatrnosti zejména ze strany pořadatelů. Jejich úkolem je zabezpečit areál nebo místo konané společenské akce ale i kontrolovat jednotlivé návštěvníky a celý průběh akce.

Je zapotřebí, aby organizátoři akcí věděli, jak se v danou chvíli zachovat. Je tedy potřeba provádět odborná školení zaměřená na tuto problematiku. Organizátor musí vědět jak danou situaci vyhodnotit a jak při ní zakročit.

Cílem práce je seznámení se s teoretickými základy zabezpečovacích systémů, zaměření se na problematiku jednotlivých bezpečnostních systémů, konkretizace zvolené společenské akce, návrh opatření pro zabezpečení společenských akcí a diskuze nad získanými výsledky.

Hlavní otázkou této diplomové práce je, zda je daný objekt dostatečně zabezpečen pro konání společenských akcí.

TEORETICKÁ ČÁST

1 SPOLEČENSKÉ AKCE

Společenskou akci lze definovat jako událost, na které se shromažďuje větší počet osob. Může se ale také jednat o méně početné skupinky lidí, to záleží na druhu společenské akce. Mezi společenské akce můžeme například zařadit:

- sportovní akce,
- kulturní akce,
- diskotéky,
- plesy,
- koncerty,
- divadlo, atd.

Lidé navštěvují společenské akce především z důvodu naplnění jejich potřeb. Mezi tyto potřeby může například patřit:

- konverzace,
- zábava,
- setkání s přáteli,
- setkání s novými lidmi,
- navázání kontaktů,
- odreagování, atd.

V rámci těchto skupin lidí tvořících společenské akce může ale také vzniknout mnoho rizik:

- panika,
- aktivní střelec,
- živelná pohroma,
- technologie,
- narušení objektu, atd. [1, 2, 18]

1.1 Bezpečnostní standardy kulturních a společenských akcí

Za každou kulturní či společenskou akci je zodpovědná nějaká osoba (pořadatel akce). Touto osobou může být kdokoliv z nás, může to být obec, organizace nebo i spolek. Záleží na druhu konané akce, ať už se jedná o ples, sportovní akci, anebo například folklorní festival. [1, 2, 21]

Každý pořadatel takové akce je povinen se řídit určitými pravidly, která jsou stanovena pro organizaci takovýchto akcí. Tyto povinnosti jsou rozdělena do několika základních kritérií, a to:

1.1.1 Zákonná úprava – co může a musí pořadatel

Základní povinnosti a možnosti pořadatele:

- Každý pořadatel má právo obracet se na Policii ČR pro ochranu bezpečnosti osob a majetku, dle § 2, § 10 odst. 1 zákona č. 273/2008 Sb., o Policii ČR.
- Přípustnost jednání v krajní nouzi nebo v nutné obraně, dle § 24, § 25 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, § 28, § 29 zákona č. 40/2009 Sb., trestní zákoník.
- Právo oznamovat přestupky, trestné činy nebo podávat jiné podněty, dle § 74 odst. 4 zákona č. 251/2016 Sb., o odpovědnosti za přestupky a řízení o nich, § 158 odst. 2 zákona č. 141/1961 Sb., trestní řád, § 42 zákona č. 500/2004 Sb., správní řád. [1]

Oprávnění obce:

- Požadovat po Policii ČR spolupráci, při zabezpečení místních záležitostí veřejného pořádku, dle § 103 odst. 4 písm. d) zákona o obcích.

Povinnosti pořadatele:

- Zdržet se všeho, čím by nad míru přiměřenou poměrům došlo k obtěžování jiného, dle § 1012 zákona č. 89/2012 Sb., OZ.
- Povinnost dodržovat povinnosti stanovené obecně závaznou vyhláškou obce nebo kraje, dle § 4 odst. 1 nebo 2 zákona o některých přestupcích.
- Užívat cizí věc pouze na základě oprávnění vyplývajícího ze zákona nebo smlouvy, dle § 8 odst. 1 písm. a) nebo b), anebo dle § 8 odst. 2 písm. a) nebo b) zákona č. 251/2016 Sb., o některých přestupcích.
- Bez zbytečného odkladu uposlechnout výzvy nebo pokynu žádosti policie nebo policisty, dle § 14 a § 18, § 114 zákona č. 273/2008 Sb., o Policii České republiky.
- Nepřekročit hygienický limit hluku nebo vibrací při pořádání veřejné produkce hudby, dle § 92 a následně zákona č. 258/2000 Sb., o ochraně veřejného zdraví.
- Chovat se tak, aby nedošlo ke vzniku požáru. [1]

1.1.2 Obsah vyhlášky – co může regulovat obec

Obecně závazná vyhláška obce může regulovat minimální počet předpokládaných účastníků konané akce nebo druhu akce. Tuto regulaci mohou stanovit z již získaných zkušeností například z předešlých akcí, které pořádala.

Organizátoři nebo pořadatelé jsou povinni ohlásit akci alespoň měsíc dopředu. Oznámení akce musí obsahovat následující aspekty. Oznámení musí obsahovat identifikační a kontaktní údaje na pořadatele akce anebo kontakt na jeho zástupce. Tyto údaje obsahují především telefonní číslo a e-mail. Musí zde být uveden datum a čas zahájení akce a to i jeho ukončení s uvedením předpokládaného počtu účastníků.

Pořadatelé musí uvést počet osob, které budou zajišťovat pořadatelskou službu a kontaktní a identifikační údaje na osobu pověřenou ke spolupráci s orgány veřejné správy.

Mimo oznamovací povinnosti pořadatele, je pořadatel také povinen zajistit:

- zabezpečení minimálního počtu členů pořadatelské služby, a to minimálně 3 pořadatele na 100 účastníků a označení těchto pořadatelů (například náprsní cedulkou *‚Pořadatel‘*),
- ukončit akci v určitou hodinu,
- být, či zajistit osobu přítomnou a zodpovědnou na konání akce,
- označení místa konání akce,
- v případě narušení akce kontaktovat Policii ČR, v případě, že se nedaří obnovit pořádek,
- zajistit aby účastníci nevnášeli na akci výbušniny, zbraně, pyrotechniku, hořlaviny anebo předměty, jimiž by mohlo dojít k násilí nebo ublížení na zdraví,
- stanovit podmínky k zabezpečení požární ochrany. [1]

1.1.3 Základní bezpečnostní doporučení pro pořadatele sportovních, kulturních a společenských akcí.

V rámci bezpečnosti konané akce ale i účastníků akce, je doporučeno, aby organizátoři nahlásili pořádání akce obci v dostatečném předstihu, informovali HZS ČR, PČR, ZZS o konání akce ihned, kdy je znám termín konání akce. Policie České republiky by měla být informována o bezpečnostních opatřeních, která jsou připravována v rámci akce.

Pro bezpečný chod akce by měla být určena osoba zodpovědná za nastavení, koordinaci a realizaci bezpečnostních opatření, která budou také kontaktním bodem pro policii a obec.

Tato osoba musí být neustále dostupná a mít k výkonu své funkce potřebné pravomoci a postavení. Musí být zajištěn také dostatečný počet pořadatelů starších 18 let.

Při konání větší akce je doporučeno zřízení kontrolního centra, kde bude probíhat monitoring radiokomunikace pracovníků bezpečnostní služby, komunikace s policií a místo pro nahlašování a vyhodnocení bezpečnostních incidentů.

Spolupráce s jednotlivými složkami integrovaného záchranného sboru a s obecní policií. V rámci konání větších akcí pomoc IZS v součinnosti při zajištění pořádané akce. Každá složka IZS plní jednotlivé úkoly:

- ZZS – zdravotnické zajištění.
- PČR – zajištění veřejného pořádku.
- HZS – zajištění protipožárního pořádku. Dále zajišťují evakuační cesty, zajištění věcných prostředků požární ochrany, informování a varování v případě nebezpečí.

Analýza hrozeb a vyhodnocení rizik by měla patřit k základním pilířům konání akce. Organizátoři by se měli zamyslet nad možnými riziky a nebezpečím, které může nastat. Mezi důležité otázky v rámci analýzy patří:

- Kde a v jakých místech lze očekávat incident?
- Jaké bude počasí a jaké rizika s sebou nese?
- Ponaučení z předešlých akcí?
- Zda bude použit nějaký druh pyrotechniky nebo hořlaviny, a jak budou tyto látky skladovány?
- Kde a kdy bude největší koncentrace lidí?

Stejně jako analýza hrozeb, tak je důležitá také bezpečnostní dokumentace. Tato dokumentace by měla obsahovat bezpečnostní plán a koordinační plán. Tyto plány se skládají z bezpečnostní procedury pro mimořádné ale i běžné situace. Dokumenty je doporučeno konzultovat se složkami IZS. [1]

Pořadatelé, personál a bezpečnostní služby, které budou mít na starost průběh akce, by měli být před jejím začátkem řádně proškoleni. Školení by mělo být zaměřeno převážně na:

- evakuační plán,
- bezpečnostní plán,
- detekce podezřelého chování a podezřelých předmětů,

- bezpečnostní procedury,
- koordinační plán,
- komunikační plán,
- jednotlivé úkoly pořadatelů, personálu a bezpečnostní služby.

Organizátoři akce by měli také vytvořit návštěvní řád, komunikační plán a varování návštěvníků.

Návštěvní řád musí být vytvořen s dostatečným předstihem a musí v něm být stanovena práva a povinnosti pořadatelské a bezpečnostní služby, práva a povinnosti návštěvníků akce a úkoly bezpečnostní a pořadatelské služby.

Komunikační plán slouží k vymezení procesu pro rutinu ale i případy incidentů. Komunikační procesy nejlépe nastavit tak, aby v případě potřeby došlo k rychlému kontaktování anebo varování organizační struktury. Všechny informace by se měli dostat k určitému centru jako například kontrolním centru pořadatele, které si organizátoři určí před začátkem akce. V tomto centru by měla být vytvořena tabulka s kontakty na jednotlivé pořadatele a bezpečnostní služby.

Varování návštěvníků probíhá předem určeným způsobem, na kterém se organizátoři předem dohodnou před začátkem akce.

Při vzniku bezpečnostního incidentu je zapotřebí všechny tyto incidenty evidovat. Je potřeba evidovat i sebemenší incidenty od začátku až do konce akce. Tyto incidenty by měly být hlášeny Policii České Republiky.

Mimo evidenci bezpečnostních incidentů je zapotřebí provádění bezpečnostních kontrol. Kontrola by měla započat ještě před zahájením akce a vstupem návštěvníků. Při kontrole vstupu se pořadatelé musí zaměřit na detekci zakázaných předmětů, platných vstupenek a na detekci podezřelého chování. Jedná-li se o větší akci, kde e využito více vstupů, tak je vhodné tyto vstupy od sebe oddělit páskou nebo zábranami, aby se nevytvářely velké davy a byl přehled o přítomných osobách ve frontách. Optimální nastavení jsou tedy maximálně 3 osoby vedle sebe. [1, 2]

2 BEZPEČNOSTNÍ SYSTÉMY

Bezpečnostní systémy patří neodmyslitelně k denním rutinám člověka. Zajištění bezpečnosti osob a majetku a vytvoření pocitu bezpečí patří mezi základní funkce, realizované na všech úrovních společenské hierarchie.

Samotné počátky lidské společnosti byly spojeny se zajištěním struktur, díky kterým v přírodě, ale později i ve společenských podmínkách umožňovali lidem přežít. Tyto postoje a struktury patří i v současné době mezi priority moderní společnosti. V posledních desetiletích vzniknul nový třetí pilíř bezpečnosti, a to nový fenomén zajištění bezpečnosti jako komerční služby. [13]

Lidé pro svou ochranu využívají různé typy bezpečnostních prvků nebo systémů. Mezi nejpoužívanější systémy se řadí:

- CCTV (Closed Circuit Television – uzavřený televizní okruh) systémy,
- EPS (Elektrická požární signalizace),
- PZTS (Poplachový zabezpečovací a tísňový systém),
- Fyzická bezpečnost.

2.1 CCTV systémy

Kamerový systém, zkráceně CCTV (Closed Circuit Television – uzavřený televizní okruh) slouží k využití kamer k monitoringu jednotlivých prostor, objektů, lidí a k archivaci natočených záběrů a zobrazení záběrů z kamer na monitorech. Tyto kamery jsou pak označovány za průmyslové televize nebo častěji za průmyslové kamery. [5, 15, 16]

Celý systém se skládá z kamer, HW vybavení (monitor a HDD) a SW. Rozšíření může například obsahovat mikrofon, reproduktory a záznamové médium pro ukládání zaznamenaných dat.

Kamerové systémy jsou využívány v dnešní době jako nástroj prevence kriminality pro podporu průmyslových společností, logistických procesů anebo jako technické prvky ochrany soukromého majetku či osob.

Problematika systémů CCTV je úzce spjata se soukromím občanů. Kamerové systémy jsou čím dál více využívaným prvkem bezpečnosti a lze je zaznamenat téměř všude. V rámci ochrany osobních údajů jsou zpracovány informace k zavedení přesných pravidel pro jejich provozování. Tyto informace zpracoval Úřad pro ochranu osobních údajů (ÚOOÚ),

který také v roce 2012 vydal metodiku s názvem „*Provozování kamerových systémů*“, který pojednává o základních povinnostech ukládaných zákonem pro ochranu osobních údajů.

Provozování kamerových systémů je považováno za zpracování osobních údajů, pokud je zaznamenáváno kromě kamer:

- provádění záznamu pořizovaných záběrů (zvukové či obrazové),
- účel pořizování záznamů je využití k identifikaci fyzických osob v souvislosti s jejich určitým jednáním.

Provozování kamerových systémů se záznamem, tedy uložením záznamové stopy na uložiště a zpracování osobních údajů je možné pouze na základě právních důvodů, jako jsou:

- důvody nezbytné pro ochranu práv a právem chráněné zájmy správce nebo jiného subjektu – nejčastěji pro ochranu majetku,
- pokud je zpracování nezbytné pro dodržení právní povinnosti správce,
- na základě souhlasu subjektů údajů – pouze, pokud je možné vymezit okruh monitorovaných osob (např. kamerové systémy v bytových domech).

V případě využití kamerových systémů na pracovišti v pracovní době musí zaměstnavatel dodržovat zákon č. 101/2001 Sb., a aplikovat ustanovení zákona č. 262/2006 Sb., zákoník práce, zejména § 316, který umožňuje zaměstnavateli monitorovat zaměstnance a narušovat jejich soukromí pouze ze závažných důvodů spočívající ve zvláštní povaze činnosti zaměstnavatele. Pokud tyto důvody nejsou dány, tak zaměstnavatel nesmí zaměstnance monitorovat, a to ani v případě, že zaměstnanec dal souhlas k jeho monitoringu. [15, 16]

Obrázek 1 – CCTV systémy [3]

2.1.1 Oznamovací povinnosti

Pořizování záznamu kamerovými systémy je považováno za zpracování osobních údajů, které podléhá zákonu č. 101/2000 Sb., § 16. K plnění oznamovací neboli registrační povinnosti lze využít elektronický formulář oznámení o zpracování osobních údajů dle § 16 zákona 101/2001 Sb., který se nachází na webových stránkách www.uoou.cz. K tomuto formuláři je potřeba doložit přílohy:

- seznamy míst zpracování,
- kopii plné moci, pokud jiný subjekt zastupuje oznamovatele.

Existují také případy, kdy se na provozování kamerových systémů nevztahují oznamovací povinnosti. Mezi tyto případy lze zařadit provozování kamerových systémů pro osobní potřebu za účelem ochrany svého majetku, monitoringu soukromého pozemku, objektu, bytu včetně vstupu atd. V tomto případě je však nutné dodržet to, aby byly kamery správně nainstalovány a nezasahovaly do veřejného prostranství. V tomto případě by došlo k porušení zákona č. 101/2000 Sb., o ochraně osobních údajů. [15, 16]

Dalším případem je provozování kamerových systémů se záznamem, jehož využití správci ukládá zvláštní zákon, nebo je ho třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona. Příklady těchto zákonů jsou např.:

- Zákon č. 273/2008 Sb., o Policii ČR, ve znění pozdějších předpisů,
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,
- Zákon č. 17/2012 Sb., o celní správě,
- Zákon č. 555/1992 Sb., o vězeňské službě a justiční stráži České republiky ve znění pozdějších předpisů,
- Zákon č. 59/2006 Sb., o prevenci závažných havárií, ve znění pozdějších předpisů.

Třetím případem může být provozování kamerových systémů v režimu on-line bez pořízení záznamu. Takový monitoring kamerovými systémy není považován za zpracování osobních údajů dle zákona č. 101/200 Sb.,

2.1.2 Norma ČSN EN 50132

Česká technická norma, která byla vydána úřadem pro technickou normalizaci, metrologii a státní zkušebnictví, zkráceně ÚNMZ v roce 1999 tvoří celkem sedm částí, kdy každá

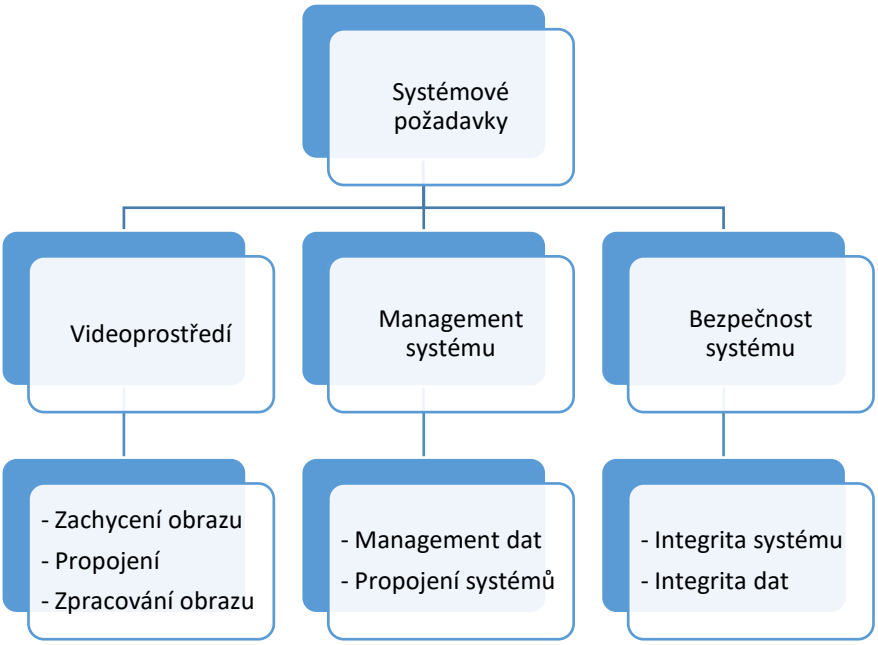
z nich řeší odlišnou problematiku kamerových systémů. Překlad evropské normy z března roku 2011 ji však revidoval pouze na 3 části, a to:

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

Tato verze byla přijata v České republice v dubnu 2013.

2.1.3 Systémové požadavky

První část normy ČSN EN 50132 – 1 Systémové požadavky se zabývá požadavky na provoz kamerových systémů. Definují se zde jednotlivé prvky kamerových systémů a jsou děleny do 3 oddílů, kdy každá z nich řeší problematiku návrhu kamerových systémů z jiného hlediska:



Obrázek 2 – Systémové požadavky [16]

Norma zde řeší rozdělení prostředí dle okolních fyzikálních jevů působící na kamerové systémy. Největší důraz je kladen na technické specifikace budovy, vlhkost a teplotu. Rozlišují se 4 třídy:

Tabulka 1 – Technické specifikace budovy [16]

Třída	Název prostředí	Teploty	Příklady
I.	Vnitřní	+5 až +40	Obytné místnosti, obchodní objekty
II.	Vnitřní všeobecné	-10 až +40	Nestálá teplota, haly, chodby, schodiště
III.	Venkovní chráněné	-25 až +50	Vně budovy, komponenty nejsou plně vystaveny environmentálním vlivům, terasy, přístřešky
IV.	Venkovní všeobecné	-25 až +60	Vně budovy, komponenty plně vystaveny environmentálním vlivům prostředí

Neméně důležitou částí je zavedení klasifikace kamerových systémů čtyřmi stupni zabezpečení. Rozdělení tohoto zabezpečení je založeno na bezpečnostních požadavcích v jednotlivých stupních zabezpečení a kritérií provozu.

- I. Stupeň (nízká rizika) – tento stupeň je určen k dohledu nad situacemi s nízkým rizikem. Neobsahuje žádnou ochranu proti narušení a nevyžaduje se monitorování základních funkcí.
- II. Stupeň (nízká až střední rizika) – stupeň určený k dohledu situací s nízkými až středními riziky. Disponuje jednoduchou ochranou proti narušení a nevyžaduje jednoduché monitorování základních funkcí.
- III. Stupeň (střední až vysoká rizika) – stupeň určený k dohledu nad středními až vysokými riziky. Tento stupeň disponuje střední ochranou proti narušení a je zde považována jednoduchá monitorování základních funkcí.
- IV. Stupeň (vysoká rizika) – stupeň určený k dohledu nad vysokými riziky. Tento stupeň disponuje vysokou ochranou proti narušení a je zde považován stálý monitoring základních funkcí. [15, 16]

2.1.4 Přenos videosignálu

Norma stanovující základní specifikace na přenosové systémy kamerových systémů, které zahrnují přenosový kanál, vysílací zařízení a vysílací zařízení. Stanovují metody ověření

splnění jednotlivých parametrů a zavádí také IP protokoly přenosu obrazu pro zařízení v bezpečnostních aplikacích a obecné požadavky kladené na přenos videosignálu.

Požadavky na videopřenosy jsou rozděleny dle normy ČSN EN 50132-5 na:

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

Norma ČSN EN 50132 – 5 zavádí rozdílné výkonové třídy podle požadavku na funkčnost využívaného zařízení pro přenos. Při návrhu kamerového systému není důležitý jen výběr a konfigurace standardizovaných videokomponentů ale také odpovídající síťová struktura. Uvádějí se také prvky, které nejvíce ovlivňují efektivnost kamerových systémů: [16]

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

2.1.5 Pokyny pro aplikaci

Tato norma obsahuje jednotlivé požadavky a doporučení pro plánování, výběr, přejímku, instalaci, údržbu a zkoušení kamerových systémů.

Norma má za cíl poskytnout pracovní rámec, který umožňuje zákazníkům stanovit jejich požadavky při volbě příslušného zařízení.

Při návrhu kamerového systému by měla být provedena analýza rizik, pro definování jednotlivých hrozeb a nebezpečí objektů. V rámci analýzy se posoudí dopad těchto hrozeb a odhadne se pravděpodobnost vzniku mimořádné události. Primárním důvodem instalace kamerového systému je zmírnění rizika, které z posouzení vyplynulo. Každý objektiv s sebou nese jiné hrozby a z tohoto důvodu se musí brát v potaz tyto prvky:

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

Finální výsledky hodnocení lze uplatnit jako informace napomáhající při realizaci kamerového systému a jeho návrhu. Dle normy ČSN EN 50132 – 5 je doporučený postup projektování a realizace takový:

1. **Vypracování funkčních požadavků** – přesné požadavky a představy zákazníka o účelu a funkčnosti kamerového systému (analýza potřeb zákazníka)
2. **Návrh systému** – zpracování funkčních požadavků a nabídky s konkrétním řešením
3. **Odsouhlasení specifikace** – ověření úplnosti, zpracování změn a vypracování technické dokumentace
4. **Instalace a ověření funkčnosti systému** – plán instalace, trasování kabeláže a jeho značení, konfigurace, montáž zařízení, revize, spuštění systému, zkoušky a zahájení provozu.
5. **Předání systému zákazníkovi** – školení, předání manuálu a dokumentace
6. **Údržba** – provádění periodicky dle plánu údržby

U kamerových systémů se musí definovat, jaký prostor bude monitorován. Norma zde napomáhá popisem proporcí snímané scény vůči výšce osoby v závislosti na rozlišení snímacího zařízení. Tento popis je označován jako stupeň identifikace osoby. Musí být shodná nastavení rozlišení zobrazovacího a snímacího zařízení, jelikož disproporce může vést ke změně množství detailů a tedy ke zkreslení informace. V rámci těchto specifikací se navrhuje řešení snímacích scén ve smyslu rozmístění kamer a volby objektivů. Při projektování kamerového systému se tedy projektant řídí funkčními požadavky, vypracovanými v tabulce níže: [15, 16]

Tabulka 2 – Funkční požadavky CCTV [16]

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

2.2 EPS

Systémy elektrické požární signalizace, zkráceně EPS, představují jeden z nejvýznamnějších technologických prvků budovy. Úkolem EPS je včasné zajištění detekce a lokalizace požáru a předání poplachové informace složkám zajišťující zásah. Některé systémy dokáží také ovlivnit funkci systému hašené a další funkce systémů budov. Konfigurace systému EPS je tvořena: [12, 15, 22]

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

Pro splnění funkcí systémů EPS je zapotřebí ústředna EPS a hlásiče požáru. Propojení ústředny EPS a hlásiče požáru se nazývá požární smyčka nebo hlásící linka. Jednotlivé požadavky na EPS jsou uvedeny v normě ČSN EN 54. Tato norma specifikuje postupy zkoušení a technické požadavky systému.

EPS se rozdělují do dvou skupin dle schopnosti identifikace místa požáru. Rozdělují se tedy na systémy s individuální adresací a na systémy s kolektivní adresací.

- Systémy s individuální adresací umožňují rozlišit jednotlivé hlásiče na hlásící lince. Moderní EPS využívají především tento systém založený na datové komunikaci mezi hlásiči požáru a ústřednou EPS. Požární smyčka zde slouží tedy jako datová sběrnice umožňující komunikaci.
- Systémy s kolektivní adresací jsou systémy, u kterých lze využít pouze požární smyčky s kolektivní adresací. Ústředny jsou tedy schopny rozlišit pouze smyčky signálu POŽÁR, ze kterých přišel, ale nezjistí již, ze kterého hlásiče tento signál byl odeslán. [15]

Obrázek 3 – EPS [7]

2.2.1 Hlásiče požáru

Hlásiče požáru slouží k lokalizaci a identifikaci požáru ve stádiu vzniku a rozvoje. Hlásiče lze rozdělit na dva typy, a to na hlásiče samočinné a na hlásiče tlačítkové.

Tlačítkové hlásiče jsou založeny na vyhodnocení požáru osobou zúčastněnou v místě požáru a jeho aktivací. Tyto hlásiče lze rozdělit na dva typy a to:

- Hlásiče s přímou obsluhou – aktivace rozbitím skla nebo posunutím ochranného prvku hlásiče.
- Hlásiče s nepřímou obsluhou – aktivace rozbitím skla nebo posunutím ochranného prvku hlásiče a zmáčknutí funkčního tlačítka hlásiče příslušnou osobou.

Samočinné hlásiče vyhodnocují požár samočinně na základě změny fyzikálních parametrů a na vyhodnocení výskytu vzniku požáru v místě instalace, nezávisle na lidském činiteli. Samočinné hlásiče lze rozdělit na: [15, 22]

- hlásiče multisenzorové,
- hlásiče plynu,
- hlásiče plamene,
- hlásiče teplot,
- hlásiče kouře:
    - hlásiče kouře optické,
    - hlásiče kouře ionizační.

2.2.2 Hlásiče kouře optické

Přítomnost pevných částic kouře, které jsou generovány požárem, ovlivňují šíření světelného paprsku emitovaného skrz vrstvu vzduchu kontaminovaného kouřem. Tento efekt lze využít k detekci požáru dvěma způsoby:

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

Hlásiče využívající vyhodnocení rozptylu jsou nejčastěji hlásiče bodové. K rozptylu dochází v důsledku interakce optického záření a pevných částic kouře. Detekční část je tvořena detekční komůrkou, ve které je zdroj optického záření a optický přijímač. Komůrka je vymezena labyrintem lamel, zabraňující průniku okolního světla do komůrky ale umožňuje průniku kouře. Pro eliminaci možného odrazu optického záření zdroje od povrchu detekční

komůrky je lamel a vnitřní část detekční komůrky vyrobena v černé barvě. Optickým vysílačem je nejčastěji LED dioda pracující v infračervené oblasti. Přijímač je tvořen infračerveným detektorem. [15]

Vyhodnocení pohlcování optického paprsku je využíváno u hlásičů lineárních. Tato metoda je založena na vyhodnocování změn intenzity záření emitovaného zdrojem k přijímači v důsledku jeho pohlcení kouřem při průchodu.

2.2.3 Hlásiče kouře ionizační

Ionizační hlásiče jsou založeny na vyhodnocování změn vodivosti ionizovaného plynného prostředí detekční komůrky v důsledku průniku a přítomnosti nezoxidovaných pevných částic kouře do komůrky.

Za normálních podmínek jsou plyny téměř nevodivé a jsou tedy dobré izolanty. Plyny tedy obsahují velmi málo iontů a stávají se vodivými jen za okolností, které jsou z nějaké příčiny příznivé vzniku a udržování iontů neboli ionizaci plynu. Ionty se v plynech při setkání s opačně nabitými částicemi mění na neutrální atomy nebo molekuly. Ke vzniku a udržení ionizace je tedy třeba neustálého vytváření iontů. Způsoby jak toho dosáhnout mohou být například:

- vysoká teplota,
- elektrické pole,
- radioaktivní záření,
- elektromagnetické záření.

2.2.4 Hlásiče teplot

Hlásiče teplot patří mezi nejstarší detekční prvky, které jsou využívány pro detekci požáru v systémech EPS. Tyto hlásiče jsou založeny na vyhodnocení teplotních změn v místě instalace, vyvoláním uvolňovaného tepla v důsledku exotermického charakteru reakce hoření. Hlásiče teplot lze rozdělit na dva typy a to:

- bodové hlásiče teplot,
- lineární hlásiče teplot.

Bodové hlásiče teplot jsou založeny na vyhodnocování a měření teplot v určitém prostoru pomocí teplotně elektrického převodníku jako například termistoru. Vyhodnocení tohoto

signálu se provádí z hlediska překročení maximální přípustné teploty v prostoru – teploty reakce nebo z hlediska překročení maximální rychlosti nárůstu teploty.

Lineární hlásiče teplot jsou založeny na vyhodnocování modulační frekvence infračerveného paprsku, který prochází z vysílače přes střežený prostor do přijímače. Tyto hlásiče lze rozdělit na lineární hlásiče teplot a na lineární hlásiče teplot liniového typu.

Lineární hlásiče teplot liniového typu se mohou dělit na hlásiče dle použitého teplocitlivého detekčního prvku, a to na hlásiče s metalickým detekčním kabelem, hlásiče s optickým detekčním kabelem a pneumatické. Hlásiče s metalickým detekčním kabelem lze dále rozdělit na hlásiče analogové a digitální. [15]

- Digitální lineární hlásiče jsou založeny na vyhodnocování skokové změny odporu detekčního metalického kabelu v důsledku zkratu vodičů detekčního kabelu.
- Analogové lineární hlásiče jsou tvořeny dvoužilovým vodičem stejně jako digitální lineární hlásič. Se vzrůstající teplotou ztrácí použitá izolace žil svou izolační schopnost. Zvyšující se teploty detekčního kabelu, který je vystaven požáru se projevuje nedokonalým zkratem mezi žílami vodiče. Do určité doby je tento jev reverzibilní, po poklesu teplot se tedy parametry detektoru vrací zpět do původních hodnot.

2.2.5 Hlásiče plamene

Dle konfigurace jsou hlásičů plamene hlásiči bodového typu. Detekce požáru je založena na vyhodnocování specifických vlastností radiace plamene. Parametry, které jsou u tohoto typu hlásiče sledovány, jsou:

- intenzita vyzařování,
- spektrální charakter vyzařování,
- frekvence oscilace plamene.

Při správné instalaci a nastavení těchto hlásičů je lze označit za hlásiče s nejkratší dobou reakce na vzniklý požár.

Hlásiče plamene lze rozdělit dle jejich orientace na danou oblast vlnových délek elektromagnetického spektra na:

- infračervené (IR) hlásiče plamene,
- ultrafialové (UV) hlásiče plamene,

- ultrafialové/infračervené (UV/IR) hlásiče plamene. [15]

2.2.6 Ústředny EPS

Základním komponentem systému EPS je ústředna EPS. Podmínkou jejího správného fungování je bezchybná a nepřetržitá funkce ústředny. Z celkového pohledu musí ústředna EPS plnit základní funkce, a to:

- Kontrola provozuschopnosti systému – ústředna musí zabezpečit kontrolu provozuschopnosti automaticky ale i manuálně.
- Ovládání zařízení propojených do systému EPS – u adresovatelných systémů je realizováno ovládacími jednotkami zapojenými do hlásící linky.
- Vyhodnocení a příjem signálu z připojených hlásičů – vyhodnocení a příjem signálu ústředny EPS je spočívá v druhu použitého systému, zda se jedná o adresovatelný nebo neadresovatelný systém.
- Optická a akustická indikace funkčních stavů systému EPS – pro bezchybné funkce systému ústředna EPS musí být schopna jak optické tak i akustické indikace minimálně u následujících funkčních stavů:
    - stav KLID,
    - stav POŽÁRNÍ POPLACH,
    - stav PORUCHA,
    - stav VYPNUTO,
    - stav TEST.
- Nepřetržité napájení komponent systémů EPS elektrickou energií – pro napájení elektrickou energií systémy EPS využívají napájecí zdroje hlavního zdroje napájení, náhradního zdroje napájení a záložního zdroje napájení. [15, 22]

2.3 Fyzická bezpečnost

Fyzická bezpečnost patří mezi nejstarší formy ochrany a ochranných opatření. Mezi jedny z prvních a jediných opatření k zajištění fyzické bezpečnosti byly mechanické zábranné prostředky. Teprve až rozvojem technologií v novověku došlo k rozšíření spektra opatření fyzické bezpečnosti, zejména o bezpečnostní technologie založené na bázi elektronických systémů. [15]

Fyzická bezpečnost je chápána jako dvojím způsobem, a to jako stav i jako soubor opatření. Jako stav vyjadřuje stupeň nebezpečí nebo bezpečí, kde se objekt nachází z pohledu

potencionálního účinku hrozeb fyzickou cestou. Jako příklad lze uvést nákup cenné věci v místě s výskytem vyšší kriminality. Majitel této cenné věci bude chtít tuto věc patřičně zabezpečit a využije tedy například prvků jako bezpečnostní dveře, mříže, PZTS nebo CCTV.

Pojem fyzická bezpečnost vyjadřuje ale i soubor opatření k zajištění stavu bezpečnosti nebo bezpečí. Jedná se o zabezpečení objektu ochrannými prostředky fyzického charakteru. Jedná se především o mechanické zábranné prostředky a systémy.

Pro zjištění míry bezpečnosti je potřeba v rámci objektu stanovit chráněný zájem nebo aktiva. V rámci fyzické ochrany se mezi aktiva řadí peníze, umělecké předměty, starožitnosti, utajované informace, aktiva duševního vlastnictví, ale lze sem zařadit také zbraně, omamné látky a jedovaté látky. Stručně lze říci, že je to vše, co je důležité ochránit před zcizením nebo zničením fyzickou cestou.

Míra bezpečnosti určuje vztah hrozeb a rizik v rámci opatření k jejich minimalizaci. Kvalita bývá obvykle odvozena od ceny aktiv nebo její potřeby ochrany. Podle pravidla ALARP/ALARA by měly náklady na bezpečnostní opatření představovat asi 10 – 15 % celkové ceny aktiv. [15]

Mezi hrozby fyzické bezpečnosti patří:

- vojenský zájem cizí moci,
- teroristický útok,
- kriminalita.

Cílem fyzické bezpečnosti je pachatele se snažit:

- odstrašit nebo odradit,
- zabránit vniku,
- zpozdit,
- identifikovat,
- zadržet a předat policii.

Tabulka 3 – Bezpečnostní třídy [15]

Třída	Čas odporu nejslabšího místa	Pravděpodobný profil pachatele a způsob vloupání
RC 1	Bez zkoušky ručního vloupání	Příležitostný pachatel - použití tělesné síly
RC 2	3 min	Příležitostný pachatel - použito jednoduché nářadí
RC 3	5 min	Zloděj – šroubovák, klíny, dlouhé páčidlo
RC 4	10 min	Zkušený pachatel – použita vrtačka, sekera, dláto
RC 5	15 min	Zkušený pachatel – použito elektrické nářadí
RC 6	20 min	Zkušený pachatel – použito výkonné elektrické nářadí

Odstrašení nebo odrazení pachatele je dosaženo rozměry a konfigurací perimetrické a plášťové ochrany. Výška a typ plotu, jeho mohutnost a obtížná překonatelnost, použití ostnatých drátů, bezpečnostních dveří, mříží a dalších prvků mohou pachatele odradit od jeho úmyslu.

Pokud se pachatel i tak svého úmyslu nevzdá, tak je úkolem fyzické bezpečnosti pachateli zabránit v jeho činu opatřeními plášťovými, perimetrickými a předmětovou a prostorovou ochranou. Jestliže pachatel tyto prvky překoná, je úkolem technických prostředků odhalit jeho překonání a identifikovat narušení prostoru. Po spuštění poplachu by mělo dojít k jeho zadržení fyzickou ostrahou a předání orgánům policie ČR. [15]

2.3.1 Systém fyzické bezpečnosti

Systém fyzické bezpečnosti označuje soubor ochranných opatření, která mají za cíl zamezit, popřípadě ztížit přístup pachatele k chráněným aktivům fyzickou cestou. Základem realizace těchto ochranných opatření je:

- Komplexnost – představuje vzájemnou návaznost a šíři detekčního a ochranného účinku přijatých opatření.

- Vícestupňovost – představuje rozdělení opatření do více oddělených vrstev, kdy každá z vrstev plní samostatnou funkci.
- Automatizace – vyjadřuje využití systémů k automatické identifikaci narušení prostoru a předání informace dohledovému poplachovému a přijímacímu centru a poté zásahové jednotce.
- Průlomová odolnost – doba potřebná k překonání opatření na bázi mechanických zábranných systémů.

Prostorové rozdělení fyzické bezpečnosti:

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

Systém fyzické bezpečnosti tvoří:

- Režimová opatření – cílem je stanovení a naplnění zásad, pravidel, oprávnění pohybu zaměstnanců a dalších osob v prostorách organizace atd. V souladu s potřebami a zákony organizace řeší režimová opatření, jakým způsobem lidé budou postupovat při ochraně organizace. Cílem režimových opatření je stanovení pravidel, zásad, způsoby provádění bezpečnostních kontrol a oprávnění pohybu osob v prostorách organizace. Mezi nejvýznamnější činnosti organizace spadající pod režimová opatření patří spisová služba. Spisová služba je nástrojem řešení správních agend. Prvky spisové služby jsou spisová registrace, spisový plán, předpisy, řády spisové pomůcky, směrnice pro spisovou agendu a užívané nebo předepsané tiskopisy. Režimová opatření mohou být organizační, administrativní a věcné uspořádání vztahů. Tato opatření se vztahují na:
    - činnosti pracovníků dané organizace,
    - pohyb a chování osob přicházejících zvenčí budovy včetně oběhu dokladů a informací uvnitř podniku,
    - výstup informací, dokumentů a dat uvnitř podniku.
- Fyzická ostraha – představuje osoby, které svou dočasnou či trvalou přítomností v objektu organizace jsou schopny zajistit ochranu aktiv. Fyzickou ostrahu provádí strážní, hlídači, hlídací služba nebo policie.

- Technické prostředky – cílem je podpoření realizace režimových opatření, zkvalitnění fyzické ostrahy, odrazení pachatele od jeho činu, popřípadě ztížit jeho úmysly činu. Mezi nejvýznamnější funkce technických prostředků patří identifikace narušení prostoru. Obvykle zahrnují poplachové zabezpečovací a tísňové systémy, mechanické zábranné systémy, systémy kontroly vstupu, kamerové systémy a elektrické zabezpečovací signalizace. [15]

2.4 Mechanické zábranné systémy

Mechanické zábranné systémy, zkráceně MZS patří mezi nejdůležitější systémy pro zabezpečení objektů. MZS poskytují ochranu díky své mechanické pevnosti. Doba, kterou pachatel musí vynaložit na překonání MZS je mnohdy delší, než je pro pachatele únosné a často tento pokus o prolomení i vzdá. MZS mají tedy za úkol vytvořit překážku určitým odporem proti destrukčnímu narušení. Snahou MZS je tedy zabránit: [16]

- možnosti umístění nebezpečného předmětu ve chráněné oblasti,
- krádeži předmětu a dalších hodnot z prostoru chráněné oblasti,
- znehodnocení techniky a zařízení uvnitř oblasti,
- násilnému proniknutí osoby do chráněné oblasti.

V rámci průmyslové komerční bezpečnosti (PKB) patří mechanické prvky mezi základní pilíře objektové bezpečnosti. Pod mechanickými prvky nalezneme kovové i nekovové prvky a součásti jiných zařízení v objektu, které tvoří komplex mechanických zábranných systémů. Každý zábranný systém lze překonat v určitém reálném čase a úkolem MZS je se pokusit tuto dobu posunout do pásma bezpečnosti. Hodnota překonání MZS záleží na:

- využití energetických zdrojů,
- kvalita a druh využité techniky,
- umístění mechanických zabezpečovacích systémů,
- znalosti konstrukce překonávaného zařízení,
- kvalita mechanických zabezpečovacích systémů.

Rozdělení MZS:

- obvodová ochrana: ploty, zdi, průchozí prvky plotů a zdí, visací zámky,
- objektová (plášťová) ochrana: dveře, okna,
- individuální (předmětová) ochrana: trezory, zámky, mříže, přenosné prostředky,

- speciální ochrana: ostatní ochrana (pečetě, plomby), chemická ochrana (laky, prášky). [8]

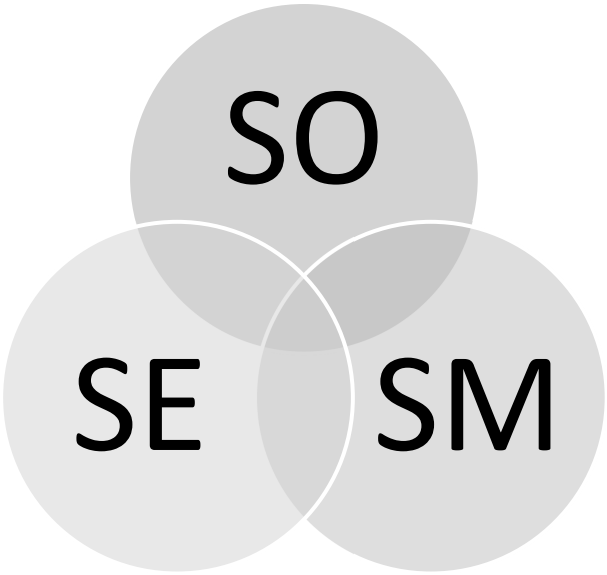
V dnešní době dochází k integraci mezi jednotlivými systémy. Integrují se elektronické a mechanické systémy, respektive bezpečnostní systémy:

- mechanické zábranné systémy (SM),
- signalizační a monitorovací systémy (SE),
- organizační opatření a ostraha (SO).

Optimální bezpečnost tedy lze vyjádřit množinou:

$$\mathbf{IBS = \{M, G\}}$$

- IBS = jednotně uspořádaný souhrn všech složek
- M = souhrn prvků systémů SM, SE, SO
- G = charakteristika systémů, která je tvořena vazbami mezi prvky M a okolím systému. [16]



Obrázek 4 – Grafické znázornění průniku společných prvků systému [16]

Nelze určit, kdy dojde k násilnému vniknutí a tomuto činu nelze zabránit. Z tohoto důvodu je třeba toto riziko minimalizovat pokud možno na co nejpřijatelnější hranici. Pro minimalizaci lze tedy uvést následující příklady:

- při stěhování, ztrátě či odcizení klíčů vždy vyměnit zámkovou vložku,
- věnovat zvýšenou pozornost bytovým dveřím, oknům, lodžií a balkonům,
- seznámit s nebezpečím všechny zúčastněné osoby,

- být dostatečně informován o kriminalitě v okolí svého bydliště,
- pojištění majetku,
- uzamykání domovních dveří, osvětlení společných prostor v objektu, sklepů, chodeb, prostor výtahu a schodiště.

Pro pochopení důležitosti MZS v rámci ochrany majetku a osob slouží následující tabulka:

Tabulka 4 – metody překonání vstupních dveří [16]

Metody překonání vstupních dveří a ochrana proti nim	
Metoda	**Ochrana**
1. Rozlomení vložky zámku	Protizlomová vložka nebo bezpečnostní kování
2. Odvrtání vložky zámku	Kování s ocelovou krytkou vložky
3. Otevření planžetou	Bezpečnostní vložka s překrytým profilem nebo s klíčem s důlky
4. Roztažení dveřního rámu	Vyplnění prostoru rámu betonem
5. Prokopnutí dveří	Oplechování vnitřní strany dveří
6. Vysazení dveří	Zábrany vysazení závěsů (pantů)
7. Vyháčkování dvoukřídlých dveří	Zajištění západek neotvíraného křídla šrouby, vzpěrou, kolíky
8. Nasazení páčidla	Obití rámu dveří z vnější strany kovovým profilem k zakrytí škvíry mezi rámem a dveřmi
9. Vyražení dveří	Zpevnění zárubně ocelovým pásem podél celého obvodu dveří

2.5 PZTS

Poplachové zabezpečovací a tísňové systémy neboli zkráceně PZTS (anglicky Intruder and Hold-up Alarm System – IaHAS) jsou systémy sloužící k signalizaci nebezpečí v daném objektu. PZTS informují o proniknutí (vloupání) do střeženého objektu ale mohou také sloužit pro signalizaci nebezpečí jako: [12, 13, 22]

- přepadení,
- zdravotní obtíže,
- únik plynu,
- požární nebezpečí,
- zaplavení,
- jiné nebezpečí.

2.5.1 Komunikátory

Jednou z nejdůležitějších funkcí systému PZTS je zajištění zaručeného kvalitního přenosu informací. Přenosová trasa je zajištěna od komunikátoru (PZTS) až po komunikátor na straně poplachového přijímacího centra díky poplachovému přenosovému systému (PPS). Systém PPS obsahuje jednotlivé sítě a zařízení využívané pro přenos informací, týkajících se jednoho nebo více PZTS. [13, 17]

V dnešní době se využívají pro komunikaci mezi poplachovými zabezpečovacími a tísňovými systémy a poplachovým přijímacím centrem následující formy spojení:

- TCP/IP – přenášení informací z PZTS prostřednictvím modulu LAN. Jedná se o přenášení dat v reálném čase za pomoci internetového připojení.
- Rádiové spojení – využívá se rádiové sítě, která je označena také za nejbezpečnější formu připojení. Kontrolní zprávy jsou odesílány každých 5 sekund. Výhodou tohoto systému je také jeho rychlost. Rádiový přenos je nejrychlejší a informace je přenesena z objektu na poplachové přijímací centrum během 3 sekund.
- GSM/GPRS – přenos dat je uskutečněn pomocí sítě GSM v hovorovém pásmu, popřípadě službou SMS nebo GPRS.
- PSTN – přenos dat pevnou telefonní sítí. [13, 17]

2.5.2 Ovládací periferie

První typy systémů PZTS byly nastavovány pomocí binární a hexadecimální soustavy. PZTS byly ovládány klávesnicí a uživatel kromě zastřežení a odstřežení nemohl udělat nic jiného. Dnešní typy PZTS mají v sobě již zabudovaný panel LCD s displejem, který umožňují plnohodnotný přístup do systému a jeho nastavení, které obsahuje i nadstandardní funkce. V rámci vylepšení systémů se začaly využívat také formy ověření jako kontaktní a bezkontaktní čipy, klíčenky, přívěšky, karty a biometrické čtečky otisků prstů. [13]

3 ZÁKLADNÍ POJMY

Základní pojmy, vyskytující se v problematice společenských akcí a bezpečnostních systémů:

- Bezpečnost – představuje stav, při kterém je přijatelná pravděpodobnost vzniku újmy na chráněných zájmech a stav, kdy jsou na nejnižší možnou míru eliminovány hrozby pro objekt a jeho zájmy na tento objekt je k eliminaci stávajících i potenciálních hrozeb efektivně vybaven a ochoten při ní spolupracovat.
- Evakuační plán – evakuační plán představuje soubor opatření k zabezpečení přemístění osob, zvířat, předmětů, kulturní hodnoty, technického zařízení, popřípadě strojů a materiálů k zachování nutné výroby a nebezpečných látek z míst zasažených nebo ohrožených mimořádnou událostí.
- Hrozba – hrozba představuje míru pravděpodobnosti vzniku mimořádné události.
- Integrovaný záchranný systém – IZS představuje koordinovaný postup složek při přípravě na mimořádnou událost a při provádění záchranných a likvidačních prací.
- Krizové situace – mimořádná událost podle zákona o IZS, narušení kritické infrastruktury, nebo jiné nebezpečí, při nichž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu.
- Krizové plánování – nedílná součást krizového řízení. Povinnost správních úřadů a jiných státních orgánů a orgánů samosprávy zpracovat krizový plán stanovuje zákon. [20]
- Mimořádná událost – představuje škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací.
- Monitoring – způsob sledování dopadů mimořádných událostí umožňující vyhodnocení a získání podkladů pro přijetí rozhodnutí k jejímu řešení.
- Operační střediska – kontaktní místa záchranné služby a policie pro příjem žádostí o poskytnutí pomoci v nouzi.
- Prevence – prevence představuje soubor opatření pro snížení nebo zamezení pravděpodobnosti vzniku mimořádné události.
- Riziko – riziko lze obecně definovat jako míru výskytu nepřijatelných dopadů vyvolaných očekávanou mimořádnou událostí v daném místě. Je to tedy možnost, že

s určitou pravděpodobností vznikne událost, která se považuje z bezpečnostního hlediska za nežádoucí.

- Terorismus – organizované použití násilí nebo hrozby násilím, obvykle zaměřená proti nezúčastněným osobám, s cílem vyvolat strach, jehož prostřednictvím mají být splněny politické, náboženské nebo ideologické požadavky jak ve vnitrostátním, tak v mezinárodním měřítku. [20, 23]

I. PRAKTICKÁ ČÁST

4 CÍLE A METODY PRÁCE

V této kapitole jsou definovány hlavní a dílčí cíle diplomové práce s použitými metodami v praktické části práce.

Hlavní cíl – návrh opatření k zabezpečení společenských akcí. Hlavním cílem tedy je návrh opatření bezpečnostních systémů společenských akcí.

Dílčí cíle:

- konkretizace zvolené akce,
- analýza současného stavu,
- návrh aplikace jednotlivých bezpečnostních systémů.

Metody:

- **Analýza –** jedná se o proces myšlenkového nebo reálného rozkladu zkoumaného objektu na jednotlivé části, které se stávají předmětem dalšího zkoumání. Patří mezi nejpoužívanější vědecké metody. Analýzy byly využity v praktické části pro realizaci návrhu nových opatření. Byla analyzována jednotlivá rizika, která mohou narušit společenské akce a vytvořena opatření pro jejich eliminaci. [24]
- **Dotazování –** lze rozdělit na několik typů. V tomto případě se jedná o formu ústního dotazování (rozhovor). Ústní rozhovory se využívají pro potřeby zjištění informací hlubšího charakteru. Tato metoda byla využita pro praktickou část práci v rámci zjištění bezpečnostních prvků vyskytujících se v objektu XY.[24]
- **KARS -** metoda KARS (kvalitativní analýza rizik s využitím jejich souvztažnosti) slouží k vytyčení nejpravděpodobnějších a největších rizik, které mohou vniknout a k jejich rozdělení do kvadrantů podle nebezpečnosti. [6]
- **SWOT -** metoda SWOT napomáhá k analýze silných a slabých stránek a také k identifikaci příležitostí a hrozeb. Lze tedy pomocí této metody poukázat na silné stránky, kterými disponujeme ale také poukázat na ty slabé a na příležitosti a hrozby a určit tak, co je zapotřebí vylepšit a na co se prioritně zaměřit. [4]

5 ZABEZPEČENÍ SPOLEČENSKÝCH AKCÍ

Společenské akce jsou nedílnou součástí kulturního vyžití každé obce či města. Odehrávají se zde plesy, kulturní akce, sportovní akce, přehlídky nebo i jiné druhy společenského vyžití. Nedílnou součástí těchto akcí je ale také jejich zabezpečení. Nikdy nevíme, co vše se může stát.

V rámci zabezpečení společenských akcí se bavíme o všech typech zabezpečení počínaje kontrolou lístků až po jednotlivé systémy (CCTV, PIR, EPS…), až po fyzickou ostrahu.

5.1 Objekt XY

V objektu XY se odehrávají společenské akce typu ples, hody, přehlídky, divadlo a další.

V objektu XY se uskutečňuje ročně asi 8 plesů. Tyto plesy patří mezi největší společenské akce uskutečňující se v tomto objektu. Je tedy potřeba tyto plesy patřičně zabezpečit pro ochranu návštěvníků ale i samotných organizátorů a objektu XY.

Před začátkem každého plesu jsou organizátoři již hodinu až dvě v areálu a probíhá zajištění objektu. V rámci bezpečnosti jsou využívány systémy CCTV, PIR, EPS a fyzická ochrana.

Na plese jsou vždy k dispozici alespoň 3 organizátoři, kteří tuto ochranu zajišťují a mají za úkol udržet klidný průběh konání akce.

Objekt XY disponuje třemi podlažími, kdy na plesy jsou zpřístupněny pouze dvě. Přízemí, kde se nachází hlavní vstup do areálu, šatna a průchod do restaurace a baru. Zbylé prostory jsou uzamčeny a kontrolovány. Mezi tyto prostory patří přístup k elektrické rozvodně, kulisám, šatně zaměstnanců a dílně, kotelně, malému loutkovému sálu a kanceláři s přístupem k CCTV systému a prodejně lístků.

Ve druhém podlaží se nachází společenský sál, kde se uskutečňují plesy, foyer se zázemím pro hosty a bar se skladem. V této části jsou uzamčeny prostory hlediště, jeviště a kanceláře.

Třetí podlaží slouží pro pracovníky. Nacházejí se zde kanceláře, sklady a rozvodna. Při konání akcí je přísný zákaz vstupu do tohoto podlaží a během konání akce jsou tyto prostory kontrolovány pořadateli.

V areálu jsou využívány základní bezpečnostní prvky pro ochranu osob a majetku. Objekt XY využívá CCTV systémy, EPS, PIR a fyzickou ochranu.

Tyto plesy navštěvuje v průměru asi 300 – 400 osob. Je tedy zapotřebí, aby zde pro klidný chod akce byli alespoň 3 pořadatelé, aby se dodrželo pravidlo jednoho pořadatele na 100 osob.

Již na začátku plesu je zapotřebí, aby pořadatelé dávali zvýšené opatrnosti. Mezi jeden z jejich úkolů, je kontrola vstupenek. Je zapotřebí, aby bylo dohlíženo na to, aby do objektu nevešla osoba, která nemá vstupenku, nebo ji zfalšovala. Již při této kontrole je také zapotřebí to, zda návštěvníci nemají u sebe nějakou nebezpečnou věc, může se jednat o zbraň, omamné látky, chemické látky, nebo jiný materiál, kterým by mohli ohrozit zdraví a životy jak návštěvníků, tak i samotných pořadatelů.

V případě, že se na ples snaží dostat osoba, která nemá platnou vstupenku, tak ji musí pořadatelé vykázat z objektu. Pravidla striktně nařizují, že se plesu smí zúčastnit pouze osoby s platnou vstupenkou. K těmto pravidlům může dále patřit také vhodné oblečení.

Mimo kontrolu vstupenek jsou pořadatelé povinni kontrolovat také prostory objektu. Během konání plesu tedy pořadatelé kontrolují veřejné, ale i uzamčené prostory, zda nedošlo k nějakému narušení, popřípadě vniknutí.

5.2 CCTV Systémy

V objektu XY je nainstalováno celkem 9 stabilizačních kamer. Tyto kamery jsou rozmístěny takto:

- I. podlaží: 4 kamery – z toho jsou 2 venkovní
- II. podlaží: 4 kamery
- III. podlaží: 1 kamera

V celém objektu jsou nainstalovány barevné kamery typu XC-4AM od společnosti SONY. Tyto kamery disponují:

Tabulka 5 – Periferie kamery XC-4AM [11]

Senzor	1/3“ SONY
Rozlišení	540 TV řádků
Rozlišení v px	752x582 pixelů
Objektiv	C/CS mount

Napájení	DC 12V
Spotřeba	160 mA
Rozměry	185mm x 175mm x 97mm
Váha	265g

Obrázek 5 – XC-4AM

Kamery jsou zapojeny do DVR rekordéru, který slouží pro kamery, které nemají své vlastní uložiště. Jedná se přesněji o typ DVR 6516, který podporuje až 16 AHD kamer a 4 audio kanály. Celý systém pracuje na operačním systému Linux a kompresí H.264. Výhodou tohoto DVR rekordéru je to, že lze zapojit a nainstalovat také IP kamery.

Tento 16ti kamerový sledovací systém není namáhavý ani na výkon počítače, tudíž je vhodný pro nepříliš namáhavé oblasti. Minimální konfigurace PC je nastavena na:

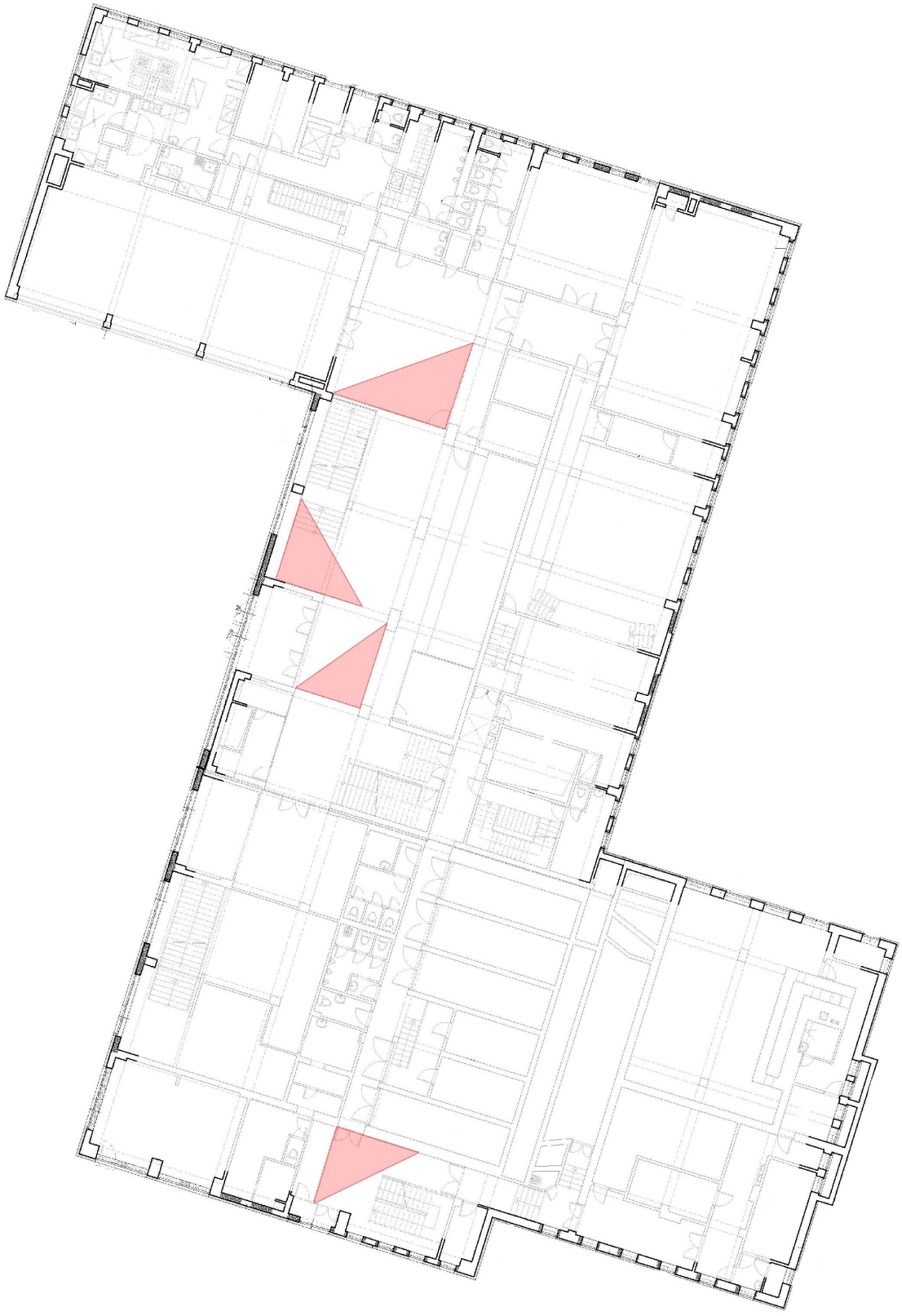
- CPU – Intel Core(™)2 DUO E4600
- Základní deska – Intel G31 / P31
- HDD – 80Gb
- RAM – 1Gb
- VGA – GMA 3100 / Nvidia GeForce 8400 / ATI Radeon HD3450

- OS – Windows 2000 (SP4) / Windows XP (SP2) / Vista
- DirectX 9.0 a vyšší

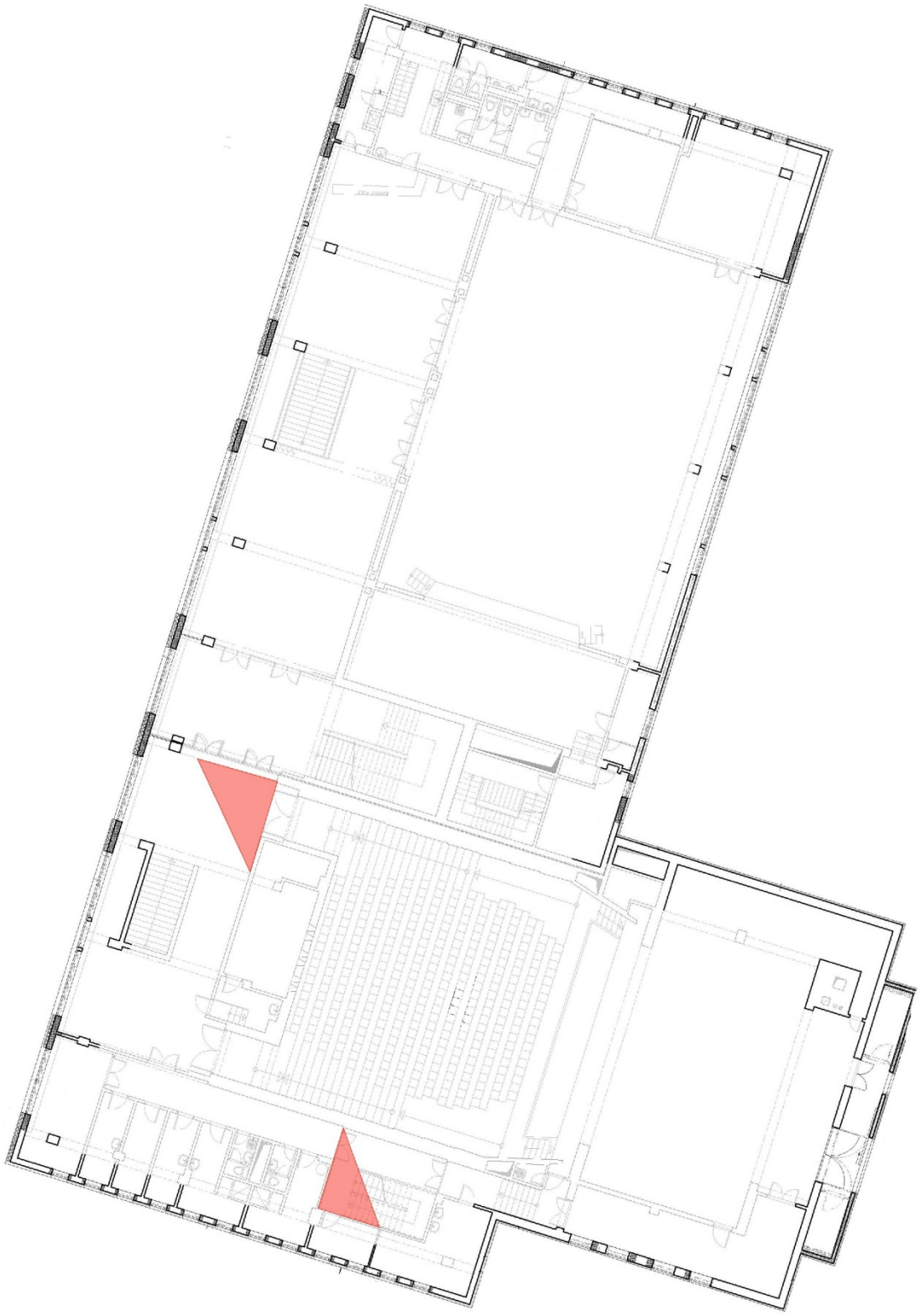
Tyto kamery jsou využívány nonstop 24 hodin denně. V rámci plnění legislativních práv vztahující se k zákonu, takzvaný zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, jsou v objektu vylepena oznámení o jejich záznamu.

Obrázek 6 – Štítek označující kamerové systémy

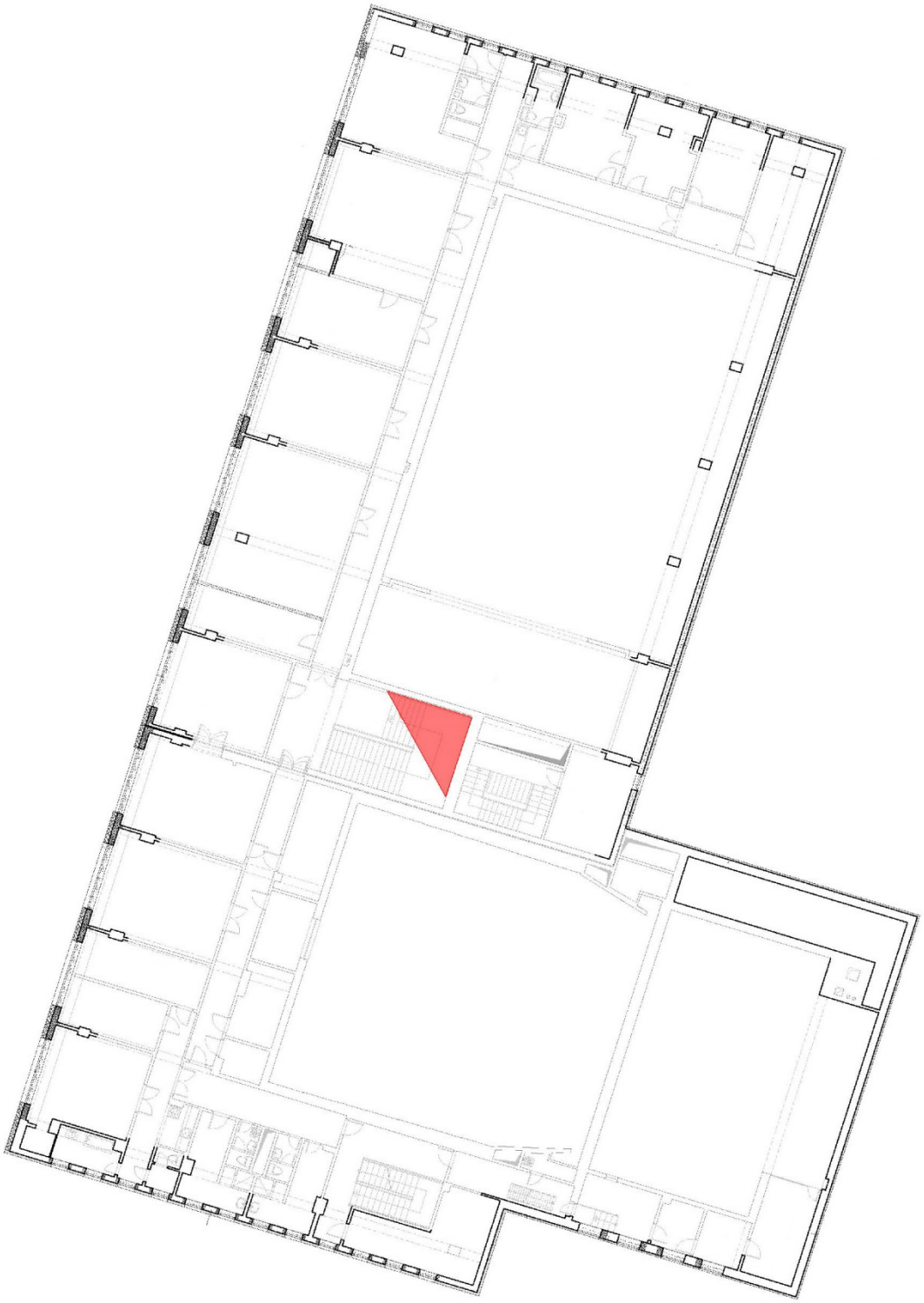
Tento CCTV systém je nastaven tak, že je schopen ukládat pořízené záběry po dobu jednoho týdne. Při vzniku nějaké újmy, napadení, vloupání, popřípadě i nějakého typu útoku, je možno tyto záběry použit a stáhnout je z rekordéru, na němž jsou záběry uloženy.



Obrázek 7 – Instalace CCTV 1. NP



Obrázek 8 – Instalace CCTV 2. NP



Obrázek 9 – Instalace CCTV 3. NP

5.3 EPS

V objektu XY se nachází elektronické požární signalizace typu JA – 80s. Tento typ EPS je jedním z komponentů systému OASIS. Je určen k detekci požáru. Systém je založen na komunikaci pomocí bezdrátového protokolu OASIS a je napájen z baterie. JA – 80s má v sobě zabudovány také sirény pro ohlášení požáru.

Detektor se skládá ze dvou detektorů, a to z teplotního detektoru a optického detektoru kouře. Signál je zpracován z obou detektorů v digitální formě. Tento formát umožňuje lepší rozpoznání falešných a reálných poplachů.

Optický detektor kouře je založen na principu rozptýleného světla a má vysokou citlivost na větší částice, které jsou obsaženy v hustém dýmu a jsou méně citlivé na menší částice v čistě hořících požárech. Detektor není schopen a nemůže detekovat produkty hořících kapalin.

Nedostatky optického kouřového detektoru řeší detektor teplot. Tento detektor má pomalejší reakce, avšak na rychle se vyvíjející teploty z požáru reaguje detektor mnohem lépe.

Produkty požáru, které jsou detekovány optickým detektorem kouře a detektorem teplot jsou přenášeny prouděním. Z tohoto důvodu jsou detektory nainstalovány na stropě, aby produkty oblaku vzniklé z požáru byly směřovány přímo do detektoru. [10]

Obrázek 10 – Požární signalizace JA – 80s

Obrázek 11 – Schéma EPS

Na schématu lze vidět umístění EPS v objektu XY v prvním patře. V celém objektu se nachází pouze jedno zařízení EPS, které není schopno zabezpečit celou budovu. Při konání plesu tedy hrozí nebezpečí, kdy může vzniknout požár ve vyšších patrech budovy a nebude tento požár zachycen systémy EPS.

5.4 PZTS

Mezi prvky poplachových zabezpečovacích a tísňových systémů jsou v objektu XY využívány, tzv. pasivní infračervené čidla (PIR).

V celém objektu je celkem nainstalováno 8 zařízení PIR. Stejně tak jako EPS tak i toto zařízení je součástí systému OASIS a jedná se konkrétně o typ detektoru JA - 80P.

Bezdrátový PIR detektor pohybu osob typu JA – 80P slouží k prostorové detekci pohybu osob v interiérech budovy. Detektor je vyráběn s čočkou se záběrem 120°. Umožňuje tedy sledovat rozlehlé prostory. [9]

Tabulka 6 – Parametry detektoru JA – 80P [9]

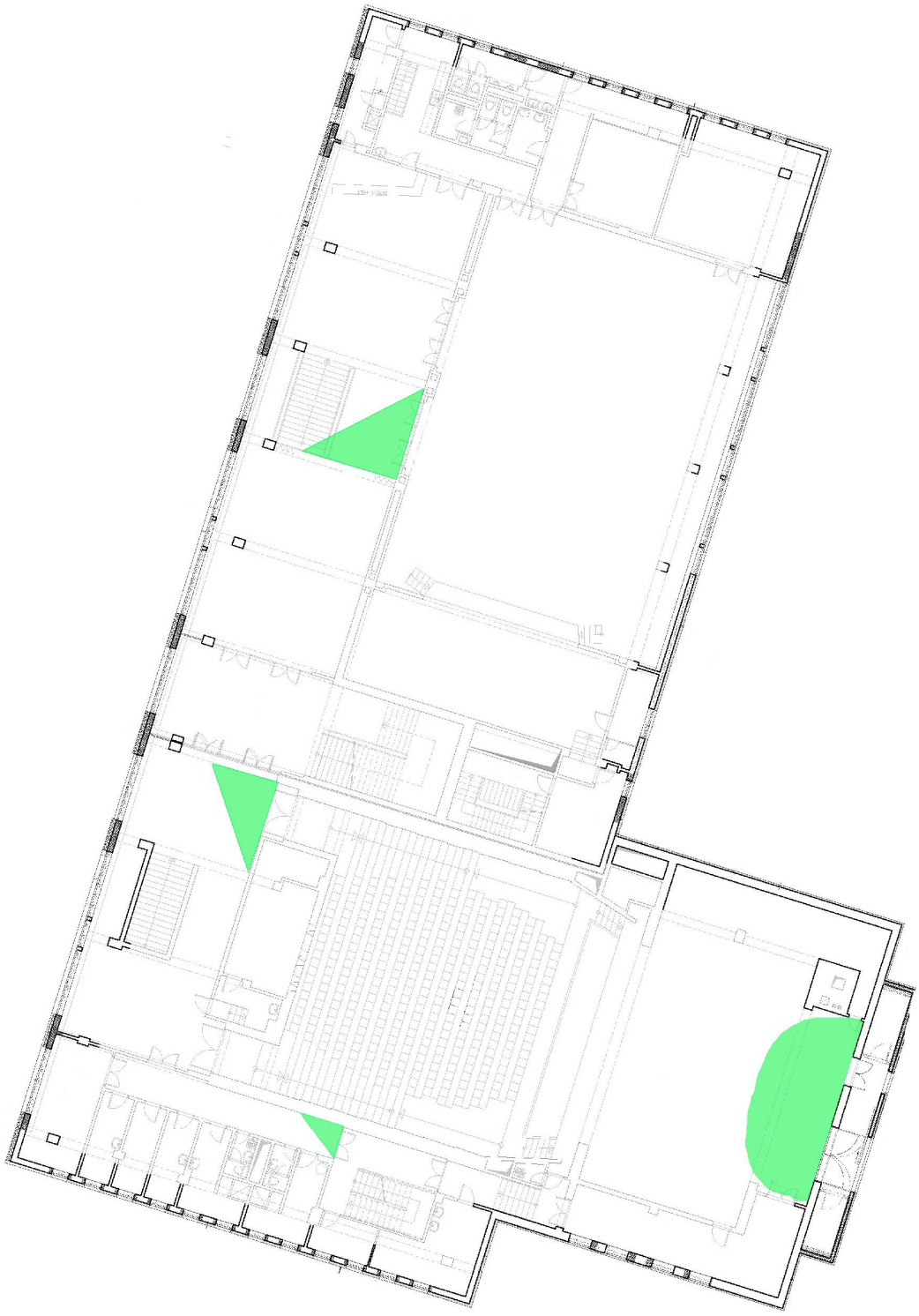
Napájení	Lithiová baterie 3,6V AA/2,4Ah
Životnost baterie	3 roky
Komunikační pásmo	868MHz, OASIS
Instalovaná výška	2,5m
Úhel detekce a délka záběru	120° a 12m
Rozsah teplot	-10 až +40 °C
Rozměry	110 x 60 x 55mm

Obrázek 12 – Detektor JA – 80P

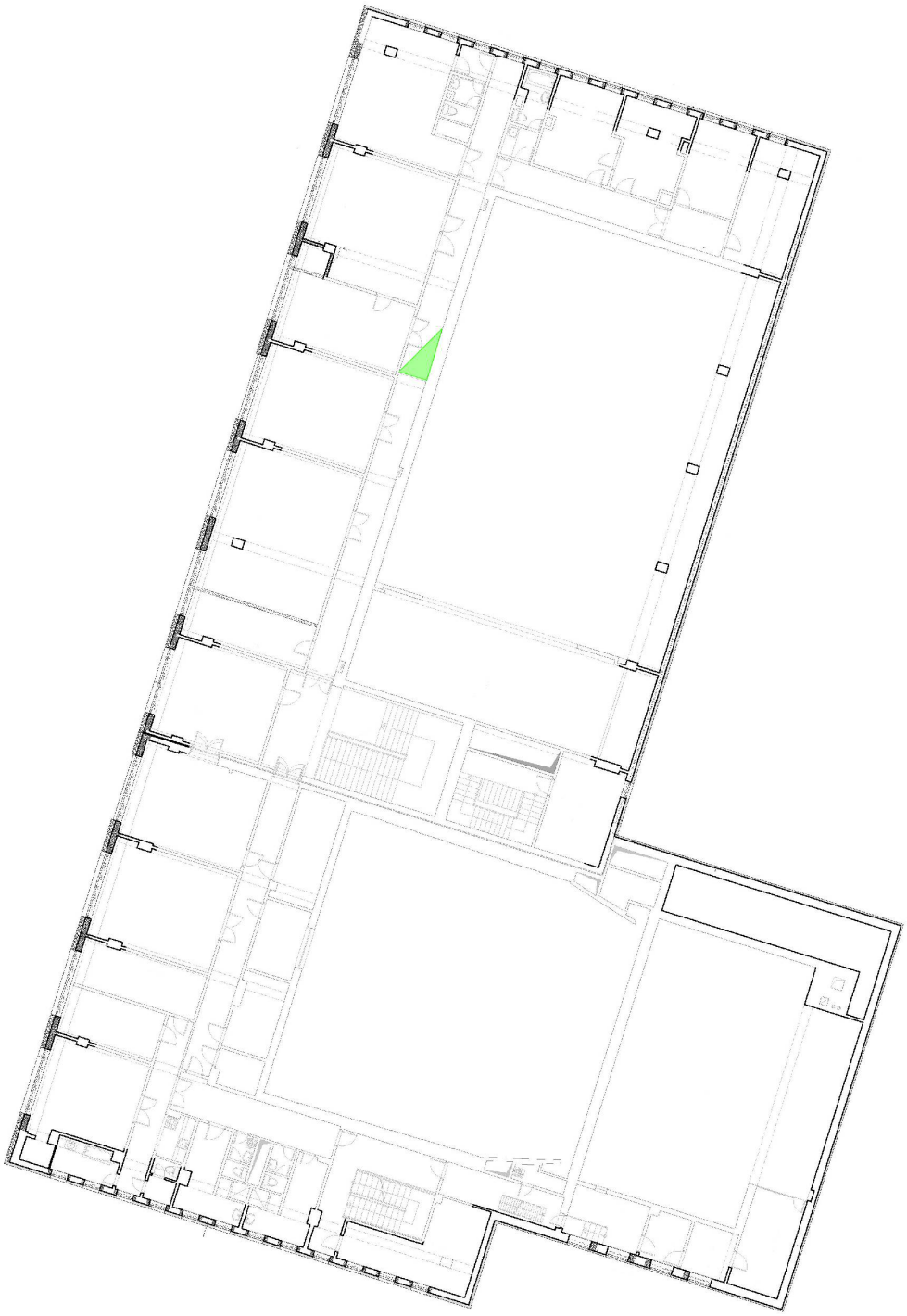
Detektory pohybu jsou v objektu umístěny na všech důležitých místech. Zajišťují tedy dostatečnou ochranu objektu. Při konání plesu jsou tedy i díky těmto systémům dostatečně zabezpečeny objekty, které jsou uzamčeny a při teoretickém vniknutí do těchto objektů, by byli zaměstnanci upozorněni.

Výhodou těchto detektorů je jejich možné rozšíření. Lze u nich vyměnit čočku, a tak tedy rozšířit jejich dosah až na 20m. Dále lze eliminovat pohyb drobných škůdců, a to čočkou JS – 7906, který nezaznamenává podlahu. Detektory, které jsou nainstalovány v objektu XY jsou instalovány se základním typem čočky, tedy s úhlem 120° a délce záběru 12 metrů. [9]

Obrázek 13 – Instalace PIR 1. NP



Obrázek 14 – Instalace PIR 2. NP



Obrázek 15 – Instalace PIR 3. NP

5.5 Fyzická ochrana

Při pořádání plesů je zapotřebí dodržet pravidlo jeden pořadatel na 100 návštěvníků. Průměrná návštěvnost plesů se pohybuje v rozmezí od 300 po 400 návštěvníků, a tak je zapotřebí alespoň 3 až 4 pořadatelů na jeden ples.

V objektu XY jsou pro pořadatelské služby využíváni zaměstnanci ale i brigádníci. Jejich úkolem je zabezpečit klidný chod akce a dohlížet na pořádek. Pořadatelé jsou na místě konání akce alespoň hodinu před začátkem a probíhá standardní příprava objektu, tzn. odemčení prostor a jejich příprava.

Mezi úkoly, které pořadatelé vykonávají, patří:

- kontrola vstupenek,
- dohlížení na pořádek,
- kontrola prostor budovy,
- komunikace s IZS při vzniku konfliktu či zranění,
- ukončení akce a uzamčení a zabezpečení objektu.

Každý z pořadatelů musí mít na sobě viditelný průkaz o tom, že je pořadatel. Toto označení je vyobrazeno formou cedulky s nápisem „*Pořadatel*“ a je nošeno po celou dobu konání akce.

Obrázek 16 – Označení pořadatele

6 ANALÝZA RIZIK

Tato kapitola je zaměřena na možná rizika, která mohou vzniknout v prostorách, nebo narušit prostory akcí pořádaných v objektu XY. Rizika jsou vyhodnocena pomocí jednotlivých metod a analýz.

6.1 Kvalitativní analýzy rizik s využitím jejich souvztažnosti (KARS)

Metoda KARS slouží k vytyčení nejpravděpodobnějších a největších rizik, které mohou vzniknout ve zkoumaném objektu. Metoda slouží k rozdělení rizik do kvadrantů podle nebezpečnosti.

Pro správné provedení metody KARS je nutné sestavit seznam rizik, která jsou vytyčena pro daný objekt a je nutno je vložit do tabulky. Pro vnitřní akci typu ples je vytyčeno těchto 10 rizik, které mohou vzniknout v objektu XY. [6]

1. Aktivní střelec
2. Požár
3. Panika
4. Výtržnosti (napadení)
5. Výpadek elektrického proudu
6. Vandalizmus
7. Násilné vniknutí
8. Zranění osob
9. Konstrukce budovy
10. Přelidnění

Tabulka 7 – Sestavení tabulky rizik

Riziko	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Součet**
1. Aktivní střelec											
2. Požár											
3. Panika											
4. Výtržnosti (napadení)											
5. Výpadek el. Proudu											
6. Vandalizmus											
7. Násilné vniknutí											
8. Zranění osob											
9. Konstrukce budovy											
10. Přelidnění											
Součet											

Kvalitativní analýza rizik s využitím jejich souvztažnosti je založena na vzájemném působení a souvztažnosti rizik. Pracuje tedy na principu ověřování, zda jedno riziko je schopné vyvolat riziko další. To znamená, že do tabulky jsou udávány hodnoty 1 nebo 0. hodnotu 1 vyplníme, pokud riziko je schopné vyvolat riziko druhé. Pokud tomu tak není, tak udáváme hodnotu 0.

Tabulka 8 – Vyplnění tabulky souvztažnosti rizik

Riziko	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Součet**
1. Aktivní střelec	**0**	1	1	1	1	1	1	1	1	1	**9**
2. Požár	0	**0**	1	1	1	1	0	1	1	1	**7**
3. Panika	0	1	**0**	1	1	1	0	1	0	1	**6**
4. Výtržnosti (napadení)	1	1	1	**0**	1	1	0	1	0	0	**6**
5. Výpadek el. Proudu	0	0	1	1	**0**	1	1	1	0	0	**5**
6. Vandalizmus	0	1	1	1	0	**0**	0	1	1	1	**6**
7. Násilné vniknutí	1	1	1	1	1	1	**0**	1	1	0	**8**
8. Zranění osob	1	0	1	1	0	0	0	**0**	0	0	**3**
9. Konstrukce budovy	0	1	1	0	1	0	1	1	**0**	1	**6**
10. Přelidnění	1	1	0	1	1	1	0	1	1	**0**	**7**
Součet	**4**	**7**	**8**	**8**	**7**	**7**	**3**	**9**	**5**	**5**	

Pro kvalifikaci rizik, které mohou vzniknout v objektu XY, 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, které jsou návazné 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, které jsou návazné na riziko označené R_i a které mohou riziko R_i následně vyvolat.

Pro vyjádření koeficientu aktivity a pasivity, bylo nutné sestavit počet kombinací. Za předpokladu, že riziko R_i nemůže vyvolat samo sebe, nebo kdy riziko R_i může vyvolat další rizika nebo 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. [6]

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

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

1. $K_{ARi} = \frac{\sum Ri}{x - 1} \,.\, 100\ [\%] = \frac{9}{10-1} \,.\, 100 = \frac{9}{9} \,.\, 100 = 99{,}99\%$
2. $K_{ARi} = \frac{\sum Ri}{x - 1} \,.\, 100\ [\%] = \frac{7}{10-1} \,.\, 100 = \frac{7}{9} \,.\, 100 = 77{,}77\%$
3. $K_{ARi} = \frac{\sum Ri}{x - 1} \,.\, 100\ [\%] = \frac{6}{10-1} \,.\, 100 = \frac{6}{9} \,.\, 100 = 66{,}66\%$
4. $K_{ARi} = \frac{\sum Ri}{x - 1} \,.\, 100\ [\%] = \frac{6}{10-1} \,.\, 100 = \frac{6}{9} \,.\, 100 = 66{,}66\%$
5. $K_{ARi} = \frac{\sum Ri}{x - 1} \,.\, 100\ [\%] = \frac{5}{10-1} \,.\, 100 = \frac{5}{9} \,.\, 100 = 55{,}55\%$
6. $K_{ARi} = \frac{\sum Ri}{x - 1} \,.\, 100\ [\%] = \frac{6}{10-1} \,.\, 100 = \frac{6}{9} \,.\, 100 = 66{,}66\%$
7. $K_{ARi} = \frac{\sum Ri}{x - 1} \,.\, 100\ [\%] = \frac{8}{10-1} \,.\, 100 = \frac{8}{9} \,.\, 100 = 88{,}88\%$
8. $K_{ARi} = \frac{\sum Ri}{x - 1} \,.\, 100\ [\%] = \frac{3}{10-1} \,.\, 100 = \frac{3}{9} \,.\, 100 = 33{,}33\%$
9. $K_{ARi} = \frac{\sum Ri}{x - 1} \,.\, 100\ [\%] = \frac{6}{10-1} \,.\, 100 = \frac{6}{9} \,.\, 100 = 66{,}66\%$
10. $K_{ARi} = \frac{\sum Ri}{x - 1} \,.\, 100\ [\%] = \frac{7}{10-1} \,.\, 100 = \frac{7}{9} \,.\, 100 = 77{,}77\%$

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

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

1. $K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100\ [\%] = \frac{4}{10-1} \cdot 100 = \frac{4}{9} \cdot 100 = 44{,}44\%$
2. $K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100\ [\%] = \frac{7}{10-1} \cdot 100 = \frac{7}{9} \cdot 100 = 77{,}77\%$
3. $K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100\ [\%] = \frac{8}{10-1} \cdot 100 = \frac{8}{9} \cdot 100 = 88{,}88\%$
4. $K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100\ [\%] = \frac{8}{10-1} \cdot 100 = \frac{8}{9} \cdot 100 = 88{,}88\%$
5. $K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100\ [\%] = \frac{7}{10-1} \cdot 100 = \frac{7}{9} \cdot 100 = 77{,}77\%$
6. $K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100\ [\%] = \frac{7}{10-1} \cdot 100 = \frac{7}{9} \cdot 100 = 77{,}77\%$
7. $K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100\ [\%] = \frac{3}{10-1} \cdot 100 = \frac{3}{9} \cdot 100 = 33{,}33\%$
8. $K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100\ [\%] = \frac{9}{10-1} \cdot 100 = \frac{9}{9} \cdot 100 = 99{,}99\%$
9. $K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100\ [\%] = \frac{5}{10-1} \cdot 100 = \frac{5}{9} \cdot 100 = 55{,}55\%$
10. $K_{PRi} = \frac{\sum Ri}{x - 1} \cdot 100\ [\%] = \frac{5}{10-1} \cdot 100 = \frac{5}{9} \cdot 100 = 55{,}55\%$

Tabulka koeficientů aktivity a pasivity:

Tabulka 9 – Koeficienty aktivity a pasivity

Riziko R_i	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
K_{ARi} [%]	99,99	77,77	66,66	66,66	55,55	66,66	88,88	33,33	66,66	77,77
K_{PRi} [%]	44,44	77,77	88,88	88,88	77,77	77,77	33,33	99,99	55,55	55,55

Výsledný graf souvztažnosti:

Graf souvztažnosti slouží ke stanovení významnosti jednotlivých rizik a jejich souvztažnosti v systému. Graf souvztažnosti je rozpolcen dvěma osami označenými jako 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

Ve výsledném grafu bývá oblast číslo I. pokryta 80 % z celkové oblasti grafu. Pro osu O_1 tedy platí:

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

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

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

$$O_1 = 99{,}99 - \frac{99{,}99 - 33{,}33}{100} . 80 = 88{,}88 - 53{,}33 = \mathbf{46{,}66\ \%}$$

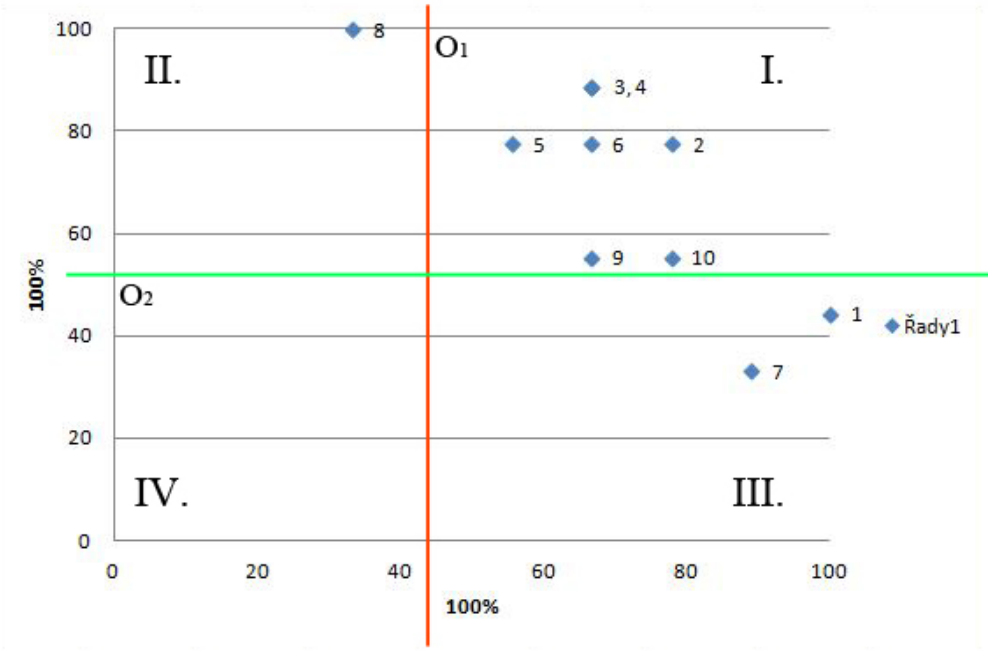
Pro osu O_2 je rovnoběžka s osou x ve vzdálenosti:

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

$$O_2 = 99{,}99 - \frac{99{,}99 - 33{,}33}{100} . 80 = 99{,}99 - 53{,}33 = \mathbf{46{,}66\ \%}$$

Vyhodnocení pomocí grafu souvztažnosti:

- Oblast I. primárně a sekundárně nebezpečných rizik – požár, panika, výtržnosti (napadení), výpadek el. proudu, vandalizmus, konstrukce budovy, přelidnění
- Oblast II. sekundárně nebezpečných rizik – zranění osob
- Oblast III. primárně nebezpečných rizik – aktivní střelec, násilné vniknutí



Obrázek 17 – Graf souvztažnosti

6.2 SWOT

Metoda SWOT napomáhá k analýze silných a slabých stránek a také k identifikaci příležitostí a hrozeb. Lze tedy pomocí této metody poukázat na silné stránky, kterými disponujeme ale také poukázat na ty slabé a na příležitosti a hrozby a určit tak, co je zapotřebí vylepšit a na co se prioritně zaměřit. [4]

Tabulka 10 – SWOT analýza

Silné stránky (S)	**Slabé stránky (W)**
Zabezpečovací systémy	Volný přístup
Personál	Stávající prvky EPS
Prostory	Schodiště
Klidná lokalita	Pronájem prostor
Spolupráce s PČR	
Příležitosti (O)	**Hrozby (T)**
Zdokonalení bezpečnostních prvků	Vstup přes bar
Zabezpečení možných vstupů do objektu	Vstup přes restauraci
Zabezpečení schodiště	Pronesení zbraně
Instalace EPS	Aktivní střelec
	Lidský faktor

Sestavením této tabulky byly tedy vytvořeny 4 kvadranty:

- silné stránky S,
- slabé stránky W,
- příležitosti O,
- hrozby T.

Pomocí vyhodnocení jednotlivých částí metody SWOT, bude ke každému faktoru v kvadrantu přidělena hodnota významnosti, která se udává v rozmezí 1 – 5 u kvadrantu silných stránek a příležitostí. U slabých stránek a hrozeb jsou hodnoty udávány v záporných hod-

notách, tedy -1 až -5, kdy -5 představuje nejvyšší nespokojenost. V kolonce váha je mezi jednotlivé faktory rozdělena hodnota 1. Musí být splněno pravidlo, že tato hodnota bude rozdělena mezi faktory tak, aby jejich součet dal právě tuto hodnotu.

Tabulka 11 – Hodnocení SWOT analýzy

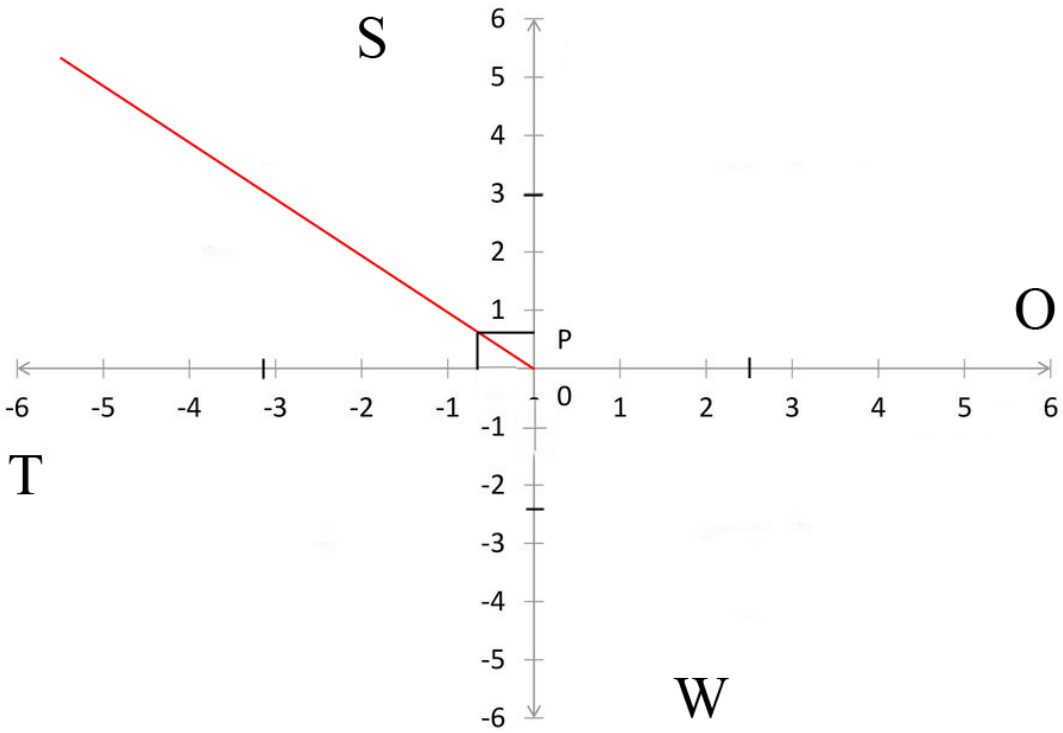
Silné stránky (S)	**Váha**	**Hodnocení**	**Součin**	**Slabé stránky (W)**	**Váha**	**Hodnocení**	**Součin**
Zabezpečovací systémy	0,30	3	0,9	Volný přístup	0,3	-3	-0,9
Personál	0,25	3	0,75	Stávající prvky EPS	0,4	-3	-1,2
Prostory	0,15	3	0,45	Schodiště	0,1	-1	-0,1
Klidná lokalita	0,12	3	0,36	Pronájem prostor	0,2	-1	-0,2
Spolupráce s PČR	0,18	3	0,54				
Součet			**3**	**Součet**			**-2,4**
Příležitosti (O)	**Váha**	**Hodnocení**	**Součin**	**Hrozby (T)**	**Váha**	**Hodnocení**	**Součin**
Zdokonalení bezpečnostních prvků	0,30	3	0,9	Vstup přes bar	0,5	-4	-2
Zabezpečení možných vstupů do objektu	0,35	3	1,05	Vstup přes restauraci	0,1	-2	-0,2
Zabezpečení schodiště	0,15	1	0,15	Pronesení zbraně	0,15	-2	-0,3
Instalace EPS	0,20	2	0,4	Aktivní střelec	0,05	-1	-0,05
				Lidský faktor	0,2	-3	-0,6
Součet			**2,5**	**Součet**			**-3,15**

Po vyhodnocení jednotlivých částí se pokračuje v sestavení matice SWOT z jednotlivých kvadrantů (S, W, O, T). V jednotlivých kvadrantech závisí na rozdílu součtu bodového ohodnocení silných a slabých stránek (interní) a součtu příležitostí a hrozeb (externí).

- Silné stránky (S) a slabé stránky (W): 3 + (-2,4) = 0,6
- Příležitosti (O) a hrozby (T): 2,5 + (-3,15) = -0,65

Posledním krokem je rozdíl interních a externích hrozeb, interní s hodnotou 0,6 a externí s hodnotou -0,65.

$$0{,}6 - (-0{,}65) = 1{,}25$$



Obrázek 18 – Matice SWOT analýzy

Na základě získaných výsledků analýzy SWOT, lze tedy poukázat, že by se v rámci objektu XY mělo zaměřit na strategii kvadrantu S – T. Strategie S – T (maxi-mini) využívá silných stránek k eliminaci hrozeb. Znamená to, že silné stránky není potřeba nijak měnit ale je potřeba se zaměřit na hrozby, které lze těmito silnými stránkami eliminovat. Nejvyšší hrozbou je vstup přes bar, na který je potřeba se důkladně zaměřit a pokusit se tuto hrozbu odstranit, popřípadě ji alespoň omezit.

7 MOŽNÁ OPATŘENÍ

Tato kapitola má za cíl nastínit možná opatření, která by mohla vylepšit zabezpečení společenských akcí (ples).

Jako největší přínos, který by přinesl větší zabezpečení, je prvek EPS. V celém objektu je nainstalován pouze jediný prvek EPS, který se nachází v prostorách rozvodny v 1. NP. Při konání plesu může dojít ke vzniku požáru. Požár může vzniknout vznícením ze zapálené svíčky na stole, nedovoleným zapálením cigarety v prostorách objektu a nedopalkem, únikem plynu, pyrotechnikou, vystoupením s použitím zápalných látek atd. Proto by bylo vhodné nainstalovat další hlásiče a to v prostorech 1. patra u společných toalet v hale propojující restauraci, bar a objekt XY. Dále by byla vhodná instalace EPS v tomtéž patře v hlavní hale u šaten. Pro druhé patro by měli být EPS nainstalovány v prostorách skladu, foyer a v hale u toalet. Ve třetím posledním patře alespoň jedno EPS instalováno ve vstupní hale mezi jednotlivými kancelářemi. Pomocí takto instalovaných EPS by se zaručila vyšší bezpečnost a prevence vzniku požáru. Celkem by tedy došlo o rozšíření šesti detektory. Návrhy lze vidět v přílohách viz. obrázky č. 23 – 25.

Dalším přínosem by bylo rozšíření CCTV systémů. Především o instalaci dalších bezpečnostních kamer a to v prvním patře v prostorách před barem, odkud je možný vstup do objektu a mohou zde také vzniknout potyčky, popřípadě zničení prostor opilými návštěvníky. Dále ve druhém patře přidání kamer do společenského sálu, k baru naproti schodišti s úhlem viditelnosti i na protější foyer a ve třetím patře do haly s jednotlivými kancelářemi. Jednalo by se tedy o rozšíření celkem o 4 bezpečnostní kamery. Levnější variantou by v tomto případě mohlo být zavedení kamerových atrap. Tato varianta by přišla na pár stovek korun ale při vzniku nějaké situace či výtržnictví by nebyli zachovány žádné audiovizuální stopy. Návrhy lze vidět v přílohách viz. obrázky č. 20 – 22.

Třetím bezpečnostním prvkem, který by měl být rozšířen je pohybové čidlo PIR. Jednalo by se pouze o jedno rozšíření a to v 1. patře v hale mezi barem a malým a loutkovým sálem. Při vniknutí do objektu, například oknem nebo prolomení dveří přes bar zde chybí pohybové čidlo, které by narušitele zaznamenalo. Proto by bylo vhodné na toto místo nainstalovat pohybové čidlo pro důkladnější zabezpečení prostor objektu. Návrhy lze vidět v přílohách viz. obrázek č. 26.

Jedním z nebezpečných faktorů na plese jsou schody. Schody, které se nacházejí v objektu XY jsou příliš ostré a kluzké. Pro zabezpečení by bylo vhodné tyto schody upravit anebo

na ně aplikovat alespoň koberec. Nedocházelo by k úrazům z důvodu uklouznutí a následnému pádu na ostrou hranu. Dalším bodem by mohlo být přidání uzamykatelné brány nad schodiště. Jedna brána je instalována nad hlavní schodiště. Vedlejší schodiště ji bohužel nemá. Kdyby byla tato brána nainstalována i na tomto schodišti, zabezpečila by ostatní prostory objektu a ulehčila i tak práci pořadatelům s kontrolou dalších prostor.

Velkým rizikem jsou průchozí místa v době konání plesu. Jen malá většina plesů má uzamčena bar pro vlastní účely. To samé platí také pro restauraci. Bar i restaurace jsou přístupné pro veřejnost a mají volný vstup do hlavní haly, odkud se lze dostat do společenského sálu po schodišti nebo výtahem. Pro pořadatele je pak prací navíc odhánět podnapilé návštěvníky baru a restaurace, kteří se pokouší dostat na tyto plesy. Dalším nebezpečím může být pronesení nebezpečných látek, zbraní nebo materiálu, které mohou ohrozit životy jak návštěvníků, tak ale i samotných pořadatelů. Jak restaurace, bar tak ale i objekt mají sdílené toalety v prvním patře. Bylo by vhodné uzamknout při konání plesu spodní dveře oddělující vstupní halu s barem a restaurací. Návštěvníci mohou navštěvovat toalety v 2. patře, které se nacházejí u společenského sálu. Předešlo by se tím tak šarvátkám a zbytečným konfliktům.

ZÁVĚR

Diplomová práce byla zaměřena na problematiku zabezpečení společenských akcí. Práce je rozdělena do dvou částí, a to na část teoretickou a praktickou. Teoretická část je složena ze tří kapitol.

V teoretické části jsou obecně popsány společenské akce, jejich rozdělení a podmínky pro jejich organizaci. Druhá kapitola obsahuje základní poznatky z oblasti bezpečnostních systémů, které jsou hojně využívány při zabezpečení společenských akcí ale i mimo ně. Poslední kapitolou jsou základní pojmy, mezi nimiž jsou vybrány ty nejdůležitější pro danou problematiku.

Praktická část práce je složena ze čtyř kapitol. Čtvrtá kapitola popisuje použité metody a analýzy v rámci diplomové práce a její hlavní a dílčí cíle. Pátá kapitola je zaměřena na zabezpečení společenských akcí ve vybraném objektu. V této práci je objekt uveden jako objekt XY. Jsou zde definovány a naznačeny jednotlivé bezpečnostní prvky, které jsou v tomto objektu nainstalovány a používány.

Šestá kapitola je zaměřena na analýzu rizik. V rámci analýzy byly zvoleny dvě metody. První metodou je metoda KARS, tedy kvalitativní analýza rizik s využitím jejich souvztažnosti. V této metodě bylo vytyčeno 10 rizik, která se mohou v rámci společenských akcí objevit. Ze vzešlých výsledků se pak zjistilo, na co je potřeba se nejvíce soustředit a jaká rizika nejsou na tolik podstatná. Druhou zvolenou metodou byla metoda SWOT analýzy. V této analýze byly vytvořeny celkem čtyři kvadranty, a to silných stránek, slabých stránek, příležitostí a hrozeb. Do každé kategorie se posléze vypsaly jednotlivé faktory, které buď byly silnou stránkou objektu, příležitostí, slabinou anebo hrozbou.

Poslední kapitolou jsou možná opatření. Zde jsou uvedena navrhnutá vylepšení, jak zajistit lepší zabezpečení společenských akcí a celého objektu.

Cíle práce byly definovány jako seznámení se s teoretickými základy zabezpečovacích systémů, zaměření se na problematiku jednotlivých bezpečnostních systémů, konkretizace společenské akce, navržení opatření pro zabezpečení společenských akcí a diskuze nad získanými výsledky. Hlavní otázkou této diplomové práce je, zda je daný objekt dostatečně zabezpečen pro konání společenských akcí. Z výsledků analýzy vyplynulo, že objekt XY je dostatečně zabezpečen pro konání společenských akcí. V objektu jsou vyhovující podmínky a bezpečnostní systémy pro organizaci a zabezpečení společenských akcí.

SEZNAM POUŽITÉ LITERATURY

[1] Bezpečnostní standardy pro pořadatele sportovních, kulturních a společenských akcí[online]. Centrum proti terorismu a hybridním hrozbám, 2017, [cit. 2019-04-22]. Dostupné z: http://www.mvcr.cz/cthh/soubor/brozura-bezpecnostni-standardy-pro-poradatele-sportovnich-kulturnich-a-spolecenskych-akci.aspx

[2] BRABEC, František. Bezpečnost pro firmu, úřad, občana. Praha: Public History, 2001, ISBN 80-86445-04-6.

[3] CCTV kamerové systémy, c2017. In: Https://lubicon.cz [online]. Praha: Lubicon [cit. 2019-04-16]. Dostupné z: https://lubicon.cz/wp-content/uploads/2016/12/CCTV-1.png

[4] CIMBÁLNÍKOVÁ, Lenka, Jana BILÍKOVÁ a Pavel TARABA, 2013. Databáze manažerských metod a technik. Ostrava: Pro Fakultu logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně vydal Repronis. ISBN 978-80-7329-380-2.

[5] DAMJANOVSKI, Vlado, c2005. CCTV: networking and digital technology. 2nd ed. Boston: Elsevier/Butterworth Heinemann. ISBN 07-506-7800-3.

[6] DŽERMANSKÝ, Martin, 2017. *KARS*. Uherské Hradiště. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení. Vedoucí práce Ing. Martin Hart, Ph.D.

[7] EPS, c2019. In: Http://gextonsecurity.com [online]. Hyderabad: Gextonsecurity [cit. 2019-04-16]. Dostupné z: http://gextonsecurity.com/wp-content/uploads/2015/09/slide4.png

[8] IVANKA, J. Systemizace bezpečnostního průmyslu. [skriptum]. Zlín: UTB, 2014. ISBN 978-80-7454-410-1.

[9] JA-80P, 2018. Jabloshop [online]. Praha: Jablotron [cit. 2019-04-22]. Dostupné z: https://www.jabloshop.cz/ja-80p-bezdratovy-pir-detektor-pohybu-osob

[10] JA-80s, 2018. Rsa-tp.cz [online]. Jablonec nad Nisou: Jablotron [cit. 2019-04-22]. Dostupné z: http://eshop.rsa-tp.cz/out/manualy/ja-80s.pdf

[11] Kamerové systémy [online], c2020. Liberec: TOREX SECURITY [cit. 2019-04-16]. Dostupné z: http://www.kamerove-systemy-torex.cz/barevne-kamery

[12] KINDL, Jiří, 2004. Projektování bezpečnostních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 80-731-8165-7.

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

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

[15] LUKÁŠ, Luděk, 2015. Bezpečnostní technologie, systémy a management. III. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-35-4.

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

[17] NEČESAL, Luboš, 2012. Ústředny PZTS. In: Www.atpjournal.sk [online]. Zlín: Zlín [cit. 2019-04-16]. Dostupné z: www.atpjournal.sk/buxus/images/cache/annotation/image_14869_30_v1.jpeg

[18] PROCHÁZKOVÁ, Dana, 2007. Bezpečnost lidského systému. V Ostravě: Sdružení požárního a bezpečnostního inženýrství. Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 978-80-86634-97-5.

[19] SONY XC-4AM, c2020. Kamerové-systémy-torex [online]. Liberec: TOREX SECURITY, spol. s r.o [cit. 2019-04-22]. Dostupné z: http://www.kamerove-systemy-torex.cz/barevne-kamery

[20] Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu. [online]. 2016, [cit. 2019-04-22]. Dostupné z: www.mvcr.cz/soubor/terminologicky-slovnik-mv-verze-ke-stazeni.aspx

[21] VACEK, Jiří. 2000. Proč se tvoří skupiny. Katedra managementu, inovací a projektů [online]. Západočeská univerzita v Plzni [cit. 2015-05-07]. Dostupné z: http://www.kip.zcu.cz/kursy/imi/www/4_skupiny/4_4.htm

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

[23] ZÁKLADY OCHRANY MĚKKÝCH CÍLŮ: METODIKA [online]. Praha: Ministerstvo vnitra České republiky, 2016 [cit. 2019-04-22]. Dostupné z: http://www.mvcr.cz/soubor/metodika-zaklady-ochrany-mekkych-cilupdf.aspx

[24] Závěrečná práce - metodika, c2007-2013. Lorenc.info [online]. Praha: VŠE [cit. 2019-04-29]. Dostupné z: http://lorenc.info/zaverecne-prace/metodika.htm

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

HZS	Hasičský záchranný sbor.
ČR	Česká republika.
PČR	Policie české republiky.
ZZS	Zdravotnická záchranná služba.
IZS	Integrovaný záchranný systém.
CCTV	Uzavřený televizní okruh.
EPS	Elektrická požární signalizace.
PZTS	Poplachový zabezpečovací a tísňový systém.
HW	Hardware.
HDD	Harddisk.
SW	Software.
ÚOOÚ	Úřad pro ochranu osobních údajů.
ČSN	Česká technická norma.
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.
IP	Identifikační číslo síťového rozhraní v počítačové síti.
LED	Elektroluminiscenční dioda.
IR	Infračervené záření.
UV	Ultrafialové záření.
UV/IR	Ultrafialové/infračervené (UV/IR) hlásiče plamene.
MZS	Mechanické zábranné systémy.
PKB	Průmyslová komerční bezpečnost.
PPS	Poplachový přenosový systém.
LAN	Lokální síť.
GSM	Global systém for mobile communications.

GPRS	General packet radio service.
SMS	Služba krátkých textových zpráv.
PSTN	Veřejná telefonní síť.
LCD	Liquid crystal display.
PIR	Detektor pohybu.
px	Obrazový prvek.
mA	Miliampér.
DVR	Digital video recorder.
AHD	Analog high definition.
RAM	Operační paměť.
VGA	Video graphics array.
OS	Operační systém.
MHz	Megahertz.
KARS	Kvalitativní analýza rizik s využitím jejich souvztažnosti.
SWOT	Analytická metoda srovnávající silné a slabé stránky, příležitosti a hrozby.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: MATODIKA ZPRACOVÁNÍ DIPLOMOVÉ PRÁCE

Výběr tématu diplomové práce.

Konzultace nad zvoleným tématem diplomové práce s vedoucím práce.

Vyhledání odborné literatury a zdrojů o dané problematice.

Nastudování literatury a dalších materiálů.

Tvorba teoretické části diplomové práce.

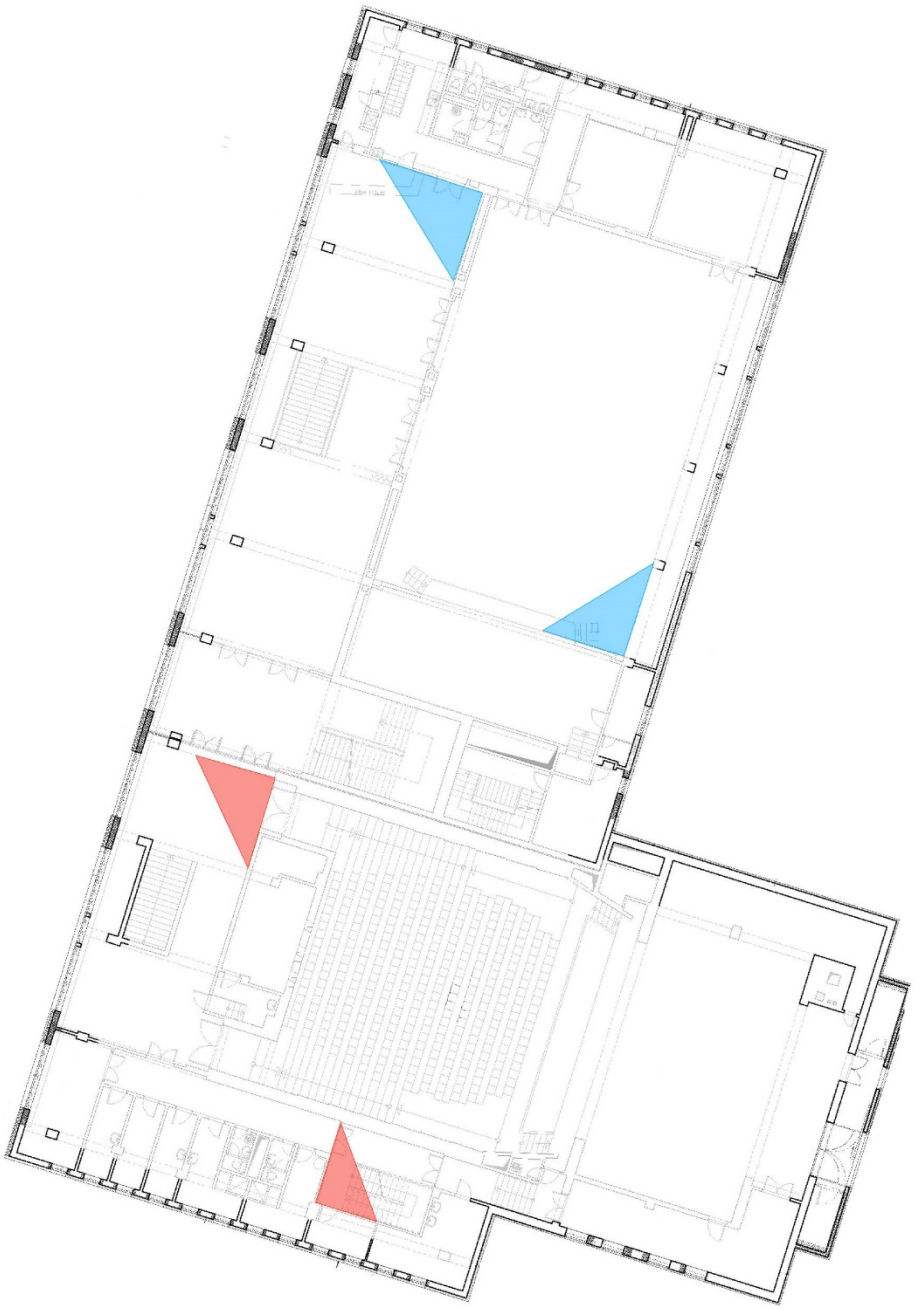
Určení metod využitých v praktické části diplomové práce.

Tvorba praktické části diplomové práce.

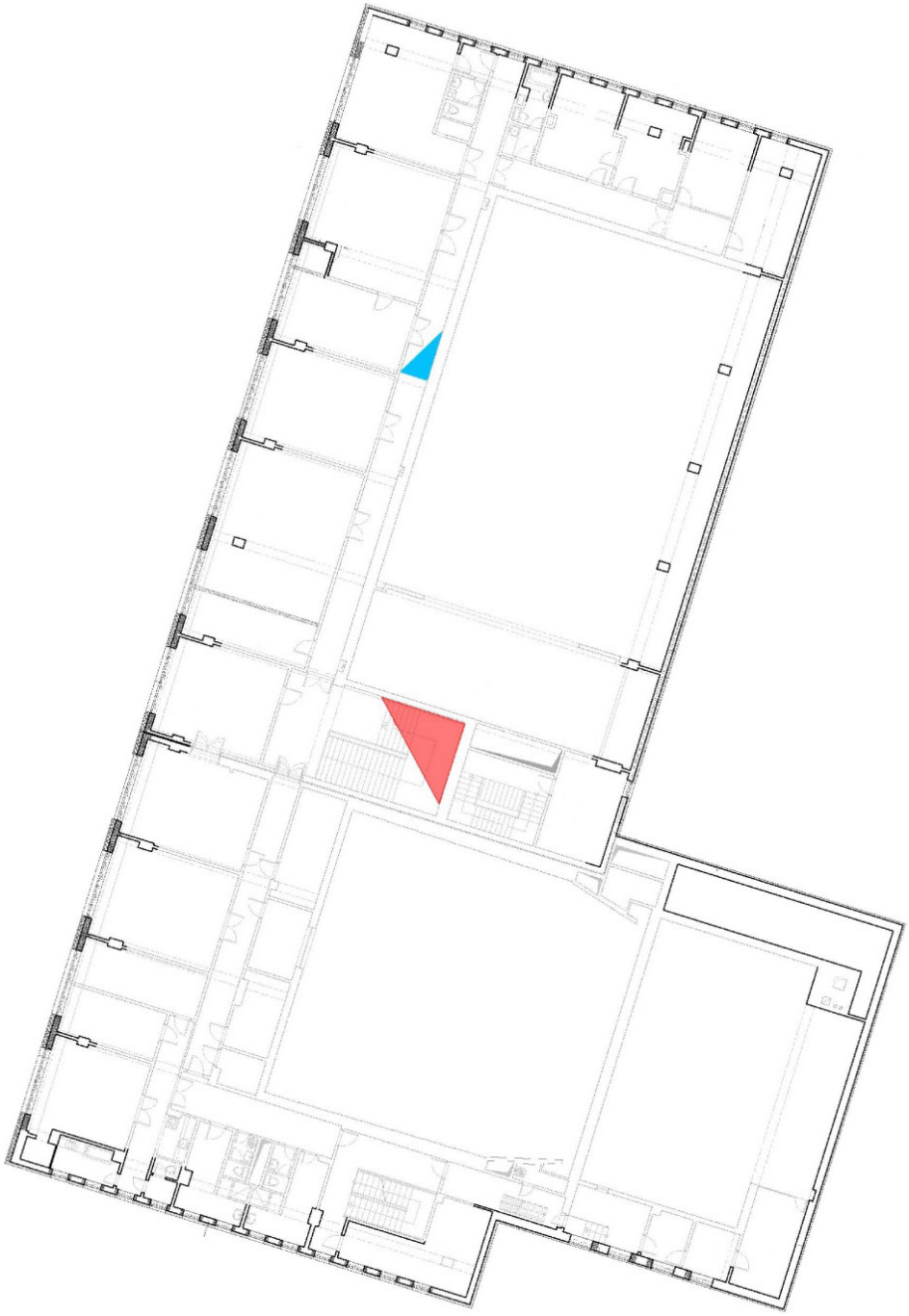
Během zpracování diplomové práce probíhali konzultace s vedoucím diplomové práce Ing. Jakubem Rakem, Ph.D.

PŘÍLOHA P II: SCHEMATICKÝ NÁVRH ROZŠÍŘENÍ BEZPEČNOSTNÍCH PRVKŮ

Obrázek 19 – Návrh rozšíření CCTV systémů 1. NP

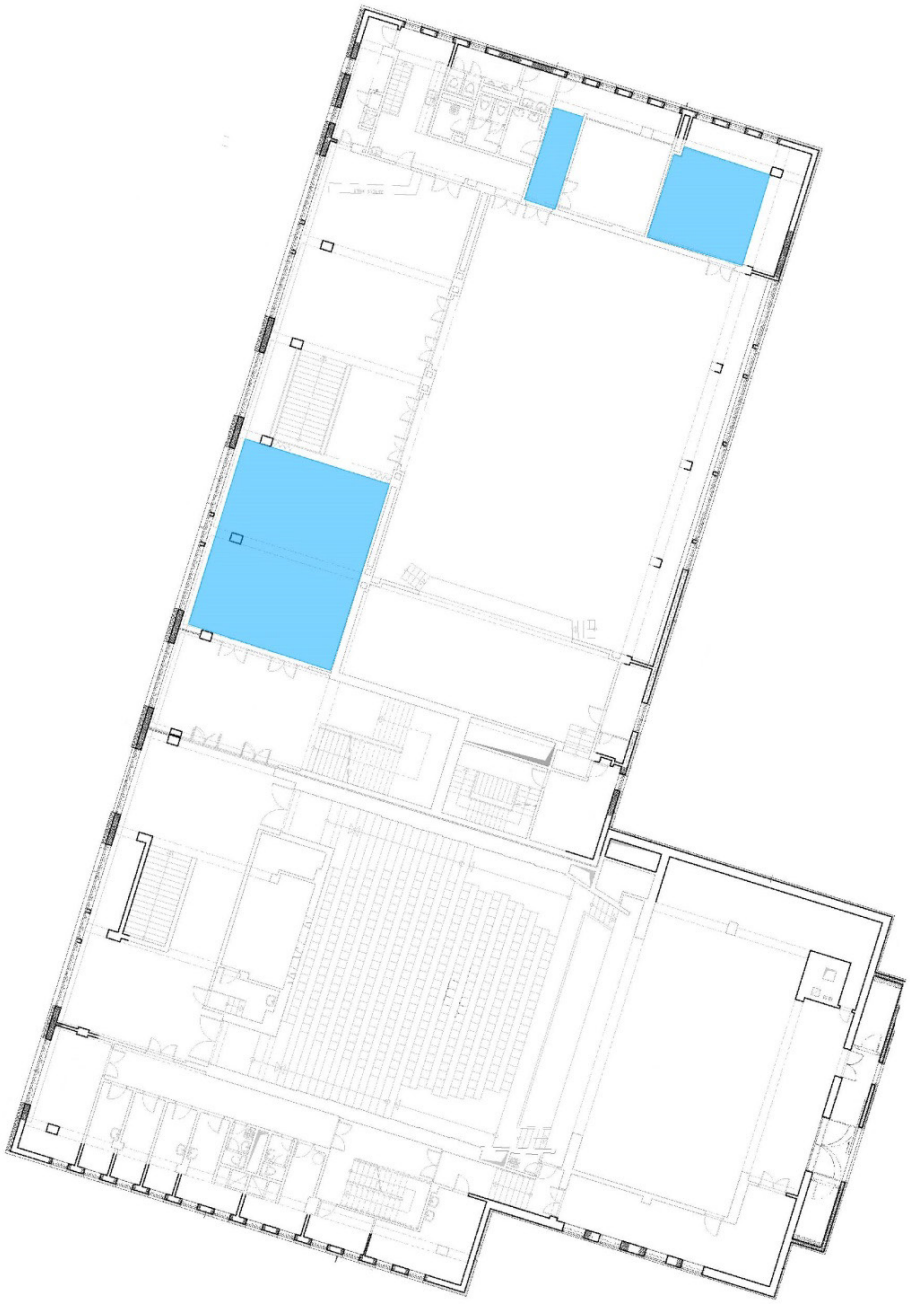


Obrázek 20 – Návrh rozšíření CCTV systémů 2. NP

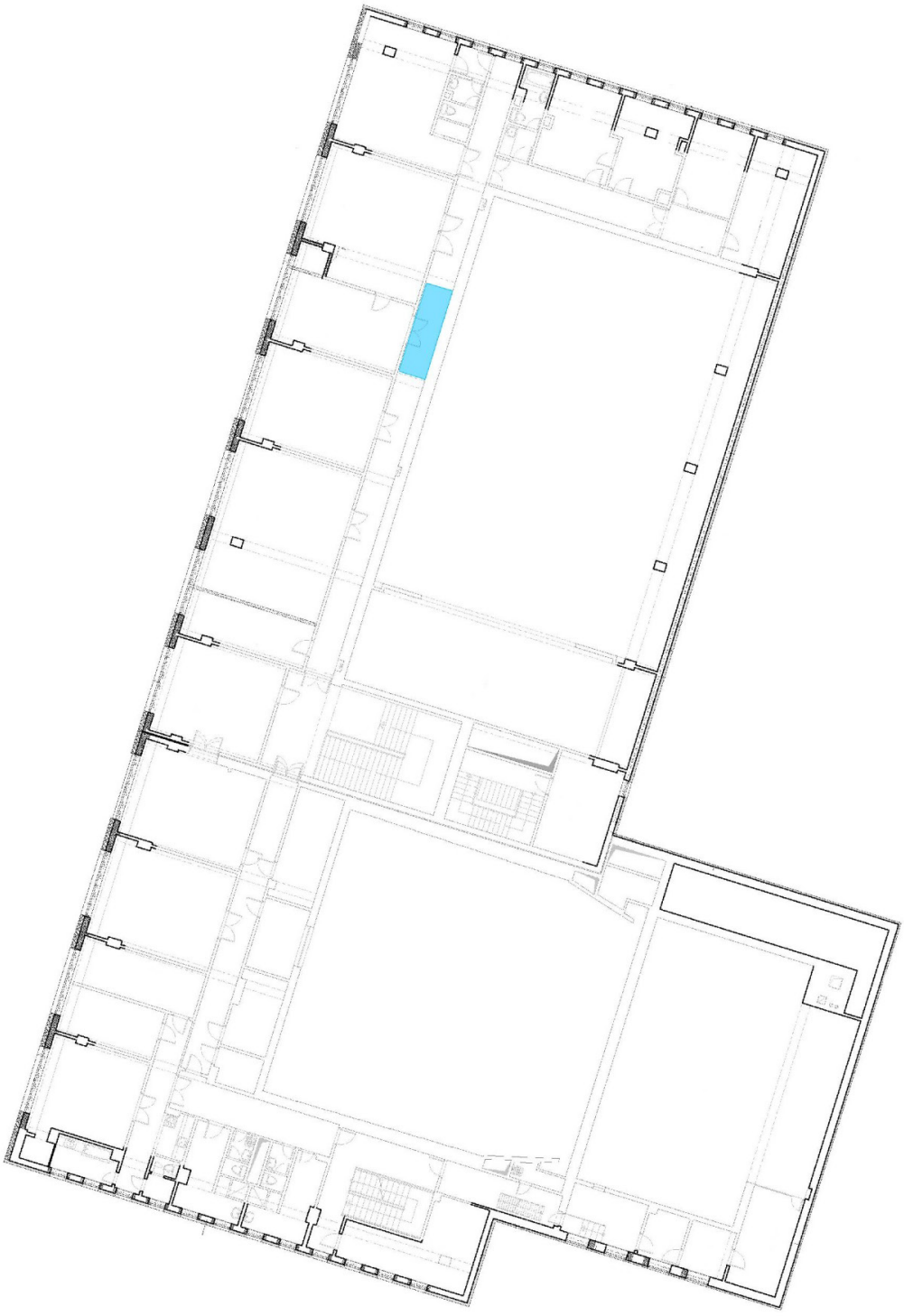


Obrázek 21 – Návrh rozšíření CCTV systémů 3. NP

Obrázek 22 – Návrh rozšíření EPS systémů 1. NP



Obrázek 23 – Návrh rozšíření EPS systémů 2. NP



Obrázek 24 – Návrh rozšíření EPS systémů 3. NP

Obrázek 25 – Návrh rozšíření PIR detektoru 1. NP