Fyzická bezpečnost vybrané instituce

Klára Burdová

Bakalářská práce
2020

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: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Klára Burdová**
Osobní číslo:	**L17176**
Studijní program:	**B2825 Ochrana obyvatelstva**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Fyzická bezpečnost vybrané instituce**

Zásady pro vypracování

1. Seznamte se teoretickými základy problematiky fyzické bezpečnosti a její aplikace ve zvolené oblasti.
2. Zvolte si objekt/organizaci pro realizaci analýzy úrovně fyzické bezpečnosti.
3. Realizuje analýzu současného stavu fyzické bezpečnosti zvoleného objektu/organizace.
4. Vyhodnoťte současný stav fyzické bezpečnosti zvoleného objektu/organizace, případně navrhněte její rozšíření.

Rozsah bakalářské práce:
Rozsah příloh:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. BAKER, Paul R. a Daniel J. BENNY. The complete quide to physical security. Boca Raton: CRC Press, c2013, xxi, 339 s. ISBN 9781420099638.
2. LOVEČEK, Tomáš. Bezpečnostné systémy : poplachové systémy. Žilina: Edis, 2015. ISBN 978-80-5541-144-6.
3. VALOUCH, Jan. Projektování bezpečnostních systémů [online]. Zlín: Univerzita Tomáše Bati ve Zlíne, 2012 [cit. 2019-10-22]. ISBN 9788074542305. Dostupné z: http://hdl.handle.net/10563/18663
4. VALOUCH, Jan. Projektování integrovaných systémů [online]. 2. vyd. Zlín, 2015 [cit.2019-10-22]. ISBN 9788074545573. Dostupné z: http://hdl.handle.net/10563/18616
Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Jakub Rak, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. listopadu 2019**
Termín odevzdání bakalářské práce: **15. května 2020**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2019

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou 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 bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 15.5.2020

Jméno a příjmení studenta: Klára Burdová

.....
podpis studenta

ABSTRAKT

Bakalářská práce se zabývá problematikou fyzické bezpečnosti vybrané instituce. Hlavním cílem této práce je identifikovat hlavní rizika a následně navrhnout vhodná bezpečnostní opatření. V teoretické části jsou popsány právní předpisy upravující fungování této problematiky a následně jsou charakterizovány pojmy bezpečnost a bezpečnostní riziko. Dále je v bakalářské práci kladen důraz na rozdělení fyzické bezpečnosti a komponentů zastupujících poplašné systémy. Poslední teoretická část je věnována detektorům narušení, kde jsou blíže charakterizovány jejich zástupci a možnosti jejich využití. Praktická část vychází částečně z teoretické, kdy je vybraná instituce detailně popsána z hlediska bezpečnostních prvků. V rámci posuzování rizik byl využit program RISKAN a zároveň uskutečněn experiment. Na základě těchto analýz byly zjištěny slabé stránky, ke kterým jsou navrhnuta vhodná opatření, která by doplňovala a rozšiřovala Fyzickou bezpečnost v tomto objektu.

Klíčová slova: bezpečnost, bezpečnostní riziko, zabezpečení, ochrana, detektor, fyzická bezpečnost.

ABSTRACT

The bachelor's thesis deals with the issue of Physical Security of a selected institution. The main aim of this work is to identify the main risks and then propose appropriate security measures. The theoretical part describes the legislation governing the functioning of this issue and then characterizes the concepts of security and security risk. Furthermore, the bachelor's thesis emphasizes the division of physical security and components representing alarm systems. The last theoretical part is devoted to intrusion detectors, where their representatives and the possibilities of their use are closely characterized. The practical part is based partly on the theoretical part, where the selected institution is described in more detailed way in terms of security features. The RISKAN program was used as part of the risk assessment and an experiment was also carried out at the same time. Based on these analyses, weaknesses were identified, for which appropriate measures are proposed, which would complement and expand the Physical Security in this institution.

Keywords: safety, security, security risk, protection, detector, physical security

Poděkování:

Tímto způsobem bych chtěla poděkovat panu Bc. Martinu Poláškovi, který mi byl nápomocný při psaní této práce. Za jeho aktivní a vřelý přístup při poskytování cenných informací a zpětnou vazbu. Zároveň chci poděkovat paní Ing. Alici Mikloškové z firmy Dormakaba s.r.o., že byla velice laskavá a vstřícná poskytnout informace k dané problematice. Dále děkuji svému vedoucímu bakalářské práce panu Ing. Jakubovi Rakovi, Ph.D za jeho rady a připomínky.

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

OBSAH

ÚVOD

Pojem bezpečnost udává jednu z nejdůležitějších hodnot u každé z komunit lidí. Pokud není zajištěna dostatečná úroveň bezpečnosti, není v tomto případě možné, aby člověk nebo skupina lidí byli dostatečně uspokojeni, a tudíž nemohou vytvářet další činnosti. I z tohoto důvodu se zajištění bezpečnosti nachází na druhé příčce v Maslowově pyramidě potřeb ihned za fyziologickými potřebami. Ochrana osob a majetku je cílem nejen Bezpečnostní politiky ČR, ale také samostatných institucí a podniků. V této bakalářské práci na téma Fyzická bezpečnost vybrané instituce bude řešena jedna konkrétní sbírkotvorná instituce, která spadá jako celek do movitého kulturního dědictví. Jedná se o muzejní instituci.

Vybrané muzeum je řazeno mezi regionální muzea v České republice, kde se každý den shlukují větší počty lidí. Jeden z nároků muzea je zajistit dostatečnou ochranu všech přítomných osob, tzn. i z řad zaměstnanců a zároveň zajistit bezpečnostní standard všech historicky cenných sbírek. Bezpečnostní prvky sbírkových exponátů jsou zaměřeny nejen proti možnému fyzickému kontaktu pachatele, ale také proti negativním vlivům klimatických podmínek, kdy by jejich špatně nastavené hodnoty měly devastační účinky na vybrané druhy historických předmětů. Dle statistik patří mezi jedny z největších ohrožujících faktorů působení lidského činitele - z toho důvodu je tato práce zaměřena na zajištění fyzické bezpečnosti.

Hlavním cílem této bakalářské práce je identifikovat bezpečnostní rizika a navrhnout optimalizaci systému ochrany před nimi. Mimo hlavní cíl, práce definuje i cíle dílčí a to definování aktiv a hrozeb a ověření dodržování režimových opatření.

Práce se dělí na dvě části, první část je věnována teorii, kde jsou popsány základní právní předpisy týkající se této problematiky. Dále jsou popsány základní typy a dělení fyzické bezpečnosti, která je strukturována na klasickou, režimovou, fyzickou a technickou ochranu. Toto rozdělení tvoří základní kámen fyzické bezpečnosti. Okrajově jsou uvedeny i teoretické základy Elektronické požární signalizace, která svým způsobem také spadá pod tuto oblast. V poslední kapitole této části je vysvětlena problematika detektorů, konkrétně jejich dělení a princip funkčnosti. V druhé části, tedy části praktické, jsou uvedeny bližší informace týkající se činnosti vybrané instituce a zároveň je zde charakterizováno a popsáno současné zabezpečení dle typů ochrany. Součástí je také posuzování rizik, kde byl s pomocí programu RISKAN vygenerován výstup, který ukazuje, jaká aktiva jsou nejzranitelnější a v jaké míře. Poté je učiněn experiment, jehož stanovená hypotéza byla parciálně potvrzena. Na základě

těchto analytických metod byly navrženy další možné prvky, které by podpořily úroveň fyzické bezpečnosti.

V práci byly použity vědecké metody a to analýza rizik, experiment a diskuze navrhovaných opatření. Metoda analýzy byla použita k ohodnocení zranitelnosti aktiv jednotlivými hrozbami. Další metoda experimentu sloužila k ověření dodržování režimových opatření a zodpovědnosti zaměstnanců. Diskuze je založena na shrnutí a posouzení reálnosti nasazení navržených opatření. Bakalářská práce vycházela z omezení, kterým byla anonymizace instituce.

I. TEORETICKÁ ČÁST

1 LEGISLATIVA

V první části kapitoly jsou sepsány právní předpisy, kterým fyzická bezpečnost objektu podléhá a zároveň je jimi upravována. Samotné téma fyzické bezpečnosti nemá v našem státě svůj vlastní upravující zákon, proto se tedy řídí několika právními předpisy. Druhá část je věnována zákonům souvisejícím s ochranou kulturních statků a muzejních exponátů, které by měly zabezpečit jejich maximální ochranu před různými vlivy.

Ústava České republiky

Ústava ČR setrvává na vrcholu právních předpisů a má vždy přednost před ostatními právními normami. Balíček zákonů byl přijat 16. prosince 1993, ale její účinnost spadá na den vzniku samostatné České republiky, a to 1. ledna 1993. Celé znění právního předpisu je zákon č. 1/1993 Sb. Ústava České republiky. Je složena z předmluvy tzv. preambule, osmi hlav a je zde obsaženo sto třináct článků. Ústava ČR, soubor právních norem, zahrnuje všechny základní pravomoci a povinnosti občana, dále charakterizuje stát, obsahuje soustavu nejvyšších státních orgánů moci a státní znaky. [44]

Listina základních práv a svobod

Listina základních práv a svobod je dána zákonem č. 2/1993 Sb., který byl v roce 1992 schválen předsednictvem ČNR a je součástí ústavního pořádku. Obsahem je šest hlav, které jsou tvořeny čtyřiceti čtyřmi články. Klade se zde důraz na ochranu a nedotknutelnost osoby - zároveň jejího soukromí, na nedotknutelnost obydlí, a právo na ochranu před nepovoleným zásahem do rodinného a soukromého života. [43]

Občanský zákoník

Zákon č. 89/2012 Sb., Občanský zákoník, je zákoník, který upravuje hmotné soukromé právo daného státu. V oblasti procesního práva je zákoník doplněn soudním řádem - v ČR je to občanský soudní řád. Občanský zákoník České republiky je složen z pěti částí, a to obecné části, rodinného práva, absolutního majetkového práva, relativního majetkového práva a páté části zabývající se ustanoveními společnými, přechodnými a závěrečnými. [51]

Trestní zákoník

Zákon č. 40/2009 Sb., Trestní zákoník, je základním předpisem trestního práva hmotného. Popisuje trestní chování a vymezuje způsob trestu za toto chování. Zákoník obsahuje čtyři sta dvacet jedna paragrafů a dělí se na dvě části, obecnou a zvláštní. První část se zabývá

působností zákona, trestní odpovědností a trestními sankcemi. Po ní následuje druhá část, pojmenována zvláštní část, která obsahuje skutkové podstaty trestných činů. [50]

Trestní řád

Zákon č. 141/1961 Sb., o trestním řízení soudním, vymezuje postup soudu a ostatních orgánů v trestním řízení. Zajišťuje tak řádné prošetření trestných činů a spravedlivé potrestání jejich pachatelů. Tento zákon se také nazývá trestní řád. [53]

Zákon č. 122/2000 Sb., O ochraně sbírek muzejní povahy a o změně některých dalších zákonů, ve znění pozdějších předpisů.

Jak již z názvu vyplývá, tak předmětem zákona je vytýčení podmínek ochrany sbírek, především uchovávaných v muzeích a galeriích, způsoby vedení evidence sbírek, práva a povinností vlastníků sbírek, veřejně prospěšné služby muzeí a potrestání za neplnění stanovených podmínek a pravidel. [52]

Vyhláška č. 275/2000 Sb., kterou se provádí zákon č. 122/200 Sb., o ochraně sbírek muzejní povahy

Vyhláška se zabývá zejména stanovením postupů pro trvalé uchovávání sbírek a jednotlivých sbírkových předmětů, vedení sbírkové evidence a inventarizaci sbírek. Například konkrétně upravuje zajištění předmětů mechanickými a elektronickými zabezpečovacími systémy, režim vstupu cizích osob, hlídání stálou ostrahou či ochranu těchto předmětů před požáry a dalšími poškozeními. [57]

Metodický pokyn č. j.: 53/2001 k zajišťování správy, evidence a ochrany sbírek muzejní povahy v muzeích a galeriích zřizovaných Českou republikou nebo územními samosprávnými celky (kraji, obcemi).

Navazuje na zákon č. 122/2000 Sb. a na vyhlášku č. 275/2000 Sb., sjednocuje postupy při práci se sbírkami. Je závazný jen pro muzea a galerie zřizované Českou republikou nebo územním samosprávným celkem (krajem, obcí). Pro ostatní představuje pouze doporučující obsah. [33]

Další zákony týkající se problematiky

Zákon č. 110/2019 Sb. o zpracování osobních údajů (GDPR), Zákon č. 20/1985 Sb. o státní památkové péči, Zákon č. 71/1994 Sb. o prodeji a vývozu předmětů kulturní hodnoty, Zákon č. 133/1985 Sb. o požární ochraně, ve znění pozdějších předpisů, Zákon č. 499/2004 Sb. o archivní a spisové službě, zákon č. 251/2007 Sb. knihovní zákon, zákon č. 101/2001 Sb.

o navrácení nezákonně vyvezených kulturních statků, zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti a další. [21]

2 BEZPEČNOST A BEZPEČNOSTNÍ RIZIKA

2.1 Bezpečnost

Pojem bezpečnost je základním kamenem bezpečnostní terminologie. Tento termín je využíván v běžném rozhovoru či vědních oborech, ve kterých dochází k jeho konkretizaci a vytvářejí se různá slovní spojení. Pokud je bezpečnost v aktivním stavu, znamená to, že jsou v absenci určité hrozby. Latinsky se tento termín překládá jako securus, kdy se jedná o stav klidný a bezstarostný. [54]

Ve dvou jazycích jsou pro bezpečnost užívány dva termíny, v anglickém jazyce to je security a safety, ve francouzském jazyce sécurité a sûreté. V jiném jazyce tento pojem nemá ekvivalent. V obou případech se jedná o stejný význam slova, avšak každý představuje jinou část bezpečnosti. Security a sécurité znamená ochrana neboli odvrácení od případných útoků. Jedná se o ochranu osob, majetku, informací, systému a procesů. V druhém případě, u pojmu safety a sûreté je bezpečnost brána jako ochrana před antropogenními a přírodními hrozbami. Řadíme zde například BOZP, požární ochranu či prevenci závažných havárií. Je zřejmé, že jejich protiopatření se v zásadě liší. [29, 30]

Lze říci, že pokud se člověk cítí zabezpečen - je tzv. mimo nebezpečí - a je schopen se dále rozvíjet, je mu odstraněna jedna z bariér, která by ho mohla zpomalovat na jeho životní cestě. Tento fakt potvrzuje americký psycholog Abraham Maslow ve své Maslowově pyramidě lidských potřeb, kde jsou kategorizovány lidské potřeby do pěti skupin. V první řadě musí lidé uspokojit potřeby nižšího stupně, což jsou fyziologické potřeby, aby mohl uspokojovat potřeby vyššího řádu. Pocit bezpečí se nachází ve druhé skupině hned za fyziologickými potřebami, a pokud člověk tyto dva požadavky splňuje, teprve potom je schopný vést spokojený život, ve kterém nalézá lásku, úctu a následně je schopný se seberealizovat. [31]

Obr. 1 - Maslowova pyramida potřeb [38]

V nynější době je problematika bezpečnosti stále vážnějším a aktuálnějším tématem, a to nejen v samotném státě, ale také v konkrétních podnicích, institucích a organizacích, kde se pomocí bezpečnostní politiky stanovují určité cíle, metody, analýzy a nástroje omezující a zabraňující působení bezpečnostních hrozeb různého charakteru.

2.1.1 Dělení bezpečnosti

Bezpečnost je obecně stav, kdy jsou co nejefektivněji eliminovány hrozby pro určitý objekt a kdy je k eliminaci potencionálních a stávajících hrozeb objekt efektivně vybaven a ochoten při ní spolupracovat. Z hlediska objektu, jehož bezpečnost má být zajištěna, se rozlišuje:

- **Vnitřní bezpečnost** – ochrana, prevence a odstraňování rizik působících zevnitř objektu
- **Vnější bezpečnost** – ochrana, prevence a odstraňování rizik působících zvnějšku objektu [54]

2.2 Bezpečnostní riziko

Vyjadřuje pravděpodobnost vzniku události, která je považována z bezpečnostního hlediska za nežádoucí. Riziko může být odvoditelné a odvozené z konkrétní hrozby. Míru rizika je možno vyhodnotit na základě tzv. analýzy rizik. Riziko vyjadřuje reakci na hrozbu neboli na aktuální stav zranitelnosti. [54]

Ani muzejní objekty se nemohou bezpečnostním rizikům vyhnout. K vyloučení hrozeb a rizik, případně zmírnění jejich dopadu, se buduje bezpečnostní systém. Ten slouží k zajištění maximálně možné bezpečnosti objektu muzea. Před zavedením bezpečnostního systému se

musí nejdříve provést identifikace hrozeb ohrožujících sbírky, majetek či návštěvníky a pracovníky. Následně se zpracovává analýza rizik, ze které vyplynou bezpečnostní rizika, na základě kterých se vyhodnocují způsoby zabezpečení těchto rizik. Výstupem je poté plán eliminace rizik (bezpečnostní plán), který zahrnuje všechna opatření, kterými se docílí jejich snížení na přijatelnou úroveň. [21, 29]

Česká republika vlastní tři typy dokumentů podrobně popisující toto téma. Audit národní bezpečnosti, Koncepce ochrany obyvatelstva a Bezpečnostní strategie České republiky. Nalezneme zde výčet největších hrozeb, které svým vlivem ohrožují nejen zmiňovaný stát, ale také kritickou infrastrukturu, měkké cíle a samotné obyvatelstvo. Výčet však není konečný, neboť samotné subjekty pak dennodenně čelí dalším hrozbám.

2.2.1 Potencionální rizika a jejich zdroje

V muzeích je uchována významná část hmotného kulturního dědictví a sbírek, které jsou prezentovány široké veřejnosti. Muzeum pořádá různé besedy, vernisáže, přednášky, koncerty, kde se během těchto akcí v daném objektu muzea vyskytuje vysoká koncentrace osob, ať už návštěvníků, zaměstnanců či pracovníků externích služeb. Potencionálnímu ohrožení a nebezpečí mohou být v těchto případech vystaveny zpřístupněné sbírky, majetek, vyskytující se osoby nebo celá budova muzea. [21]

Muzejní objekty mohou ovlivnit tyto hrozby:

- **Extrémní vnější vlivy** – ty můžeme rozdělit na klimatické a ostatní. Do klimatických se řadí extrémní projevy změn počasí (kalamity, krupobití), povodně, zemětřesení, pád tělesa, aj. Mezi ostatní se řadí únik nebezpečných látek, výbuchy, radiační havárie, epidemie, apod.

- **Požár** – při požáru hrozí nebezpečí narušení stability objektu, destrukce sbírek a ohrožení života osob.

- **Selhání dodávek médií, služeb, zařízení** – jedná se o různá selhání a havárie ovlivňující chod objektu. Např. výpadek dodávky energií (plyn, voda, elektřina), selhání komunikačních či počítačových služeb, nefunkčnost prostředků technické ochrany, aj.

- **Únik, ohrožení nebo ztráta chráněných informací** – v dnešní době se vyskytují zejména ve formě hackerských útoků, kdy je zasažen informační systém objektu.

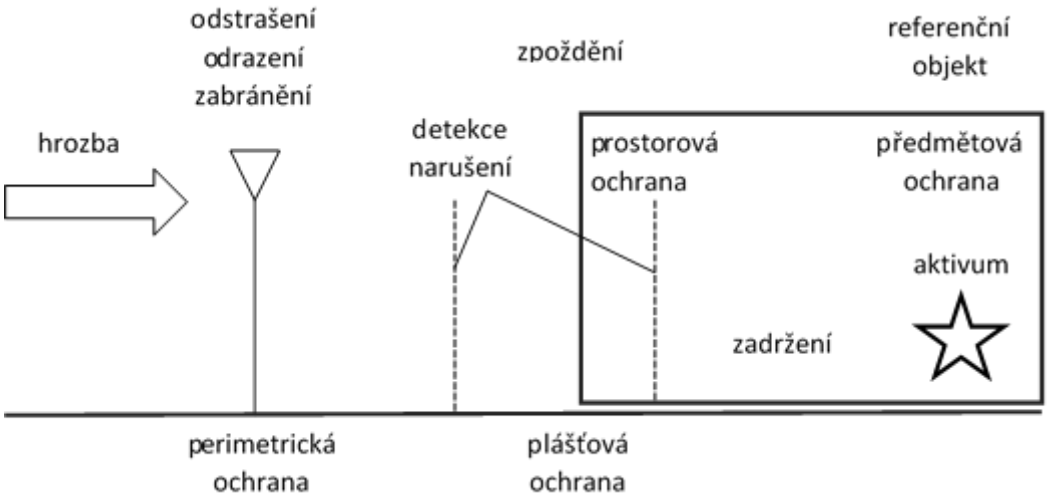
- **Vniknutí do objektu** – vloupáním do objektu může dojít ke krádeži sbírek či jiných cenných předmětů, k vandalismu či zcizení chráněných dat.

- **Krádeže, podvodná jednání, sabotáž a jiná jednání proti organizaci** – téměř vždy hrozí riziko krádeže, podvodná jednání nebo různá úmyslná poškození provedená cizími osobami či samotnými zaměstnanci.
- **Veřejné akce s potencionálními dopady** – např. demonstrace, vandalismus, obsazení objektu nebo jeho části.
- **Terorismus a další násilné a kriminální jednání** – může se jednat o různé bombové útoky, použití zbraní nebo jiných látek, únosy, držení rukojmích, vydírání a další.

Následky výše zmíněných hrozeb mohou mít podobu ohrožení života a zdraví vyskytujících se osob, zničení a poškození majetku a uměleckých děl, ohrožení a únik informací, poškození jména objektu, případně jeho destrukce, způsobení havárie, atd. [21, 24]

3 FYZICKÁ BEZPEČNOST

Fyzická bezpečnost je souhrn bezpečnostních prvků, které jsou jako alfa a omega. Všechny zabezpečovací prostředky mají svůj význam a dohromady tvoří jeden systém. Jedná se o nepostradatelný článek bezpečnostní politiky. Účelem fyzické bezpečnosti je zamezení vniknutí osobám neoprávněným vstoupit na vybrané území, čímž ho chrání před poškozením nebo odcizením majetku. Jedná se o přírodní překážky, stavby, mechanické zábranné systémy, zařízení, technologie a další zabezpečovací prostředky. Tyto prvky ochrany jsou multifunkční, a to v tom smyslu, že nemusí plnit pouze bezpečnostní funkci, ale rovněž funkci estetickou, společenskou nebo architektonickou. Aby mohla být prováděná fyzická bezpečnost, musí být identifikovány základní hrozby v daném objektu a zároveň stanovena aktiva, která mají být chráněna. Odvětví fyzické bezpečnosti se neustále rozšiřuje a je zapotřebí sledovat nová technická vylepšení bezpečnosti a vyhodnocovat jejich případné využití. [1, 29]



Obr. 2 - Prostorové uspořádání opatření systému fyzické bezpečnosti (převzato a upraveno) [29]

Systém fyzické bezpečnosti

Systém fyzické bezpečnosti vyjadřuje soubor ochranných opatření, která slouží k tomu, aby zamezila nebo alespoň zkomplikovala narušiteli přístup k zabezpečeným objektům fyzickou formou. Základními kameny fyzické bezpečnosti jsou komplexnost, vícestupňovost, automatizace a průlomová odolnost. Je však podstatné znát primární hrozby, aby se logicky sestavil systém fyzické bezpečnosti.

1. **Komplexnost** reprezentuje rozsah a vzájemnou souvislost ochranného a detekčního účinku uplatněných opatření.
2. **Vícestupňovost** vyjadřuje rozčlenění jednotlivých zabezpečení do více samostatně vymezených vrstev, kde každá z nich plní svou jedinečnou funkci.
3. **Automatizace** představuje použití jednotlivých systémů k tomu, aby automaticky rozpoznaly narušení zabezpečené oblasti a vyslaly dále informace dohledovému poplachovému a přijímacímu centru a následně zásahové jednotce.
4. **Průlomová odolnost** charakterizuje čas, který je potřebný ke zdolání všech zabezpečovacích opatření na bázi mechanických zábranných systémů. To znamená, že se volí zejména taková průlomová odolnost, která svou dobou překonání převýší únosnou dobu pachatele pro pokus o vniknutí. [29]

3.1 Typy ochrany

V tomto systému jsou rozlišovány čtyři typy ochrany, které prezentují určité stupně zabezpečení. Rozlišují se podle toho, jakou část objektu monitorují. Jsou schopny detekovat narušení běžného stavu.

Perimetrická ochrana

Perimetrická ochrana je synonymem ochrany obvodové, která se zaměřuje na obvod parcely, jinými slovy hranice pozemku, a zároveň na obvod samotného chráněného objektu (stavby). Nejčastěji jsou to překážky v podobě živých i umělých plotů, branek či řek. Kolem nich mohou být instalovány prvky technické ochrany pro zefektivnění zabezpečení. Vzhledem k tomu, že může dojít k porušení prvků z naturogenních příčin, musejí být vyrobeny z odolnějšího materiálu. Zároveň je u tohoto typu ochrany nevýhodou, že často dochází k planým poplachům zapříčiněných zvěří pohybující se na pozemku. [20, 27]

Plášťová ochrana

Tento typ ochrany, jak už z názvu vyplývá, je prováděn na plášťové části objektu. Souhrn bezpečnostních prostředků, které jsou zde využity, zabraňují neoprávněnému vniknutí pachateli přímo dovnitř budovy. Tvoří ho okna, dveře, zámkové systémy, střecha, mříže nebo bezpečnostní fólie. [20, 27]

Prostorová ochrana

Záměrem prostorové ochrany je detekovat vniknutí pachatele dovnitř objektu, zároveň zpomalit jej při nelegálních činech. Bezpečnostní prvky jsou rozmístěny tak, aby bylo možné

monitorovat vstupní část budovy, schodiště do dalších pater a místnosti, u kterých je to žádané. Řadíme zde dveře, okna, zámkové systémy, systémy kontroly vstupu, kamerový systém nebo poplachový zabezpečovací systém. [46]

Předmětová ochrana

Cílem předmětové ochrany je zabezpečit předmět tak, aby nedošlo k jeho porušení či odcizení. Tento typ ochrany je využíván především na cenných předmětech, u kterých není žádána manipulace nepovolanou osobou. Prvky, které tvoří předmětovou ochranu, jsou kamerové systémy, poplachové bezpečnostní systémy, vitríny, trezory, ale také prvky MZS. Díky této ochraně jsou předměty neustále pod dohledem i tehdy, když prostorová ochrana bude na určitou dobu přerušena. Princip předmětové ochrany spočívá v detektorech, jenž se dělí podle funkcí. [46]

4 DĚLENÍ FYZICKÉ BEZPEČNOSTI

4.1 Klasická ochrana

Klasická ochrana je brána jako nejstarší, nejrozšířenější a nejčastější způsob ochrany objektu. Jedná se o prostředky, které nemají jen bezpečnostní význam, slouží také jako ohraničující či právní komponent. Při tomto typu ochrany jsou nejčastěji využívány mechanické zábranné systémy, jejichž nedílnou funkcí je zpomalení pachatele při vstupu na zabezpečené území či prevence před nekalým úmyslem dotyčné osoby. V nynější době je tento typ ochrany doplněn ještě dalšími druhy bezpečnostních prvků pro zkvalitnění zabezpečení. Podle normy ČSN EN 1627 jsou rozlišovány čtyři fáze bezpečnosti, které zastupují úrovně ochrany a jsou u nich stanoveny požadavky na odolnost těchto zábranných systému. [46]

4.1.1 Mechanické prvky bezpečnosti

Mechanické prvky tvoří Mechanické zabezpečovací systémy (dále jen MZS), jenž ztěžují nebo razantně znesnadňují vstup do chráněného objektu nepovolaným osobám. Snaží se odolávat násilnému vniknutí. Tento systém je primárním zabezpečením před násilným vstupem na chráněné území. Nejedná se pouze o plášťovou nebo obvodovou ochranu, ale jsou to i specifické prvky určené pro předmětovou a prostorovou ochranu. Při zajišťování zabezpečení objektu nebo daného prostoru je důležité zprvu vypracovat analýzu hrozeb, aby bylo jasné, proti kterým hrozbám je zapotřebí zajistit dostatečnou ochranu. Mezi typické prvky MZS řadíme ploty, dveře, okna, tvrzená skla, dveřní kukátka, komorové trezory, zámkové systémy, závory, jakož i další prvky, které nějakým způsobem mechanicky chrání daný objekt. [19, 45]

Obvodová ochrana

Do obvodové ochrany řadíme prostředky, které znemožňují vstup nepovolaným osobám na soukromý pozemek a také vymezují hranici pozemku. Nejčastěji je k těmto účelům využíváno oplocení, které může být klasické drátěné, bezpečnostní nebo vysoce bezpečnostní. Ploty lze vybavit dalšími bezpečnostními prvky - například podhrabovou překážkou či vrcholovou zábranou. Pokud jde o více střežený objekt, jsou stavěny kamenné zdi či závory. [19]

Podhrabová překážka je vytvořena z betonového patníku pod konstrukcí plotu nebo jiným pevným podložím. Zvyšuje bezpečnost oplocení, nedochází k podhrabování či podlézání plotu. [45]

Vrcholová zábrana je tvořena nebezpečnými ostnatými dráty, na kterých mohou být namotány přídavné ostré předměty, které mají na pachatele působit nebezpečně.

Obr. 3 - Pyramida bezpečnosti [36]

4.2 Režimová ochrana

Režimová ochrana je komplexní souhrn organizačních a administrativních opatření, zásad a pravidel za účelem zdokonalení systému ochrany objektu. V praxi si ji můžeme spojit například s pracovním, školním či organizačním řádem, který se využívá pro obeznámení zaměstnanců a návštěvníků objektu. Slouží k vymezení bezpečnostních pravidel dané organizace, které mají zajistit zabezpečovací standard. Režimová ochrana se dělí na vnitřní a vnější. V rámci zabezpečení objektu se nevyužívají pouze elektronické a mechanické prostředky, ale konkrétně v režimové ochraně je hojně zapojen i lidský faktor. Řádně proškolené pověřené osoby zaujímají funkci například vrátných, recepčních, strážných, kdy jejich sebemenší pochybení může způsobit ohrožení vnějšího i vnitřního ohrožení objektu. [20, 27, 46]

Vnější režimová opatření

Hlavním úkolem při tomto opatření je monitorování vstupní a výstupní brány objektu, ať už pro osoby nebo vozidla. Je kontrolován pohyb všech osob vstupujících na území objektu a následně mohou být revidovány i osobní věci těchto osob.

Vnitřní režimová opatření

Stanovují bezpečnostní pravidla uvnitř objektu a lpí na dodržování bezpečnostních směrnic. [20]

Například:

- do celé nebo určité části objektu mohou vstupovat pouze pověřené osoby s identifikačním prostředkem, tzn., že pohyb osob a vozidel je omezen,
- nakládání s předměty může být omezeno časově i prostorově, aby nedocházelo ke ztrátě skladových zásob.

4.3 Fyzická ochrana

Fyzická ochrana je jednou z nejstarší a nejvyužívanější formy ochrany různých objektů, případně i subjektů. Jedná se zejména o fyzickou ostrahu, kterou provádí řádně zkušený a profesionální personál. Tento personál je u vybraného objektu (nebo subjektu) trvale či dočasně přítomen a na základě toho je schopen zajistit ochranu a znemožnit různému způsobu napadení. Chrání nejen samotný objekt, ale i přítomné osoby, majetek a v neposlední řadě veřejný pořádek. Výhodou této ochrany je reakce provedení bezpečnostních opatření a praktik. Může se jednat například o odhalení a zadržení narušitele, zamezení odcizení majetku, provedení různých havarijních opatření apod. Fyzickou ostrahu provádí zejména strážníci, hlídači, soukromé hlídací služby, bezpečnostní dohled či státní zaměstnanci hájící bezpečnost ve státě (Police ČR, Armáda ČR). [22, 29]

Fyzická ochrana se dělí dle časové působnosti v objektu:

- fyzická ochrana závisející na pracovní době v objektu
- fyzická ochrana nepřetržitá
- fyzická ochrana nepravidelná [29]

Fyzická ochrana členěná dle charakteru výkonu:

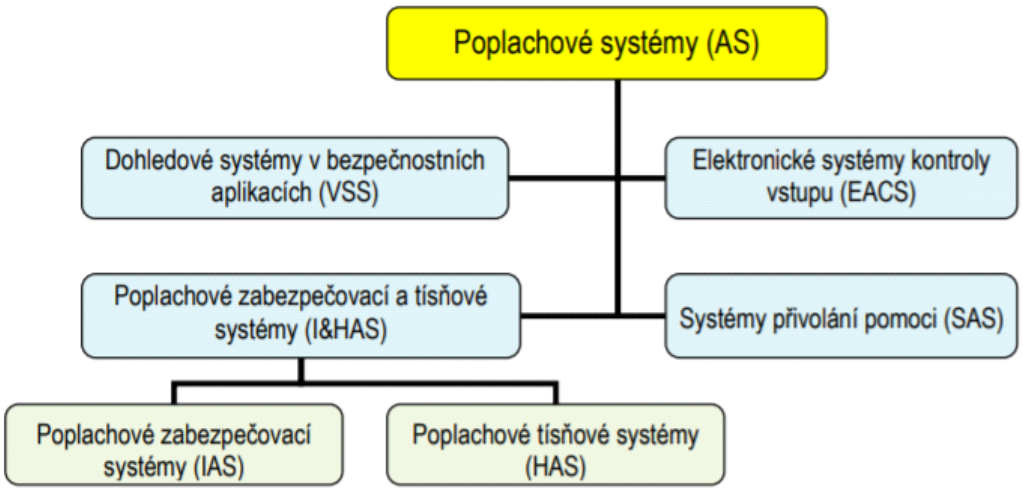
- propustková
- obvodová
- celoplošná
- přehledová dozorová
- zásahová
- aktivní víceúčelová [29]

4.4 Technická ochrana

Je ochrana, při které je vytvářen komplexní systém vícesložkových technických prvků, které napomáhají monitorovat a udržovat bezpečnostní standard vybraného objektu, a tím rychle reagovat na nežádoucí změny v chráněném objektu. Tento systém znemožňuje nekompetentním osobám vstup do chráněného objektu a navíc ohlašuje vznik požáru nebo nějakou změnu běžného stavu, která by mohla zapříčinit větší havárii. Zároveň zajišťuje včasné informování pracovníků na příslušných místech, například ostrahy objektu, bezpečnostní agentury či PČR, aby se mohlo včas zakročit a tím předejít k rozšíření těchto nahodilých situací. Technickou ochranu dělíme na následující dvě skupiny, konkrétně na Mechanické zábranné systémy a poplachové systémy. [27, 46]

4.4.1 Elektronické bezpečnostní systémy

V dnešní době můžeme pozorovat zajímavý vývoj v oblasti bezpečnostních technologií a systémů. Při volbě způsobu zajištění bezpečnosti objektu musíme brát v úvahu jak jeho vlastnosti, tak i stále důležitější ekonomickou stránku. Pro někoho, kdo se pohybuje v bezpečnostní oblasti, bude vždy bezpečnost jako taková na prvním místě ještě před financemi. Ovšem pokud se na to podíváme z pohledu vlastníků firmy, kteří musí zhodnotit pro a proti každé investice, kterou udělají, aby viděli jistou návratnost financí, tak se nemůžeme divit, že se vždy snaží vybrat si tu nejpřijatelnější variantu. To pro ně znamená vyvážený poměr ceny a funkčnosti systému. Ani výrobci těchto systémů jim to příliš neulehčují, jelikož každý výrobce se snaží podporovat pouze své výrobky. V praxi to znamená, že ve většině případů nemůžete kombinovat různé části systému od různých výrobců, protože tato zařízení potom nejsou schopna spolu komunikovat a správně fungovat. Ovšem i výrobci by měli pochopit, že v rámci bezpečnosti nejsou navzájem konkurencí, ale měli by se snažit o spolupráci, která by urychlila vývoj v této oblasti a každá firma by poté mohla nabízet mnohem širší spektrum výrobků s mnohem větší variabilitou a možností přizpůsobit se pro většinu zákazníků. [26, 27]



Obr. 4 - Klasifikace poplachových systémů (převzato) [47]

Dohledová a poplachová přijímací centra

Dohledová a poplachová přijímací centra, dříve známá jako pult centralizované ochrany, se vyznačuje pracoviště, které přijímá a vyhodnocuje informace vysílající z chráněného objektu a v případě narušení prostoru zajistí vyslání příslušných jednotek. V nynější době, jak už bylo zmíněno, počet kriminálních činů stále roste a pachatelé jsou zkušenější, proto je zapotřebí dbát na dostatečnou ochranu svého majetku a také svých životů. Mezi základní instalované systémy jsou řazeny EACS, SAS, PTZS a VSS, jejichž koncové prvky jsou napojeny na bezpečnostní složky, u některých významných budov na městskou nebo státní policii. Ty vyšlou zásahové jednotky na místo určení a po jejich zpětné informační vazbě zpět na stanici se situace vyhodnotí a povolají se jednotky IZS. Historicky řadíme první PCO do doby sovětského svazu, nazýval se Něva a v tehdejší době byl napojen do jednotné telefonní sítě, jednalo se o primitivnější systém. Po určitém procesu vývoje se dnes dostáváme do doby, kdy zařízení fungují na principu rádiového přenosu s využitím GSM technologie, využívány jsou také datové a hlasové kanály. Systém podléhá normě ČSN EN 50131-1 ED.2 a samotný přenos informací a činnost DPPC se nachází v normě ČSN EN 50 136-7. Střežené objekty jsou stupňovány podle své důležitosti, podle toho se odvíjí i požadavky na provoz PCO neboli DPPC. [27, 47, 48]

Elektronické systémy kontroly vstupu (EACS)

Systémy kontroly vstupu (dále jen SKV) jsou primárním zabezpečením vnitřní ochrany. Dochází k autentizaci všech osob hodlajících vstoupit do chráněného objektu a následně je umožněn vstup i výstup oprávněným osobám. Jedná se o souhrn bezpečnostních opatření

fyzického, mechanického i elektronického charakteru, při kterých se vede evidence všech osob a vozidel nacházejících se v areálu chráněného objektu, sledování osob při průchodu přes zámky do míst se zvýšenou ostrahou či dozor nad opakovanými vstupy do objektu. V některých případech je součástí telefonická a poštovní služba, dochází k evidenci také všech přijatých hovorů skrz přepojovací centrálu a vede se přehled o převzaté poště adresované na danou adresu. Celý systém podléhá normě ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty, a následně normám, které specifikují jejich rozšířené provozní vlastnosti, a také normám ČSN EN 60839-11-2 Poplachové a elektronické bezpečnostní systémy - Část 11-2: Elektronické systémy kontroly vstupu - Pokyny pro aplikace. [20, 47]

Lidé oprávnění vstoupit do areálu nebo do konkrétní části podniku jsou nuceni prokázat svou identitu, a to buď přístupovým heslem, iButton čipem, RFID čipem, čárovým kódem nebo biometrickým údajem. Tento údaj je detekován pomocí snímacího zařízení, které posuzuje, zdali máte koncesi vstoupit do objektu nebo ne. Rozlišujeme tři typy snímačů, a to: základní (neinteligentní), polointeligentní, inteligentní. [24, 27]

Součástí SKV bývá také docházkový systém, jenž ukládá informace sloužící ke kontrole docházky zaměstnanců a oproti samotných SKV je ve firmě pouze jeden, ale záleží na počtu zaměstnanců a velikosti objektu.

Systémy přivolání pomoci (SAS)

Social alarm systém je nepřetržitá pomoc v nahodilých závažných situacích, které mohou způsobit újmu na zdraví a životech občanů nebo kde může dojít k bezprostřednímu ohrožení objektu. Systém funguje na principu vyvolání poplachu uživatelem, a to zmačknutím tlačítkového dálkového ovladače, kdy následně dojde k identifikaci poplachu na příslušném místě a je vyslána jednotka určená k zásahu. Systém je určený do objektů, především měkkých cílů, kde je větší pravděpodobnost vloupání a ohrožení životů zaměstnanců (např. banky, školy, nákupní centra, muzea apod.) Produkt je napojen buď na příslušnou sociální či ústavní službu nebo na dozorující osoby v domově důchodců, také na dohlížející pověřené osoby, DPPC, PČR či městskou policii. Tento systém podléhá technické normě ČSN EN 50134-1,2 Poplachové systémy. [48]

Poplachové zabezpečovací a tísňové systémy (PTZS)

Poplachové zabezpečovací a tísňové systémy (dále jen PTZS), se řadí mezi poplachové systémy a zároveň primární elektronické bezpečnostní systémy, které využívají kombinovanou soustavu. Tento systém identifikuje a detekuje úmyslné vniknutí do objektu nepovolaným osobám, či pokus o vniknutí se záměrem napadnout nějakým způsobem chráněný objekt. Součástí konstrukce je výchozí část tvořená senzorem, ten reaguje na různé fyzikální změny a zároveň zaznamenává jakékoliv vibrace, které by mohly být příznakem narušení běžného stavu objektu. Informace o tomto činu je zaslána na příslušné poplachové přijímací centrum, to je připojené na ústřednu konkrétního PTZS. Jelikož jde o elektronický systém složený z několika komponentů například ústředny, detektorů, napájecích zdrojů, výstražných zařízení či klávesnice, musí být dodržen pracovní postup při jeho manipulaci a zároveň vše musí být v souladu s právními předpisy a normami. Uživatel, který má na starost funkčnost PTZS, musí být řádně zaškolen, aby mohl správně spravovat tento systém dle technické normy ČSN EN 50131-1 ČSN CLC/TS 50131-7. Ve starší publikaci je možné se setkat také s názvem EZS neboli elektronické zabezpečovací systémy a jsou to systémy stejného typu jako nahrazující PTZS, ale mají již neaktuální verzi provedení a jsou uváděny v již neplatných normách, které byly nahrazeny novými a to od roku 2007. PTZS můžeme dále dělit na další dva typy systému, a to: [27, 47]

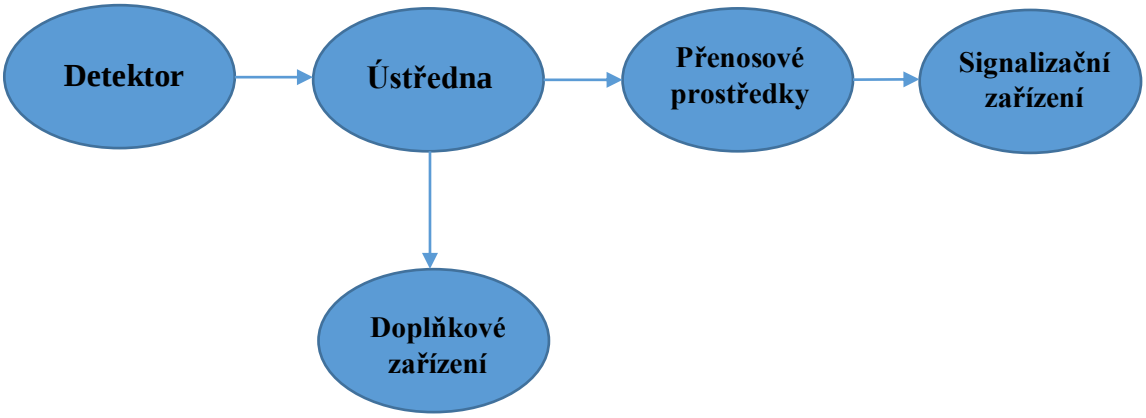
Poplachové zabezpečovací systémy (IAS)

Jak už z názvu můžeme vyčíst, jedná se o poplachový zabezpečovací systém, který odhaluje narušitelovo vniknutí do střeženého objektu a následně jeho přítomnost. Tento typ systému není vybaven prostředkem, který zabezpečuje spuštění tísňového poplachu. [47]

Poplachové tísňové systémy (HAS)

V tomhle případě se jedná o systém určený pro uživatele, který má funkci záměrného spuštění poplachu, a to v případě, že jsou ohroženy osoby a jejich zdraví, majetek či životní prostředí. Tento typ systému indisponuje detektorem vniknutí. Dříve se poplachové tísňové systémy uváděly a rozebíraly v několika evropských normách, ale od října 2006 jsou

zahrnuty v normě ČSN EN 50131-1 společně s poplachovými zabezpečovacími systémy, nemají svou speciální normu. [47]



Obr. 5 - Blokové schéma EZS/PTZS (převzato a upraveno) [46]

Stupně zabezpečení

Stupeň 1 - nízké riziko

U úrovně nízkého rizika se očekává, že pachatelé narušující konkrétní objekt či území nejsou dostatečně vybavení a znalí funkčností PTZS.

Stupeň 2 - nízké až střední riziko

V tomto případě mají pachatelé obecnou znalost funkčností PTZS a mají možnost využít běžné prostředky k narušení.

Stupeň 3 - střední až vysoké riziko

U třetího stupně se očekává, že pachatelé jsou zběhlí a disponují rozsáhlým sortimentem nástrojů a zařízení k překonání bezpečnostního systému.

Stupeň 4 – vysoké riziko

U nejvyššího stupně rizika se předpokládá vyšší úroveň znalostí PTZS a režimu bezpečnostního systému. Je zapotřebí brát v potaz, že pachatelé jsou profesionály v oboru a objekt či území musí být zabezpečeno na nejvyšší úrovni. [20]

Podle úrovně rizika prolomení bezpečnostních systémů je zvoleno vhodné zabezpečení fyzické bezpečnosti tak, aby nedocházelo k častému prolomení ochranných prvků objektu.

Dohledové videosystémy (VSS)

Dohledové videosystémy jsou nejčastěji známé pod dříve běžně užívanou zkratkou CCTV, Closed Circuit Television, přeloženo do češtiny jako uzavřené televizní okruhy. V současné době je používána zkratka VSS, která reprezentuje první písmena anglických slov Video

Surveillance Systems. Dohledové videosystémy (dále už jen VSS), patří k jedním z nejpoužívanějších prvků ochrany objektu. Můžeme ji najít pod zastaralejším názvem CCTV (Closed Circuit Television), v překladu to znamená uzavřené televizní okruhy, nyní je název obměněn na název VSS (Video Surveillance Systems). Systém je určen k monitorování daného objektu či plochy, k pozorování, detekování, zaznamenávání událostí, k identifikaci osob, k rozpoznávání a hojně je využíván při vyšetřování trestných činů či přestupků. Jeho velkou výhodou je, že objekt, kde jsou samotné kamery nainstalovány, můžeme sledovat online a tyto záznamy ukládat na dobu nezbytně nutnou. Tyto záznamy jsou ukládány na pevný disk a je možné je kdykoliv přehrát znova i na vyžádání Policie ČR. Pokud objekt chce tento systém využívat, musí se registrovat na Úřadu pro ochranu osobních údajů. Dle zákona č. 110/2019 Sb. O zpracování osobních údajů, nesmí kamery omezovat zaměstnance - u vstupního prostoru je zapotřebí vyvěsit označení, že je zde používán kamerový systém se záznamem. [28, 47, 48]

Tento systém se skládá z kamer, hardwarové části a softwarové části, ale může být připojen i mikrofon nebo reproduktor. Samotné kamery mohou mít odstrašující funkci, jelikož pachatel vykonávající protiprávní čin si uvědomuje, že je sledován a záznamy mohou být použity jako důkaz při vyšetřování. Samotná instalace závisí na požadavcích zákazníka a na samotném objektu, pokud si to situace vyžaduje, lze k tomuto systému doplnit další prvky jako je reproduktor či mikrofon. VSS podléhají normě ČSN EN 62676-1-1 Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 1-1: Systémové požadavky – Obecně. [23, 28]

Díky jejich drobné konstrukci, snadné manipulaci a širšímu využití dokážeme snímat i obrovské plochy, jejichž kamerové záznamy jsou pověřenou vyškolenou osobou nepřetržitě kontrolovány. Nejčastěji se kamerový systém instaluje do prostoru vjezdu či vstupu do objektu, vnitřních prostor objektu, v perimetru plochy, na přilehlá parkoviště/garáže a další místa s velkým pohybem osob.

Kamerové systémy se dělí na:

- Analogové
- Digitální
- Hybridní [28]

4.5 Elektronická požární signalizace

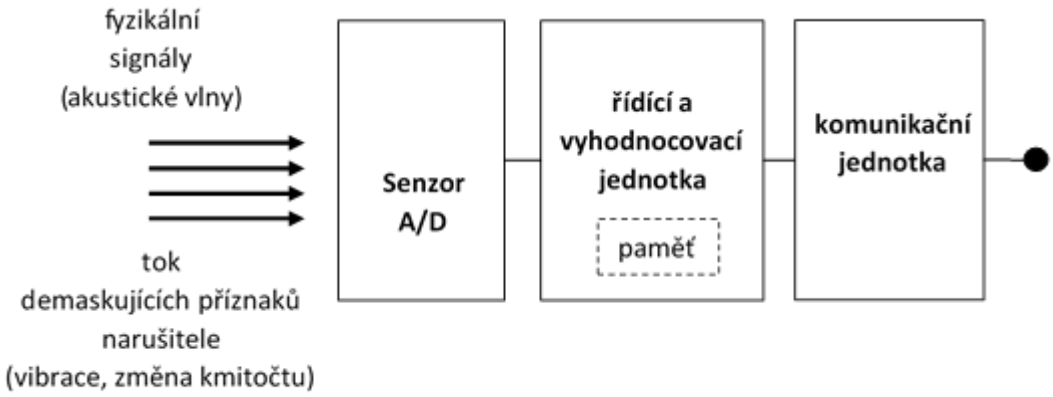
Elektrická požární signalizace je systém (dále jen EPS), který slouží k okamžité detekci vzniklého požáru nebo k prevenci vzniku požáru. Při aktivování požární sirény či signalizaci požáru, jsou na místo povolány osoby schopné vzniklý požár uhasit a zároveň je o vzniklém požáru obeznámena jednotka Hasičského záchranného sboru. Mezi dílčí úkoly EPS řadíme především zajištění bezpečnosti lidí a ochrany majetku, rychlé a spolehlivé určení místa požáru. Elektrická požární signalizace funguje na principu vyhlášení poplachu, kdy dochází k aktivaci evakuačního systému v zasaženém objektu a k aktivaci ovládání různých zařízení, která mohou bránit šíření požáru. Primární funkci při vzniku požáru zastávají samotné detektory, avšak existují i tlačítkové hlásiče, které mohou být použity osobou, která detekovala požár v daném objektu - následně vzniká stejný proces, viz výše. [26, 29]

EPS se skládá z ústředen, hlásičů požáru a dalších zařízení, která jsou součástí systému, jenž akusticky, opticky nebo obojími způsoby upozorní na vzniklé ohnisko požáru. Ve vybraném objektu jsou rozmístěny hlásiče, které jsou spojeny s ústřednou pomocí hlásících linek. Ty jsou z ústředny napájeny a v protichůdném směru posílají do ústředny informace o požáru. Činnost hlásicích linek je neustále kontrolována ústřednou a v případě poruchy je o ní obsluha seznámena. EPS podléhá následujícím technickým normám ČSN 73 0875 a ČSN 34 2710. [26, 29]

Obr. 6 - Topologie EPS [16]

5 DETEKTORY NARUŠENÍ

Zastaralejší název tohoto termínu zní čidla narušení, momentálně se s tímto názvem můžeme setkat ve starších publikacích, normách a předpisech. Pojem je definován coby mechanismus, který rozpozná fyzikální a mechanické změny, které by mohly značit nežádoucí narušení v chráněném objektu či manipulaci s předměty. Pokud dojde k detekci narušení objektu, v tu chvíli je vyslána zpráva na příslušnou ústřednu. Zde se taková informace zpracuje a dochází k ovládání konkrétního bezpečnostního systému. Dále pak následují přenosové prostředky, signalizační zařízení a v neposlední řadě doplňková zařízení, ty usnadňují celý proces. [27, 48]



Obr. 7 - Blokové schéma detektoru narušení (převzato a upraveno) [27]

5.1 Detektory se mohou dělit podle několika faktorů

- **Nenapájené** detektory nejsou zapojeny do elektrického zdroje.
- **Destrukční detektory** mají pouze jednorázovou platnost, tzn., že při prvním odhalení narušení objektu jsou zničeny (fóliové polepy).
- **Nedestrukční** detektory - při jejich spuštění následují vratné změny (vibrační a magnetický kontakt).
- **Napájené** detektory jsou závislé na elektrickém zdroji, a to buď na vlastním zásobovacím či místním zdroji nebo na dálkovém dobíjení skrz metalické vedení. [27, 46]

5.2 Rozdělení detektorů

5.2.1 Elektromechanické detektory

Elektromechanické detektory, jak už z názvu můžeme vyčíst, detekují mechanické změny, které detektor transformuje na poplachový signál.

Do kategorie mechanických změn zařazujeme:

- sepnutí či rozepnutí spínače
- přerušení elektrického obvodu
- změna elektrického parametru senzoru (odpor, kapacita, napětí, elektrický náboj)
- změna frekvence nebo amplitudy signálu v důsledku mechanických vibrací

Dělení elektromechanických detektorů:

- mechanické detektory-spínače
- magnetické detektory
- tenzometrické detektory
- kontaktní detektory destrukce skleněných ploch
- nášlapné detektory
- diferenciální tlakové detektory [27, 46]

a) Mechanické detektory spínače

Jedná se o mikrospínače, které se namontují do rámu dveří a slouží k uzavření zabezpečovacího elektrického obvodu. Při nepovoleném vstupu vyšle detektor zprávu na ústřednu, kde se situace vyhodnotí. Tento mikrospínač se využíval také při předmětové ochraně a konkrétně v muzeích při ochraně sbírkových exponátů. Systém funguje stejně, akorát zde se detektor zabudovává pro výstavní předmět a při nežádoucí manipulaci je ihned odeslán varovný signál. [23]

Typy mechanických detektorů:

- Drátové detektory
- Rozpěrné tyče
- Vibrační detektory [27]

b) Magnetické detektory

Jedná se o jedny z nejrozšířenějších kontaktních čidel, které jsou produkovány v širokém spektru provedení a variant. Jsou tvořeny dvojicí komponentů – jazýčkový kontakt a magnet. Využívají se jako prvky plášťové ochrany pro ochranu různých stavebních konstrukcí (okna, dveře). Nicméně využití mají také v předmětové ochraně nebo proti sabotáži.

Dle funkce a konstrukčního uspořádání jsou děleny do skupin

- s jedním jazýčkovým kontaktem,
- s více jazýčkovými kontakty,
- s vestavěným ochranným odporem zapojeným sériově nebo paralelně,
- s funkcí spínací nebo rozpínací,
- bez vestavěné ochranné smyčky nebo s vestavěnou ochrannou smyčkou,
- s ochrannou smyčkou bez ochranného odporu nebo s ochranným odporem,
- s tzv. předmagnetizací. [27]

Magnetické detektory se mohou lišit také dle úrovně odolnosti proti překonání, kdy některé můžeme jednoduše překonat, zatímco jiné s obtížemi. Např. u klasických, běžně používaných magnetických kontaktů stačí využít dostatečně silný magnet, s jehož pomocí lze bez spuštění poplachu otevřít chráněný objekt. Jednotlivé typy magnetů mohou mít řadu výše zmíněných vlastností. Pro efektivní použití musí být magnetický kontakt umístěn tak, aby při běžném pohybu s předmětem nedošlo k jeho aktivaci. Zejména musí ohlásit jakékoliv otevření, ať už běžné nebo nahodilé, jako např. vylomení dveří.

Výhodami těchto detektorů je jednoduchá montáž, dlouhá životnost a dostatečná odolnost proti působení externích vlivů. Vzhledem k jejich široké škále provedení umožňují jak povrchovou, zapuštěnou, tak i skrytou montáž přímo do vybraného tělesa, dveří nebo oken. [20]

V problematice zabezpečení muzejních exponátů či vzácných předmětů mají podstatný význam. Princip spočívá v monitorování změn odporu, jenž vzniká manipulací s chráněným předmětem. Pokud se s předmětem nějak zachází, je na tenzometru zaznamenána změna postavení a informace je zaslána na případnou ústřednu.

Dělíme dle materiálu a konstrukce:

- Kovové (drátové, fóliové a napařované)
- Polovodičové (monokrystalické, polykrystalické) [27]

c) **Kontaktní detektory destrukce skleněných ploch**

Kontaktní detektory spadají především do plášťové ochrany, používají se pro zabezpečení prosklených prvků, oken či výkladních skříní. Zaznamenávají změny, které by mohly být vyvolány nepovoleným vniknutím s úmyslem rozbití výkladní skříně za účelem krádeže a další. Mezi kontaktní detektory patří poplachové fólie, skla, fóliové polepy nebo prvky pasivních kontaktních detektorů. Všechny typy kontaktních detektorů mají zabudovanou poplachovou smyčku, ty jsou napojeny na koncentrátory a následně dochází ke komunikaci s případnou ústřednou o nežádoucí změně. [27]

d) Nášlapné detektory (koberce)

Jedná se o jeden stěžejní prvek ochrany, který závisí především na elektrickém proudu. Je vyroben ze dvou navzájem propojených elektricky vodivých vrstev. Při aktivaci zaznamenávají nežádoucí pohyb na konkrétním místě a jsou vysílány signály pro spuštění alarmu. Využívány jsou buď fóliové koberce či páskové. Nevýhodou tohoto typu detektoru je přílišná citlivost na dlouhodobější zátěž tím, že jsou instalovány do podlah v objektu. Je také zřejmé, že jejich životnost mohou zkracovat ostré věci např. obuv. Pokud má být ochrana co nejefektivnější, musí být tento systém pečlivě skrytý. [27, 46]

5.2.2 Elektromagnetické detektory

Detektory elektromagnetické jsou specifické tím, že fungují na bázi elektromagnetické kompatibility. Což znamená, že je využíváno vzájemné působení dvou polí, elektrického a magnetického.[29]

Dělení detektorů dle pohybu:

- mikrovlnné detektory
- rádiové bariéry a detektory VKV
- kapacitní detektory [20]

a) Pasivní infračervené detektory

Pasivní infračervené detektory neboli PIR - Passive Infra Red detectors jsou považovány za jedny z nejrozšířenějších a nejpoužívanějších typů detektorů. Elektromagnetické zařízení funguje tak, že vyhodnocuje změny, které vznikly na ploše, kde je možné detekovat změny infračerveného záření. Uvnitř zařízení se nachází pyroelektrický snímač dříve známý pod názvem pyroelement, který začíná být aktivní při změnách v zóně dopadajícího záření, jinými slovy, pokud detekuje v poli těleso s odlišnou teplotou než má okolí. Jelikož živé organismy mají odlišné infračervené záření díky své tělesné teplotě, je potom snadné rozpoznat narušitele v chráněném objektu. Pokud se narušitel dostane do zorného pole detektoru, je detektor schopný vyhodnotit informaci a spustit poplašný systém. I když se tyto typy detektorů využívají zejména uvnitř budov, vyskytuje se jich i několik pro venkovní použití. Venkovní PIR jsou vybaveny kryty s vyšší odolností proti dešti a jsou navrženy pro práci v nižších teplotních podmínkách. [20, 35]

b) Infračervené bariéry, závory a záclony

Infračervené bariéry a závory spadají do skupiny neviditelných světelných detektorů. Infračervené závory jsou zařízení dělící se na dvě části, první aktivní část tvoří vysílač (V) a druhou pasivní část je tvořena přijímačem (P). Jsou instalovány přes objekt a maximální odstup mezi oběma částmi může být maximálně 250 metrů. Vysílač vytváří infračervené paprsky, které vysílá směrem k přijímači, a ten je přijímá a zachycuje. Aby byl pachatel detekován, musí vstoupit do detekčního pole, které je tvořeno zmiňovanými paprsky. Infračervené bariéry fungují na podobném principu jak předešlá zařízení, avšak v tomto případě jsou V a P umístěny střídavě na obou stojanech, které jsou propojené infračervenými paprsky, a to ve více směrech a může docházet i ke křížení. To z toho důvodu, aby byla podpořena efektivita detektoru. [20, 35]

c) Štěrbinové kabely

Jedná se o zařízení zabezpečující vnější bezpečnost, které je zabudované ve vnitřním prostředí, konkrétně v podlaze. Tento typ detektoru se obvykle skládá ze dvou koaxiálních kabelů, vysílací kabel a přijímací kabel. Ty mají na svém plášti "štěrbiny", skrz které je vyzařován signál z vysílacího kabelu dopadající na protější přijímací kabel. To způsobuje vznik elektromagnetického pole mezi oběma kabely, které je elipsového tvaru, a při jeho narušení pachatelem je spuštěn poplašný systém. U většiny případů instalace tohoto zařízení

jsou kabely budovány přibližně 2 metry od sebe zhruba 30 centimetrů pod povrchem. [23, 29]

d) Laserové detektory

Jedná se o detektor, který je hojně využíván v obvodové ochraně daného předmětu. Princip spočívá v tom, že detektor vytváří infračervenou reflexní širokoúhlou záclonu. Laserový detektor je uložen nad střeženým předmětem nebo objektem, kolem něj vede laserová záclona tvořená z neviditelných paprsků a nakonec chráněnou zónu ukončuje reflexní páska, která uzavírá tento systém. Paprsky se při dopadu na reflexní pásku přemění na elektrický signál vracející se k přijímači. Při narušení této laserové záclony je spuštěn poplašný systém. [46]

5.2.3 Elektroakustické detektory

Elektroakustické detektory zaznamenávají veškeré fyzikální změny v podobě například otřesů či rozbití. Narušitel při těchto podobných činech vytváří akustické vlny, které se dále šíří a jsou následně vyhodnoceny přítomnými detektory, které spustí poplašný systém. [46]

Dělení podle zdroje akustického signálu:

- **aktivní** - Při narušení či poškozování chráněného objektu jsou rozpoznány určité změny akustického vlnění. Je zde přítomen vysílač signálu i přijímač.
- **pasivní** - V tomto případě je zařízení vybaveno pouze přijímačem signálů, jenž zaznamenává změny v chráněném objektu při narušení pachatelem.

podle použitého frekvenčního pásma:

- ultrazvukové
- využívající akustické pásmo [20, 27]

a) Detektory rozbití skla

Tyto detektory se dělí na několik druhů, jedno však mají společné, všechny detekují narušení chráněné skleněné plochy, oken, vitrín či dveří. Nejčastěji jsou využívány pasivní akustické detektory rozbití skla, které vyhodnocují pouze změny akustického tlaku na chráněném prostoru. [27, 46]

5.2.4 Detektory na ochranu uměleckých předmětů

a) Závěsné detektory

V tomto případě se jedná se o detektor zabezpečující dostatečnou ochranu zavěšených, ale i nástěnných exponátů před jakoukoliv manipulací. Předměty jsou zavěšeny okem neviditelným drátkem na hák, kde se nachází samotný detektor zhruba 50- 200 centimetrů nad předmětem. Pokud dojde k sebemenší manipulaci s exponáty, je spuštěn poplachový systém. [20, 27]

b) Polohové detektory

Tento typ detektoru je instalován mezi pevnou konstrukcí a exponátem například u obrazů, mohutných rámů s plátnem či gobelínů. Zařízení je složeno z mechanického kontaktu, který detekuje nepovolenou manipulaci. Je přesně nastaven rozměr (vzdálenost) mezi pevnou konstrukcí a předmětem, a pokud dojde ke snížení nebo zvětšení prostoru mezi nimi, je spuštěn poplašný systém. [20, 46]

c) Váhové detektory

Váhové detektory mají výhodu, že se nemusejí instalovat nikde kolem předmětu, ale nachází se přímo pod exponátem. Slouží především k ochraně sošek, nábytku a dalších vzácných předmětů, které lze nějakým způsobem odcizit či porušit. Při spojení napájecího napětí, nacházejícího se na spodní straně předmětu a detektoru, je změřena hmotnost. Jakékoliv zvýšení či snížení hmotnosti je bráno jako porušení a dochází ke stejnému postupu jak u všech předešlých detektorů. Jsou respektovány i minimální odchylky způsobené různými vzruchy. [20, 27]

II. PRAKTICKÁ ČÁST

6 VYBRANÁ INSITUCE

Vybraná instituce patří mezi historické klenoty České republiky, neboť se řadí mezi největší muzea v České republice, spravuje a uchovává historické a kulturní sbírky. Zároveň zaujímá přední příčky v registru nejstarších muzeí na našem území. Jeho založení se datuje k počátku 19. století. Instituce je současně i vědeckovýzkumným ústavem a odborně metodickým střediskem muzejní a vlastivědné práce.

Konkrétní muzejní budova, kterou se ve své práci zabývám, je jednou z několika expozičních objektů a areálů, které spadají pod jednu instituci. Tato kulturní památka spadá pod působnost Ministerstva kultury a je jejím ústředním orgánem dle §8 zákona č. 2/1969. Budova se nachází v Moravskoslezském kraji České republiky. Je umístěna v historickém jádru krásného města. Pyšní se více než dvěma milióny sbírkovými předměty, avšak počet se liší dle aktuálních krátkodobých výstav, které instituce obměňuje. Mezi výstavními exponáty jsou předměty z živé i neživé přírody ze všech koutů republiky. Instituce se zaměřuje na prezentaci přírodních a kulturně historických fenoménů kraje, kde je objekt umístěn. [22, 41]

6.1 Popis budovy

Analyzovaná pseudorenesanční stavba je situována do klidného prostředí města, a to přesněji do jednoho ostrovního městského parku. Lze do ní vstoupit třemi vchody, avšak pouze dva jsou určeny pro návštěvníky. Po obvodu parku vedou silnice, takže je zde velmi dobrá dostupnost. Levá boční fasáda muzea je situovaná do zmiňovaného parku a pravá strana budovy s bočním vchodem na silnici, na které se rovněž nachází gymnázium. Bohatě zdobené průčelí budovy se obrací do městského parku. Zadní a pravá boční část budovy ústí do dvora, naproti kterého leží druhý výstavní objekt a také střední průmyslová škola. Vzhledem k nestabilnímu a neúnosnému podloží jsou základové zdi vystavěny na metr široké betonové vrstvě, uložené na pilotech a dřevěném roštu. Jeho celková zastavěná plocha činí 1028,28 metrů čtverečních.
Vybraný objekt má tří podlaží a využívané sklepní prostory, které jsou převážně určeny k prezentaci vybraných expozic.

V prostoru suterénu se nachází kolosální expozice. Jeho součástí je také edukační místnost, místnost pro zaměstnance, prostor pro kočárky a kola, místnost pro rodiče s dětmi, toalety, výtahový prostor a v neposlední řadě je zde výstupní prosklený prostor, který propojuje

objekt s další historickou budovou. Výška sklepů měří kolem třech metrů, avšak na některých místech je dlažba o 80 centimetrů snížená.

V přízemí je tzv. vstupní podlaží, do kterého se vchází širokým kamenným schodištěm přes trojici obloukových portálů do úzké předsíně, kudy se dostaneme do vstupního vestibulu. Zde je situováno informační centrum s prodejem vstupenek, které pak návštěvníci musí oskenovat na čtecím zařízení zabudovaném v turniketech. V samotném vnitřním prostoru můžeme nalézt dětské muzeum, multifunkční sál, odpočinkový prostor, výstavní sál a další z expozic, které prezentují vědu, techniku a umění rakouského Slezska od konce 18. století do 1. světové války, výtahový prostor a také rozsáhlou halu, kde po krajích nalezneme část trvalé expozice.

První patro je věnováno v pořadí třetí z expozic, nachází se zde galerie a opět je patro vybaveno výtahovým systémem. Na stejném patře mohou být návštěvníci zároveň obohaceni informacemi z historické expozice. Podkroví není využíváno pro výstavní účely.

7 POPIS OCHRANY VYBRANÉ INSTITUCE

Typy ochrany

Následující kapitola je věnována popisu reálného zabezpečení budovy, která je členěna do následujících čtyř typů ochrany. Rozlišují se podle toho, jakou část objektu monitorují. Jsou schopny detekovat narušení běžného stavu.

Jak již bylo zmíněno v teoretické části, rozlišujeme čtyři základní typy zajištění ochrany. V následující kapitole budou podrobněji popsány prostředky zajišťující fyzickou bezpečnost, které vybraná instituce používá. Technické informace, jež jsou obsaženy v následující kapitole, byly sepsány na základě rozhovoru uskutečněným s mým konzultantem, pracujícím ve vybrané instituci, panem Poláškem ve dnech 19. 12. 2019 a 21. 2. 2020. Zároveň byly pro psaní této práce využity neveřejné technické publikace a vlastní observace.

EPS

EPS je v tomto objektu navržena a následně provedena dle normy ČSN 73 0875, ČSN 34 2710 a Vyhlášky č. 268/2011Sb., o technických podmínkách požární ochrany staveb. Technické vybavení celého tohoto systému je opět pod záštitou společností Trade FIDES, a.s. Nachází se zde ústředna EPS typu Esser IQ8control M, na niž jsou napojeny samočinné hlásiče, které se nachází na všech místech, kde může hrozit riziko vzniku požáru. Jedná se o multisenzorový hlásič IQ8Quad, který detekuje potencionální požár. Součástí technického vybavení jsou také tlačítkové hlásiče požáru, ty nalezneme ve většině případů u únikových cest, a to z toho důvodu, aby byly na lehce dosažitelném a přístupném místě v případě nouze. Nedílnou součástí EPS zařízení jsou samozřejmě sirény upozorňující na vznik požáru, v objektu se nachází jedna. Pro upozornění o požáru pro osoby nacházející se v objektu je instalován zábleskový maják, což je svítilna s barevným krytem, který je umístěn u vstupního prostoru. Další podstatná část systému EPS je Obslužné pole požární ochrany a LCD zobrazovací panel, které se nachází se vstupním vestibulu. Celý tento systém je napojen na příslušnou stanici HZS, která je připravena, v případě potřeby, okamžitě zasáhnout. Tato jednotka vlastní i klíče od klíčového trezoru, ve kterém se nachází záložní klíč od vstupních dveří. Pravidelně dochází k revizi těchto technických prostředků. [16, 17]

Obr. 8 – Požární hlásič

Obr. 9 - Tlačítkový hlásič požáru

7.1 Perimetrická ochrana

Jedná se o obvodovou ochranu, v tomto případě je vybraná instituce omezena prostorem, neboť větší část parku je ve vlastnictví města, a proto mohou být prvky spadající do perimetrické ochrany instalovány pouze v těsné blízkosti budovy tak, aby nezasahovaly do veřejného prostoru, což je dáno legislativou. Z mechanických zábranných systémů je využito oplocení z pravé boční strany, které ohraničuje hranice a zároveň slouží jako překážka pro pachatele, kteří by se úmyslně chtěli dostat na soukromý pozemek. Tento prostor slouží pro zaměstnance a pověřené osoby, které zde mohou zajet primárně motorovým vozidlem. Je trvale uzamčen a funguje zde režimová ochrana, kterou má

na starost vedoucí pracovník tohoto objektu. Schvaluje osobám vjezd na pozemek a zároveň vlastní klíče ke vstupu do vybraných místností. Tento prostor slouží i jako nástupní plocha pro jednotky IZS. Ze zástupců technické ochrany je využit kamerový systém, který také snímá hranici objektu. Tyto záznamy jsou ukládány na několika zdrojích a jsou pod neustálou dvojitou kontrolou pověřených osob.

7.2 Plášťová ochrana

U plášťové ochrany se nabízí využití většího množství prvků pro zajištění bezpečnosti, tudíž můžeme zde nalézt široké spektrum zabezpečovacích prostředků. Pokud bychom se zaměřili na svrchní část, tzn. na střechu, tak ta je sestavena z plechového materiálu, nachází se zde celkem pět průlezů, avšak dva z nich nejsou plně zhotoveny. Na všechny provozuschopné průlezy jsou instalovány magnetické detektory typu MAS 303 a jejich případné narušení je zaznamenáváno PČR, která v případě pokusu o vniknutí do budovy vyšle své jednotky na místo. Technický stav těchto průlezů je pravidelně kontrolován a dochází k běžné údržbě. Několikrát došlo jak k drobným, tak větším rekonstrukcím.

Okna jsou specificky zabezpečena. Zvenčí jsou chráněna prvkem mechanických zábranných systémů, konkrétně mřížemi. Samotné okno je tvořeno kastlovou konstrukcí, ne však takovou, jak je známa. Vnější okenní sklo je vyrobeno z odolnějšího skla, které je pokryto bezpečnostní folií a vnější bezpečnostní tabulka je sestrojena jako „sendvič“. První vrstva je tvořena hliníkem, druhá vrstva je z dřevěného materiálu a třetí vrstva je opět tvořena hliníkem. Je mnohem odolnější proti dobývání se pachatelem, nelze ho jednoduše prokopnout ani poškodit primitivním prostředkem. Zároveň je z vnitřní části této tabulky použit otřesový detektor typu Audiodetektor FG-73, který při detekování narušení spustí alarm a informace o tomto stavu je přenesena na blízkou stanici Policie České republiky, jejíž jednotky jsou ihned vyslány na místo.

Obr. 10 - Okenní mříže

Obr. 11 - Okno z vnitřního prostoru s otřesovým detektorem

Obr. 12 - Okno z vnitřního prostoru

Co se týče hlavních vstupních dveří, ty jsou z vnější strany opatřeny mřížemi. Na prosklené části samotných dveří je bezpečnostní fólie. Využit je zde i element spadající do technické ochrany, a to konkrétně systém, který zajišťuje automatické otáčení dveří. Je opět ovládán odpovědnou osobou vykonávající činnost na informačním pultu, ta má oprávnění manipulovat s tímto komponentem. Tento dveřní systém je instalován pouze na jedny ze tří vstupních čelních dveří. Princip spočívá v tom, že dveře je možno otevírat automaticky při detekování blížící se osoby, zároveň je lze manuálně otevřít, zavřít a v neposlední řadě se zde nachází možnost bezpečnostního uzavření. V případě potřeby je zde i možnost zmáčknutí bezpečnostního tlačítka, po jehož stisknutí se ihned uzavřou vstupní dveře se zmiňovaným systémem a turnikety nacházející se uvnitř budovy.

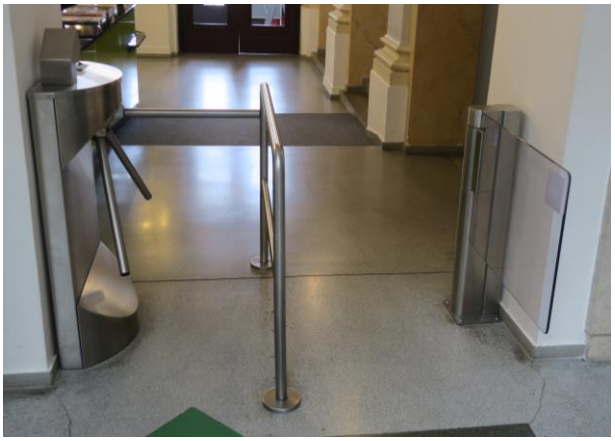
Obr. 13 – Systém automatického otáčení dveří

Obr. 14 - Ovládací panel dveřního systému

7.3 Prostorová ochrana

Záměrem zajištění prostorové ochrany je odhalit vniknutí pachatele dovnitř objektu a zároveň zpomalit jej při nelegálních činech.

Ve vnitřním prostoru objektu je na bezpečnost kladen velký důraz a můžeme zde nalézt opravdu široké zastoupení bezpečnostních prvků. Z mechanických zábranných systémů jsou v prostoru využívány bezpečnostní skleněné dveře, které oddělují vestibul či halu od výstavních sálů. Dalším zástupcem této ochrany jsou turnikety ve vstupním vestibulu, které fungují jako brána, kterou může v jeden moment projít pouze jeden člověk. Každý z návštěvníků musí po zaplacení vstupného projít turniketem. Jak už bylo zmíněno v perimetrické ochraně, v případě jakéhokoliv druhu ohrožení mohou být turnikety automaticky uzavřeny tak, že jimi nikdo neprojde ven, avšak nejsou dostatečně vysoké, aby pachateli neumožnily je překonat.



Obr. 15 - Vstupní turnikety

Pohyb návštěvníků je samozřejmě ve vnitřním prostoru objektu z části omezen. Musí dodržovat provozní řád, což znamená například dostatečný odstup od závěsných exponátů a obecně od všech předmětů a chodit jen na povolená místa apod. V případě, že by někdo tato pravidla nedodržel, lze lehce tento čin identifikovat skrze snímání VSS. V ten moment je napomenut pověřenou osobou o jeho činu, což je v tomto případě místní lektor. Pokud by došlo k opakování jeho činu či neslušnému chování, může být návštěvník také vyprovozen k východu. U předmětů, které jsou na podstavci a nejsou chráněny skleněnou vitrínou, je vyčleněna diskrétní zóna, kam až návštěvníci mohou jít. Často je ohraničena zábranou ze železných kůlů propojených červeným lanem či lanem přírodních barev.

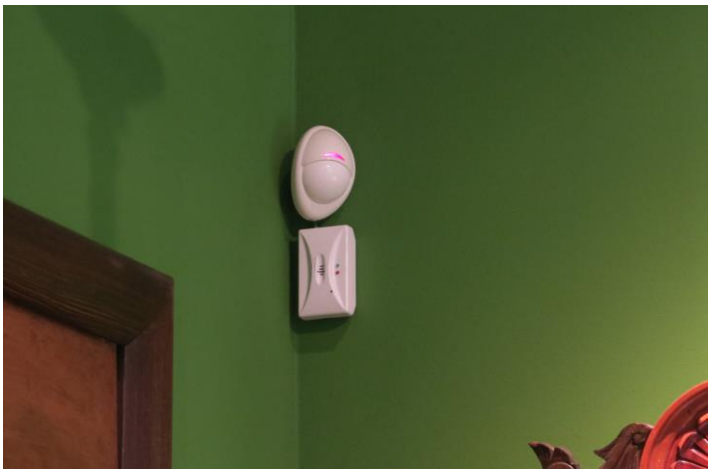
Obr. 16 - Vyčleněná diskrétní zóna s MZS

Základní kámen prostorové ochrany tvoří prvky technické ochrany. Z široké škály nabízených detektorů na trhu jsou využity:

7.3.1 Prostorové detektory

V této budově je hojně využíván detektor COBALT od firmy Trade Fides a.s., který má v sobě zabudován pasivní infračervený a mikrovlnný senzor. Jednou z jeho největších výhod je dostatečná odolnost vůči falešným poplachům. Pyrosenzor i mikrovlnný senzor jsou napojeny zvlášť. Optika, která zabezpečuje infračervenou oblast, funguje na stejném principu, který je použit u detektorů AQUA. Duální detektory COBALT, COBALT Plus a COBALT Pro mohou pracovat ve dvou režimech:

- Základní režim – V tomto režimu stačí k aktivaci poplachu detekce pohybu oběma senzory. První systém (MW nebo IR), který detekuje pohyb, aktivuje tří sekundovou prodlevu. Během této doby musí detekovat pohyb druhý senzor. Pokud dojde k zachycení pohybu druhým senzorem, je spuštěn poplach.
- Mikrovlnný režim – Jedná se o detektor, který spouští poplach ve dvou případech, na základě detekce od obou systémů, ale také po 16 podnětech od mikrovlnného senzoru bez narušení PIR. [27, 42]



Obr. 17 - PIR

Zároveň můžeme v objektu nalézt bezdrátové optické závory, které se nachází ve třech místnostech. Ty jsou určeny pro detekci protnutí infračervených paprsků s osobou procházející mezi vysílačem a přijímačem.

Obr. 18 - Detektor optické závory

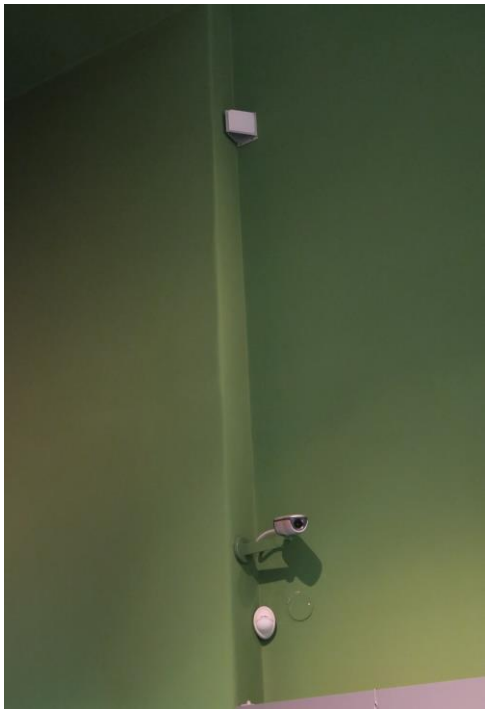
7.3.2 Detektory tříštění skla

V tomto případě se jedná o duální detektor, který s dosahem devíti metrů dokáže detekovat rozbití skla na základě změn tlaku vzduchu v místnosti (flex detekce) a pomocí detekce zvuku rozbíjeného skla (audio detekce). Opět je využit již zmiňovaný Audiodetektor FG-730. [42]

7.3.3 Dohledové videosystémy

Ve vybraném objektu je VSS ve full HD kvalitě a jejich záznamy jsou uchovávány po dobu třech měsíců. Použité kamery jako HIKVISION DS-2CE16D5T-AVFIT3 venkovního provedení a HIKVISION DS-2CD2620F-I mají své záznamové zařízení. Mezi jejich přední vlastnost patří rozpoznávání obličejů, což se využívá v případě, že je zapotřebí dohledat určitou osobu. Tento systém dokáže vygenerovat i více záznamů, na kterých se osoba vyskytuje v různém časovém úseku. Tyto záznamy slouží nejen pro potřeby vybrané instituce, ale hojně jsou využívány Policií ČR pro vyhledávání pachatelů. Všechny kamery jsou vybaveny infračerveným snímáním. V každém patře a u vstupních dveří je umístěna ještě pohyblivá IP kamera s možností odposlechu, která slouží jako doplňující bezpečnostní prvek. Během provozní doby instituce jsou záznamy ze všech instalovaných kamer sledovány pověřenými osobami u informačního pultu nacházejícího se u vstupních dveří. Zaměstnanci se zaměřují na případné podezřelé chování návštěvníků, nepovolenou manipulaci s předměty sbírek, krádeže, nedodržování návštěvního řádu a samozřejmě preventivně hlídají celý objekt. Není to jediná kontrola snímků z kamerových záznamů, druhou provádí výše postavená osoba vykonávající profesi bezpečnostního kontrolora a projektanta zabezpečovacích systémů.

Obr. 19 – VSS s pohyblivou kamerou



Obr. 20 - VSS a PIR

Obr. 21 - Záložní zdroj

Jedna věc k zamyšlení je, zda je vhodně vybrán distributor kamer, neboť se jedná o čínské technologie, které v dnešní době jsou dosti spekulativní a označují se za bezpečnostní riziko. To je často způsobené výběrem levnějších produktů na úkor jejich bezpečnostních vlastností. Podle podnikatele Pavla Švadlenky, který působí na české pobočce Hikvisionu, se v tomto případě jedná pouze o obchodní válku mezi Spojenými státy a Čínou. V rozhovoru s internetovým deníkem Lupou uznává, že jsou již doložené případy v České republice, kdy šlo o problémy se zabezpečením dat, a že bylo možné se do zařízení dostat. Na svou obhajobu však konstatuje, že se tento problém děje i v dalších velkých technologických společnostech, a že všude se dá něco najít. Zarážející je, že na otázku kladenou redaktorem: „*Máte obavy z toho, že by se aféra kolem Huawei a ZTE mohla dotknout také působení Hikvision na českém trhu?“* odpověděl: „*Myslím si, že ne. Neděláme dodávky do kritické infrastruktury. Důvodem toho, proč jsme lídrem na trhu, je fakt, že si o to trh řekl.*“ [39]

Nicméně po nahlédnutí do registru smluv s touto společností, je možné zjistit, že tato odpověď se neshoduje s realitou. Je tedy zřejmé, že je možné si na základě této skutečnosti vytvořit obrázek ohledně věrohodnosti informací podané zástupcem této firmy. Tržní nabídka v tomto segmentu je v dnešní době opravdu rozšířená, a jak je možné vidět, každá společnost prosazuje své produkty pokud možno v nejlepším světle. Tímto způsobem propagace pak může dojít k zakrytí případných bezpečnostních rizik, kterých si uživatel zpočátku nevšimne.

Konkrétní případy se následně řešily aktualizacemi, ale největší problém podle něj je ten, že síť, na kterou je napojen kamerový systém, není chráněna zvnějšku. Společnost Hikvision je chráněna tím, že v jejich nabídce je pouze samotný VSS, avšak pokud zákazník využívá

možnosti vzdáleného přístupu, je na něm, aby toto připojení dostatečně zabezpečil. Přístup českých uživatelů hodnotí jako dosti laxní, což potom způsobuje jisté problémy. [39]

V konečném důsledku je na uživateli, ať si udělá názor sám, ale měl by si uvědomit, že peníze nejsou více než bezpečnost. Proto je důležité vybírat produkty zajišťující bezpečnost opravdu svědomitě a před koupí racionálně vyhodnotit vhodnost daného produktu a výrobce.

7.3.4 Tísňové systémy

Neboli systémy přivolání pomoci jsou zde instalovány jednotlivě na každém patře a jeden přenosný se nachází u informačního pultu. Tento typ mají lektoři nosit u sebe v průběhu prohlídek muzea. Nebyl však doposud využit.

7.3.5 Fyzická ochrana

V tomto případě je zde pověřená skupina zaměstnanců složená ze čtyř osob, kteří jsou nazýváni lektory. Tito lektoři jsou rozděleni na různá působiště, ať už jako obsluha informačního pultu s prodejem vstupenek, jako kontrola kamerových záznamů, jako průvodci či bezpečnostní dohled v provozní době. Je nutno podotknout, že ani jeden ze zaměstnanců neabsolvoval zkoušku odborné způsobilosti pro dílčí kvalifikaci „strážný“.

7.3.6 Úprava vzduchu

V objektu se nachází několik zařízení, které zbavují vzduch prachu a jiných nečistot a zároveň ho zvlhčují. V historických budovách, ve kterých se nachází předměty citlivé na mikroklimatické podmínky, je to bezpochyby nepostradatelný komponent. Typ tohoto zařízení je BRUNE B 300 s možností UV desinfekce.

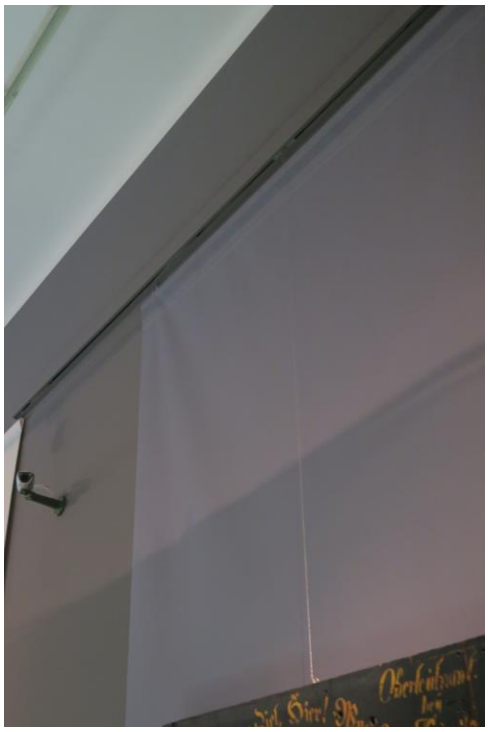
Obr. 22 - Čistič vzduchu

7.4 Předmětová ochrana

Účelem zajištění předmětové ochrany je zabezpečit předmět tak, aby nedošlo k jakékoliv nepovolené manipulaci s chráněným předmětem. V této vybrané instituci je na tento typ ochrany kladen velký důraz, jelikož historické sbírky a předměty jsou obohaceny jak o speciální zabezpečovací komponenty, tak o zabezpečení regulující mikroklima.

7.4.1 Technická ochrana

V první řadě je potřeba zmínit speciální detektory určené převážně pro předmětovou ochranu. Skoro u všech předmětů je možné nalézt nainstalované pohybové čidlo, které funguje stejným způsobem jako u prostorové ochrany. U závěsných předmětů, jako jsou například obrazy a gobelíny, je použit váhový detektor. Ten má uložen v paměti hmotnost vystaveného kusu, a v případě manipulace je spuštěn poplašný systém. Třetí typ se nazývá magnetický detektor, který je možné nalézt u vitrín, u kterých by mohlo dojít k jejich sejmutí či posunutí. Při tomto typu manipulace je opět spuštěn poplašný systém.

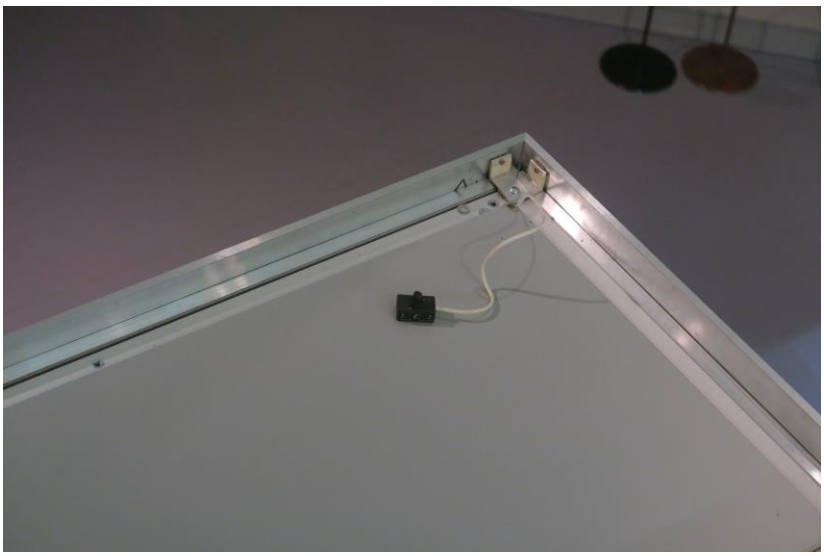


Obr. 23 - Váhový detektor

A. Běžné vitríny

Jedná se o vitríny, kterými je chráněna většina předmětů sbírek, až na několik výjimek v řádu desítek, které si žádají vyšší úroveň zabezpečení. Klasická vitrína je tvořena ze skleněné části, která je složena ze dvou materiálů na sebe vrstvených, a to sklo, fólie, sklo. To z toho

důvodu, že pokud by došlo k jejímu rozbití, omezilo by to poranění osoby, která sklo rozbila neopatrností, či pachatele, který k tomu měl motiv. Zároveň to ztěžuje dostání se k předmětu, jelikož je fólie vyrobena z velice pevného materiálu. Jako zástupce prvků technické ochrany zde nalezneme detektory tříštění skla, které reagují na manipulaci s vitrínou, a které následně spouští alarm. Detektor je napojen na Policii České republiky, která je připravena zasáhnout v případě vzniklého problému.



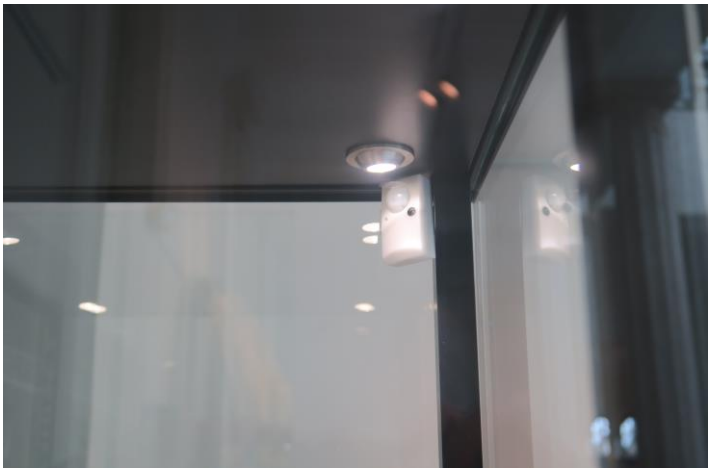
Obr. 24 - Napojení na detektor tříštění skla

B. Vitríny nejvyšší ostrahy

Jak už bylo zmíněno, některé vybrané předměty sbírek vyžadují vyšší úroveň zabezpečení, jedná se o předměty opravdu cenné či zapůjčené na speciální krátkodobou výstavu. Tento typ vitríny má svou skleněnou konstrukci složenou z tzv. „sendvičového skla“, které je mnohem více odolné proti sejmutí, rozbití či jinému poničení. Exponát nacházející se uvnitř je položen na tlakové podložce s pohybovým čidlem. Pokud by se pachateli podařilo nějakým způsobem dostat k exponátu bez aktivace některého z užitých detektorů, je opravdu minimální pravděpodobnost, že nedojde k aktivaci detektoru právě zde. Tato podložka je pohyblivá a zároveň multifunkční. Případné spuštění poplašného systému či odpojení z jedné ze tří ústředen znamená přesun historického předmětu z vitríny do podstavce, na kterém je vitrína instalována. Dojde ke skrytí předmětu do úkrytu na potřebně dlouhou dobu. Zároveň se zde nachází speciální detektor tříštění skla, který reaguje na vysoké frekvence zvuku, viz obrázek 27.

Obr. 25 - Vitrína nejvyšší ostrahy

Obr. 26 - Exponát na tlakové podložce



Obr. 27 – Detektor tříštění skla

Mikroklima

Uvnitř vitrín jsou snímače systému Hanwell typu ML4000, což je bezdrátový systém navržený a vyvinutý především pro muzea, galerie, zámky, hrady, depozitáře, archivy či památkově chráněné objekty, který je napojen na regulační systém obsluhy. Zde se kontrolují hodnoty tepla a vlhkosti. Hodnoty se musí pohybovat mezi 21-24ºC a 42-45% vlhkosti. Zá roveň je měřeno umělé osvětlení uvnitř vitrín.

Obr. 28 - Měřič mikroklimatu

Tento typ ochrany je využíván především u cenných předmětů, u kterých není žádána manipulace nepovolanou osobou. Mezi zabezpečovací prvky tvořící předmětovou ochranu patří VSS, poplachové bezpečnostní systémy, vitríny, trezory, ale také další prvky MZS.

7.4.2 Separátní okruhy

Všechny zde užité zabezpečovací systémy mají dvojitou ochranu před poškozením či nevyžádanou manipulací. První je přímo zdroj konkrétního detektoru, který je instalován na potřebném místě. Druhý typ ochrany znamená, že každý souhrnný systém vede ke své určené ústředně, a to z toho důvodu, že kdyby pachatel chtěl odpojit kompletně celý zabezpečovací systém v budově, nepodaří se mu to přes jednu ústřednu. Dveře a okna mají svou ústřednu, vnitřní prostor vede k druhé ústředně a na třetí ústřednu je napojeno zabezpečení předmětů sbírek. Tyto ústředny jsou dostatečně skryty a zároveň jsou pod přísnější kontrolou.

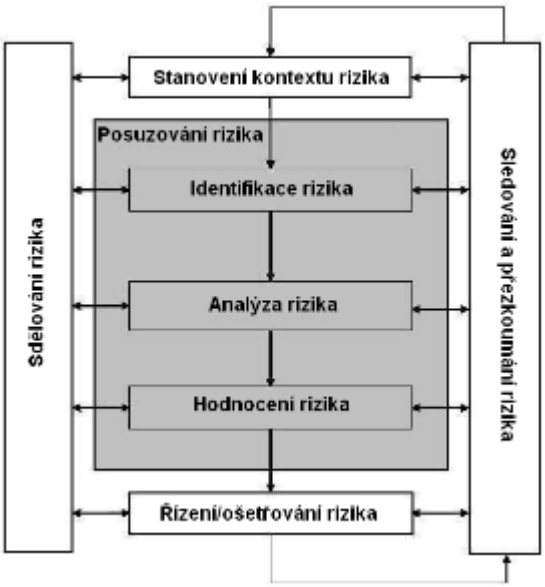
Obr. 29 - Elektronická ústředna

.

8 POSUZOVÁNÍ RIZIK

Tato kapitola je věnována posuzování bezpečnostních rizik vybrané instituce. Vybraný objekt je anonymní a slouží spíše jako obecná předloha pro analyzování všech historických památek podobného charakteru. V tomto případě je posuzování rizik zaměřeno na fyzickou bezpečnost, kde jsou rizika napřed identifikována, následně zanalyzována a ohodnocena a nakonec je navrženo další možné ošetření identifikovaných rizik. Je vycházeno z vlastního analyzování objektu, z rozhovoru s osobou, která se s těmito problémy setkává denně, a z konzultace s experty z firem zabývajících se konstruováním zabezpečovacích komponentů a příslušenství.

Pomocí programu RISKAN a vlastního experimentu je vytvořeno subjektivní posouzení rizika souvisejícího s analyzovaným ohrožením. Na obrázku číslo 30 je zobrazen algoritmus procesu řízení rizik, který je možné nalézt v normě ISO 31000:2009, ze které je také vycházeno. [2]



Obr. 30 - Proces managementu rizik (převzato) [40]

8.1 Program RISKAN

V této kapitole byl pro sestavení rizikové analýzy využit program RISKAN. Jedná se o subvenční prostředek, jímž jsou vyhodnocovány aktiva a hrozby pomocí programové matice rizik. V programu byl vytvořen zástupce subjektu, ve kterém byly vytvořeny dva seznamy vytvořené z 30 různých aktiv a hrozeb. Uživatel zároveň určuje hodnoty výsledného rizika.

V tomto případě jsou hodnoty nastaveny následovně:

1. nízké riziko 0 – 30,
2. střední riziko 31 – 60,
3. vysoké riziko 61 – 90.

Zhodnocení rizik v programu RISKAN obsahuje:

- identifikaci aktiv a jejich ohodnocení,
- identifikaci hrozeb a ohodnocení jejich pravděpodobnosti,
- ohodnocení zranitelnosti aktiv jednotlivými hrozbami,
- výpočet výsledného rizika pro každou relevantní dvojici aktivum-hrozba,
- roztřídění výsledných rizik na „nízká, střední a vysoká“ dle stanovených

kritérií. [15]

Výstup dosavadní práce byl převeden do Microsoft Office Excel, kde se pracuje s vytvořenou maticí rizik. Napřed se však v tabulce vyjádří hodnota aktiv a pravděpodobnost hrozeb, a to stupnicí od 0-5, kde je číslo 5 bráno jako nejvyšší možná volba. V druhém kroku se pracuje v již zmiňované matici, kde se postupně hodnotí zranitelnost aktiv jednotlivými hrozbami. Po dokončení této části došlo k zobrazení výsledků, jimiž jsou barevně zbarvená políčka, která určují, o jakou míru rizika se jedná.

Provedení analýzy rizik s využitím softwarového produktu RISKAN umožňuje zrychlit celý proces, připravit přehledné výstupy a závěry pro rozhodování o dalším postupu ze strany vedení organizace i specialistů bezpečnosti. Kromě toho tento postup usnadňuje opakování analýzy při změně podmínek analyzovaného systému (prostředí) nebo jeho bezpečnosti a celý proces urychluje. Výstupy je možné převést do tabulek v Microsoft Office Excel a průběžně s nimi pracovat.

Identifikace a hodnocení aktiv:

Nízká:

- nulový dopad pro společnost
- minimální dopad pro společnost

Střední:

- problémy a finanční ztráty organizace

Vysoká:

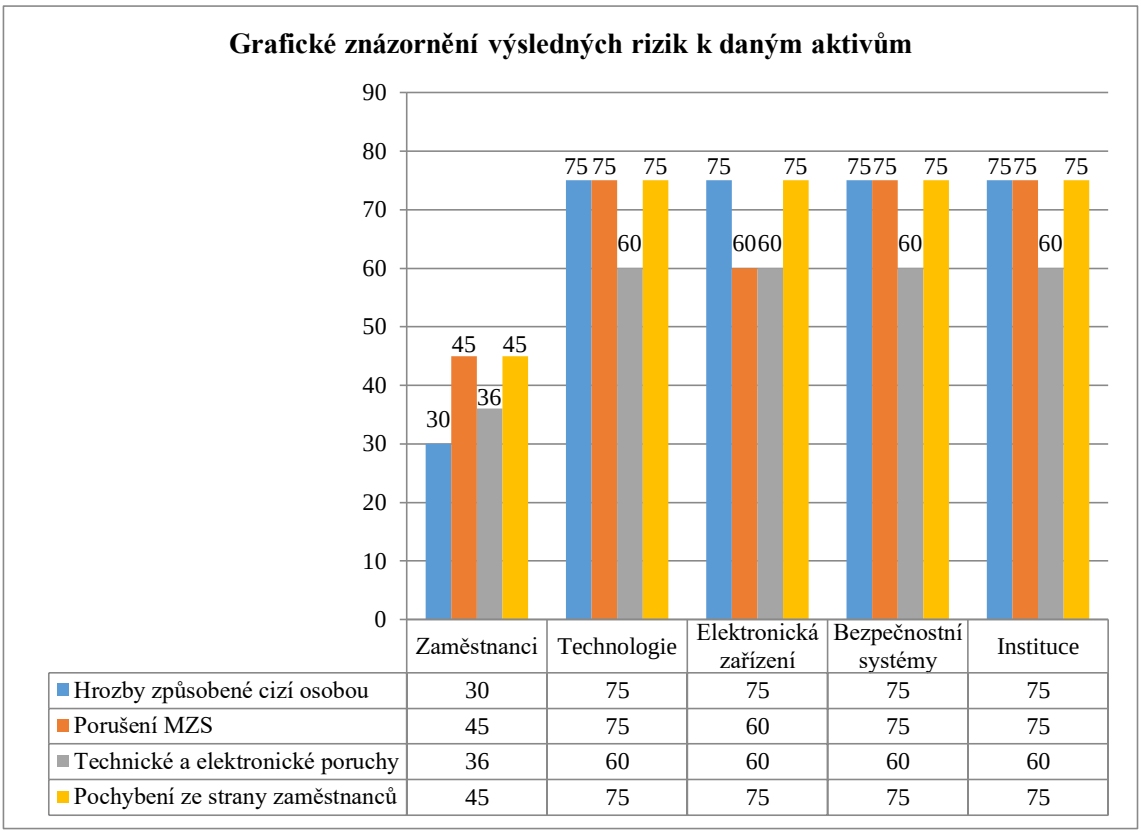
- velké problémy a finanční ztráty organizace
- ohrožení dalšího fungování organizace

Tabulka 1 – Seznam hrozeb s číselným vyjádřením pravděpodobnosti

Hrozby	Pravděpodobnost
1. Hrozby způsobené cizí osobou	5
1.1 Napadení zaměstnance	3
1.2 Krádež exponátu	3
1.3 Kybernetický útok	5
1.4 Nastražená bomba	3
1.5 Odpojení elektrického jističe	3
1.6 Vandalismus na majetku	5
1.7 Neukázněné chování návštěvníků	5
1.8 Krádež peněz	3
1.9 Narušení inženýrských sítí	4
1.10 Neoprávněný vstup cizí osoby	3
1.11 Sabotáž EBS	3
2. Porušení MZS	5
2.1 Zdolání zámkového systému	5
2.2 Překonání dveří	4
3. Technické a elektronické poruchy	3
3.1 Porucha EBS	4
3.2 Porucha EPS	3
3.3 Poškození rozvodny	1
3.4 Poškození detektorů	3
3.5 Přerušení dodávky energií	1
3.6 Vznik požáru (zkrat)	3
3.7 Selhání záložních zdrojů	4
3.8 Hluché místa v PTZS	2
4 Pochybení ze strany zaměstnanců	5
4.1 Nedodržení kontrolních postupů	5
4.2 Přehlížení podezřelé osoby	4
4.3 Infiltrace interních informací	5
4.4 Pronesení nebezpečného předmětu	4
4.5 Chybné nastavení mikroklima	2

Tabulka 2 – Seznam aktiv s číselným vyjádřením hodnoty aktiv

Aktiva	Hodnota aktiv
1. Zaměstnanci	3
1.1 Interní	3
1.2 Externí	3
1.3 Proškolení	3
2. Technologie	5
2.1 Moderní výbava	5
2.2 Pravidelná aktualizace	4
2.3 Komplexní přehled o dění	5
2.4 Napojení na PČR	5
2.5 Napojení na HZS	4
2.6 Nastavené mikroklima	5
3. Elektrické zařízení	5
3.1 Reproduktory	4
3.2 Datové sítě	3
3.3 Počítače	4
3.4 Wi-fi	3
3.5 Rozvodny	5
4. Bezpečnostní systémy	5
4.1 Dohledové videosystémy	5
4.2 Vstupní terminál	3
4.3 Čtečky vstupenek	3
4.4 PTZS	5
4.5 EPS	4
4.6 Stabilní hasící zařízení	4
4.7 Detektory	5
5. Instituce	5
5.1 Exponáty	5
5.2 Eko., soci. a kul. rozvoj	4
5.3 Dotace a granty	5
5.4 Legislativa	1



	Zaměstnanci	Technologie	Elektronická zařízení	Bezpečnostní systémy	Instituce
Hrozby způsobené cizí osobou	30	75	75	75	75
Porušení MZS	45	75	60	75	75
Technické a elektronické poruchy	36	60	60	60	60
Pochybení ze strany zaměstnanců	45	75	75	75	75

Obr. 31 - Grafické znázornění výsledných rizik k daným aktivům

8.1.1 Zhodnocení výstupních dat z programu RISKAN

Nyní jsme vyhodnotili zranitelnost jednotlivých hrozeb vůči daným aktivům, které jsou rozděleny do následujících skupin:

- Zaměstnanci
- Technologie
- Elektronická zařízení
- Bezpečnostní systémy
- Instituce

Vzájemné vztahy mezi nimi jsou v následující podkapitole detailněji popsány. Na základě výsledků z této analýzy rizik jsou navrženy další možné prvky spadající do fyzické bezpečnosti.

Zaměstnanci

Na základě výsledků matice je možno usoudit, že žádná z hrozeb nepředstavuje pro zaměstnance vysoké riziko. Všechny hrozby se pohybují v pásmu středního rizika, kde nejvýznamnější hrozby z hlediska rizika jsou porušení MZS a pochybení ze strany zaměstnanců. Z hlediska pochybení z řad zaměstnanců jsou významná rizika jako nedodržení kontrolních postupů či infiltrace informací, které by měly spíše dopad na zaměstnané osoby. Samotné aktivum není bráno jako významně rizikové, avšak jejich jednání či nedodržení pracovního řádu může znamenat značné riziko pro konkrétní objekt.

Technologie

Aktivum technologie je jedním z nejrizikovějších aktiv, které může být postiženo danými hrozbami. Technologie jsou obecně v dnešní době nedílnou součástí téměř všech společností, institucí, objektů a možnosti jejich napadaní jsou velmi rozšířené. Nejvyšší hodnoty rizikovosti vyšly u oblasti hrozby zaviněné cizí osobou, u porušení MZS a pochybení ze strany zaměstnanců.

Největší hrozbou zaviněnou cizí osobou je zejména kybernetický útok. Ty v dnešní době nabírají na vzestupné tendenci, kdy se takzvaní hackeři „nabourají“ do systému určité společnosti či instituce a požadují výkupné za uvolnění informačního systému do zpětného chodu. Touto hrozbou je nejvíce ohrožena moderní výbava, komplexní přehled o dění

v objektu a napojení na PČR, neboť tato aktiva nejvíce zaštiťují zabezpečení vzácných předmětů v objektu, a v případě jejich systémového napadení by to mohlo způsobit obrovské problémy. Instituce může mít systémové zabezpečení na velmi vysoké úrovni, avšak v dnešní době se „šikovnost" hackerů posunula o úroveň výše a v mnohých případech je opravdu obtížné jim čelit.

Při porušení MZS, a to přesněji zdoláním zámkového systému a překonáním dveří, je rizikové hlavně napojení na Policii ČR, které může být při úspěšném prolomení odpojeno a tím vyřazeno z provozu. Obdobně na tom je i napojení na hasiče.

Asi největším nebezpečím pro dané aktivum je pochybení ze strany zaměstnanců. Pochybení může nastat při nedodržení pracovních postupů při kontrolách, při přehlížení podezřelé osoby nebo při infiltraci interních informací. Jak bylo zmíněno v předešlém odstavci, technologie jsou v tomto případě stěžejní pro běžný chod v kulturních památkách a pochybení ze strany zaměstnanců by mělo fatální následky nejen pro samotný objekt, ale také konkrétní zaměstnance.

Vysokým rizikem ohrožení jsou i hrozby ze skupiny technických a elektronických poruch. Tyto poruchy mohou mít dopad zejména na selhání PTZS, EPS a záložních zdrojů. Což by znamenalo vyřazení daných nejdůležitějších komponentů zajišťujících běžnou ochranu instituce a samozřejmě by bylo vyřazeno z provozu vše, co je závislé na elektrickém zdroji.

Elektronická zařízení

Elektronická zařízení jsou na tom z hlediska rizika hrozeb velmi obdobně jako předchozí aktivum technologie. Nejrizikovější jsou hrozby zaviněné cizí osobou a pochybení ze strany zaměstnanců. Cizí osoby mohou provést kybernetický útok nebo poškodit dané aktivum svým vandalismem. Rizikem jsou ovšem také možnosti nastražení bomby, odpojení elektrického jističe nebo krádež vzácného exponátu.

Při pochybení ze strany zaměstnanců z matice rizik vyplývá, že nejvyšších hodnot dosahují: přehlížení podezřelé osoby, infiltrace interních informací a pronesení nebezpečného předmětu. Všechny tyto pochybení ohrožují aktivum rozvodny a taktéž počítače. U rozvoden může dojít k přerušení přenosu potřebných energií k chodu části objektu, čímž může být poté objekt jednodušeji zasažen například krádežemi apod. U počítačů je riziko nabourání se do nich cizí osobou a zneužití citlivých interních informací.

Do třetí skupiny hrozeb se řadí technické a elektrické poruchy, kdy nejzávaznější jsou porucha PTZS, EPS, poškození detektorů, vznik požáru a selhání záložních zdrojů. Například při výpadku energií a rovněž selhání záložních zdrojů nebudou elektronická zařízení fungovat a vybraný objekt nebude moct provozovat svou činnost, čímž přijde o tržby. Požár může mít také velmi nepříznivé dopady, jelikož může systémy nevratně poškodit a tím i nečekaně navýšit náklady instituce, která bude nucena pořídit nová zařízení.

Poslední skupinou hrozeb je porušení MZS. Například při zdolání zámkového systému se mohou neoprávněné osoby dostat k počítačům, které mohou infiltrovat a provést krádež citlivých dat.

Bezpečnostní systémy

Aktivum bezpečností systémy je na tom z hlediska rizikovosti hrozeb stejně jako aktivum technologie. Nejvýznamnější skupinou hrozeb jsou ty, které zaviní cizí osoba. Zejména tedy formou kybernetického útoku, vandalismem, neukázněným chováním nebo nastraženou bombou. Zde jsou nejvíce zranitelná aktiva jako kamerový systém a PTZS, neboť na těchto dvou komponentech závisí fyzická bezpečnost. Pokud dojde k jejich narušení, znamená to razantní oslabení systému a může být nechtěně manipulováno s vystavenými exponáty.

Druhou skupinou nejvýznamnějších hrozeb je pochybení ze strany zaměstnanců. Na bezpečnostní systémy mají velký dopad infiltrace interních informací, nedodržení pracovních postupů při kontrole, přehlížení podezřelé osoby nebo pronesení nebezpečného předmětu. Tímto může být zasaženo poplachové a tísňové zabezpečení, které mohou cizí osoby přerušit nebo poničit. Nicméně těmto hrozbám se dá vyvarovat, a to dostatečně proškoleným personálem a vstupní kontrolou.

Další skupinou významných hrozeb pro bezpečnostní systémy je porušení MZS. V rámci těchto hrozeb může, jako u předchozí skupiny, dojít k poničení nebo zneužití detektorů a dalších zabezpečení. V případě, že je pachatel znalý v těchto systémech, může dojít k odpojení detektorů na napojení PČR.

Posledními hrozbami jsou technické a elektrické poruchy. Poruchy či poškození bezpečnostní systémů mají dopad na chod a bezpečnost objektu. Do středního rizika, v tomto případě, řadíme poruchu PTZS, neboť více než polovina aktiv je řazena do PTZS. Následně pak selhání záložního zdroje, a to v případě, kdy dojde k odpojení elektrické energie a záložní zdroj by selhal, a tím nelze zajistit dostatečné zabezpečení vybraného objektu.

Instituce

Aktivum instituce je ze všech aktiv jedním z nejméně zranitelných. To zejména hrozbami zaviněnými cizími osobami. Tak jako u ostatních aktiv je největším rizikem kybernetický útok, nicméně také krádež peněz nebo exponátu. Samotné exponáty jsou zranitelné vůči vandalismu na majetku, neboť poničení historického předmětu je nenávratné. Ztrácí svou hodnotu, a pokud by se jednalo o exponát vypůjčený na krátkodobou výstavu, znamenalo by to i finanční vyrovnání s druhou stranou.

Vysokým rizikem se vyznačují také hrozby pochybení ze stran zaměstnanců. Zde dosahuje nejvyšších hodnot nedodržení pracovních postupů při kontrole. Může například dojít ke skryté kontrole, která má vyhodnotit práci zaměstnanců, a na základě této kontroly poté poskytnout dotace a granty nebo finanční ocenění samotných zaměstnanců. Pokud zaměstnanci nedodrží předepsané postupy, tak tím mohou zapříčinit neudělení těchto peněžních plnění.

Za zmínku stojí také technické a elektrické poruchy a porušení MZS. Nejvíce ohroženým aktivem jsou v tomto případě exponáty, které by mohly být pachatelem následně odcizeny nebo poškozeny.

8.2 Experiment

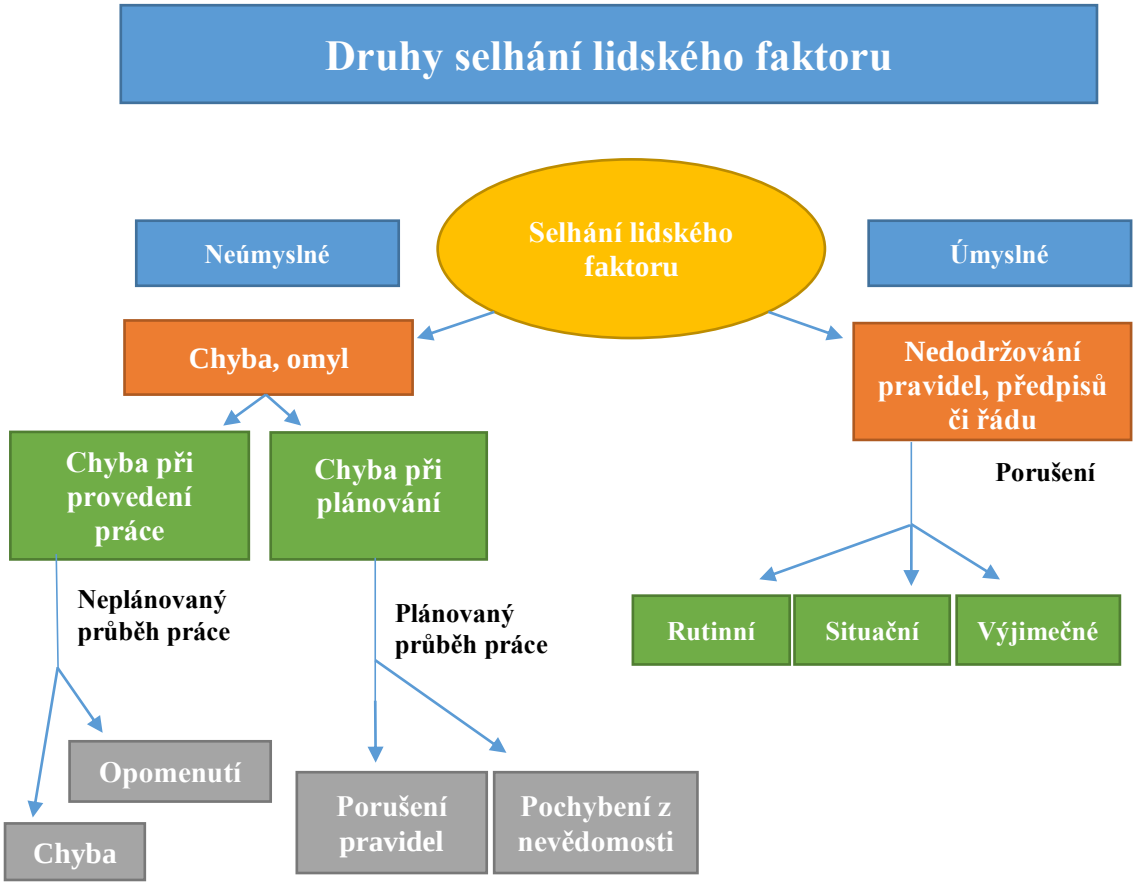
Tento pojem vznikl z latinského názvu experimentum, což v překladu znamená pokus nebo zkouška. Jedná se o vědeckou metodu. Princip tohoto experimentu spočívá v tom, že dochází ke zkoumání určitého procesu, při kterém je na místě, že experiment zůstane neprozrazený, neboť úmyslem je dosáhnout co nejreálnějších výsledků. Jen tak je možné nejlépe zhodnotit stanovené počáteční hypotézy. [25]

8.2.1 Princip experimentu

Jinými slovy záměrem je otestovat profesionalitu a odpovědnost k práci ze strany zaměstnanců v instituci XY. Důvod, proč byl zrovna tento způsob vybrán, je, že lidský faktor je v předních příčkách hrozeb, a to jak na straně zaměstnanců, tak samozřejmě samotných pachatelů, kteří mají v úmyslu škodit. Tento experiment se tomu přímo nabízel.

Zde je pozornost zaměřena na personální rizika, která jsou způsobena například chybným provedením práce, nesprávným jednáním, vynecháním jednoho zásadního kroku při uložené práci, porušením vnitřních pravidel instituce nebo protizákonným jednáním. Tyto úkony jsou děleny na úmyslné a neúmyslné. Dle mezinárodních statistik se potvrzuje fakt, že příčinou podnikových nedostatků, ať již podstatných odchylek od výkonových požadavků či mimořádných událostí, je z 80 % chyba ze strany zaměstnanců.

V tomto případě se jedná o selhání lidského činitele v působnosti bezpečnostního dozorce a lektora v jedné osobě. Práce bezpečnostního pracovníka vyžaduje vykonávat jeho práci co nejsvědomitěji, neboť jeho nesprávný krok ohrožuje zdraví i životy desítek až stovek lidí. Proto musí být na této pozici osoba k této práci vhodná ať už po fyzické, psychické a mentální stránce. V případě, že zaměstnavatel zaměstná člověka, který k této práci nemá předpoklady, dostatečné fyzické vybavení, nevytváří zájem o práci či nemá potřebné znalosti, není možné dosáhnout bezpečnostního standardu zajištěného právě s pomocí fyzické ostrahy. [32]



Obr. 32 - Druhy selhání lidského faktoru (převzato a upraveno) [18]

Selhání zaměstnance

Je to způsobeno hned z několika důvodů, například přijímáním nevhodných zaměstnanců (nedostatečná kontrola osoby žádající o pozici), nevhodnou motivací ze strany vedení instituce či firmy, nedostatečnou kontrolou jejich výkonu, špatně nastaveným systémem trestů po nesprávném kroku zaměstnance, nedostatečným proškolením při vstupním programu či nedostatečně nastaveným risk managementem vybrané instituce.

Z výše uvedeného diagramu je možné vyčíst, co vše následuje po selhání lidského faktoru.

8.2.2 Stanovená hypotéza

Samotný experiment vycházel z hypotézy, která stanovuje personál, respektive dodržení režimových opatření jako nejslabšího článku zabezpečení daného objektu. Předpokládá se, že při provádění experimentu nebude dostatečně zajištěno režimové opatření a v zásadě při testování zaměstnanců, jejichž hlavní náplní práce je zajišťování bezpečnosti osob nacházejících se v objektu, kontrola sbírek a návštěvníků, poskytování informací či zajištění

klidného chodu v provozní době, dojde k jejich pochybení. Tento fakt by znamenal docela znepokojující zjištění a následně by bylo vhodné tuto situace řešit preventivními kroky.

8.2.3 Scénář experimentu

Po podání návrhu konzultantovi byl sepsán konkrétní scénář, který by zaručil dostatečné prověření správného přístupu k práci, posloupnosti pracovních kroků, zodpovědnosti zaměstnanců či jejich profesionalitu.

Tabulka 3 – Scénář experimentu

Časový harmonogram	Akce
21.02.2020 v 8 hod.	Zahájení plánované schůzky s konzultantem mimo vybraný objekt.
21.02.2020 v 9:30 hod.	Konzultant vchází do zmiňovaného objektu.
21.02.2020 v 10 hod.	V tuto dobu vcházím do budovy já s připraveným proslovem.
21.02.2020 v 10:02 hod	Vstupuji do vestibulu bez osobní identifikace, pouze na základě vymyšlené záminky.
21.02.2020 v 10:03 hod	Střetávám se s konzultantem a probíráme provedení experimentu s jeho konečnými výsledky.
21.02.2020 v 10:06 hod	Procházíme budovu a konzultujeme nynější zabezpečení.
21.02.2020 v 10:40 hod	Odcházíme z budovy.

Při zkoumání celkového zabezpečení objektu byl identifikován nedostatek v zabezpečení - kdy v rámci režimových opatření chybí evidence zaměstnanců přítomných v rámci instituce, avšak v daný okamžik se vyskytujících v jiných objektech areálu instituce. Tento nedostatek však nepředstavuje zásadní narušení bezpečnosti.

8.2.4 Průběh experimentu

Naplánovaný experiment započal vstupem mého konzultanta do vybrané historické budovy s tím, že nebude místní zaměstnance nijak informován o návštěvě druhé osoby. Jeho námět návštěvy byl zkontrolovat přípravu na plánovanou výstavu. To znamenalo, že se nacházel někde uvnitř budovy, aby nebylo možné ho přivolat ke vstupnímu turniketu.

Posléze byl naplánován příchod mé osoby, jejímž úkolem bylo otestovat nastavené režimové opatření. Nikdo ze zaměstnanců neznal mou identitu. Byla jsem oblečena neformálně a v kabelce přes rameno byl umístěn pepřový sprej. Při příchodu se postupovalo podle vymyšleného scénáře. Při rozhovoru s recepční obsluhou, které bylo sděleno, že mám uvnitř domluvenou schůzku s konzultantem, kterého zde všichni znají, a zdali se mohu odebrat rovnou za ním dovnitř budovy. Během této situace došlo ze strany pracovníků k menšímu pochybení, avšak bylo mému konzultantovi navrhnuto v této problematice zaměstnance více proškolovat a klást důraz na jejich obezřetnost při vykonávání práce.

Zaměstnanec informačního pultu, se kterým byla vedena konverzace, neměl nijak potvrzené, že schůzka je opravdu sjednaná a že se nejedná o osobu, která konzultanta sledovala při vstupu do budovy a schůzka s ním byla pouze smyšlená. Pokud by byl vstup povolen bez jakékoliv identifikace a schůzka by opravdu byla smyšlená a šlo by o pouhou záminku, znamenalo by to, že pachatel vstupuje dovnitř budovy zadarmo a zároveň může vykonávat nějaký protizákonný čin.

8.2.5 Vyhodnocení hypotézy

Experiment parciálně prokázal potvrzení stanovené hypotézy, tedy zranitelnost bezpečnostního systému v části fyzická ochrany, respektive režimových opatření. Konzultantovi bylo na základě výsledků experimentu navrhnuto zaměstnance v této problematice více proškolovat a klást důraz na jejich obezřetnost při vykonávání práce. Stanovená hypotéza se z části potvrdila, avšak momentálně se dosti efektivně pracuje na tom, aby se předešlo k opakování takových pochybení z řad zaměstnanců. Nejen na základě tohoto experimentu jsou v současnosti realizována opatření k nápravě a snížení rizika plynoucího z této zranitelnosti. Jedno z možných opatření je motivační systém odměňování vázaný na výsledky práce.

9 NÁVRHY NA DALŠÍ ZABEZPEČENÍ

Při navrhování dalších zabezpečovacích prostředků je vycházeno z analýzy vybraného objektu. Účelem je tvorba doporučení, která by mohly vylepšit zabezpečení.

9.1 Fyzická ochrana

První z návrhu na zlepšení zabezpečení budovy je zaměstnat jednoho bezpečnostního pracovníka s platnou zkouškou profesní klasifikace strážného. Jeho pracovní náplní by bylo dohlížet na klidný chod v provozní době, dohlížet na vstupující a odcházející osoby a v případě, že by bylo potřeba, provést bezpečnostní zásah za účelem odvrácení nebezpečí.

Odpovídal by za bezpečnost celého objektu, a to prostřednictvím dohledových bezpečnostních kamer, pochůzkovou činností, kontrolou bezpečnosti v rámci objektu, eliminací neukázněných návštěvníků nebo celkovou ochranou a ostrahou majetku instituce.

Tento pracovník by byl nasazen vybranou bezpečnostní agenturou, která by uzavřela s vybranou institucí smluvní dohodu o poskytování externích bezpečnostních služeb.

9.2 Průchozí bezpečnostní brána

Průchozí brána je jedním z dalších zabezpečovacích prvků, které dokáží zcela přesně detekovat určitou hrozbu. Tyto brány jsou určeny i k ochraně důležitých objektů, kde se nachází historicky cenné exponáty či jiné vzácné věci.

Dnešní trh nabízí širokou škálu těchto bezpečnostních zařízení, záleží na požadavcích zákazníka, neboť každý produkt se odlišuje svými vlastnostmi a zároveň svou účelností.

Fyzickou bezpečnost ve vybrané instituci lze rozšířit velice efektivním prvkem a to průchozí bránou. Konkrétně se jedná o bránu Ebinger SC 900. Mezi její přední vlastnosti patří jednoduchá obsluha, detekce všech nebezpečných předmětů, přesná lokalizace tohoto předmětu, snadná montáž, odolná konstrukce, zvuková signalizace či automatická kontrola zařízení. Dokáže zkontrolovat až 60 osob a jsou zde zabudována dvě detekční pole - a to ve vodorovné a svislé straně. Uživatel je oprávněn nastavovat citlivost těchto polí dle svých potřeb. Užitá technologie použitá v modelu SC 900 je kontrolována pokročilým mikroprocesorem a je čistě digitální. [34]

Zařízení splňuje všechny mezinárodní standardy, a dokonce i certifikaci NATO. Jeho účelnost v této historické budově by byla využita k zabránění pronášení nebezpečných

předmětů, které by mohly způsobit škody nejen na majetku, ale zároveň by mohlo dojít k ohrožení dalších osob.

Mezi další možné varianty, jak současné zabezpečení vylepšit z prvků zajišťující fyzickou bezpečnost, jsou senzorové bariéry. Vybraná instituce vlastní základní turnikety s čtecím zařízením vstupenek, tím pádem by se jednalo pouze o modernizaci dosavadního stavu.

Velice oblíbené a užívané senzorické bariéry jsou od firmy Dormakaba Česko s.r.o., jejíž produkty se nachází i v Národním muzeu v Praze. Konkrétně se jedná o senzorovou bariéru Argus HSB či HSG, která je vyráběna ve dvou výškových provedeních. Součástí konstrukce turniketů mohou být i dvě odlišná čtecí zařízení, jedno RFID čtecí zařízení, které by sloužilo jako skener vstupenek návštěvníků, a ve druhém případě by se jednalo o komponent spadající do režimové ochrany. Tím je myšlen přístupový a docházkový systém. Informace byly poskytnuty prostřednictvím konzultace s odbornicí pracující v této firmě, jejíž práce spočívá v projektizaci turniketů, zodpovídá za stavební připravenost pro montáž těchto turniketů a v neposlední řadě se zabývá vedením prodeje projektů. Konzultace na danou problematiku byla vedena s paní Ing. Alicí Mikloškovou dne 24. 3. 2020 prostřednictvím telefonického rozhovoru.

9.3 Vchodové dveře

Vzhledem k tomu, že se jedná o historickou budovu, která musí splňovat určité architektonické prvky a standardy, je dosti obtížné navrhnout přebudování vchodových dveří s doplňujícími bezpečnostními prvky. Jeden z návrhů je rozšíření instalace systému automatického otáčení dveří na všechny tři hlavní vchodové dveře. Zároveň by bylo zapotřebí zabudovat zde mechanické panikové hrazdy. Což je jedna z možností, jak zvýšit úroveň fyzické bezpečnosti v této budově.

Druhý plán je otázkou do budoucích let, kdy by došlo k nahrazení současných dveří za bezpečnostní dveře modernějšího charakteru, které by s vysokou spolehlivostí zabraňovaly neoprávněnému vniknutí. Jedna z nabízejících se možností je spolupráce s architekty a projektanty, kteří na základě požadavků instituce vytvoří projekt, který bude po schválení realizován vybranou společností. V České republice figuruje velké množství firem s tímto zaměřením. Po srovnání internetových nabídek se jevila společnost OGB s.r.o. jako vhodný kandidát. Po zhlédnutí její činnosti a práce bylo rozhodnuto tuto společnost kontaktovat za informativním účelem, neboť již má s rekonstrukcí historické budovy,

konkrétně dveřních prostor, předešlé zkušenosti. Firma prováděla rozsáhlou rekonstrukci ve Vlastivědném muzeum ve Slaném (viz fotografie). Komunikace probíhala 24. 3. 2020 s majitelem firmy, který konstatoval, že vychází vždy z požadavků zákazníka, kdy se snaží co nejlépe realizovat na základě probraných informací s odborníky plánovanou rekonstrukci, a to s důrazem na bezpečnost. Zároveň mohou být doinstalovány potřebné komponenty technické ochrany. Na obrázku je znázorněna modernizace ve zmíněném muzeu.

Obr. 33 - Vlastivědné muzeum ve Slaném [37]

9.4 Elektronický systém kontroly vstupu

Čtvrtý navrhovaný komponent je samostatný docházkový systém. Ten by se zde mohl nacházet v případě, že by nebyl zabudován již v turniketech, jednalo by se o samostatný prvek.

Slouží k automatické evidenci příchodů a odchodů zaměstnanců, zaznamenávání přerušení pracovní doby, a to buď za pracovním či osobním účelem, a v neposlední řadě rozliší, zda má osoba oprávnění vstoupit do budovy. Samotné programování terminálů se přizpůsobuje požadavkům zákazníka. Zaměstnavateli i zaměstnancům to ulehčuje práci. Princip byl popsán již v teoretické části této práce.

Již zmiňovaná společnost Dormakaba s.r.o. nabízí také tento prvek a jedná se konkrétně o model DORMAKABA Terminal 96 00, který by byl v tomto případě optimálním řešením

Obr. 34 - DORMAKABA Terminal 96 00 [14]

9.5 Dohledové videosystémy

V problematice prostorové ochrany (konkrétně kamerových systémů), byla zmíněna kauza se společností, která poskytuje zákazníkům tento typ zabezpečovacích komponentů. Instituce by měla být obeznámena s těmito informacemi, a pokud ne, navrhuji zvážit výběr dodavatele VSS do vybraného objektu. Na dnešním trhu je mnoho certifikovaných firem, které mají dlouholetou tradicí a jsou rovněž ověřeny zákazníky. S tím by souviselo i navýšení počtu kamer, které by byly doplněny do konkrétních výstavních sálů, vstupního prostoru a venkovního prostoru, který spadá do majetku instituce. Nevytvářelo by to změny ve struktuře nynějšího kamerového systému a zvýšil by se přehled dění v objektu.

10 DISKUZE NAVRHOVANÝCH OPATŘENÍ

Prostřednictvím multikriteriální analýzy bylo zjištěno, že nynější bezpečnostní systém ve vybraném objektu si žádá rozšíření o další ochranné a bezpečnostní prvky. Výsledky z využitých metod dokazují, že působení a činnost lidského faktoru patří mezi největší rizika, proto je zapotřebí zvýšit úroveň fyzické bezpečnosti právě v této oblasti.

Mezi stěžejní a podstatné opatření patří přijetí bezpečnostního pracovníka. Ten by nesl zodpovědnost jak za návštěvníky, tak samotné zaměstnance. Ačkoliv se může zdát toto opatření jako zbytečné, poněvadž doposud zde nebyl zaznamenán žádný případ, kdy by byl ohrožen život a zdraví osob nacházejících se v budově. Bezpečnostní pracovník by v tomto případě převzal zodpovědnost za klidný chod při běžném provozu, kdy jeho náplň práce zahrnuje monitoring celého objektu, ať už přes kamerové záznamy, tak fyzický dohled. Zároveň lze konstatovat, že při napomenutí návštěvníků, kteří se nechovají dle návštěvního řádu, vytváří větší respekt než běžný lektor zastávající momentálně danou funkci.

V daném ORP se nachází více než čtyři bezpečnostní agentury, které nabízejí ostrahové služby. Druhá možnost je zaměstnání nového pracovníka, který by měl vhodnou kvalifikaci na danou pozici.

Při navrhování druhého opatření proběhla konzultace problematiky s odborníkem v oboru. Jedná se o navržení průchozí bezpečnostní brány a nového vstupního turniketu. Dle autorova názoru je důležité včasně odhalit potencionální riziko před jeho vznikem než zavádět opatření až po nepříjemném incidentu. Proto jedním z preventivních opatření je průchozí bezpečnostní brána, která detekuje všechny nebezpečné předměty. Zavedením zmíněného bezpečnostního prvku by se snížilo riziko napadení zaměstnanců osobou vstupující do instituce a zároveň poslouží jako preventivní ochrana místních exponátů. Cena této položky se pohybuje mezi 129 000,- Kč, případně vyšší, záleží, zda by muselo dojít k úpravě konstrukce tak, aby byla zachována památková struktura.

Následujícím navrženým prvkem je obměna stávajícího turniketu. Tento prvek byl konzultován s odbornicí na turnikety z firmy Dormakaba s.r.o., která objasnila fungování celého mechanismu a zároveň uvedla příklad, jak je možné daný turniket nakonfigurovat na různou funkcionalitu. Po zhodnocení daných informací byl vybrán typ turniketu, který by splnil požadované nároky na provoz. Oproti dosavadnímu turniketu by byl vybaven navíc přístupovým a docházkovým zařízením. To by napomohlo většímu

přehledu o pohybu zaměstnanců přímo v instituci. Například v momentě nějakého incidentu lze snadno a rychle zjistit, kdo se nacházel uvnitř a mohl by být primárním svědkem. Zároveň může tento komponent zvýšit efektivnost práce ve smyslu, že zaměstnanci budou svůj příchod a odchod evidovat. Je tedy možné plně využít funkcionality docházkového systému, včetně evidence odpracované doby atd. Dle informací je možné konstrukci celého turniketu upravit, aby zapadal do kontextu muzea. Cena je velice flexibilní a záleží na nastavené konfiguraci turniketu. Dle zmíněných parametrů se cena pohybuje od 220 000 Kč případně vyšší. Elektronický systém kontroly vstupu je možné instalovat samostatně. Jedná se o další navržený komponent, který může fungovat samostatně v případě, že by se instituce rozhodla pro levnější variantu.

Mezi další možné prvky je rekonstrukce dveří, které by byly nahrazeny modernějšími a odolnějšími. Díky tomu je možné uplatnit širší škálu bezpečnostních komponentů. Současně by byly splněny architektonické normy a standardy budovy. Dosavadní vchod do budovy je složen ze tří vstupních dveří. Pouze jedny z nich jsou automaticky otočné, čímž zajišťují bezbariérový přístup. Dle autorova názoru by daná rekonstrukce zajistila vyšší úroveň zabezpečení. Automatický dveřní systém by bylo možné zabudovat do všech tří vstupních dveří. Součástí konstrukce dveří by byla také mechanická paniková hrazda, která se běžně využívá u vchodových dveří a únikových východů.

V momentě, kdy by vstupní dveře sloužily jako zábranný prvek před útěkem pachatele, bude moci fyzická ostraha nebo jiný zaměstnanec tyto dveře uzamknout pomocí dálkového ovladače. Nicméně ostraha musí být připravena i na situaci, že v tu samou chvíli bude potřeba evakuace osob v budově, například kvůli požáru. To znamená, že tento únikový východ musí být co nejrychleji otevřen, aby bylo osobám umožněno opustit budovu.

ZÁVĚR

Cílem této bakalářské práce bylo zhodnotit současný stav fyzické bezpečnosti a zároveň identifikovat případné hrozby, které by mohly mít značně negativní působení na vybranou instituci. Následně na základě získaných výsledků z analýzy vybrané instituce navrhnout prvky na její rozšíření či vylepšení současného zabezpečení.

Práce byla rozdělena na dvě části, první část byla věnována teorii, ve které byly popsány základní právní předpisy týkající se této problematiky. Následující kapitola byla věnována podrobnému vysvětlení pojmu bezpečnost a bezpečnostní riziko s případnými příklady. Dále následovalo seznámení se základními typy a dělením fyzické bezpečnosti, které je členěno na klasickou, režimovou, fyzickou a technickou ochranu. Toto rozdělení je pro fyzickou bezpečnost velice stěžejní. Závěrečná kapitola obsahovala objasnění problematiky detektorů, kde bylo detailněji popsáno jejich rozdělení a stručně popsán výčet jejich zástupců.

V praktické části této bakalářské práce byly zpočátku uvedeny základní informace týkající se vybrané instituce. Následující kapitola obsahovala popis současného stavu, kde bylo vycházeno z poskytnutých materiálu, z rozhovoru s konzultantem, z vlastních poznatků a materiálů. Hlavním cílem této části bylo co nejprecizněji identifikovat možná rizika, která by z důsledku nedostatečného zajištění bezpečnosti značně ohrožovala současný stav. K analyzování byl zvolen program RISKAN, kde byly na základě jeho výstupů vytýčeny hrozby, které jsou více ohrožující pro stanovená aktiva. Zároveň byl proveden i experiment, jehož kontext byl zaměřen na spolehlivost a profesionalitu lidského faktoru. Na základě těchto dvou analytických metod byly zhodnoceny výsledky, které zároveň napomohly vytvořit plán na rozšíření fyzické bezpečnosti instituce. V poslední kapitole byla navrhnuta opatření na zabezpečení, která byla vykonstruována na základě analýzy, a zároveň by podpořila úroveň fyzické bezpečnosti.

SEZNAM POUŽITÉ LITERATURY

[1] BAKER, Paul R. a Daniel J. BENNY. The complete guide to physical security. Boca Raton: CRC Press, 2013. ISBN 9781420099638.

[2] BURDOVÁ, Klára a Kristýna DOBIÁŠOVÁ. Analýza rizik ORP Opava. Uherské Hradiště, 2018. Semestrální práce. Univerzita Tomáše Bati ve Zlíně.

[3] ČSN CLC/TS 50131-7 - Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 7: Pokyny pro aplikace. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Česká technická norma.

[4] ČSN CLC/TS 50136-7 - Poplachové systémy - Poplachové přenosové systémy a zařízení - Část 7: Pokyny pro aplikace. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018. Česká technická norma.

[5] ČSN EN 1627 - Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání - Požadavky a klasifikace. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012. Česká technická norma.

[6] ČSN EN 50131-1 ED.2 - Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2007. Česká technická norma.

[7] ČSN EN 50134-1 - Poplachové systémy - Systémy přivolání pomoci - Část 1: Systémové požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2003. Česká technická norma.

[8] ČSN EN 50134-2 - Poplachové systémy - Systémy přivolání pomoci - Část 2: Aktivační zařízení. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2001. Česká technická norma.

[9] ČSN EN 60839-11-1 - Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Česká technická norma.

[10] ČSN EN 60839-11-2 - Poplachové a elektronické bezpečnostní systémy - Část 11-2: Elektronické systémy kontroly vstupu - Pokyny pro aplikace. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016. Česká technická norma.

[11] ČSN EN 62676-1-1 - Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 1-1: Systémové požadavky – Obecně. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Česká technická norma.

[12] ČSN 34 2710 - Elektrická požární signalizace - Projektování, montáž, užívání, provoz, kontrola, servis a údržba. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Česká technická norma.

[13] ČSN 73 0875 - Požární bezpečnost staveb - Stanovení podmínek pro navrhování elektrické požární signalizace v rámci požárně bezpečnostního řešení. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Česká technická norma.

[14] DORMAKABA. Dormakaba Terminal 96 00. In: Dormakaba [online]. Praha: dormakaba Group, 2020 [cit. 2020-04-16]. Dostupné z: https://www.dormakaba.com/cz-cs/produkty/produkty/elektronicke-pristupove-systemy/dochazkovy-system/dormakaba-terminal-96-00-333666

[15] DROZDEK, Marek a Katarína JELŠOVSKÁ. Informační podpora krizového řízení [online]. Opava, 2013 [cit. 2020-04-17]. Dostupné z: http://projects.math.slu.cz/AM/activ/soubory/opory/InfPodKrR.pdf. Projekt inovace bakalářských studijních oborů se zaměřením na spolupráci s praxí. Slezská univerzita v Opavě.

[16] ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE A OSTATNÍ ELEKTRONICKÉ SYSTÉMY. In: FASS [online]. [cit. 2020-04-15]. Dostupné z: https://www.fass.cz/elektricka-pozarni-signalizace-a-ostatni-elektronicke-systemy

[17] FUS, Alois. Projektová dokumentace: Elektrická požární signalizace EPS provizorní zabezpečení. Opava, 2015.

[18] HEALTH AND SAFETY EXECUTIVE. Human factors: Managing human failures. In: Health and Safety Executive [online]. London: HSE, 2008 [cit. 2020-05-04]. Dostupné z: https://www.hse.gov.uk/humanfactors/topics/humanfail.htm

[19] IVANKA, Ján. MECHANICKÉ ZÁBRANNÉ SYSTÉMY [online]. Zlín: Univerzita Tomáše Bati ve Zlíně, 2014 [cit. 2020-04-15]. ISBN 978-80-7454-427-9. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/18575/Mechanicke_zabranne_systemy-obsah.pdf?sequence=2&isAllowed=y

[20] IVANKA, Ján. SYSTEMIZACE BEZPEČNOSTNÍHO PRŮMYSLU [online]. Zlín: Univerzita Tomáše Bati ve Zlíně, 2014 [cit. 2020-04-15]. ISBN 978-80-7454-410-1. Dostupné z: https://digilib.k.utb.cz/handle/10563/27488

[21] JIRÁSEK, Pavel. Modernizace bezpečnostních systémů v prostředí muzea - galerie: manuál bezpečnosti sbírek : vzdělávací modul [online]. V Praze: Národní galerie, c2011 [cit. 2020-04-15]. Metodický materiál (Národní galerie v Praze). ISBN 978-80-7035-471-1.

[22] KALUS, Jaromír, Jiří PERNES a Vladimír TKÁČ. Muzea na Moravě a ve Slezsku. Ostrava: Profil Ostrava, 1988. ISBN 48-020-88.

[23] KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 3. S.l.: Cricetus, 2006. ISBN 80-902-9382-4.

[24] LAWRENCE, Fennelly. Effective Physical Security. Fitfh edition. Amsterdam: Butterworth-Heinemann, 2016. ISBN 9780128044629.

[25] LORENC, Miroslav. Závěrečné práce - metodika. In: LORENC.INFO [online]. Praha: Miroslav Lorenc, 2013 [cit. 2020-04-16]. Dostupné z: https://lorenc.info/zaverecne-prace/metodika.htm

[26] LOVEČEK, Tomáš, Andrej VEL'AS a Martin ĎUROVEC. Bezpečnostné systémy: Poplachové systémy. Žilina: Žilinská univerzita v Žiline, 2015. ISBN 978-80-554-1144-6.

[27] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. Zlín: Radim Bačuvčík - VeRBuM, 2011. ISBN 978-80-87500-05-7.

[28] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management II. Zlín: Radim Bačuvčík - VeRBuM, 2012. ISBN 978-80-87500-19-4.

[29] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management III. Zlín: Radim Bačuvčík - VeRBuM, 2013. ISBN 978-80-87500-35-4.

[30] MADDOX, Maeve. Safety and Security. In: DAILYWRITINGTIPS [online]. London: Daily Writing Tips, 2010 [cit. 2020-04-16]. Dostupné z: https://www.dailywritingtips.com/safety-and-security/

[31] MASLOW, Abraham Harold. O psychologii bytí. Přeložil Hana ANTONÍNOVÁ. Praha: Portál (vydavatelství), 2014. ISBN 978-80-262-0618-7.

[32] MEDIA, OUR. Engage Hill: Mladí zaměstnanci se brání přesčasům v práci. In: PARLAMENTNÍ LISTY.cz [online]. Praha: OUR MEDIA a.s.., 2013 [cit. 2020-04-16]. Dostupné z: https://www.parlamentnilisty.cz/zpravy/tiskovezpravy/Engage-Hill-Mladi-zamestnanci-se-brani-prescasum-v-praci-294227

[33] MINISTERSTVO KULTURY. Metodický pokyn k zajišťování správy, evidence a ochrany sbírek muzejní povahy v muzeích a galeriích zřizovaných ČR nebo územními samosprávnými celky. In: MINISTERSTVO KULTURY [online]. Praha: Ministerstvo kultury, 1999 [cit. 2020-04-19]. Dostupné z: https://www.mkcr.cz/metodicky-pokyn-k-zajistovani-spravy-evidence-a-ochrany-sbirek-muzejni-povahy-v-muzeich-a-galeriich-zrizovanych-cr-nebo-uzemnimi-samospravnymi-celky-633.html

[34] MLEJNSKY. Průchozí brána Ebinger SC 900. In: MLÉJNSKÝ DETEKTORY [online]. Praha: Mlejnský Marek – detektory mlejnsky, 2020 [cit. 2020-04-16]. Dostupné z: https://www.detektory-mlejnsky.cz/pruchozi-brana-ebinger-sc-900

[35] NORMAN, Thomas L. Electronic Access Control [online]. Burlington: Butterworth-Heinemann, 2011 [cit. 2020-05-16]. ISBN 9780123820297. Dostupné z: http://web.a.ebscohost.com/ehost/detail/detail?vid=0&sid=2030d3df-e0a7-494d-826f-300b131ed296%40sessionmgr4006&bdata=Jmxhbmc9Y3Mmc2l0ZT1laG9zdC1saXZl#db=nlebk&AN=407848

[36] NOVELO. Pyramida bezpečnosti. In: NOVELO [online]. Brno: FAB Brno, Novelo 91 [cit. 2020-04-16]. Dostupné z: https://www.novelobrno.cz/odborne-clanky/pyramida-bezpecnosti.htm

[37] OGB. Uplatnění skla při rekonstrukci historické budovy. In: OGB [online]. Velemín: OGB, 2014 [cit. 2020-04-19]. Dostupné z: http://www.ogb.cz/architekti/

[38] PROCHÁZKOVÁ, Tereza. Teorie motivace podle Maslowa. In: MENTEM [online]. Brno: Mentem – brain training, 2018 [cit. 2020-04-16]. Dostupné z: https://www.mentem.cz/blog/teorie-motivace/Maslowova pyramida potřeb a pracovní výkon. In: BusinessAnimals.cz [online]. 2018 [cit. 2020-04-15]. Dostupné z: https://www.businessanimals.cz/maslowova-pyramida-potreb/

[39] SEDLÁK, Jan. Čínské kamery Hikvision poběží na českém softwaru Angelcam. Má jim dodat důvěryhodnost. In: LUPA.cz [online]. Praha: Internet Info, 2019

[cit. 2020-04-16]. Dostupné z: https://www.lupa.cz/clanky/cinske-kamery-hikvision-pobezi-na-ceskem-softwaru-angelcam-ma-jim-dodat-duveryhodnost/

[40] SKŘEHOT, Petr, Radim DOLEŽAL a Pavel FUCHS. Analýza a hodnocení rizik s ohledem na lidský faktor: materiály z 50. semináře odborné skupiny pro spolehlivost, Praha, únor 2013 : [sborník přednášek] [online]. Praha: Česká společnost pro jakost, 2013 [cit. 2020-04-16]. ISBN 978-80-02-02434-7.

[41] SZM. Expozice. In: Slezské zemské muzeum [online]. Opava: Slezské zemské muzeum, 2012 [cit. 2020-04-17]. Dostupné z: http://www.szm.cz/rubrika/10/expozicni-arealy/historicka-vystavni-budova-opava/expozice.html

[42] TRADE FIDES A.S. Projektová dokumentace slaboproudé rozvody PZTS. Opava, 2013.

[43] Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 19. 4. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/1993-2

[44] Ústavní zákon č. 1/1993 Sb., ústava České republiky. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 19. 4. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/1993-1

[45] UHLÁŘ, Jan. Technická ochrana objektů 1. díl: Mechanické zábranné systémy. Praha: Vydavatelství PA ČR, 2004. ISBN 80-725-1172-6.

[46] UHLÁŘ, Jan. Technická ochrana objektů 2. díl: Elektrické zabezpečovací systémy. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-312-3.

[47] VALOUCH, Jan. PROJEKTOVÁNÍ BEZPEČNOSTNÍCH SYSTÉMŮ [online]. Zlín: Univerzita Tomáše Bati ve Zlíně, 2019 [cit. 2020-04-15]. ISBN 978-80-7454-858-1. Dostupné z: https://digilib.k.utb.cz/handle/10563/45863

[48] VALOUCH, Jan. PROJEKTOVÁNÍ INTEGROVANÝCH SYSTÉMŮ [online]. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013 [cit. 2020-04-15]. ISBN 978-80-7454-296-1. Dostupné z: https://digilib.k.utb.cz/handle/10563/25814

[49] Vyhláška č. 275/2000 Sb., Ministerstva kultury, kterou se provádí zákon č. 122/2000 Sb., o ochraně sbírek muzejní povahy a o změně některých dalších zákonů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 19. 4. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-275

[50] Zákon č. 40/2009 Sb., trestní zákoník. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 19. 4. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[51] Zákon č. 89/2012 Sb., občanský zákoník. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 19. 4. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2012-89

[52] Zákon č. 122/2000 Sb., o ochraně sbírek muzejní povahy a o změně některých dalších zákonů. In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 19. 4. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-122

[53] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád). In: Zákony pro lidi.cz [online]. © AION CS 2010-2020 [cit. 19. 4. 2020]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141

[54] ZEMAN, Petr, ed. Česká bezpečnostní terminologie: výklad základních pojmů. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002. ISBN 80-210-3037-2. Dostupné také z: http://www.digitalniknihovna.cz/mzk/uuid/uuid:7ae54b60-e10d-11e5-984e-005056827e52

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AS Alarm systém přeloženo do českého jazyka Poplachové systémy

Bc. Baccalaureus přeloženo do českého jazyka bakalář

BOZP Bezpečnost a ochrana zdraví při práci

CCTV Closed circuit television přeloženo do českého jazyka Uzavřený televizní okruh

Č. číslo

Č. j. číslo jednací

ČNR Česká národní rada

ČR Česká Republika

ČSN Česká státní norma

DPPC Dohledová a poplachová přijímací centra

EACS Electronic Access Controll Systems přeloženo do českého jazyka Elektronické systémy kontroly vstupu

EBS Elektronické bezpečnostní systémy

EN Evropská norma

EPS Elektrická požární signalizace

EZS Elektrické zabezpečovací systémy

GDPR General data protection regulation přeloženo do českého jazyka Obecné nařízení o ochraně osobních údajů

GSM Global System for Mobile Communicatio přeloženo do českého jazkya Slobální systém pro mobilní komunikaci

HAS Hold-up alarm system přeloženo do českého jazyka Poplachový tísňový systém

HD High Definition přeloženo do češtiny plné rozlišení

HZS Hasičský záchranný sbor

IAS Intruder alarm systém přeloženo do českého jazyka Poplachový zabezpečovací systém

IP Internet Protocol přeloženo do češtiny internetový protokol

ISO International organization for standardization přeloženo do českého jazyka Mezinárodní organizace pro normalizaci

IZS Integrovaný záchranný systém

LCD Liquid crystal display přeloženo do češtiny Displej z tekutých krystalů

MZS Mechanické zabezpečovací systémy

MW Micro Wave

Např. Například

P přijímač

PČR Policie České republiky

PIR Passive Infra Red detectors

PTZS Poplachový zabezpečovací a tísňový systém

RFID Radio Frequency Identification přeloženo do českého jazyka identifikace na rádiové frekvenci

SAS Social alarm systém přeloženo do českého jazyka Systémy přivolání pomoci

Sb. sbírka

SKV Systémy kontroly vstupu

s.r.o. Společnost s ručeným omezeným

Str. Strana

Tzn. To znamená

Tzv. Takzvaně

UV Ultraviolet přeloženo do českého jazyka ultrafialové záření

V Vysílač

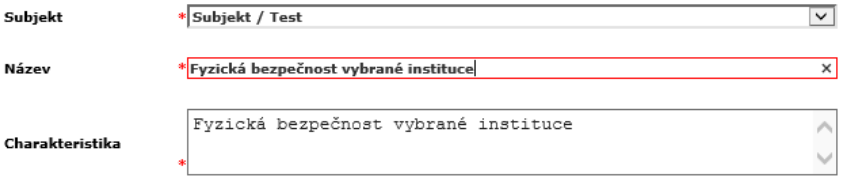
VSS Video Surveillance Systems přeloženo do českého jazyka Dohledové videosystémy

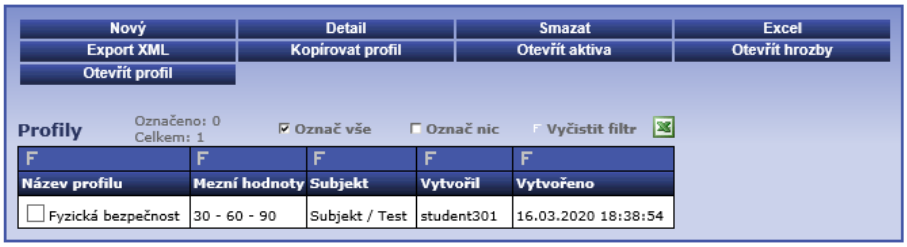
SEZNAM OBRÁZKŮ

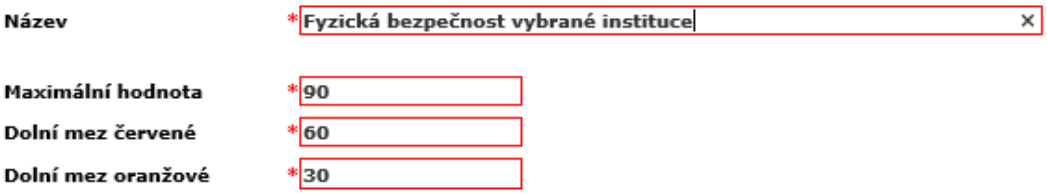
SEZNAM TABULEK

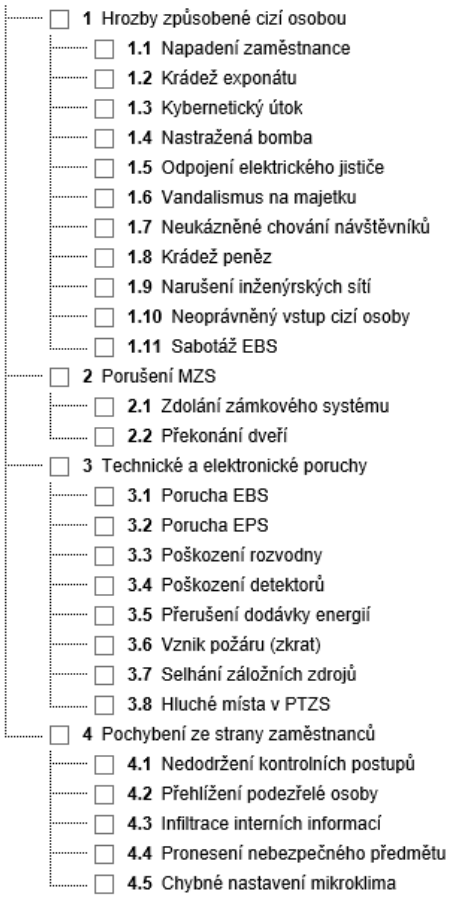
SEZNAM PŘÍLOH

PŘÍLOHA P I: RISKAN









- 1 Zaměstnanci
  - 1.1 Interní
  - 1.2 Externí
  - 1.3 Proškolení
- 2 Technologie
  - 2.1 Moderní výbava
  - 2.2 Pravidelná aktualizace
  - 2.3 Komplexní přehled o dění
  - 2.4 Napojení na PČR
  - 2.5 Napojení na HZS
  - 2.6 Nastavené mikroklima
- 3 Elektronická zařízení
  - 3.1 Reproduktory
  - 3.2 Datové sítě
  - 3.3 Počítače
  - 3.4 Wi-fi
  - 3.5 Rozvodny
- 4 Bezpečnostní systémy
  - 4.1 Dohledové videosystémy
  - 4.2 Vstupní terminál
  - 4.3 Čtečky vstupenek
  - 4.4 PTZS
  - 4.5 EPS
  - 4.6 Stabilní hasící zařízení
  - 4.7 Detektory
- 5 Instituce
  - 5.1 Exponáty
  - 5.2 Eko., soci. a kul. rozvoj
  - 5.3 Dotace a granty
  - 5.4 Legislativa

HODNOTA AKTIVA	
0	zanedbatelná
1	velmi nízká
2	nízká
3	střední
4	vysoká
5	velmi vysoká

PRAVDĚPODOBNOST HROZBY	
0	žádná
1	zanedbatelná
2	nízká
3	střední
4	vysoká
5	velmi vysoká
6	jistá

ZRANITELNOST AKTIVA	
0	Žádná
1	Nízká
2	Střední
3	Vysoká

VÝSLEDNÉ RIZIKO	
Nízké	0 - 30
Střední	31 - 60
Vysoké	61 - 90

MAXIMÁLNÍ MOŽNÉ RIZIKO	90

RIZIKOVÝ KALKULÁTOR

T-SOFT

		Aktiva		AKTIVA - CELKEM	Zaměstnanci	Interní	Externí	Proškolení	Technologie	Moderní výbava	Pravidelná aktualizace	Komplexní přehled o dě	Napojení na PČR	Napojení na HZS	Nastavené mikroklima	Elektronická zařízení	Reproduktory	Datové sítě	Počítače	Wi-fi	Rozvodny	Bezpečnostní systémy	Dohledové videosystém	Vstupní terminál	Čtečky vstupenek	PTZS	EPS	Stabilní hasicí zařízení	Detektory	Instituce	Exponáty	Eko., soci. a kul. rozvoj	Dotace a granty	Legislativa
					1	1.1	1.2	1.3	2	2.1	2.2	2.3	2.4	2.5	2.6	3	3.1	3.2	3.3	3.4	3.5	4	4.1	4.2	4.3	4.4	4.5	4.6	4.7	5	5.1	5.2	5.3	5.4
		Hodnoty aktiv		5	3	3	3	3	5	5	4	5	5	4	5	5	4	3	4	3	5	5	5	3	3	5	4	4	5	5	5	4	5	1
				velmi vysoká	střední	střední	střední	střední	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	střední	vysoká	střední	velmi vysoká	velmi vysoká	velmi vysoká	střední	střední	velmi vysoká	vysoká	vysoká	velmi vysoká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi nízká
Hrozby		Pravděpodobnost																																
HROZBY - CELKEM		5	velmi vysoká	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
1	Hrozby způsobené cizí osobou	5	velmi vysoká	3	3	3	2	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	1
1.1	Napadení zaměstnance	3	střední	3	3	3	2	2	2	1	0	2	2	2	1	2	0	1	2	0	2	2	2	1	1	2	2	2	2	3	0	3	1	0
1.2	Krádež exponátu	3	střední	3	3	2	1	3	3	3	1	3	1	0	0	1	0	0	1	0	1	1	1	0	0	1	0	0	1	3	3	3	3	0
1.3	Kybernetický útok	5	velmi vysoká	3	2	2	2	1	3	3	2	3	3	3	2	3	2	3	3	3	3	3	3	2	3	3	3	2	3	3	2	3	3	0
1.4	Nastražená bomba	3	střední	3	3	3	2	1	3	3	2	3	2	2	3	3	3	3	3	3	3	3	3	1	3	3	3	3	3	3	3	3	3	0
1.5	Odpojení elektrického jističe	3	střední	3	2	2	1	1	3	3	1	2	3	3	2	3	3	3	3	3	3	3	3	3	0	3	3	0	3	2	2	2	0	0
1.6	Vandalismus na majetku	5	velmi vysoká	3	0	0	0	0	2	2	0	1	1	1	2	3	3	1	1	0	0	3	2	0	2	2	3	3	1	3	3	0	0	0
1.7	Neukázněné chování návštěvník	5	velmi vysoká	3	2	2	1	1	1	1	1	1	1	0	1	2	2	0	0	0	0	3	1	1	2	3	2	3	1	2	2	0	1	1
1.8	Krádež peněz	3	střední	3	1	1	1	0	1	1	1	0	0	0	0	1	0	0	1	0	0	1	1	0	0	1	0	0	0	3	1	3	3	0
1.9	Narušení inženýrských sítí	4	vysoká	2	1	1	0	0	2	2	1	0	1	1	0	1	1	1	1	0	1	2	2	1	0	1	2	0	0	1	1	1	0	0
1.10	Neoprávněný vstup cizí osoby	3	střední	2	2	2	2	2	2	2	1	1	2	2	1	2	1	2	2	0	2	2	0	2	1	1	2	1	1	2	2	0	0	0
1.11	Sabotáž EBS	3	střední	3	2	2	1	1	3	3	2	2	3	3	1	2	0	2	2	1	2	3	3	3	2	3	2	0	3	2	2	0	0	0

RISKAN RIZIKOVÝ KALKULÁTOR

T-SOFT

			Aktiva	AKTIVA - CELKEM	Zaměstnanci	Interní	Externí	Proškolení	Technologie	Moderní výbava	Pravidelná aktualizace	Komplexní přehled o dě	Napojení na PČR	Napojení na HZS	Nastavené mikroklima	Elektronická zařízení	Reproduktory	Datové sítě	Počítače	Wi-fi	Rozvodny	Bezpečnostní systémy	Dohledové videosystém	Vstupní terminál	Čtečky vstupenek	PTZS	EPS	Stabilní hasicí zařízení	Detektory	Instituce	Exponáty	Eko., soci. a kul. rozvoj	Dotace a granty	Legislativa
			Hodnoty aktiv	5	3	3	3	3	5	5	4	5	5	4	5	5	4	3	4	3	5	5	5	3	3	5	4	4	5	5	5	4	5	1
				velmi vysoká	střední	střední	střední	střední	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	střední	vysoká	střední	velmi vysoká	velmi vysoká	velmi vysoká	střední	střední	velmi vysoká	vysoká	vysoká	velmi vysoká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi nízká
Hrozby		Pravděpodobnost																																
HROZBY - CELKEM		5	velmi vysoká	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
1	Hrozby způsobené cizí osobou	5	velmi vysoká	3	3	3	2	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	1
2	Porušení MZS	5	velmi vysoká	3	3	3	2	1	3	2	0	1	3	2	1	3	0	2	3	1	2	3	2	1	1	2	1	2	3	3	3	1	1	0
2.1	Zdolání zámkového systému	5	velmi vysoká	3	3	3	2	1	3	2	0	1	3	2	1	3	0	2	3	1	2	3	2	1	1	2	1	2	3	3	3	1	1	0
2.2	Překonání dveří	4	vysoká	3	3	3	1	0	3	2	0	1	3	2	1	3	0	2	3	1	2	2	2	1	1	2	1	2	2	3	3	1	1	0

RISIKOVÝ KALKULÁTOR

T-SOFT

Aktiva			AKTIVA - CELKEM	Zaměstnanci	Interní	Externí	Proškolení	Technologie	Moderní výbava	Pravidelná aktualizace	Komplexní přehled o dě	Napojení na PČR	Napojení na HZS	Nastavené mikroklima	Elektronická zařízení	Reproduktory	Datové sítě	Počítače	Wi-fi	Rozvodny	Bezpečnostní systémy	Dohledové videosystém	Vstupní terminál	Čtečky vstupenek	PTZS	EPS	Stabilní hasicí zařízení	Detektory	Instituce	Exponáty	Eko., soci. a kul. rozvoj	Dotace a granty	Legislativa
				1	1.1	1.2	1.3	2	2.1	2.2	2.3	2.4	2.5	2.6	3	3.1	3.2	3.3	3.4	3.5	4	4.1	4.2	4.3	4.4	4.5	4.6	4.7	5	5.1	5.2	5.3	5.4
Hodnoty aktiv			5	3	3	3	3	5	5	4	5	5	4	5	5	4	3	4	3	5	5	5	3	3	5	4	4	5	5	5	4	5	1
			velmi vysoká	střední	střední	střední	střední	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	střední	vysoká	střední	velmi vysoká	velmi vysoká	velmi vysoká	střední	střední	velmi vysoká	vysoká	vysoká	velmi vysoká	velmi vysoká	velmi vysoká	velmi vysoká	velmi vysoká	velmi nízká
Hrozby		Pravděpodobnost																															
HROZBY - CELKEM		5 velmi vysoká	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
1	Hrozby způsobené cizí osobou	5 velmi vysoká	3	3	3	2	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	1
2	Porušení MZS	5 velmi vysoká	3	3	3	2	1	3	2	0	1	3	2	1	3	0	2	3	1	2	3	2	1	1	2	1	2	3	3	3	1	1	0
3	Technické a elektronické poruch	4 vysoká	3	3	3	3	1	3	3	2	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	2	3	3	3	2	2	0
3.1	Porucha EBS	4 vysoká	3	3	3	3	0	3	3	1	3	3	1	2	3	2	2	2	0	3	3	3	3	3	3	1	0	3	3	3	1	0	0
3.2	Porucha EPS	3 střední	3	3	3	3	0	3	3	1	3	2	3	3	3	2	1	3	2	3	3	2	2	2	3	3	2	2	3	3	2	0	0
3.3	Poškození rozvodny	1 zanedbatelná	3	3	3	3	0	3	3	0	3	3	2	1	3	3	2	3	1	3	3	3	3	3	3	3	0	3	2	2	0	0	0
3.4	Poškození detektorů	3 střední	3	2	2	1	0	3	2	0	3	3	3	3	3	1	1	2	0	3	3	2	2	3	3	3	1	3	3	3	1	0	0
3.5	Přerušení dodávky energií	1 zanedbatelná	3	2	2	1	0	3	3	2	3	2	2	1	3	0	3	3	2	3	3	3	3	3	3	2	0	2	2	2	0	0	0
3.6	Vznik požáru (zkrat)	3 střední	3	3	3	3	1	3	3	2	3	3	2	3	3	3	2	3	0	3	3	3	3	3	3	3	1	3	3	3	0	2	0
3.7	Selhání záložních zdrojů	4 vysoká	3	3	3	2	1	3	3	2	3	2	3	2	3	3	3	3	2	3	3	3	3	3	3	2	0	3	2	1	2	0	0
3.8	Hluché místa v PTZS	2 nízká	3	3	3	2	0	3	2	1	3	3	1	1	3	1	2	3	0	1	3	3	1	1	3	1	2	3	2	2	1	0	0

RIZIKOVÝ KALKULÁTOR

T-SOFT

				Aktiva	AKTIVA - CELKEM	Zaměstnanci	Interní	Externí	Proškolení	Technologie	Moderní výbava	Pravidelná aktualizace	Komplexní přehled o dě	Napojení na PČR	Napojení na HZS	Nastavené mikroklima	Elektronická zařízení	Reproduktory	Datové sítě	Počítače	Wi-fi	Rozvodny	Bezpečnostní systémy	Dohledové videosystém	Vstupní terminál	Čtečky vstupenek	PTZS	EPS	Stabilní hasicí zařízení	Detektory	Instituce	Exponáty	Eko., soci. a kul. rozvoj	Dotace a granty	Legislativa
						1	1.1	1.2	1.3	2	2.1	2.2	2.3	2.4	2.5	2.6	3	3.1	3.2	3.3	3.4	3.5	4	4.1	4.2	4.3	4.4	4.5	4.6	4.7	5	5.1	5.2	5.3	5.4
				Hodnoty aktiv	5	3	3	3	3	5	5	4	5	5	4	5	5	4	3	4	3	5	5	5	3	3	5	4	4	5	5	5	4	5	1
					velmi vysoká	střední	střední	střední	střední	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	střední	vysoká	střední	velmi vysoká	velmi vysoká	velmi vysoká	střední	střední	velmi vysoká	vysoká	vysoká	velmi vysoká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi nízká
Hrozby		Pravděpodobnost																																	
HROZBY - CELKEM		5	velmi vysoká	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
1	Hrozby způsobené cizí osobou	5	velmi vysoká	3	3	3	2	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	1
2	Porušení MZS	5	velmi vysoká	3	3	3	2	1	3	2	0	1	3	2	1	3	0	2	3	1	2	3	2	1	1	2	1	2	3	3	3	1	1	0
3	Technické a elektronické poruch	4	vysoká	3	3	3	3	1	3	3	2	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	2	3	3	3	2	2	0
4	Pochybení ze strany zaměstnanc	5	velmi vysoká	3	3	3	3	1	3	3	1	3	3	2	3	3	1	3	3	1	3	3	3	2	2	3	3	2	3	3	3	2	3	3
4.1	Nedodržení kontrolních postupů	5	velmi vysoká	3	3	3	3	1	3	3	1	3	2	2	3	2	0	2	2	1	2	3	1	2	2	3	3	2	2	3	3	2	3	2
4.2	Přehlížení podezřelé osoby	4	vysoká	3	3	3	2	1	3	3	0	3	2	2	1	3	0	2	3	1	3	3	3	1	2	3	3	2	3	3	3	2	1	1
4.3	Infiltrace interních informací	5	velmi vysoká	3	3	3	3	1	3	3	1	3	3	2	1	3	0	3	3	1	3	3	3	1	2	3	2	1	3	3	2	1	2	3
4.4	Pronesení nebezpečného předn	4	vysoká	3	3	3	2	1	3	3	0	3	3	2	1	3	1	2	3	0	3	3	2	2	2	3	3	2	2	3	3	2	2	0
4.5	Chybné nastavení mikroklima	2	nízká	3	2	2	1	1	3	2	1	1	0	0	3	1	0	0	1	0	1	1	1	0	0	0	0	1	0	3	3	2	1	1

RIZIKOVÝ KALKULÁTOR

T-SOFT

Generátor grafů | Export do XML

Hrozby		Pravděpodobnost		Aktiva	AKTIVA - CELKEM	Zaměstnanci	Interní	Externí	Proškolení	Technologie	Moderní výbava	Pravidelná aktualizace	Komplexní přehled o děn	Napojení na PČR	Napojení na HZS	Nastavené mikroklima	Elektronická zařízení	Reproduktory	Datové sítě	Počítače	Wi-fi	Rozvodny	Bezpečnostní systémy	Dohledové videosystémy	Vstupní terminál	Čtečky vstupenek	PTZS	EPS	Stabilní hasicí zařízení	Detektory	Instituce	Exponáty	Eko., soci. a kul. rozvoj	Dotace a granty	Legislativa
						1	1.1	1.2	1.3	2	2.1	2.2	2.3	2.4	2.5	2.6	3	3.1	3.2	3.3	3.4	3.5	4	4.1	4.2	4.3	4.4	4.5	4.6	4.7	5	5.1	5.2	5.3	5.4
				Hodnoty aktiv	5	3	3	3	3	5	5	4	5	5	4	5	5	4	3	4	3	5	5	5	3	3	5	4	4	5	5	5	4	5	1
					velmi vysoká	střední	střední	střední	střední	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	střední	vysoká	střední	velmi vysoká	velmi vysoká	velmi vysoká	střední	střední	velmi vysoká	vysoká	vysoká	velmi vysoká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi nízká
HROZBY - CELKEM		5	velmi vysoká		75	45	45	45	27	75	75	40	75	75	60	75	75	60	45	60	45	75	75	75	36	45	75	60	60	75	75	75	60	75	15
1	Hrozby způsobené cizí osobou	5	velmi vysoká		75	30	30	30	27	75	75	40	75	75	60	50	75	60	45	60	45	75	75	75	30	45	75	60	60	75	75	75	60	75	5
1.1	Napadení zaměstnance	3	střední		36	27	27	18	18	30	15	0	30	30	24	15	30	0	9	24	0	30	30	30	9	9	30	24	24	30	36	0	36	15	0
1.2	Krádež exponátu	3	střední		45	27	18	9	27	45	45	12	45	15	0	0	15	0	0	12	0	15	15	15	0	0	15	0	0	15	45	45	36	45	0
1.3	Kybernetický útok	5	velmi vysoká		75	30	30	30	15	75	75	40	75	75	60	50	75	40	45	60	45	75	75	75	30	45	75	60	40	75	75	50	60	75	0
1.4	Nastražená bomba	3	střední		45	27	27	18	9	45	45	24	45	30	24	45	45	36	27	36	27	45	45	45	9	27	45	36	36	45	45	45	36	45	0
1.5	Odpojení elektrického jističe	3	střední		45	18	18	9	9	45	45	12	30	45	36	30	45	36	27	36	27	45	45	45	27	0	45	36	0	45	36	30	36	0	0
1.6	Vandalismus na majetku	5	velmi vysoká		75	0	0	0	0	50	50	0	25	25	20	50	60	60	15	20	0	0	60	50	0	30	50	60	60	25	75	75	60	0	0
1.7	Neukázněné chování návštěvníků	5	velmi vysoká		75	30	30	15	15	25	25	20	25	25	0	25	40	40	0	0	0	0	75	25	15	30	75	40	60	25	60	50	60	25	5
1.8	Krádež peněz	3	střední		45	9	9	9	0	15	15	12	0	0	0	0	12	0	0	12	0	0	15	15	0	0	15	0	0	0	45	15	36	45	0
1.9	Narušení inženýrských sítí	4	vysoká		48	12	12	0	0	40	40	16	0	20	16	0	20	16	12	16	0	20	40	40	12	0	20	32	0	0	48	20	48	0	0
1.10	Neoprávněný vstup cizí osoby	3	střední		36	18	18	18	18	30	30	12	15	30	24	15	30	12	18	24	0	30	24	0	18	9	15	24	12	15	36	30	36	0	0
1.11	Sabotáž EBS	3	střední		45	18	18	9	9	45	45	24	30	45	36	15	30	0	18	24	9	30	45	45	27	18	45	24	0	45	36	30	36	0	0
2	Porušení MZS	5	velmi vysoká		75	45	45	30	15	75	50	0	25	75	40	25	60	0	30	60	15	50	75	50	15	15	50	20	40	75	75	75	20	25	0
3	Technické a elektronické poruchy	4	vysoká		60	36	36	36	12	60	60	32	60	60	48	45	60	48	36	48	24	60	60	60	36	36	60	36	24	60	60	60	32	30	0
4	Pochybení ze strany zaměstnanců	5	velmi vysoká		75	45	45	45	15	75	75	20	75	75	40	75	75	16	45	60	15	75	75	75	30	30	75	60	40	75	75	75	40	75	15

RIZIKOVÝ KALKULÁTOR

T-SOFT

Generátor grafů | Export do XML

Hrozby		Pravděpodobnost		Aktiva	AKTIVA - CELKEM	Zaměstnanci	Interní	Externí	Proškolení	Technologie	Moderní výbava	Pravidelná aktualizace	Komplexní přehled o dění	Napojení na PČR	Napojení na HZS	Nastavené mikroklima	Elektronická zařízení	Reproduktory	Datové sítě	Počítače	Wi-fi	Rozvodny	Bezpečnostní systémy	Dohledové videosystémy	Vstupní terminál	Čtečky vstupenek	PTZS	EPS	Stabilní hasicí zařízení	Detektory	Instituce	Exponáty	Eko., soci. a kul. rozvoj	Dotace a granty	Legislativa
						1	1.1	1.2	1.3	2	2.1	2.2	2.3	2.4	2.5	2.6	3	3.1	3.2	3.3	3.4	3.5	4	4.1	4.2	4.3	4.4	4.5	4.6	4.7	5	5.1	5.2	5.3	5.4
				Hodnoty aktiv	5	3	3	3	3	5	5	4	5	5	4	5	5	4	3	4	3	5	5	5	3	3	5	4	4	5	5	5	4	5	1
					velmi vysoká	střední	střední	střední	střední	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	střední	vysoká	střední	velmi vysoká	velmi vysoká	velmi vysoká	střední	střední	velmi vysoká	vysoká	vysoká	velmi vysoká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi nízká
HROZBY - CELKEM		5	velmi vysoká		75	45	45	45	27	75	75	40	75	75	60	75	75	60	45	60	45	75	75	75	36	45	75	60	60	75	75	75	60	75	15
1	Hrozby způsobené cizí osobou	5	velmi vysoká		75	30	30	30	27	75	75	40	75	75	60	50	75	60	45	60	45	75	75	75	30	45	75	60	60	75	75	75	60	75	5
2	Porušení MZS	5	velmi vysoká		75	45	45	30	15	75	50	0	25	75	40	25	60	0	30	60	15	50	75	50	15	15	50	20	40	75	75	75	20	25	0
2.1	Zdolání zámkového systému	5	velmi vysoká		75	45	45	30	15	75	50	0	25	75	40	25	60	0	30	60	15	50	75	50	15	15	50	20	40	75	75	75	20	25	0
2.2	Překonání dveří	4	vysoká		60	36	36	12	0	60	40	0	20	60	32	20	48	0	24	48	12	40	40	40	12	12	40	16	32	40	60	60	16	20	0
3	Technické a elektronické poruchy	4	vysoká		60	36	36	36	12	60	60	32	60	60	48	45	60	48	36	48	24	60	60	60	36	36	60	36	24	60	60	60	32	30	0
4	Pochybení ze strany zaměstnanc	5	velmi vysoká		75	45	45	45	15	75	75	20	75	75	40	75	75	16	45	60	15	75	75	75	30	30	75	60	40	75	75	75	40	75	15

RISIKOVÝ KALKULÁTOR

T-SOFT

Generátor grafů | Export do XML

Hrozby		Pravděpodobnost		Aktiva	AKTIVA - CELKEM	Zaměstnanci	Interní	Externí	Proškolení	Technologie	Moderní výbava	Pravidelná aktualizace	Komplexní přehled o dění	Napojení na PČR	Napojení na HZS	Nastavené mikroklima	Elektronická zařízení	Reproduktory	Datové sítě	Počítače	Wi-fi	Rozvodny	Bezpečnostní systémy	Dohledové videosystémy	Vstupní terminál	Čtečky vstupenek	PTZS	EPS	Stabilní hasicí zařízení	Detektory	Instituce	Exponáty	Eko., soci. a kul. rozvoj	Dotace a granty	Legislativa
						1	1.1	1.2	1.3	2	2.1	2.2	2.3	2.4	2.5	2.6	3	3.1	3.2	3.3	3.4	3.5	4	4.1	4.2	4.3	4.4	4.5	4.6	4.7	5	5.1	5.2	5.3	5.4
				Hodnoty aktiv	5	3	3	3	3	5	5	4	5	5	4	5	5	4	3	4	3	5	5	5	3	3	5	4	4	5	5	5	4	5	1
					velmi vysoká	střední	střední	střední	střední	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	střední	vysoká	střední	velmi vysoká	velmi vysoká	velmi vysoká	střední	střední	velmi vysoká	vysoká	vysoká	velmi vysoká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi nízká
HROZBY - CELKEM		5	velmi vysoká		75	45	45	45	27	75	75	40	75	75	60	75	75	60	45	60	45	75	75	75	36	45	75	60	60	75	75	75	60	75	15
1	Hrozby způsobené cizí osobou	5	velmi vysoká		75	30	30	30	27	75	75	40	75	75	60	50	75	60	45	60	45	75	75	75	30	45	75	60	60	75	75	75	60	75	5
2	Porušení MZS	5	velmi vysoká		75	45	45	30	15	75	50	0	25	75	40	25	60	0	30	60	15	50	75	50	15	15	50	20	40	75	75	75	20	25	0
3	Technické a elektronické poruchy	4	vysoká		60	36	36	36	12	60	60	32	60	60	48	45	60	48	36	48	24	60	60	60	36	36	60	36	24	60	60	60	32	30	0
3.1	Porucha EBS	4	vysoká		60	36	36	36	0	60	60	16	60	60	16	40	60	32	24	32	0	60	60	60	36	36	60	16	0	60	60	60	16	0	0
3.2	Porucha EPS	3	střední		45	27	27	27	0	45	45	12	45	30	36	45	45	24	9	36	18	45	45	30	18	18	45	36	24	30	45	45	24	0	0
3.3	Poškození rozvodny	1	zanedbatelná		15	9	9	9	0	15	15	0	15	15	8	5	15	12	6	12	3	15	15	15	9	9	15	12	0	15	10	10	0	0	0
3.4	Poškození detektorů	3	střední		45	18	18	9	0	45	30	0	45	45	36	45	45	12	9	24	0	45	45	30	18	27	45	36	12	45	45	45	12	0	0
3.5	Přerušení dodávky energií	1	zanedbatelná		15	6	6	3	0	15	15	8	15	10	8	5	15	0	9	12	6	15	15	15	9	9	15	8	0	10	10	10	0	0	0
3.6	Vznik požáru (zkrat)	3	střední		45	27	27	27	9	45	45	24	45	45	24	45	45	36	18	36	0	45	45	45	27	27	45	36	12	45	45	45	0	30	0
3.7	Selhání záložních zdrojů	4	vysoká		60	36	36	24	12	60	60	32	60	40	48	40	60	48	36	48	24	60	60	60	36	36	60	32	0	60	32	20	32	0	0
3.8	Hluché místa v PTZS	2	nízká		30	18	18	12	0	30	20	8	30	30	8	10	24	8	12	24	0	10	30	30	6	6	30	8	16	30	20	20	8	0	0
4	Pochybení ze strany zaměstnanc	5	velmi vysoká		75	45	45	45	15	75	75	20	75	75	40	75	75	16	45	60	15	75	75	75	30	30	75	60	40	75	75	75	40	75	15

RISIKOVÝ KALKULÁTOR

T-SOFT

Generátor grafů | Export do XML

	Hrozby	Pravděpodobnost		Aktiva	AKTIVA - CELKEM	Zaměstnanci	Interní	Externí	Proškolení	Technologie	Moderní výbava	Pravidelná aktualizace	Komplexní přehled o dění	Napojení na PČR	Napojení na HZS	Nastavené mikroklima	Elektronická zařízení	Reproduktory	Datové sítě	Počítače	Wi-fi	Rozvodny	Bezpečnostní systémy	Dohledové videosystémy	Vstupní terminál	Čtečky vstupenek	PTZS	EPS	Stabilní hasicí zařízení	Detektory	Instituce	Exponáty	Eko., soci. a kul. rozvoj	Dotace a granty	Legislativa
						1	1.1	1.2	1.3	2	2.1	2.2	2.3	2.4	2.5	2.6	3	3.1	3.2	3.3	3.4	3.5	4	4.1	4.2	4.3	4.4	4.5	4.6	4.7	5	5.1	5.2	5.3	5.4
				Hodnoty aktiv	5	3	3	3	3	5	5	4	5	5	4	5	5	4	3	4	3	5	5	5	3	3	5	4	4	5	5	5	4	5	1
					velmi vysoká	střední	střední	střední	střední	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	vysoká	střední	vysoká	střední	velmi vysoká	velmi vysoká	velmi vysoká	střední	střední	velmi vysoká	vysoká	vysoká	velmi vysoká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi nízká
	HROZBY - CELKEM	5	velmi vysoká		75	45	45	45	27	75	75	40	75	75	60	75	75	60	45	60	45	75	75	75	36	45	75	60	60	75	75	75	60	75	15
1	Hrozby způsobené cizí osobou	5	velmi vysoká		75	30	30	30	27	75	75	40	75	75	60	50	75	60	45	60	45	75	75	75	30	45	75	60	60	75	75	75	60	75	5
2	Porušení MZS	5	velmi vysoká		75	45	45	30	15	75	50	0	25	75	40	25	60	0	30	60	15	50	75	50	15	15	50	20	40	75	75	75	20	25	0
3	Technické a elektronické poruchy	4	vysoká		60	36	36	36	12	60	60	32	60	60	48	45	60	48	36	48	24	60	60	60	36	36	60	36	24	60	60	60	32	30	0
4	Pochybení ze strany zaměstnanc	5	velmi vysoká		75	45	45	45	15	75	75	20	75	75	40	75	75	16	45	60	15	75	75	75	30	30	75	60	40	75	75	75	40	75	15
4.1	Nedodržení kontrolních postupů	5	velmi vysoká		75	45	45	45	15	75	75	20	75	50	40	75	50	0	30	40	15	50	75	25	30	30	75	60	40	50	75	75	40	75	10
4.2	Přehlížení podezřelé osoby	4	vysoká		60	36	36	24	12	60	60	0	60	40	32	20	60	0	24	48	12	60	60	60	12	24	60	48	32	60	60	60	32	20	4
4.3	Infiltrace interních informací	5	velmi vysoká		75	45	45	45	15	75	75	20	75	75	40	25	75	0	45	60	15	75	75	75	15	30	75	40	20	75	50	50	20	50	15
4.4	Pronesení nebezpečného předmět	4	vysoká		60	36	36	24	12	60	60	0	60	60	32	20	60	16	24	48	0	60	60	40	24	24	60	48	32	40	60	60	32	40	0
4.5	Chybné nastavení mikroklima	2	nízká		30	12	12	6	6	30	20	8	10	0	0	30	10	0	0	8	0	10	10	10	0	0	0	0	8	0	30	30	16	10	2

PŘÍLOHA P II: TECHNICKÉ NORMY

1. **ČSN EN 1627** Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání - Požadavky a klasifikace – norma se zabývá určením požadavků a systému vlastností odolnosti proti vloupání u dveří, oken, lehkých obvodových plášťů, mříži a okenic. [5]

2. **ČSN EN 50131-1 ED.2** - Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky – stanovuje systémové požadavky poplachových zabezpečovacích a tísňových systémů, jako např. provedení, vlastnosti ad. [6]

3. **ČSN CLC/TS 50136-7** Poplachové systémy - Poplachové přenosové systémy a zařízení - Část 7: Pokyny pro aplikace – obsahuje vhodné kroky při definování systémů pro přenos poplachových signálů a indikační a ovládací zařízení spolu a s požadavky týkajícími se jejich přímé aplikaci. [4]

4. **ČSN EN 50134-1** Poplachové systémy - Systémy přivolání pomoci - Část 1: Systémové požadavky – definuje minimální požadavky, které by měly být splněny při systému přivolání pomoci. [7]

5. **ČSN EN 50134-2** Poplachové systémy - Systémy přivolání pomoci - Část 2: Aktivační zařízení – specifikuje požadavky a zkoušky na ručně spouštěná aktivační zařízení, která jsou součástí systému přivolání pomoci. [8]

6. **ČSN CLC/TS 50131-7** Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 7: Pokyny pro aplikace – předmětem je soubor pokynů navrhování, přípravy realizace, montáže, uvedení do provozu a údržby poplachových zabezpečovacích a tísňových systémů. [3]

7. **ČSN EN 62676-1-1** Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 1-1: Systémové požadavky – Obecně – zaměřením normy je vymezení minimálních požadavků a poskytnutí doporučení pro dohledové videosystémy, které jsou využívány pro bezpečnostní funkce objektu. [11]

8. **ČSN 73 0875** Požární bezpečnost staveb - Stanovení podmínek pro navrhování elektrické požární signalizace v rámci požárně bezpečnostního řešení – platí pro navrhování elektrické požární signalizace při vypracování nových stavebních objektů a při projektování změn stávajících objektů a technologických souborů. [13]

9. **ČSN 34 2710** Elektrická požární signalizace - Projektování, montáž, užívání, provoz, kontrola, servis a údržba – předmětem je stanovení zásad pro projektování, navrhování, montáž, uvedení do provozu, údržbu a opravy systému EPS. [12]

10. **ČSN EN 60839-11-1** Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty – norma vymezuje minimální funkčnost, požadavky na provozní vlastnosti a metody zkoušení pro elektronické systémy kontroly vstupu a komponenty používané pro fyzický přístup v budovách a jejich okolí a chráněných prostorách. [9]

11. **ČSN EN 60839-11-2** Poplachové a elektronické bezpečnostní systémy - Část 11-2: Elektronické systémy kontroly vstupu - Pokyny pro aplikace – definuje minimální požadavky a další pokyny pro montáž a provoz elektronických systému kontroly vstupu nebo jiného příslušenství tak, aby vyhovovaly odlišným úrovním ochrany. [10]