Poplachové zabezpečovací a tísňové systémy k zajištění bezpečnosti informací

Tomáš Veselý

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:	**Tomáš Veselý**
Osobní číslo:	**L17358**
Studijní program:	**B2825 Ochrana obyvatelstva**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Poplachové zabezpečovací a tísňové systémy k zajištění bezpečnosti informací**

Zásady pro vypracování

1. Zpracujte rešerši současného stavu předmětné problematiky.
2. Identifikujte hrozby relevantní pro problematiku bezpečnosti informací.
3. Analyzujte problematiku projektování prvků poplachových zabezpečovacích a tísňových systémů.
4. Navrhněte opatření k zajištění bezpečnosti informací za užití prvků poplachových zabezpečovacích a tísňových systému.

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

Seznam doporučené literatury:

1. KINDL, Jiří. *Projektování bezpečnostních systémů*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007. ISBN 978-80-73185-54-1.
2. LOVEČEK, Tomáš, Andrej VEĽAS a Martin ĎUROVEC. *Bezpečnostné systémy : poplachové systémy*. V Žiline : Žilinská univerzita: EDIS-vydavateľské centrum ŽU, 2015. Vysokoškolské učebnice. ISBN 978-80-55411-44-6.
3. LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-05-7.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda**
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: Tomáš Veselý

.....
podpis studenta

ABSTRAKT

Bakalářská práce se zaměřuje na poplachové zabezpečovací a tísňové systémy pro zajištění bezpečnosti informací ve vybraném subjektu. Teoretická část se věnuje rešerši současné problematiky Poplachových zabezpečovacích a tísňových systémů s vymezením základních pojmů a norem, a dále problematiku bezpečnosti informací v současné době. V praktické části je nejprve prezentován aktuální stav subjektu, následně jsou identifikovány rizika pro problematiku projektování poplachových zabezpečovacích a tísňových systému pro zajištění bezpečnosti informací pomocí diagramu příčin a následků. Pro analýzu rizik v areálu je provedena SWOT analýza a následné ohodnocení rizik pomocí polokvantitativní metody. Výstupem práce jsou navržené opatření k zajištění bezpečnosti informací pomocí prvků Poplachových zabezpečovacích a tísňových systémů v daném subjektu.

Klíčová slova: analýza rizik, bezpečnost informací, detektor, hrozba, opatření.

ABSTRACT

The bachelor's thesis is focused on alarm security and emergency systems to ensure the security of information in a selected entity. Theoretical part is devoted to a search of current issues of alarm security and emergency systems with the definition of basic concepts and standards, as well as the issue of information security at present. The practical part first presents the current state of the subject, then identifies the risks for the design of alarm security and emergency systems to ensure the security of information using a diagram of causes and consequences. For the risk analysis in the area, a SWOT analysis is performed and a subsequent risk assessment using a semi-quantitative method. The output of the work are the proposed measures to ensure the security of information using elements of alarm security and emergency systems in the subject.

Keywords: risk analysis, information security, detector, threat, measures, security.

Rád bych poděkoval svému vedoucímu práce panu Ing. Petru Svobodovi, Ph.D. za čas, který mi věnoval, zvlášť v tomto letním období při vedení mé bakalářské práce. Také nesmím opomenout na kolegy z práce, kteří byli vstřícní a umožnili mi více se věnovat studiu. Samozřejmě nesmím zapomenout na rodinu, která mě plně podporovala a v neposlední řadě velký dík patří této škole, na které jsem poznal mnoho skvělých profesorů a spolužáků a vedli mě napříč dalšímu vzdělání.

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

OBSAH

ÚVOD

V dnešní době, kdy je zvýšená kriminalita a možné ohrožení bezpečnosti informací, je potřeba správná identifikace všech hrozeb, které můžou ovlivnit zabezpečení střeženého areálu.

Velké množství firem musí vynakládat větší množství peněz na fyzickou bezpečnost svých areálu. Dále také vznikají novější hrozby pro bezpečnost informací. Tyto aspekty stále ovlivňují trh s Poplachovým zabezpečovacím a tísňovým systémem (dále jen „PZTS“) a jejich aktuálním technickým rozvojem.

Velmi důležitá je kombinace PZTS s Video Surveillance System v českém překladu Video dohledový systém (dále jen „VSS/VDS“) a fyzickou ostrahou, pro co nejkvalitnější zabezpečení areálu. V dnešní době se prvky PZTS zajištění bezpečnosti informací stále rozvijí o kvalitnější a modernější prvky z důvodu vyšších nároku uživatelů, zmíněné systémy neslouží jen k zabránění vstupu do střeženého objektu, ale také k upozornění o narušení areálu. Pro zajištění plně funkčního systému je potřeba kvalitní zpracování návrhu zabezpečení objektu i s možnostmi hrozeb, které můžou nastat pro zvolený objekt. Často se stává největší problém u zabezpečení objektu finanční část, která bývá u některých projektů podhodnocena.

Cílem mé práce je analýza rizik u problematiky PZTS pro zajištění bezpečnosti informací, dále navrhnou opatření k zajištění bezpečnosti informací pomocí prvků PZTS v rámci vybraného objektu (který z důvodu bezpečnosti a citlivosti dat nebude konkrétně jmenován). Teoretická část se věnuje vymezením základních pojmů, norem a rešerši současné problematiky poplachových zabezpečovacích a tísňových systémů pro problematika bezpečnosti informací v současné době. V praktické části je nejprve provedena aktuální charakteristika subjektu, následně jsou identifikovány hrozby pro problematiku projektování poplachových zabezpečovacích a tísňových systému pro zajištění bezpečnosti informací pomocí diagramu příčin a následků. Pro analýzu rizik v areálu je provedena SWOT analýza a následné ohodnocení rizik pomocí PNH metody. Výstupem práce jsou navržené opatření k zajištění bezpečnosti informací pomocí prvků Poplachových zabezpečovacích a tísňových systémů v areálu firmy.

I. TEORETICKÁ ČÁST

1 POPLACHOVÉ ZABEZPEČOVACÍ A TÍSŇOVÉ SYSTÉMY

Poplachové zabezpečovací a tísňové systémy (PZTS), které byly dříve označovány pod pojmem Elektrická zabezpečovací signalizace (EZS), jsou komplexem technických prostředků, které řeší ochranu objektu proti neoprávněnému vstupu nepovolaných osob. Včasnou signalizací do místa obsluhy tak eliminují rozsah materiálních a případně jiných škod. V technických normách se také používá anglická zkratka I&HAS - Intruder and hold-up alarm system. Který popisuje například samotný výrobek, jeho celkovou konstrukci, použití materiál a základní bezpečnostní požadavky. Poplachový zabezpečovací systém spadá do kategorie technické ochrany. Ta se dále dle prostoru člení na obvodovou, plášťovou, prostorovou, předmětovou a tísňovou.

1.1 Základní pojmy

Aktivum – je jakákoliv entita, mající hodnotu pro zabezpečovaný objekt. Hodnota aktiva může být zmenšena působením hrozby. Aktiva lze rozdělit na hmotná a nehmotná. Za hmotná považujeme například nemovitosti, cenné papíry, šperky a elektroniku. Příkladem nehmotných je informace. (Lukáš a kolektiv, 2011, s. 201)

Analýza hrozeb – je zkoumání činností a událostí, které by mohly negativně ovlivnit kvalitu služby. (Jirásek, Novák, Požár, 2015, s. 17)

Analýza rizik – je proces pochopení povahy rizika a určení úrovně rizika. (Jirásek, Novák, Požár, 2015 s. 18)

Bezpečnost – je stav, kdy systém (soubor prvků) je schopen odolat všem vnitřním nebo vnějším hrozbám, které mohou negativně ať přímo nebo nepřímo hrozit některým prvků systému. Důležité je, aby byla zachována celistvost struktury prvků, jejich funkčnost a spolehlivost. (Jirásek, Novák, Požár, 2015, s. 23)

Detektor – je primární zdroj informace slouží k měření okolního prostředí, tj. ke snímání všech dostupných fyzikálních veličin. Převádí informaci obsaženou v jistém typu energie na informaci s jiným typem energie (nejčastěji energii). Pojem detektor je ekvivalentní pojmu snímač, převodník nebo senzor. (Lukáš a kolektiv, 2011, s. 27)

Hodnocení rizik – je proces porovnání výsledků analýzy rizika s kritérií rizika k určení, zda riziko a jeho závažnost jsou přijatelná (akceptovatelná) nebo tolerovatelná. (Jirásek, Novák, Požár, 2015, s. 51)

Hrozba – rozumíme vlastnost, sílu, událost, aktivitu nebo osobu, která působí bud přímo na aktivum nebo na bezpečnostní opatření s cílem získat přístup k aktivu. Aby mohla hrozba

působit, musí být nejprve aktivována, k čemu slouží zdroj hrozby. (Lukáš a kolektiv, 2012, s. 75)

Identifikace – je akt nebo proces, během kterého entita předloží systému nějaký identifikátor, na jehož základě systém může rozpoznat entitu a odlišit od jiných entit. (Lukáš a kolektiv, 2014, s. 64)

Informace – je každý znakový projev, který má smysl pro komunikátora i příjemce. (Jirásek, Novák, Požár, 2015, s. 54)

Opatření – jsou prostředky modifikující riziko, včetně politik, strategií, postupů, směrnic, obvyklých postupů (praktik) nebo organizačních struktur, které mohou být administrativní, technické, řídící nebo právní povahy. (Jirásek, Novák, Požár, 2015, s. 79)

Posuzovaní rizika – je celkový proces identifikace rizika, analýzy rizika a hodnocení rizika. (Jirásek, Novák, Požár, 2015, s. 89)

Projekt – je jedinečný proces sestávající z řady koordinovaných a řízených činností s daty zahájení a ukončení, prováděný pro dosažení cíle, který vyhovuje specifickým požadavkům, včetně omezeni daných časem, náklady a zdroji. Technický projekt je možné blíže definovat jako komplexní proces přípravy a realizace navrhovaného technického zařízení, systému, technologického celku nebo stavby včetně jeho uvedení do provozu a předání zadavateli nebo uživateli. (Lukáš a kolektiv, 2015, s. 229)

Riziko – je nebezpečí, možnost škody, ztráty, nezdaru. (Jirásek, Novák, Požár, 2015, s. 99)

Závada – je provozní nefunkčnost, vynechání, nebo přehlednutí, která umožnuje, aby byly ochranné mechanizmy obejity nebo vyřazeny z činnosti. (Jirásek, Novák, Požár, 2015, s. 134)

Zdroj rizika – je prvek, který sám nebo v kombinaci s jinými prvky má vnitřní potenciální schopnost způsobit riziko. (Jirásek, Novák, Požár, 2015, s. 134)

Zranitelnost – je parametr, určující míru nedokonalosti analyzovaného aktiva, který může přímo ovlivnit naplnění hrozby. Zranitelnost se tedy vztahuje ke konkrétnímu aktivu, na které působí daná hrozba. (Lukáš a kolektiv, 2011, s. 201)

1.2 Technické normy

ČSN EN 50131-1 ed. 2 Poplachové systémy - Poplachové zabezpečovací a tísňové systémy -- Část 1: Systémové požadavky. Norma stanoví systémové požadavky poplachových zabezpečovacích a tísňových systémů. Specifikuje požadavky na provedení a vlastnosti instalovaných systémů, neobsahuje však požadavky pro návrh, projekci, instalaci, provoz a údržbu (požadavky pro návrh, projekci, instalaci, provoz a údržbu obsahuje ČSN CLC/TS 50131-7). Systémové požadavky se vztahují na poplachové zabezpečovací a tísňové systémy, mající společné prostředky detekce, vzájemného propojování, ovládání, komunikace a napájecích zdrojů s jinými systémy. Norma stanoví stupně zabezpečení a třídy prostředí, nestanoví však konkrétní požadavky, kladené na jednotlivé komponenty systémů.

ČSN EN 62676-1-1 Dohledové video-systémy pro použití v bezpečnostních aplikacích - Část 1-1: Systémové požadavky – Obecně. Tato norma předepisuje minimální požadavky a poskytuje doporučení pro dohledové video-systémy (VSS), doposud zvané CCTV, používané pro bezpečnostní aplikace. Tato norma specifikuje minimální výkonnostní a funkční požadavky, které mají být sjednané mezi zákazníkem a dodavatelem v rámci provozních požadavků pro zajištění bezpečnostních služeb, ale neobsahuje požadavky pro návrh, plánování, montáž, testování, provozování nebo údržbu. Tato norma se nezabývá instalací vzdáleně monitorovaných detektorů, aktivujících VSS.

ČSN EN 1627 Dveře, okna, lehké obvodové pláště, mříže a okenice – Odolnost proti vloupání - Požadavky a klasifikace. Tato norma určuje požadavky a systém klasifikace vlastností odolnosti proti vloupání u dveří, oken, lehkých obvodových plášťů, mříží a okenic. Vztahuje se na následující způsoby otevírání: otevírání, sklápění, skládání, otevírání a sklápění, posunování (vodorovné a svislé) a navinování jakož i na pevné konstrukce. Také zahrnuje výrobky, jako jsou kryty dopisních schránek nebo větrací mřížky. Určuje požadavky na odolnost stavebního výrobku proti vloupání (jak je definováno v 3.1 této normy).

ČSN EN 1630+A1 Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání - Zkušební metoda pro stanovení odolnosti proti manuálním pokusům o vloupání. Tato norma určuje zkušební metodu pro stanovení odolnosti proti manuálním pokusům o násilné vloupání k hodnocení vlastností odolnosti proti násilnému vloupání u dveří, oken,

lehkých obvodových plášťů, mříží a okenic. Vztahuje se na následující způsoby otevírání: otevírání, sklápění, skládání, otevírání a sklápění, posunování (vodorovné a svislé) a navinování jakož i na pevné konstrukce. Norma nezahrnuje přímo odolnost zámků a cylindrických vložek napadených paklíči. Také nezahrnuje napadení elektricky, elektronicky a elektromagneticky ovládané stavební výrobky odolné proti násilnému vniknutí použitím metod napadení, které by mohly tyto charakteristiky zničit. Norma neplatí pro dveře, vrata a závory určené k montáži v oblastech s pohybem osob, pro které je hlavním určeným použitím zajistit bezpečný vstup zboží a nákladních vozidel doprovázených nebo řízených osobami v průmyslových, komerčních nebo obytných prostorech, které jsou řešeny EN 13241-1.

1.3 Struktura normy ČSN 5013x

Struktura norem ČSN 5013x popisující poplachové systémy.

Tabulka 1 – Struktura souboru norem ČSN 5013x;
Zdroj: ČSN EN 50131-1 ed. 2: Poplachové systémy (vlastní zpracování)

Označení normy	Problematika
ČSN EN 50130-4	Poplachové systémy (Elektromagnetická kompatibilita) Norma skupiny výrobků: Požadavky na odolnost komponentů požárních systémů, zabezpečovacích systémů a systému přivolání pomoci
ČSN EN 50131-1-1 ED.2	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy- Systémové požadavky
ČSN EN 62676-1-1	Dohledové videosystémy pro použití v bezpečnostních aplikacích
ČSN EN 60839-11-1	Poplachové systémy - Elektronické systémy kontroly vstupu
ČSN EN 50134-1	Poplachové systémy - Systémy přivolání pomoci
ČSN EN 50136-1	Poplachové systémy - Poplachové přenosové systémy a zařízení
ČSN EN 50398-1	Poplachové systémy - Systémy kombinované nebo integrované

Parametry a podmínky poplachových zabezpečovacích a tísňových systému jsou formulovány v ČSN CLC/TS 50131-1-1 ED.2. Ta byla vypracována evropskou technickou komisí CENELEC/TC79, která se zabývá poplachovými systémy. V České republice tyto normy schvaluje a vydává Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Tabulka 2 – Obecné rozdělení skupiny norem ČSN 5013x;
Zdroj: ČSN EN 50131-1 ed. 2: *Poplachové systémy* (vlastní zpracování)

Označení normy	Problematika
ČSN EN 50131-1 ED.2	Systémové požadavky (funkce, typy, definice)
ČSN EN 50131-2-4	Požadavky na komponenty systému
ČSN EN 50131-5-3 ED.2	Požadavky na komunikaci a propojení
ČSN EN 50131-6 ED.2	Požadavky na napájení
ČSN CLC/TS 50131-7	Pokyny pro aplikace (návrh, montáž, provoz)

Samotné komponenty PZTS podléhají NV č. 616/2016 Sb., o technických požadavcích na výrobky z hlediska jejich elektromagnetické kompatibility. To znamená, že zařízení bude uspokojivě fungovat v elektromagnetickém prostředí, aniž by samo způsobovalo nepřípustné elektromagnetické rušení jiného zařízení v tomto prostředí.

ČSN EN 50131-1 ED.2

Soubor norem a technických specifikací s označením ČSN 50131-1 ED. 2 se vztahuje na poplachové zabezpečovací a tísňové systémy. Specifikuje poplachové zabezpečovací a tísňové systémy instalované v budovách. Obsahuje následující části.

Tabulka 3 – Jednotlivé části normy ČSN EN 50131;
Zdroj: ČSN EN 50131-1 ed. 2: *Poplachové systémy* (vlastní zpracování)

Číslo části	Název
Část 1	Systémové požadavky
Část 2-2	Požadavky na pasivní infračervené detektory
Část 2-3	Požadavky na mikrovlnné detektory
Část 2-4	Požadavky na kombinované infračervené a mikrovlnné detektory
Část 2-5	Požadavky na kombinované infračervené a ultrazvukové detektory
Část 2-6	Požadavky na kontakty dveří (magnetické)
Část 2-7	Detektory vniknutí – detektory rozbíjení sklad akustické nebo otřesové
Část 3	Ústředny EZS
Část 4	Výstražná zařízení
Část 5-3	Požadavky na zařízení využívající bezdrátové propojení
Část 6	Napájecí zdroje
Část 7	Pokyny pro aplikace
Část 8	Zabezpečovací zamlžovací zařízení

1.4 Stupně zabezpečení objektu

Nejdůležitějším kritériem pro zatřídění příslušného prvku PZTS jsou tzv. stupně zabezpečení, které jsou definovány v normě ČSN EN 50131-1 ed. 2. Ty jsou rozděleny podle míry rizika do čtyř stupňů. Riziko se stanovuje dle předpokládaných znalostí a vybaveností narušitele.

Tabulka 4 – Stupně zabezpečení objektů;
Zdroj: ČSN EN 50131-1 ed. 2: *Poplachové systémy* (vlastní zpracování)

Stupeň	Míra rizika	Použití
1	Nízké	Garáže, chaty, byty, rodinné domy, strojovny
2	Nízké až střední	Komerční objekty
3	Střední až vysoké	Zbraně, ceniny, informace, narkotika
4	Vysoké	Zejména objekty národního a vyššího zájmu

Stupeň 1 Nízké riziko

Narušitel má malou znalost PZTS a disponují omezeným sortimentem snadno dostupných zdrojů.

Stupeň 2 Nízké až střední riziko

Narušitel má určité znalosti o PZTS a používá omezený sortiment běžného nářadí a přenosných přístrojů.

Stupeň 3 Střední až vysoké riziko

Narušitel je obeznámen s PZTS a disponují rozsáhlým sortimentem nástrojů a elektronických zařízení.

Stupeň 4 Vysoké riziko

Narušitel je schopen nebo má možnost zpracovat podrobný plán vniknutí a má kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících komponentů PZTS. (Lukáš a kolektiv, 2011, s. 18-19)

1.5 Třídy prostředí

Pro zajištění správné činnosti PZTS je potřeba zvážit v jakém prostředí se budou tyto komponenty nacházet.

Tabulka 5 – Třídy prostředí;

Zdroj: ČSN EN 50131-1 ed. 2: *Poplachové systémy* (vlastní zpracování)

Třída	Název prostředí	Popis prostředí, příklady	Rozsah teplot
I	Vnitřní	Vytápěná obytná nebo obchodní místa	+5˚C až +40˚C
II	Vnitřní všeobecné	Přerušovaná vytápěná nebo nevytápěná místa (chodby, schodiště, skladové prostory)	-10˚C až +40˚C
III	Venkovní chráněné	Prostředí vně budov, kde komponenty nejsou trvale vystaveny vlivům počasí (přístřešky)	-25˚C až +50˚C
IV	Venkovní všeobecné	Prostředí vně budov, kde komponenty jsou trvale vystaveny vlivům počasí	-25˚C až +60˚C

Z důvodu, že některý prvky PZTS ve venkovním prostředí nemusí korektně fungovat z důvodu určení jen pro vnitřní prostory.

1.6 Základní dělení ochrany

Ochrana střeženého objektu musí být komplexní a se systémovým přístupem k úkolu. Nesmíme se zaměřovat pouze na vnější ochranu, ale i na další druhy ochrany. Ideální je kombinace fyzické ochrany s kamerovým systémem a vnějšími detektory po obvodu areálu. Ochranu objektů dělíme do několika podskupin.

1.6.1 Klasická ochrana – Zábranné systémy

Klasická ochrana spočívá v tom, že zajištění příslušného objektu se použije takových mechanických zařízení, která ho umožní ochránit. Je možné se ní setkat v různé úrovni prakticky na každém objektu. Prostředky klasické ochrany nejsou schopny beze zbytku chráněné objekty skutečně zabezpečit, což potvrzuje celý historický vývoj i současné zkušenosti. Z tohoto důvodu zde hovoříme především o tzv. zpožďovacím faktoru, který nám říká, jak dlouho je konkrétní prostředek klasické ochrany schopen odolávat klasifikovanému napadení dostupnými metodami a nástroji. (Kindl, 2007, s. 94)

1.6.2 Technická ochrana – Poplachové systémy

Technická ochrana dělá podporu klasické ochraně a je nejspolehlivější a nejhůře překonatelná z hlediska dnešních požadavků i technických možností. Technická ochrana sama o sobě ovšem není ochranou v pravém slova smyslu (tedy ochranou, která by znemožňovala napadení chráněných zájmů pachatelem), ale lze ji označit a charakterizovat spíše jako detekční systém, který zajišťuje a předává informace o situaci v chráněném

prostoru či objektu a o jeho případném napadení. Můžeme tedy říci, že technická ochrana podstatně zvyšuje efektivnost klasické i fyzické ochrany z hlediska možnosti rychlé reakce na situaci vyvolanou pachatelem v chráněném objektu. (Kindl, 2007, s. 94)

1.6.3 Fyzická ochrana

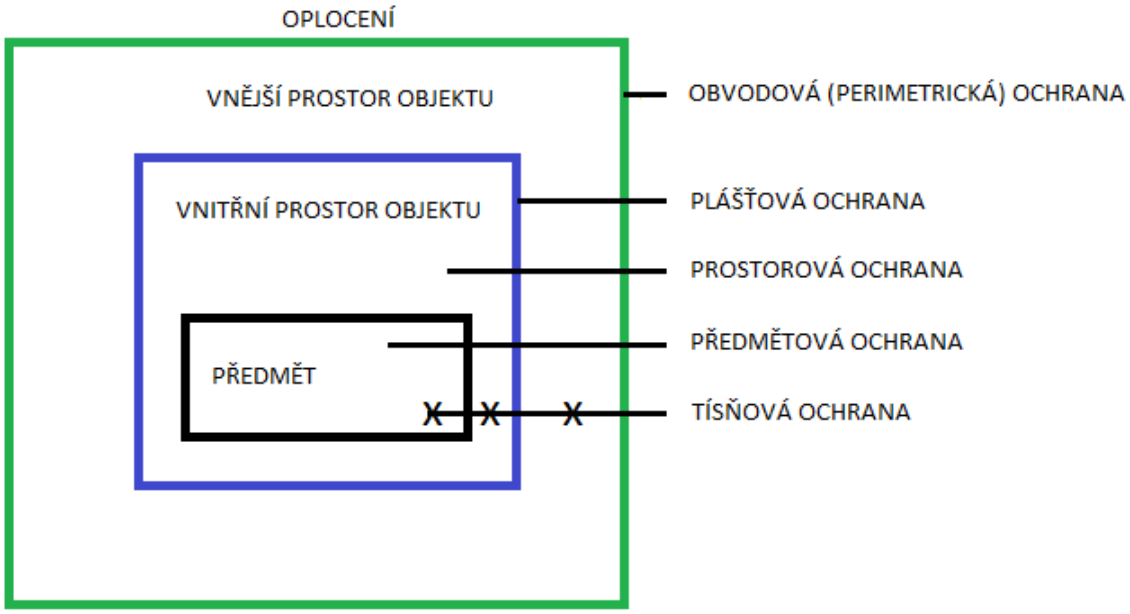
Bezpečnostní situace zahrnují v rámci zajištění fyzické bezpečnosti široké spektrum událostí. Adekvátní reakce vyžadují určené a speciálně připravované osoby, schopné zajistit bezpečnost chráněných aktiv efektivní cestou a s minimálními dopady. Fyzická ostraha, že zajištující fyzickou ochranou objektu, plní v této oblasti významnou roli. Svojí trvalou či dočasnou přítomností v objektu organizace je schopna v souladu s režimovými opatřeními zajistit ochranu aktiv. Jedná se o především o odhalení a zadržení narušitele, zamezení zcizení aktiv, realizaci protipožárních a havarijních opatření. Fyzická ochrana bývá prováděna strážnými, hlídači, hlídací službou či policisty. Většina organizací zajištuje svoji fyzickou ochranu jako službu poskytovanou jinými právním subjektem, zpravidla soukromou bezpečnostní službou. Zajištují fyzické ochrany ostrahou bývá finančně nejnákladnější způsob zajištění bezpečnosti. (Kindl, 2007, s. 94)

1.6.4 Režimová ochrana

Režimová ochrana je soubor organizačně administrativní opatření a postupů, které směrují k zajištění požadovaných podmínek pro smysluplnou funkci zabezpečovacího systému a jeho sladění s provozem chráněného objektu. V praxi se jedná o psaná pravidla pro pohyb osob a dopravních prostředků do a z objektu, jejich pohyb v samotném areálu, pokyny pro manipulaci s materiálem a jeho dalších nakládáním, pro užívání informací, činnost sboru bezpečnostní služby, provoz technických ochran. Režimová ochrana je dělena na vnější režimová opatření, které zahrnují, především vstupní a výstupní podmínky chráněného objektu a vnitřní režimová opatření, které se týkají opatření pro omezení pohybu osob a vozidel ve střeženém objektu. (Kindl, 2007, s. 94)

1.7 Prostorové členění technické ochrany

PZTS spadají do kategorie technické ochrany a dle prostoru zabezpečení se dají rozdělit na obvodovou (perimetrickou), plášťovou, prostorovou, předmětovou a tísňovou ochranu.



Obrázek 1 – Prostorové členění technické ochrany;
Zdroj: (vlastní zpracování)

1.7.1 Obvodová (perimetrická) ochrana

Obvodová ochrana představuje všechny bezpečnostní opatření fyzické bezpečnosti a slouží pro signalizaci narušení obvodu objektu. Obvod objektu definujeme nejčastěji jako katastrální hranice, která je realizována obvykle přírodními zábranou například vodním tokem nebo umělými bariérami jako plot nebo zdí. Účelem obvodové ochrany je odradit nebo zachytit pachatele. Perimetrická ochrana je speciální aplikací technických, elektronických a mechanicko venkovních zabezpečovacích systému. Hlavním prvkem obvodové ochrany jsou mechanické zábranné systémy. Ty tvoří prostředky pro ohraničení prostor jako zdi, ploty, vstupní systémy vrat, branek, dveří, oken, mříže, bezpečnostní skla a fólie. (Lukáš a kolektiv, 2011, s. 17)

1.7.2 Plášťová ochrana

Plášťová ochrana je realizována na plášti budovy, čímž jsou tím myšleny zdi, stropy, dveře, okna a další bezpečnostní prvky jako zámky, mříže, bezpečnostní skla, bezpečnostní fólie, kamerové systémy atd. Cílem plášťové ochrany je odstrašení, znemožnění průchodu a odhaleni narušitele. Plastová ochrana signalizuje narušení plaste budovy. Plášťovou obranu tvoří stěny, okna, budovy, dveře, zámky a zámkové systém, mříže, bezpečnostní folie, kamerové systémy, detektory narušení. (Lukáš a kolektiv, 2011, s. 17)

1.7.3 Prostorová ochrana

Prostorová ochrana slouží jako ochrana důležitých míst v objektu, které musí pachatel projít, aby se dostal k předmětům a cenným hodnotám. Jedná se o chodby, schodiště, vstupy a výstupy. Může být tvořena dveřmi, zámky, mřížemi a různými bezpečnostními prvky jako kamerové systémy a detektory narušení. (Lukáš a kolektiv, 2011, s. 18)

1.7.4 Předmětová ochrana

Předmětová ochrana se zabývá zabezpečením samotných cenných aktiv a předmětů v chráněném prostoru, aby bylo zamezeno jejich odcizení či neoprávněné manipulaci s nimi. Chráněná aktiva jsou předměty, které mají vyšší hodnotu. Mezi prvky předmětové ochrany patří různé typy trezorů například skříňové a účelové trezory nebo bezpečnostní schránka (skříň). (Lukáš a kolektiv, 2011, s. 18)

1.7.5 Tísňová ochrana

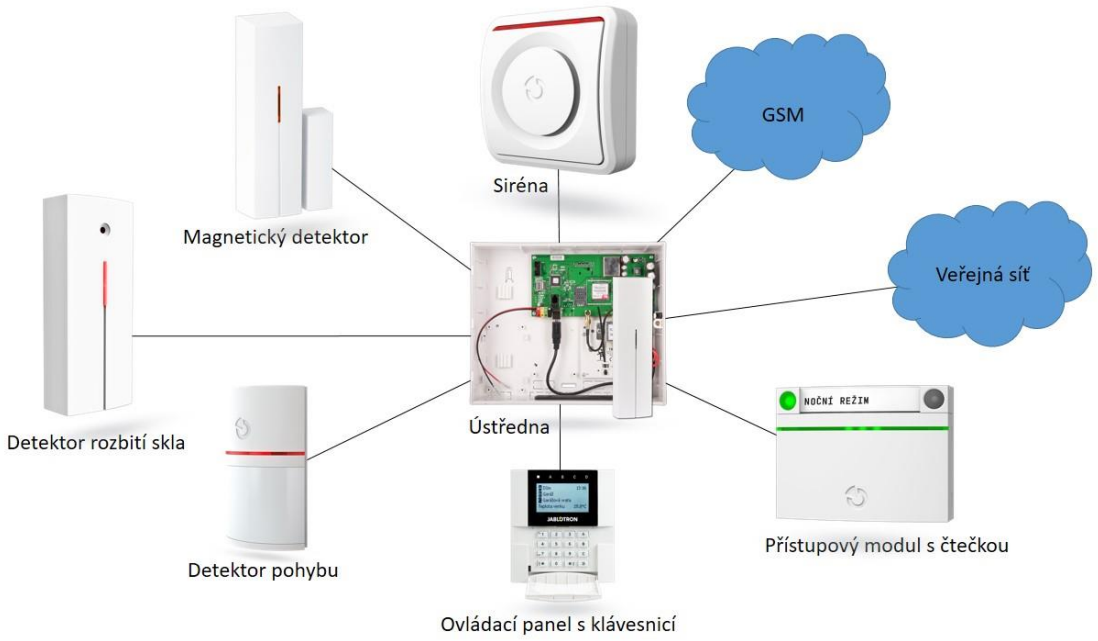
Tísňovou ochrana popisujeme jako ochranu objektu a všech jeho pracovníků, kteří se můžou ocitnout v přímém ohrožení např. krádež nebo napadení (Kindl, 2007, s. 95)

2 PRVKY POUŽÍVANÉ V POPLACHOVÝCH ZABEZPEČOVACÍCH A TÍSŇOVÝCH SYSTÉMECH

Poplachové zabezpečovací a tísňové systémy slouží k signalizaci nebezpečí ve střeženém prostoru a hlavní úkol je informování obsluhy o narušení či vniknutí do objektu.

Komponenty PZTS jsou následující:

- **Ústředny** – řídící a indikační zařízení, obsahuje i napájecí síťový zdroj a náhradní napájecí zdroj.
- **Ovládací zařízení** – slouží pro usnadnění ovládání systému, jeho pomocí je možné zařízení uvádět do stavu střežení nebo klidu. Nejčastěji ovládacími zařízeními jsou klávesnice, prvky s radiofrekvenční identifikací (Radio Frequency Identification, dále jen „RFID“) jako karty, klíčenky, přívěsky, náramky, čipy, čtecí zařízení, tísňové tlačítka). (Loveček, Veľas, Ďurovec, 2015, s. 38)
- **Čidla (detektory narušení)** – zařízení určené k vyslání poplachové signálu nebo zprávy na základě jevů souvisejících s narušením střeženého objektu či prostoru.
- **Výstražné zařízení** – sirény, majáky, zábleskové světla.
- **Poplachové přenosové systémy a zařízení** – zajišťují přenos výstupních informací z ústředny k poplachovému příjímacímu centru (dále jen „PPC“) nebo pult centralizované ochrany (dále jen „PCO“) a následné ovládání poplachového systému. (Loveček, Veľas, Ďurovec, 2015, s. 38)
- **Doplňkové zařízení –** paměťové zařízení, automatizační zařízení.
- **Prvky pro obvodovou (perimetrickou) ochranu.**
- **Prvky pro plášťovou ochranu.**
- **Prvky pro prostorovou ochranu.**
- **Prvky pro předmětovou ochranu.**
- **Prvky tísňové ochrany.**



Obrázek 2 – Schéma zapojení PZTS;
Zdroj: *Jablotron, 2020* (upraveno)

Tyto základní komponenty se kombinují v různých podobách a stupních složitosti. Ty mohou být následně ještě doplněny o tísňové hlásiče a záznamová zařízení. Začlenění jiných prvků je možné pokud nebude ovlivněna funkce komponentů PZTS.

2.1 Poplachové ústředny

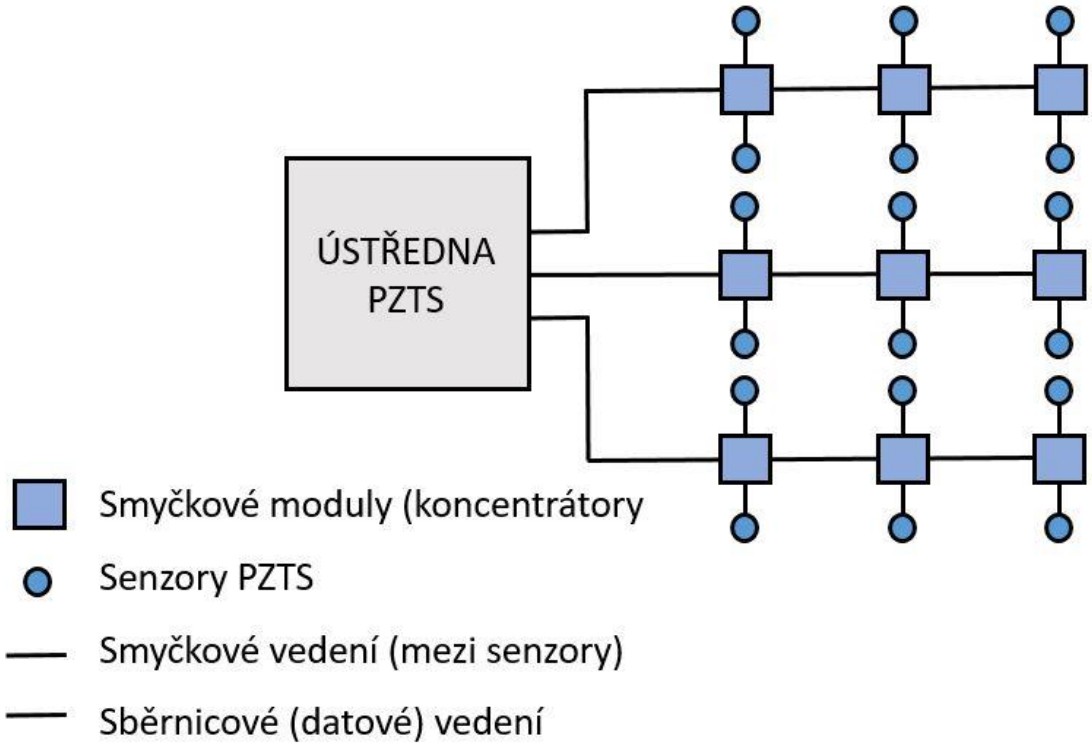
Poplachové ústředny mají hlavní účel:

- Slouží k příjmu a vyhodnocení výstupních elektrických signály od čidel PZTS.
- Ovládají všechna zařízení, ať už signalizační, přenosové, zapisovací a jiná, která indikují narušení.
- Funguje jako hlavní napájecí prvek pro čidla a další prvky PZTS.
- Umožnuje diagnostiku systému.

Je ovládán pomocí elektromagnetických nebo kódových zámků, popřípadě vlastních ovládacích klávesnic, které umožňují PZTS nebo jeho části změnu stavu na zastřežení nebo na klidový stav. (Křeček, 2006, s. 107)

2.1.1 Smyčková ústředna

Ústředna má pro každou poplachovou smyčku vstupní vyhodnocovací obvod, který je řešen pro připojení smyček o stanovené hodnotě a toleranci. Smyčka je zakončena zakončovacím odporem tak, aby měla předepsanou hodnotu odporu pro konkrétní typ ústředny. Pokud dojde v některé smyčce ke změně odporu, znamená to, že někde došlo k narušení a systém vyhlásí poplach. Poplachové smyčky jsou nejčastěji tvořeny sériovým zapojením rozpínacích kontaktů čidel. (Křeček, 2006, s. 108)



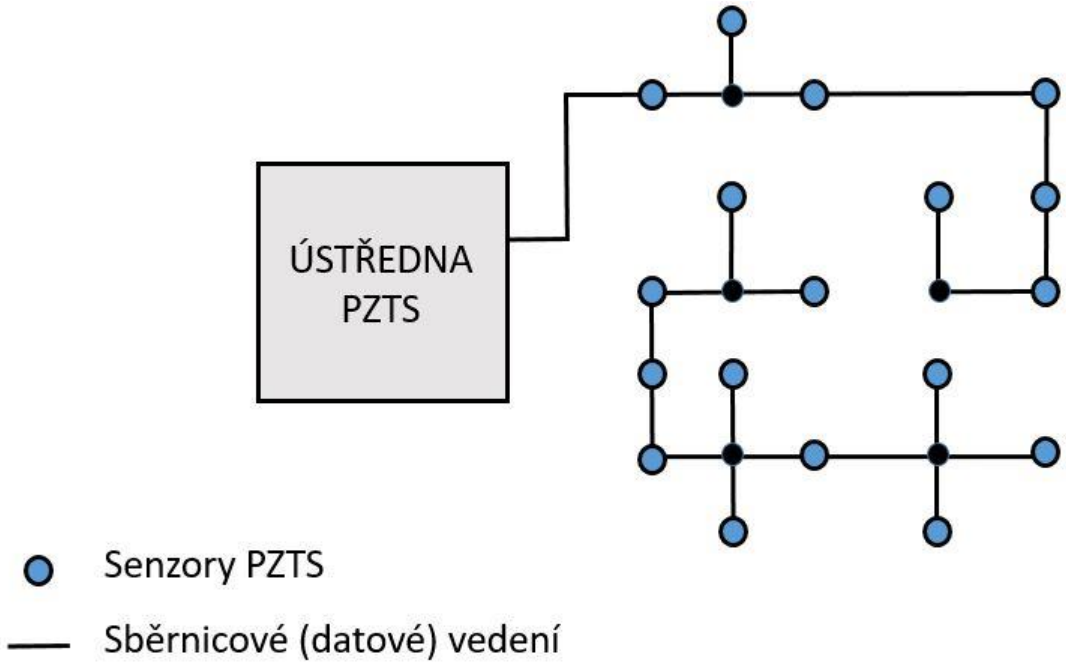
Obrázek 3 – Schéma zapojení smyčkové ústředny;
Zdroj: KŘEČEK, *Příručka zabezpečovací techniky.* 2003 (upraveno)

2.1.2 Ústředny s přímou adresací čidel

Ústředna pracuje na principu komunikace po datové sběrnice ústředna – čidla. Adresy jednotlivých čidel jsou periodicky generována ústřednou, která je pak přijímá od čidel podle příslušné odezvy. Každé čidlo má svůj vlastní komunikační modul. Čidla jsou připojena v libovolném pořadí pomocí čtyř nebo osmy žilového kabelu například ethernetový kabel. Dva vodiče slouží pro napájení čidla a dva jako datové sběrnice. Velkou výhodou tohoto systému je, že pokud dojde k narušení objektu, ústředna oznámí, které konkrétní čidlo bylo aktivované a jaký je druh narušení.

Kabelový systém je zde velmi jednoduchý, ale problém nastává v případě, kdybychom chtěli pro datovou sběrnici přidat další dodatkové funkce pro čidla. Stejně tak má svá omezení i dodatečná konfigurace kabelové sítě.

Při návrhu je nutné propočítat odběr všech částí systému a nezapomenout na úbytky na napájecích vodičích. Počet přímo adresovaných čidel se v tomto systému pohybuje v řádově v desítkách. (Křeček, 2006, s. 108-109)



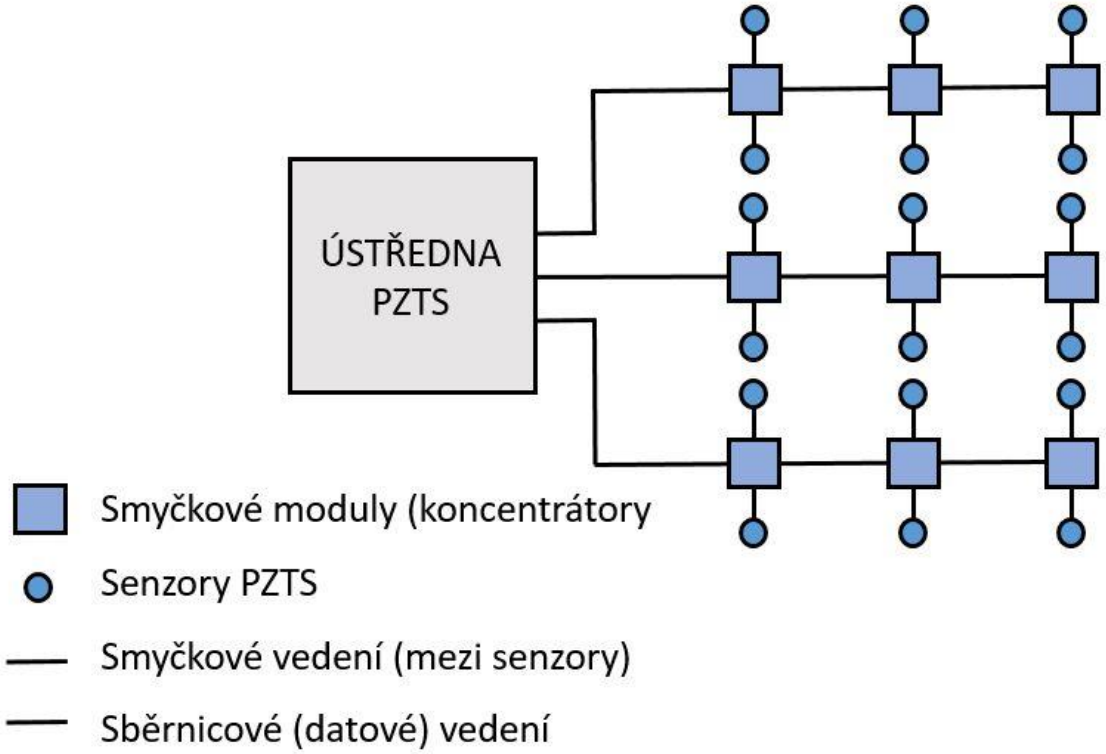
Obrázek 4 – Schéma zapojení ústředny s přímou adresací;

Zdroj: KŘEČEK, *Příručka zabezpečovací techniky.* 2003 (upraveno)

2.1.3 Ústředny smíšené

Datová komunikace u této ústředny probíhá podle principu ústředna – koncentrátor (tzv. sběrnicový modul smyček), tyto dva prvky komunikují pomocí datové nebo analogové sběrnice. Na určené koncentrátory jsou čidla připojena pomocí smyček, stejně jako tomu je u smyčkových ústředen. Vlastní vyhodnocování probíhá podle typu ústředny. Jednou variantou je analogový multiplex, kdy se na sběrnici připojují postupně, jednotlivé smyčky a vyhodnocení impedance smyčky s příslušnou odezvou provádí ústředna. Dalším případem je integrace vyhodnocovací logiky včetně vyrovnávací logiky přímo do koncentrátoru. Komunikace zde probíhá v datové podobě. Umožňuje-li to kapacita ústředny, je možné, na jednotlivé vstupy koncentrátorů připojit přímo jednotlivá čidla. Tak přejde tento typ ústředny na ústřednu s přímou adresací čidel se všemi jejími výhodami. Nevýhodou tohoto sytému

jsou ovšem náklady na vybudování. Důležité je správně rozvrhnout čidla do smyček, aby byla zachovány z hlediska uživatele účelná úroveň adresace. (Křeček, 2006, s. 109-110)

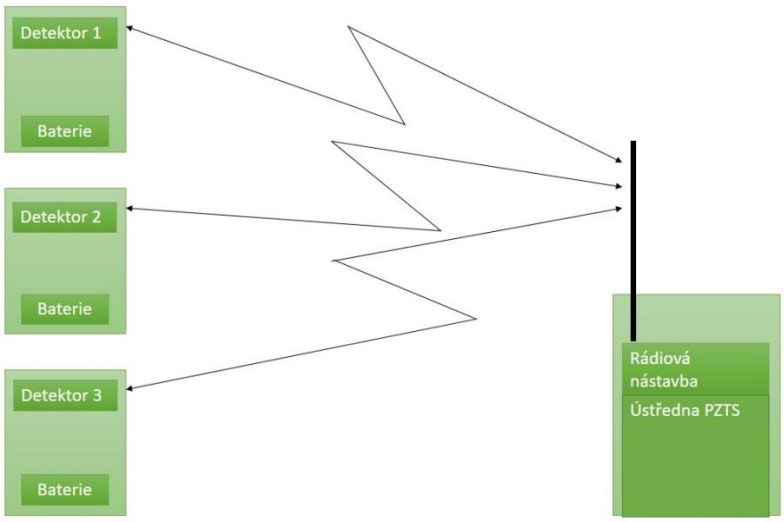


Obrázek 5 – Schéma zapojení smíšené ústředny;
Zdroj: KŘEČEK, *Příručka zabezpečovací techniky.* 2003 (upraveno)

2.1.4 Ústředny s bezdrátovým připojením

Jedná se o skupinu ústředen, které se aplikují v dnešní době velice často. Pracují v pásmu telemetrie (433Hz). Ve volném prostředí je dosah 100 – 200 m. V objektech musíme počítat s menšími vzdálenostmi. Napájení čidel je buď lithiovou baterií nebo 9V destičkovým článkem. Napětí baterie je hlídáno a podle provedení dojde při poklesu napětí k místní akustické signalizaci interním bzučákem nebo se informace přenese do poplachové ústředny. Obecně se dají identifikovat u bezdrátových systému následující výhody:

- Velmi snadná instalace.
- Možnost instalace do stávajících objektů s minimem stavebních úprav.
- Snadné rozšíření systému o další prvky (čidla).
- Snadná změna konfigurace (jednoduché přemístění detektorů při úpravách). (Křeček, 2006, s. 110)



Obrázek 6 – Bezdrátová komunikace detektorů;

Zdroj: (vlastní zpracování)

Ústředny s jednosměrnou komunikací

Jednosměrně pracující základní ústředny. Skládá se z čidla jako vysílače a v ústředny jako přijímače. Problém je, že starší systémy, které byly řešené tímto způsobem, nemají žádnou kontrolu funkčnosti jednotlivých detektorů. Pokud by tedy došlo k poruše prvku nebo jeho násilnému poničení nebo odcizení, ústředna o této změna stavu neobdrží žádnou informaci. Modernější systémy využívají principu viditelné kontroly přenosové cesty vysíláním kontrolních telegramů. Zde je ovšem problém počtem kontrol hlášení, který zkracuje životnost baterie, které napájejí jednotlivé prvky. V praxi je většinou četnost kontrol jednou za několik hodin. V případě, že je ale některý prvek mimo provoz, tak se to ústředna dozví s určitým zpožděním. (Křeček, 2006, s. 111)

Systémy s obousměrnou komunikací

Nejnovější typ bezdrátových systémů pracuje obousměrně (duplexně) a každý prvek v systému je vybaven vysílačem i přijímačem. Tyto moduly jsou schopny najít si ve vyhrazeném kmitočtu pásma dva volné kanály pro přenos a automaticky se na ně naladit. Dojde-li k velkému rušení vysílacího kanálu, jsou schopny se přeladit odlišný kanál, který není tak ovlivněn rušením. (Křeček, 2006, s. 111)

2.2 Ovládací periférie

K správné a plnohodnotné funkci systému, musí být umožněno uvádět systém jak do stavu střežení, tak i naopak do stavu klidového. K tomu jsou právě určena ovládací zařízení.

Vhodný typ ovládacího zařízení, je volen podle stupně zabezpečení a požadavků vlastníka. Cílem je, aby obsluha byla jednoduchá a byla minimalizována možnost vyvolat při manipulaci planý poplach. Způsobů jak přepínat stavy ze střežení, do stavu klidu, je mnoho a záleží na typu ústředny.

Blokovací zámek

Je to kombinovaný prvek mechanického zabezpečení stupních dveří spolu s ovládáním systému PZTS. Je montován jako přídavný zámek vstupních dveří. Je to z pohledu uživatele nejjednodušší druh ovládacího zařízení, ale přitom je to nejbezpečnější prvek PZTS. Jeho konstrukce je taková, že je jí zajištěno spolehlivé uvádění do stavu střežení a naopak. Zámek lze uzamknout, jen pokud je systém v normálním stavu. V případě poruchy či opomenutí obsluhy (otevřené okno), elektromagnetická západka znemožní uzamčení blokovacího zámku, a tak i uvedení systému do stavu střežení. Pokud jde zámek uzamknout, může si být uživatel jist, že je systém v pořádku.

Při vstupu do objektu musí být systém odblokován, protože nejdříve musíme odemknout, abychom mohli vstoupit. Tím že odemkneme blokovací zámek, systém přejde automaticky do stavu klidu

Použitím blokovacího zámku se nám dostává nejlepšího způsobu, jak můžeme ovládat systém, ale jeho použití je poměrně nákladné. Vlastní zámek je chráněn proti odvrtání celoplošným vodivým meandrem zapojeným do samostatné zajišťovací (sabotážní) smyčky. (Lukáš a kolektiv, 2011, s. 201)

Kódové klávesnice

Mohou být využity jako spínací zámky. Pro používání jako ovládací díl PZTS je nezbytné, aby elektronika klávesnice byla umístěna v samostatné skříni a ve střežených prostorech.

Pro uživatele kódové klávesnice přinášejí nutnost zapamatovat si správný přístupový kód.

Prevencí je po určité době změnit kód, jelikož stoupá riziko jeho prozrazení a fyzické opotřebení tlačítek, které snižuje počet kombinací kódu, toho by mohli zneužít lupiči.

Výhodou je možné použití tísňového kódu, dojde-li k rizikovému vstupu do objektu.

Lépe vybavené typy lze používat také jako ovládání elektrického vrátného nebo ovládání osvětlení. (Hart, 2015, s. 16)

Obrázek 7 – Klávesnice s displejem a RFID čtečkou;
Zdroj: *Jablotron, 2020*

Čtečky bezkontaktních karet

Čtečky bezkontaktních karet se používají u systému PZTS při kombinaci systému s kamerovým systémem a systému kontroly vstupu. Jsou montovány za účelem zjednodušení ovládání uživatelem.

Obrázek 8 - Bezdrátový přístupový modul s RFID čtečkou;
Zdroj: *Jablotron, 2020*

Poplachové přenosové systémy a zařízení

Poplachový přenosový systém je určený na přenos informací, které se týkají stavu jednoho nebo vícero PZTS, do jednoho či více poplachových přijímacích center. Dohledová a poplachová přijímací centra (dále jen „DPPC“) také označovány jako pult centralizované ochrany (PCO) je dispečerské zařízení (s trvalou obsluhou), do kterého jsou přeneseny všechny informace, týkající se stavu PZTS a VSS systémů v zastřeženém objektu. Signály z jednotlivých částí systému jsou na PCO přenášeny různými způsoby:

- Rádiová síť.
- Mobilní síť.
- Internet.

Výstražné zařízení

Signalizační (výstražné) prvky mají za úkol okamžitě upozornit na vzniklý poplachový stav. Mezi nejpoužívanější prvky lze zařadit signalizaci akustickou a optickou.

Obrázek 9 – Siréna vnitřní;

Zdroj: *Jablotron, 2020*

Akustická signalizace

Akustická signalizace je označována nejčastěji jako zvukové sirény. Zvukové sirény se vždy skládající z akustického měniče, který je doplněn o generátor kolísavého tónu a zesilovač. Dle konstrukce sirény se rozdělují na sirény pro vnitřní a vnější použití. (Kindl, 2007, s. 94)

Optická signalizace

Optická signalizace je součást krytu sirény a funguje jako světelný maják, který je tvořen buď žárovkou, nebo výbojkou a při aktivaci vydává silné přerušované světlo. Světelný maják bývá doplněn i o akustickou signalizaci a to z důvodu rychlejší lokalizace narušeného objektu. Doporučená barva optické signalizace je oranžová. (Kindl, 2007, s. 94)

2.3 Prvky pro obvodovou ochranu

Prvky (detektory) pro obvodovou ochranu signalizují narušení vnější části objektu. Jejich účelem je mít kontrolu na zastřežených místech. Řadíme sem mikrofonní kabely, senzorové kabely a perimetrické závory.

2.3.1 Mikrofonické kabely

Chrání oplocení jak pletivové, tak i z betonových částí. Kabely jsou připevněny k pevnému předmětu a pomocí nich lze zjistit průnik do střeženého prostoru, či poničení, řezání a jinou manipulaci s kabelem. Základní charakteristika pro tento detekční systém je, že výstupní signál z kabelu má charakter nízkofrekvenčního signálu v akusticko-frekvenčním pásmu, co umožnuje při zesílení připojit k vyhodnocující jednotce reproduktor pro akustický připoslech. Tato funkce umožnuje obsluze odhalit charakter vlivů působící na plot a tak odlišit falešný poplach od skutečného narušení. Díky této společné vlastnosti se kabel nazývá mikrofonní. Hrozí však možnost vytvoření falešných poplachů při silném větru, dešti, vichřici nebo přítomnosti divoké zvěře. (Křeček, 2006, s. 100)

2.3.2 Senzorové kabely

Umísťují se nejčastěji na oplocení, kde slouží k detekci narušení perimetru, které vzniká při jeho překonávání. Dají se rozdělit na několik druhů podle toho, na kterém fyzikálním principu je detekce vibrace založena. Z hlediska detekce je rozdělujeme na pasivní a aktivní detekční systémy. Pasivní systémy pracují na principu detekce vibrace vzniklé při překonávání oplocení. Aktivní detekční systémy fungují na principu, že naslouchají na senzorovém kabelu a při překonává oplocení na základě odezvy na trvalý nebo impulzový

vysokofrekvenční signál, který je vysílán do kabelu a je okamžitě vyhodnocován. Existuje několik druhů senzorických kabelů, které se používají k perimetrické ochraně. Mezi nejpoužívanější patří:

- Koaxiální kabely
- Magnetické kabely
- TDR kabel. (Lukáš a kolektiv, 2011, s. 91)

2.3.3 Perimetrické závory

Perimetrické závory jsou nejčastějším druhem perimetrické ochrany. Účelem je zastřežení perimetru a kontrola detekce. Výhodou je nezávislost na klimatických podmínkách. Perimetrické závory patří do kategorie aktivních prvků, tudíž mají jak přijímač, tak i vysílač. Princip střežení spočívá, že vysílač vysílá jistý druh záření podle typu perimetrické závory směrem k přijímači, a pokud dojde k přerušení spojení mezi vysílačem a přijímačem, tak zařízení vyhodnotí informaci jako poplach. Podle formy záření rozdělujeme perimetrické závory na:

Infračervené perimetrické závory

Infračervené závory fungují na principu toho, že vysílače vyzařují pomocí infračervené záření směrem k přijímači signál a pokud je jeden z nich přerušen, je vyhlášen poplach. Pro vyšší odolnost infračervené bariéry obsahují zařízení proti zarosení a povětrnostním vlivům. Maximální dosah infračervených závor je 250 metrů.

Mikrovlnné perimetrické bariéry

Mikrovlnné bariéry se skládají z dvou prvků a to mikrovlnného vysílače a přijímače, které jsou montovány odděleně. Takto namontované vysílače a přijímače vytvářejí elektromagnetické pole ve tvaru elipsy. Když dojde k narušení elektromagnetického pole bariéry pachatelem, má to za následek, že přijímač vyhodnotí změnu stavu a je spuštěn poplach. Velkou výhodou mikrovlnných bariér je dosah, který je až 300 metrů a také velká odolnost vůči počasí oproti infračerveným závorám.

Štěrbinové kabely

Tento způsob ochrany vytváří neviditelnou bariéru, tudíž nehrozí zneškodnění systému. Kabely jsou vedeny v párech pod povrchem v hloubce 30cm a vzdálenosti přibližně 2m od

sebe. Systém detekuje pohyb pomocí elektromagnetického pole mezi vysílacím a přijímacím kabelem. (Lukáš a kolektiv, 2011, s. 65-70)

2.4 Prvky pro plášťovou ochranu

Jejich úkolem je signalizace narušení pláště budovy. Plášť objektu tvoří všechny otvory objektu jako dveře, okna a další. Nejpoužívanější jsou magnetické kontakty a čidla na ochranu skleněných ploch.

2.4.1 Magnetické detektory

Magnetické detektory, též také magnetické kontakty se využívají pro detekci narušení stavebních prvků budov jako dveří, oken, mříží, bran, nebo pro detekování manipulace s důležitými částmi PZTS (například vypnutí napájecího zdroje). Konstrukce magnetických detektorů umožnuje mnoho různých způsobu zapojení: povrchová instalace, zapuštěná instalace a skrytá instalace.

Magnetické kontakty – jsou vhodné pro střežení stavebních otvorů (okna, dveře), výhoda je snadná instalace a vysoká životnost. Dělíme na:

- **jazýčkový kontakt**, ten se montuje na pevnou část např. rám okna nebo zárubně.
- **permanentním magnetem,** ten je trvale umístěn na pohyblivou část např. křídla dveří nebo oken.

Obrázek 10 – Magnetický detektor;
Zdroj: *Jablotron, 2020*

Princip detekce narušení je založen u magnetických detektorů na vhodném umístění jazýčkového kontaktu do silného magnetického pole, s permanentním magnetem. Vložením

jazýčku do magnetického pole se zmagnetizují, a na koncích kontaktů se pak vytvoří opačná magnetická polarita, díky tomu dojde k sepnutí jazýčků. Dále pokud dojde k oddálení magnetu od jeho jazýčku, dojde k následnému odmagnetizování a jazýčky se okamžitě rozpojí, a způsobí vyhlášení poplachu. (Lukáš a kolektiv, 2011, s. 41)

2.4.2 Detektory na ochranu skleněných ploch

Kontaktní detektory rozbití skleněných ploch se využívají k ochraně oken, prosklených dveří a výkladních skříní. Pro svou funkci využívají vyhodnocování pomocí mechanických změn, které provází destrukci skleněných ploch. Mezi nejčastěji prakticky používané kontaktní detektory destrukce skleněných ploch lze zařadit především následující:

Poplachové fólie, tapety a skla

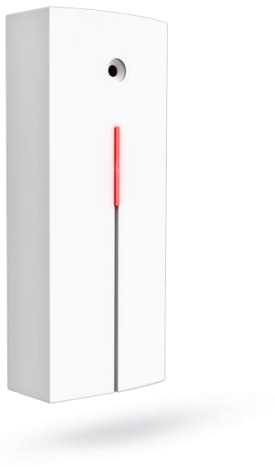
Poplachové fólie, tapety a skla jsou zařazeny jako pasivní kontaktní destrukční detektory. Základem je vodivý prvek (jemným drátkem), který pokrývá celou plochu skleněné výplně. Detekce poplachu je založena na principu přerušení vodivého prvku, kdy následuje vyhlášení poplachu. (Lukáš a kolektiv, 2011, s. 50)

Fóliové polepy

Detekční prvek u foliových polepů je tenká vodivá hliníková fólie o tloušťce cca 0,08 mm a šířce 8 až 12 mm). Tato hliníková fólie se musí nalepit na postranní části skla ve vzdálenosti 50 až 100 mm od okraje rámu. Detekce poplachu je založena na přerušení poplachové smyčky, v důsledku zničení skleněné výplně. (Lukáš a kolektiv, 2011, s. 50)

Pasivní kontaktní detektory rozbití skla

Detekčním prvkem je piezoelektrický senzor, který je naladěn na rezonanční kmitočet (40 kHz do 120 kHz). Detekce se určuje pomocí porovnávání frekvence kmitání piezosenzoru, vyvolaného mechanickým namáháním skleněné plochy, když je sklo rozbito. Detektory se instalují na spodní hraně skleněné plochy ve vzdálenosti 50 mm od hrany rámu a jejich dosah je 1,5 až 3 metry v závislosti podle druhu skla. (Lukáš a kolektiv, 2011, s. 51)



Obrázek 11 – Detektor rozbití skla;
Zdroj: *Jablotron, 2020*

2.4.3 Vibrační detektory

Patří k prvkům střežení pláště budovy, pro hlídání průrazů stěn a stavebních konstrukcí. Základem je elektromechanický měnič, který tvoří mechanické setrvačné kontakty doplněné vyhodnocovací technikou. Osazují se podle konstrukčního provedení na riziková místa možného průchodu zdí či rámy dveří a oken nebo oplocení objektu. (Lukáš a kolektiv, 2011, s. 40)

2.5 Prvky pro prostorovou ochranu

Tyto prvky střeží pohyb osob, které již překonaly plášťovou ochranu a vnikly do vnitřního prostoru budovy (například chodba, schodiště). Prvky (detektory) pro prostorovou ochranu detekují změny stavu (narušení) v prostoru areálu. Detektory pro prostorovou ochranu fungují na principu detekce změn fyzikálních veličin, které vyvolá narušitel pohybující se ve střeženém prostoru. Tyto detektory pohybu dělíme na dvě skupiny aktivní a pasivní.

- **Pasivní detektory pohybu**

Princip pasivního snímaní je, detekce změn v měřené fyzikální veličině, která je vyvolána pohybem narušitele, který se vyskytuje v chráněném prostoru. Pasivní detektory pohybu obsahují pouze přijímač, nikoliv vysílač. Řadí se sem pasivní infračervené detektory (dále jen „PIR“) čidla.

Pasivní infračervené detektory

Pasivní infračervené detektory fungují pomocí zachycení změn v infračerveném pásmu kmitočtového spektra elektromagnetického vlnění z důvodu, že každé těleso vyzařuje vlnění v infrapásmu kmitočtového spektra laicky řečeno každé těleso vyzařuje teplo. PIR detektor je složen s pyroelektrického senzoru, který zachycuje teploty od 25° C do 40° C) to jsou teploty blízké povrchu lidského těla.

PIR detektory jsou nejrozšířenější druhy detektorů pohybu, jsou určené k prostorové a perimetrické ochraně střežených objektů. Mají mnoho výhod, jsou nenáročné na instalaci, patří mezi nejlevnější prvky a mají nízkou spotřebu energie. Největší nevýhodou PIR detektorů je detekovaní změny teplot vyvolaných pohybujícími se objekty (zvířaty, proměnlivý zdroji tepla, přímým nebo nepřímým působením světla, atd.), citlivost detektoru na umístění (jeli detektor umístěn například nestabilním prostředí nebo v průvanu, tak může docházet k falešným poplachům.

Obrázek 12 – PIR infračervený detektor;
Zdroj: *Jablotron, 2020*

- **Aktivní detektory pohybu**

Aktivní detektory fungují na rozdíl od pasivních pomocí vytváření vlastního akustického nebo elektromagnetické pole, které přenášejí do střeženého prostoru, a reagují na změnu v poli, které si vytvořili. Aktivní detektory na rozdíl od pasivních obsahují přijímač i vysílač (patří se ultrazvuková čidla).

Aktivní infračervené detektory

Aktivní infračervené detektory (dále jen „AIR“) jsou na rozdíl od PIR detektorů, které obsahuje jenom přijímač, vybaveny i vysílačem. AIR detektory využívají stejných fyzikálních principů, jako PIR detektory, avšak AIR vysílá do prostoru signál, který pak přijme zpět a dojde k vyhodnocení. Výhoda u AIR detektorů je v tom, že se nedají vyřadit pomocí jejich zastínění nebo přestříkání barvou.

Aktivní mikrovlnné detektory

Mikrovlnné detektory (microwave detectors dále jen „MW“) fungují na podobném principu, jako ultrazvukové detektory, akorát s jiným elektromagnetickým vlněním a to mikrovlnami v odlišném frekvenčním pásmu (9 až 11 GHz). Mikrovlnné detektory patří mezi aktivní detektory. Základním principem je Dopplerův jev. Dopllerův jev je změna vlnové délky elektromagnetických nebo akustických vln vyvolané relativním pohybem zdroje a pozorovatele. Když v jednom bodě zdroj záření s vyzařovanou konstantní frekvencí (vysílač) a přijímač, čím blíže se pohybuje objekt ke zdroji záření, tým vyšší frekvenci odraženého signálu příjme přijímač. V případě, že se objekt od zdroje záření vzdaluje, frekvence přijímaná přijímačem klesá. Intenzita odrazu se mění v závislosti na velikosti odrazové plochy a materiálu, z kterého je konstruovaná. Tento princip se používá v radarech. MW detektor tak nevyhodnocuje odraz od nepohyblivých předmětů, ale je nastaven na reakci na odraz signálu, který pokud byl změněn tak je spuštěn poplach. (Lukáš a kolektiv, 2011, s. 67)

Aktivní ultrazvukové detektory

Aktivní ultrazvukové detektory (ultrasonic detectors dále jen „US“) jsou detektory využívané pro prostorovou, plášťovou i předmětovou ochranu. AIR detektory fungují na principu vysílání konstantního akustického signálu o frekvenci 20 až 60 kHz (frekvence z oblasti, které nejsou v lidských sluchem slyšitelné), tento akustický signál se po odrazu od předmětu vrací zpět do přijímače, který tak vyhodnotí změny jeho amplitudy, frekvence a fáze a pokud detekuje změnu, tak je spuštěn poplach.

Duální detektory

Duální detektory pracují na principu kombinace dvou funkčně odlišných typů detekce. Vývoj duálních čidel vychází z faktu, že každá technologie je jinak náchylná na plané poplachy (různá čidla fungují na různých fyzikálních principech). Kombinací různých technologií, různých fyzikálních jevů, se sníží počet špatně vyhodnocených případů.

Detektor vyhlásí poplach jen v případě, dojde-li ve stanoveném intervalu k aktivaci obou senzorů. Nejčastější kombinace duálních detektorů jsou infračervený a mikrovlnný (PIR + MW) nebo infračervený a ultrazvukový detektor (PIR + US). (Loveček, Veľas, Ďurovec, 2015, s. 67)

2.6 Prvky pro předmětovou ochranu

Předmětová ochrana se zabývá ochranou samotných cenných hodnot a předmětů, a signalizuje jejich napadení nebo neoprávněnou manipulaci. Pro ochranu vybraných předmětu se využívají především trezory nebo bezpečnostní skříně.

Závěsové detektory

Závěsové detektory slouží na ochranu zejména uměleckých předmětů, jakou jsou obrazy nebo tapisérie. Princip detekce funguje na zavěšení střeženého předmětu na nerezový drát a kleštiny v senzoru detektoru a ten vyhodnocuje velikost síly, kterou na něj střežený předmět působí. Dojde-li ke změně velikosti síly, tak je spuštěn poplach. Závěsové detektory patří mezi velice citlivé detektory a dokážou zaznamenat pohyb střeženého předmětu i o několik tisícin milimetru.

Váhové detektory

Váhové detektory se využívají především na střežení váz, částí nábytku, sošek, číší. Váhový detektor se umístí pod střežený objekt, který je na něm položen. Po připojení napájecího napětí k detektoru je zaznamenána výchozí hmotnost střeženého objektu a následně vyhodnocována pouze její změna. Podle nastavené citlivosti je detektor schopen reagovat na jakoukoliv manipulaci se střeženým objektem nebo na její dotyk. (Lukáš a kolektiv, 2011, s. 47)

Seismické (otřesové detektory)

Seismické detektory se využívají převážně pro střežení trezor a trezorových skříní. Princip detekce, je snímání vibrací v okolí a měření amplitud, frekvencí a času. Tyto vibrace vznikají mechanických nebo tepelným působením pachatele. Zachycením této vibrace se spustí alarm (poplach).

2.7 Prvky tísňové ochrany

Prvky tísňové ochrany slouží jako ochrana při ohrožení objektu, zaměstnanců a veřejnosti. Ochrana spočívá ve vyslání tísňového signálu na místo, odkud vyrazí pomoc. Tísňový signál

může být vyvolán, pomocí manuálního aktu (stiskem nouzového tlačítka) nebo automaticky bez přímého přispění lidského faktoru. Existují různé typy jako veřejné, skryté, osobní, automatické a speciální hlásiče.

2.8 Dohledový videosystém VSS

VSS se skládá z kamerového vybavení, úložiště, monitorovacího a souvisejících zařízení pro účely přenosu obrazu a ovládání. Uzavřený televizní okruh (Closed circuit Televison, dále jen „CCTV“) jsou součástí obecnějšího pojmu „VSS“, slouží k monitoringu střeženého objektu. Umožnuje sledovat v reálném čase při správném pokrytí venkovní a většinu vnitřního areálu. Dále umožnuje archivaci záznamu pomocí síťového video rekordéru (Network Video Recorder, dále jen „NVR“) na ukládací prostor na disku. Podle kapacity disku umožnuje různou dobu uložení všech záznamů z kamer. (Lukáš a kolektiv, 2012, s. 18)

VSS je tvořen prvky:

- Kamery.
- Objektiv.
- Zobrazovací zařízení.
- Kamerové přepínače.
- Záznamové zařízení.

Pod dohledem nad chráněným perimetrem je možné díky VSS:

- Monitorovat.
- Detekovat.
- Pozorovat.
- Rozpoznávat.
- Identifikovat.
- Vyšetřovat.

Základní prvky kamery

- Ohnisková vzdálenost.

- Světelnost.
- Clona.
- Hloubka ostrosti.
- Uchyceni objektivu.

IP kamera

Síťová kamera nebo také IP kamera, lze jednoduše popsat jako kombinaci kamery a počítače v samostatně fungujícím celku. Hlavními komponenty jsou: Objektiv, obrazový snímač, jeden nebo více procesoru, paměti, a komunikační rozhraní. IP kamery se dělí na fixní kamery a PTZ IP kamery.

Fixní IP kamery

Nemají řídící jednotku na pohyb a jsou fixně nastaveny na určitý pozorovací úhel.

PTZ IP kamery

PTZ IP kamery obsahují řídící jednotku díky, které může používat funkci dálkového nastavování polohových hlavic (PAN, TILT, ZOOM) česky znamená „natočit, naklonit, přiblížit“ (Loveček, Veľas, Ďurovec, 2015, s. 98)

- Mechanické IP PTZ kamery.
- Nemechanické kamery IP PTZ kamery.
- IP PTZ dome kamery.

Obrázek 13 – Kamera vnitřní/vnější 2MP;
Zdroj: *Jablotron, 2020*

2.9 Systém kontroly vstupu

Systém kontroly vstupu (dále jen „SKS“) je systém obsahující všechny konstrukční a organizační prvky, které se týkají zařízení nutných pro řazení přístupu. Rozhoduje o tom, kdo má poskytnutý přístup, kde může být přístup získaný a kdy je přístup získaný. Slouží pro minimalizaci rizika nepovoleného vstupu.

Místo přístupu

Je místo, kde přístup může být ovládaný pomocí ovládacích prvků a senzorů místa přístupu. Mezi ovládací prvky patří elektronické zámky, turnikety, závory. Mezi senzory místa přístupu patří spínače, tlakové signalizační zařízení a dveřní spínače.

Turniket

Je mechanická zábrana, která na základě otáčivého mechanismu umožnuje vstupovat osobám do zabezpečeného prostoru.

Radiofrekvenční identifikační karty (RFID)

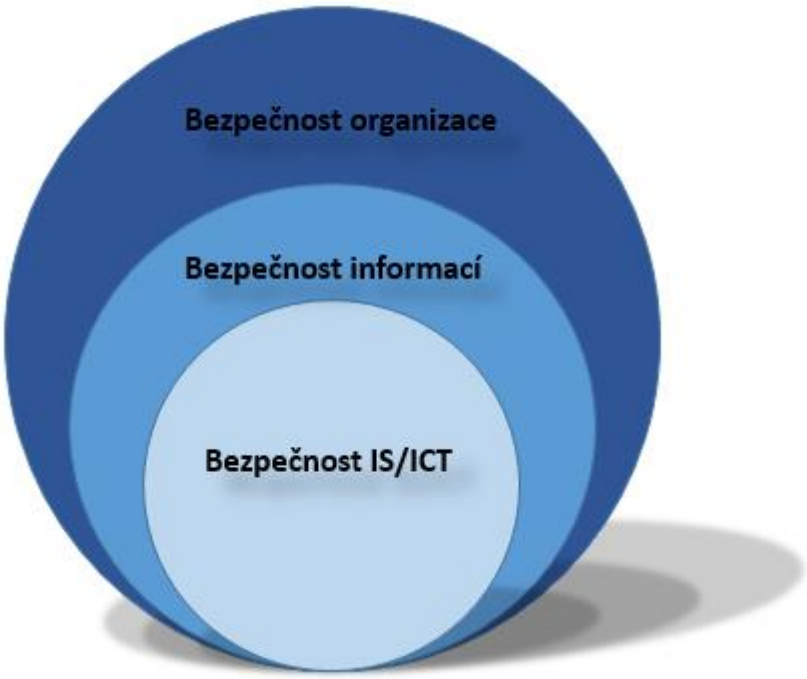
Je technologie identifikace objektů pomocí radiofrekvenčních vln. Informace jsou v elektronické formě uložené do malých čipů a umožnují pomocí čtecích zařízení čtení a zápis těchto údajů. (Loveček, Veľas, Ďurovec, 2015, s. 125)

3 BEZPEČNOST INFORMACÍ

Bezpečnost informací je především ochranou důvěrnosti, integrity a dostupnosti informací. Lze do ní zahrnout také další vlastnosti například autenticitu, odpovědnost, nepopíratelnost a spolehlivost.

Jedná se zejména o uplatnění obecných bezpečnostních opatření a postupů, které chrání informace před ztrátou či nežádoucí změnou, jako je nedůvěryhodnost, celistvost a další jako ztráta autentičnosti nebo odpovědnosti. Pokud je takový stav zjištěn, je nezbytné postupovat podle předem stanovených pravidel (směrnic), podle nichž musí být stav co nejrychleji napraven. V rámci práce s údaji je také nezbytný rozsah oprávnění přiděleným osobám, které mají s informacemi nakládat.

Úrovně bezpečnosti si můžeme rozdělit podle obrázku 14.



Obrázek 14 – Vztah úrovní bezpečnosti v organizaci;
Zdroj: (vlastní zpracování)

Každá úroveň má za úkol chránit jen část aktiv. V rámci bezpečnosti IS/ICT jsou chráněna pouze aktiva, které jsou nedílnou součástí informačního systému firmy založené na informačních a komunikačních systémech. Součástí je také hmotná aktiva jako je technické vybavení, to však může mít mnohem nižší hodnotu než informace obsažené v nich. Mezi nehmotná aktiva můžeme zařadit pracovní postupy, data organizace, které jsou nezbytné pro

provoz. Také služby, mezi které řadíme zajištění základních služeb jako je osvětlení, topení či klimatizace. (Zelená, 2019, s. 18)

3.1 Technické normy v souvislosti s bezpečností informací

Technickými normami, které se nás týkají oblasti bezpečnosti informací, jsou normy International Organization for Standartization (dále jen „ISO“) 27000. Tato norma definuje pojmy a terminologický slovník pro všechny další normy z této série. Dále také Česká technická norma (dále jen „ČSN“) ISO/IEC 27001, která představuje požadavky na ustanovení, impletaci, udržení a neustále zlepšování systému řízení bezpečnosti informací, slouží také pro zhodnocení odolnosti organizace vůči možným bezpečnostním incidentům.

Norma ČSN ISO/IEC 27002, poskytuje organizaci pokyny, jak impletovat obecně přijatá opatření bezpečnosti informací. Ukazuje možnosti pro zabezpečení pomocí vhodných opatření, včetně politik, procesů a postupů.

Norma ISO/IEC 27006, uvádí požadavky pro akreditaci orgánu provádějící certifikaci systému řízení bezpečnosti informací a stanovuje podmínky pro udělení certifikací. (Zelená, 2019, s. 29)

3.2 Identifikace hrozeb

Hrozba nastává v případě, že dojde k ohrožení střeženého objektu, nebo prvků v něm obsažených. Jedná se o příčinu nechtěného incidentu, například k poškození, zničení, napadení nebo ztráty hodnoty aktiva. Je to reálné, známé nebo potenciální nebezpečí. Mezi další hrozby řadíme bezpečnostní incident, který využívá zranitelných míst střeženého objektu a snaží se o průnik nebo jinou nepovolenou škodlivou činnost. Expozici, jež je místem, které je vystavené riziku, kde může dojít k potenciálnímu poškození nebo ztrátě informací či snížení funkčnosti systému. Průnik, což je zneužití informačního systému.

3.3 Fyzická bezpečnost

Fyzická bezpečnost je nedílnou, důležitou a bohužel mnohdy podceňovanou součástí bezpečnosti objektu.

Fyzická bezpečnost v sobě zahrnuje řadu opatření, mezi které patří:

- Zajištění perimetru.
- Kontrola přístupu.

- Vnitřní bezpečnost.
- Ochrana prvků PZTS před rozebráním, úpravou nebo připojením periférií k vstupně výstupním portům.
- Ochrana před nepříznivými přírodními vlivy.
- Splnění elektrotechnických a požárních předpisů.
- Zajištění vhodného prostředí pro všechny prvky PZTS.
- Zajištění redundance. (Kolouch, Bašta, 2019, s. 411)

3.3.1 Zajištění perimetru

V pojetí fyzické bezpečnosti se obvykle za perimetr považuje oblast, která bezprostředně obklopuje prostor, v kterém jsou chráněná aktiva (data, informace ale i prvky ICT).

Přesné vymezení toho, jaké části perimetru je potřeba mít pod kontrolou je otázkou provedení analýzy rizik, na základě které je také následně možné posoudit, jaké opatření v rámci jednotlivých prostor a aktiv je třeba zvolit k jejich účinné ochraně.

Perimetr je možné zajistit elektronickými systémy detekce pohybu, kamerovými systémy, či například společnou recepcí, která je schopna identifkovat a monitorovat jejích pohyb v rámci chráněného prostoru.

V případě využívaní kamerových systému je však třeba respektovat podmínky (zejména v rovině práva na ochranu osobních údajů) stanovené právními předpisy pro využívání těchto systémů. (Kolouch, Bašta, 2019, s. 411)

3.3.2 Kontrola přístupu

Kontrola přístupu zajišťuje, aby se přes perimetr dostaly pouze osoby k tomu oprávněné. Cílem kontroly přístupu je chránit aktiva (ICT systémy, data, informace) před neoprávněnými zásahy do nich.

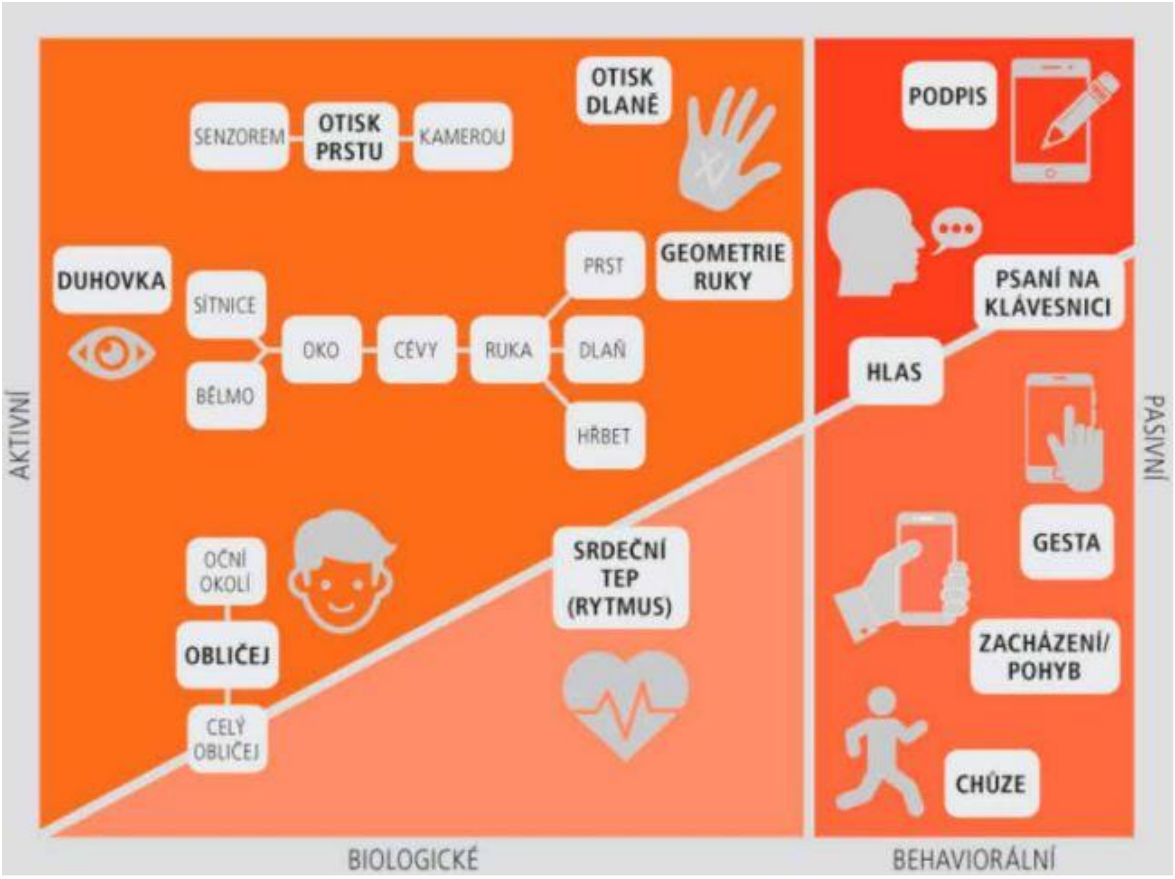
Mechanismů pro kontrolu přístupu a jejich kombinací existuje celá řada. Počínaje klasickými zámky, přes elektronické systémy schopné registrovat docházku zaměstnanců, až po kontrolu lidskou ostrahou. Uvedená řešení je možné kombinovat, avšak při implementaci je třeba zohlednit výhody a nevýhody toho kterého řešení kontroly přístupu.

V případě výběru zámku je třeba pamatovat na to, že existuje šest bezpečnostních tříd (třídy 5 a 6 se běžně nevyužívají), které jsou definovány časem, který je potřeba k jejich překonání

za použití určité síly, zkušenost a nástrojů. Určitých případech je vhodné využívat systém generálního klíče, kdy zaměstnanec disponuje klíčem, který odemyká jeho kancelář, ředitel daného úsek pak může klíč, který mu umožní přístup do všech kanceláří jeho podřízených a ostraha objektu či ředitel firmy může mít k dispozici generální klíč, kterým v případě nouze odemkne jakékoliv dveře ve firmě.

V případě kontroly přístupu pomocí elektronického systému je třeba zvážit, jaký účel je primárně sledován. Zda jde pouze o kontrolu přístupu osoby vlastnící nějaký token (např. čip, kartu), či zda je smyslem tohoto elektronického systému současně i ověřit, že s tímto vstupním tokenem manipuluje její oprávněný držitel.

V praxi je možné nalézt systémy, které využívají přístupový kód, token, snímají biometrické údaje či kombinují uvedené varianty. Dále se lze setkat i se systémy využívající turnikety a branky, které by měly zajistit, že do budovy nemůže na jeden token vstoupit více než jedna osoba.



Obrázek 15 – Možnosti biometrické identifikace osoby;
Zdroj: Biometrie je více než otisk prstu - Hospodářské noviny, 2017

Z hlediska zajištění bezpečnosti aktiv je vhodné využívat kombinované systémy umožňující kontrolu přístupu za pomoci tokenu a druhotné autentizace (např. zadáním kódu, využitím biometrických údajů oprávněn osoby). Kombinovaný systém může zabránit zneužití tokenu například při jeho ztrátě či krádeži a zároveň eliminuje škody, kdy oprávněný uživatel například půjčí token jiné osobě.

Uvedené systémy je možné dále propojit například se systémy pro kontrolu docházky a systémy PZTS, což ještě zvyšuje možné kombinace jejich využití. (Kolouch, Bašta, 2019, s. 411-413)

3.3.3 Vnitřní bezpečnost

Prostory určené pro uložení požadovaných aktiv je vhodné vybavit:

- Kombinovaný systém přístupu, který současně zaznamenává na jiný systém jednotlivé přístupy.
- Kamerovým systémem s automatickým zaznamenáním při detekci pohybu.
- PZTS napojeným na pult centrální ochran PCO nebo na dohledová a poplachová příjímací centrum (DPPC).
- Klimatizaci a zdroj nepřerušovaného napájení (UPS).
- Redundantním připojením na jiný záložní zdroj energie v případě delšího výpadku proudu (elektrocentrála).
- Vhodný hasicí přístroj. (Kolouch, Bašta, 2019, s. 415)

4 POUŽITÉ METODY PRO ANALÝZU RIZIK

Pro identifikaci hrozeb a zjištění rizik se používá různé druhy metod. Zde si shrneme jen ty, které použijeme v této práci. Jedná se o Ishikawův diagram pro analýzu problematiky projektování prvků PZTS, metodu SWOT pro analýzu aktuálního stavu PZTS v areálu a PNH metodu.

4.1 Ishikawa diagram

Tato metody, též zvaná jako diagram ryb kosti (Fishbone Diagram) slouží k předběžné kvalitativní analýze formou grafického znázornění. Pomáhá vytvořit model a strukturu procesu nebo identifikovat možná rizik, které můžou v dané problematice nastat. Určí nepravděpodobnější příčiny problému, který jsou následně řešeny a formou grafického znázornění jsou analyzovány příčinné faktory, které způsobují řešený následek. Každý faktor je možné dále analyzovat a vyhledat příčiny. (MANAGEMENTMANIA, 2015)

4.2 SWOT analýza

SWOT analýza je univerzální analytická technika zaměřená na zhodnocení všech vnitřních a vnějších faktorů, které ovlivňují úspěšnost organizace nebo konkrétního cíle. Je používaná jako situační analýza v rámci strategického řízení. Charakteristické rysy daného úkolu jsou děleny na silné stránky (Strenghts), slabé stránky (Weaknesses), příležitosti (Opportunities) a hrozby (Threats). (Vargová, 2018)

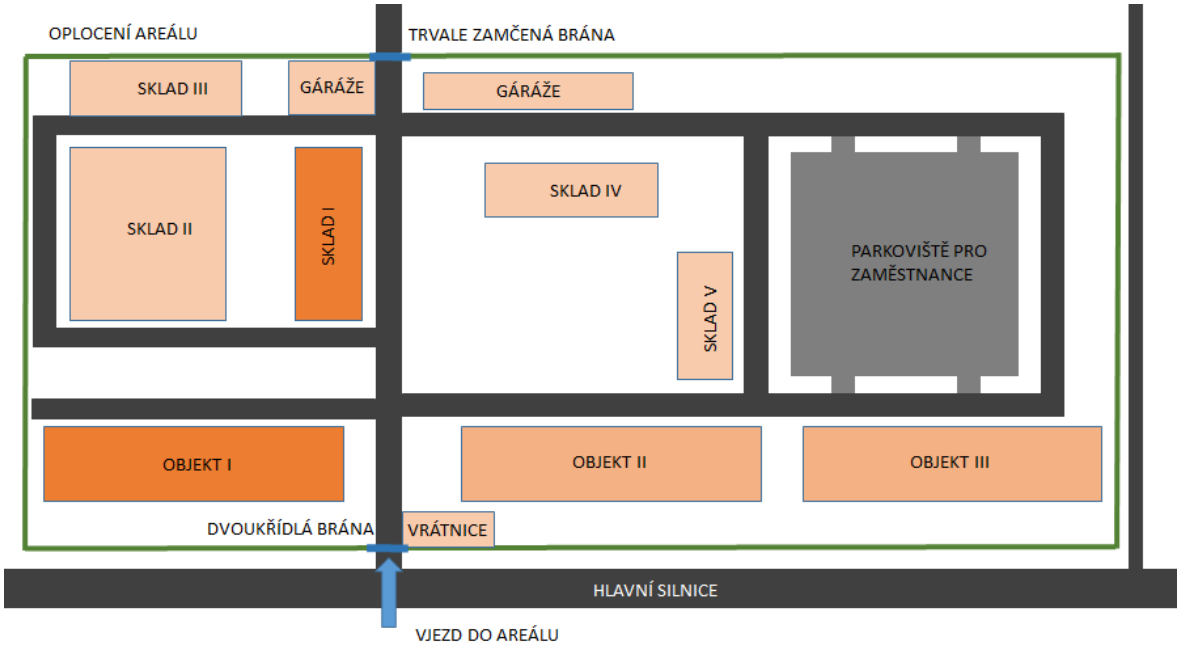
4.1 PNH metoda

Metoda PNH je jednoduchá polokvantitativní bodová metoda k vyhodnocení rizika. Tato metoda je použita k řešení a vyhodnocení daných rizik, které můžou nastat. Popisuje druh činnosti, které daný objekt může provádět, zdroje rizika, identifikaci nebezpečí a následné opatření, které by měli být přijaty k omezení rizika. (Koudelka, 2006)

II. PRAKTICKÁ ČÁST

5 POPIS OBJEKTU A JEHO SOUČASNÉ ZABEZPEČENÍ

Pro praktickou část byl vybrán reálný areál, ale bezpečnostních důvodů nebude uveden název ani lokace subjektu využívající areál. Jižní stranu areálu lemuje hlavní silnic ve městě, kde se nachází hlavní vchod do areálu. Ze západní strany je areál obklopen soukromými objekty. Na severní straně se nachází pozemky dalších firem. Na východní straně se nachází cesta a soukromá firma.



Obrázek 16 – Půdorys areálu;
Zdroj: (vlastní zpracování)

Celková plocha areálu je přibližně 50000 m^2 a skládá se z předních budov pojmenované objekt I., II., III., které fungují převážně jako kanceláře, šatny a učebny. Ostatní budovy v areálu jsou sklady materiálu a garáže.

Objekt I je po kompletní rekonstrukci a v celé budově je zapojen systém PZTS. Skládá se ze tří pater a vstupuje se pouze s platnou čipovou kartou. Objekty II. a III. čeká rekonstrukce a aktuálně, zde chybí prvky PZTS. Sklad I. Obsahuje prvky PZTS jako jediný z důvodu uložení aktiv. Ostatní sklady obsahují různé druhy materiálu a jsou zabezpečeny mechanickým zábranným systémem a pečetí o neporušení.

Hlavním chráněným zájmem je materiál, který je umístěn v objektu I. a skladu I., v zabezpečené místnosti. Zde jsou uloženy IP šifrátory pro zabezpečené videokonference a hlas, a další prvky pro zajištění šifrované komunikace v hodnotě více než 50 000 000 Kč.

Pak je zde další množství různého materiálu na dalších skladech jako pneumatiky, náhradní baterie do vozidel, skříně a různé druhy elektro zařízení jako počítače, projektory, notebooky, radiostanice a elektro instalační materiál.

5.1 Klasická ochrana obvodová

Oplocení je situováno po celém obvodu areálu a jeho obvod je 1000m. Oplocení je vyznačeno na obrázku č. 15 zelenou barvou. Tvoří hranici pozemku v kombinaci plechového oplocení s kovovými sloupky po většinu areálu a kovového designového oplocení do výšky 2m osazené v betonovém tarasu z jižní strany areálu. Jako vrcholová zábrana je použit ostnatý drát kromě jižní strany. Hlavní bránu tvoří dvoukřídlá železná brána. Pro otevření brány je zapotřebí fyzického kontaktu ochranné směny na vchodu. Po obvodu není použito žádné PZTS.

5.2 Klasická ochrana plášťová

Konstrukce objektů je cihlového charakteru. Plášť budovy tvoří stavební prvky a okna s dveřmi. U objektů se nachází podzemní prostory. Objekt I. má okna opatřená detektorem rozbití skla. Dveře ze severní strany jsou plastové bezpečnostní se skleněnou výplní. Na noc se dveře zamykají. Objekty II. a III. nemají bezpečnostní klávesnici a nejsou připojeny do centrálního PZTS. Dveře na budovách jsou opatřeny cylindrickou vložkou typu FAB.

5.3 Technická ochrana

K MZS jsou na plášti objektu I. a skladu I. umístěny kamery, které jsou umístěny u vchodů u objektu a vevnitř objektu. Přenos z kamer se ukládá do nahrávacího zařízení. Záznam slouží k zpětnému dohledání, dojde-li k bezpečnostnímu ohrožení či incidentu. Záznam se ukládá po dobu 2 měsíců. Na monitoru u velitele stráže je zobrazeno 9 kamer. Pro venkovní osvětlení jsou použity halogenové reflektory, ale s manuálním spínačem, chybí jim pohybové čidlo. Pro vstup do objektu I. a skladu I. slouží kódová klávesnice s blokovacím zámkem a také jsou vybaveny detektory pohybu a hlásičem požáru na chodbách. Každý zaměstnanec má vlastní čip a svůj přístupový kód do budovy. Ostatní objekty nemají systém PZTS a po pracovní době se jen zamykají na klíč strážnými. Na všech budovách jsou umístěné přístroje na hašení požáru podle požární ochrany.

5.4 Režimová ochrana

V areálu je stálá směna, která se skládá z 5 lidí ostrahy, která se střídá po 24 hodinových intervalech. Po konci pracovní doby provedou kontrolu zamčení všech budov a objekt I. elektronicky zastřeží. Je zaveden systém výdeje krabiček s klíči, které se ukládají do uzamykatelného boxu pomocí čipové karty. Klíče od budov jsou uloženy v schránce se sešitem, kde se zapisuje datum vypůjčení, jméno a příjmení, podpis a datum vrácení klíče dozorčímu. Hlavní brána se přes noc zamyká a klíče má uložené stráž na vchodu. Brána je po celou dobu zavřená, a otvírá se jen při příjezdu a výjezdu vozidel. Při tom je prováděna kontrola zavazadlové prostoru a kontrola osádky vozidla s povolením ke vstupu. Jednotlivé budovy jsou zamčené a klíče jsou uloženy u dozorčího areálu v krabičkách.

5.5 Fyzická ochrana

Stráž na vchodu chodí pravidelně každé 2 hodiny na obchůzku perimetru a po pracovní době na kontrolu uzamknutí u budov oken, dveří a vrat. Při tom jsou v kontaktu pomocí přenosné malé radiostanice. Přes den stráž kontroluje všechny osoby, co vcházejí do areálu, tím že se musí všichni legitimovat pomocí platné vstupní karty. Zaměstnanci cizích firem musí mít povolení ke vstupu jednorázové či krátkodobé, které jim je vystaveno předem nebo při příjezdu vedením areálu.

5.6 Zranitelnost objektu a jeho hrozby

Pachatel může se do areálu dostat přes některé části plotu například přední část. Sklady obsahuji minimální množství oken o malých rozměrech, ale klasické otevírací vrata s cylindrickou vložkou typu FAB. Objekty I. až III. mají velké množství oken, které jsou přístupné, ale na objektu I. jsou okna a dveře vybaveny detektory a kamerovým systémem. U objektu II. a III. tento systém zatím chybí a u skladů II. až V., v kterých ještě neproběhla modernizace. Možným pachatel může být i zaměstnanec, který je obeznámen se situací v areálu.

6 POUŽITÍ METOD ISHIKAWA DIAGRAMU, SWOT ANALÝZY A PNH

Pomocí legislativy ČSN EN 50131-1 ed. 2 Poplachové systémy jsme určily základní příčiny, které ovlivňují projektování a funkčnost systému PZTS. Tu jsme pak aplikovali v metodách analýzy pomocí Ishikawa diagram pro projektování PZTS a metoda SWOT pro analýzu rizik, které můžou nastat v zmíněném areálu. Dále jsme zhodnotily rizika projektování zabezpečení objektu PNH metodou. Ta se skládá z různých druhů metod, které vedou k určení povahy rizika a jeho úrovně. Riziko může být přijatelné, kterému nemusíme věnovat pozornost a nepřijatelné, pro které by měla být přijata opatření.

Tabulka 6 – Postup při analýze rizik;
Zdroj: (vlastní zpracování)

Analýza rizik
Identifikace aktiv
Stanovení hodnoty aktiv
Identifikace hrozeb a slabin
Stanovení závažnosti

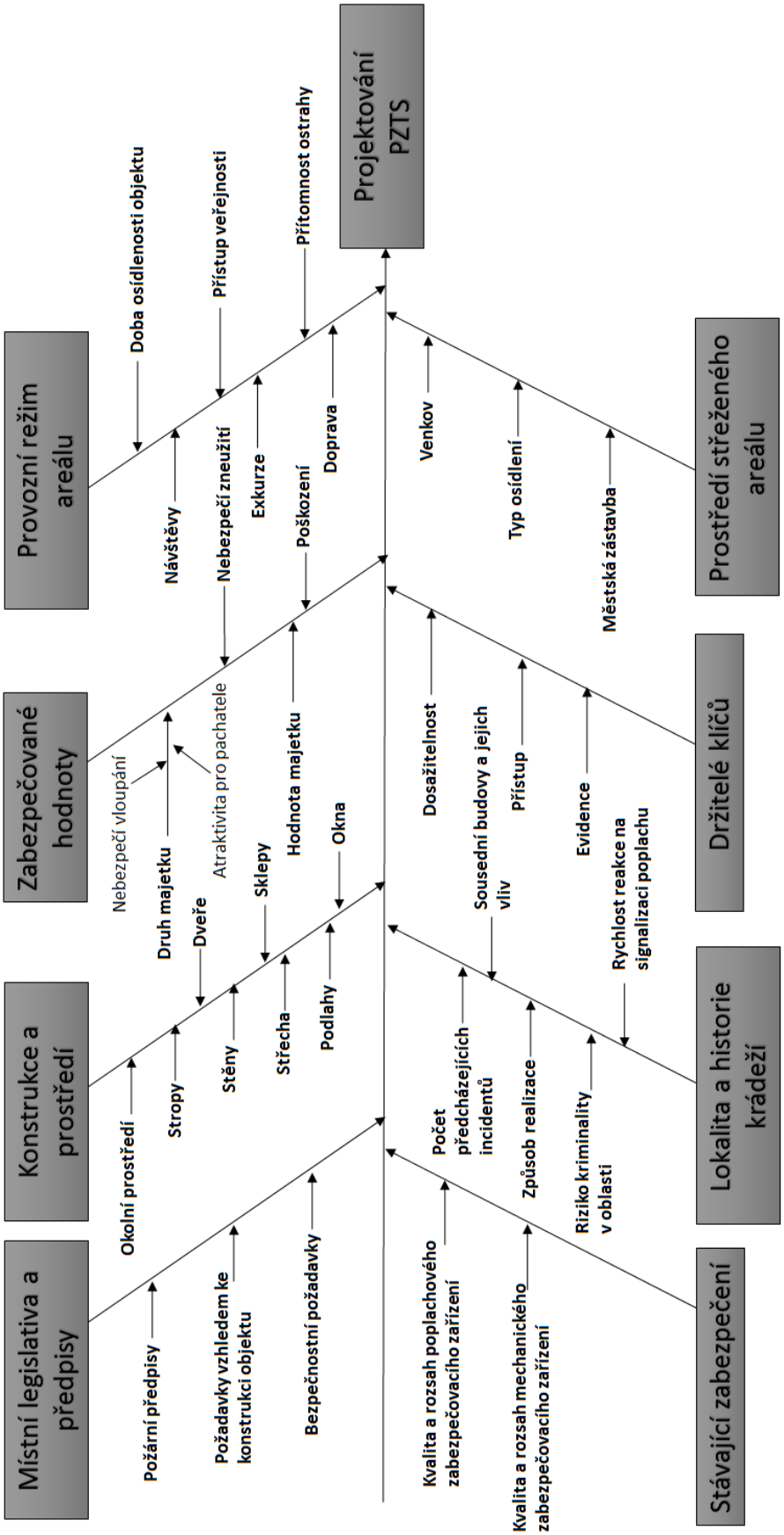
6.1 Identifikace aktiv

Aktiva je označení pro majetek či hospodářské prostředky, které jsou předmětem ochrany. Je to především takový majetek, který má vyšší hodnotu. Aktiva můžou být nehmotné, jako například informace či software, nebo hmotné kam můžou patřit nemovitosti, cennosti, elektronická zařízení, peníze atd.

6.2 Ishikawa diagram

Pro analýzy rizik jsme použily metodu brainstormingu a popisu projektování PZTS podle normy a ty následně doplnily do Ishikawa diagramu.

Na obrázku 17 je graficky znázorněná souvislost mezi následkem a možnými příčinami. Ishikawův diagram neboli diagram rybí kosti, též známý jako diagram příčin a následků. Tento diagram je vhodný pro zjištění příčin, které mohou vést ke konkrétnímu problému.



Obrázek 17 – Ishikawa diagram;

Zdroj: (vlastní zpracování)

Pomocí Ishikawa diagramu jsme provedly zjištění problematiky projektování PZTS, pomocí příčin (skupin), které ovlivňují vytvoření a modernizaci projektu PZTS.

- Místní legislativa a předpisy.
- Konstrukce a prostředí.
- Zabezpečované hodnoty.
- Provozní režim areálu.
- Stávající zabezpečení.
- Lokalita a historie krádeží.
- Držitelé klíčů.
- Prostředí střeženého areálu.

6.2.1 Místní legislativa a předpisy

Hlavní části legislativy je norma ČSN EN 50131-1 ed. 2 Poplachové systémy - Poplachové zabezpečovací a tísňové systémy**.** Ta určuje bezpečnostní požadavky, které se dodržují při návrhu a následném provozovaní PZTS, dále kvůli ochraně zaměstnanců a všech osob, co se pohybují v areálu, ovlivňují také požadavky ke konstrukci areálu, kdy je potřeba udržovat funkčnost všech prvků pomocí pravidelných kontrol a revizí a dodržování požárních předpisů pro zajištění funkčnosti systému a minimalizace závad a ohrožení např. zkratem elektrického zařízení s následkem požáru. Z důvodu, že některé prvky PZTS můžou mít problém s venkovním použitím a vnitřním, uzpůsobenost pro použití ve vlhkém prostředí a teplotou.

6.2.2 Konstrukce a prostředí

Je děleno na venkovní oplocení areálu, stěny budov, střech, podlah, stropu, sklepu, oken, dveří a okolního prostředí. U oken možnost doplnění mřížemi, detektory rozbití skla, u dveří zase detektor pro kontrolu otevření a uzamknutí. Obvodová ochrana je prvotním prvkem, který může zabránit napadení či krádeži, proto by neměla být nikdy podceňována možnost soustředění detekčních prvků PZTS ve větším množství už v zmíněné obvodové ochraně. Pro ploty nebo obvodové zdi je vhodná kombinace železo a betonu s doplněním o aktivní (čidla) a pasivní (ostnatý drát) ochranné prvky.

6.2.3 Zabezpečené hodnoty

Zabezpečené hodnoty se určí podle druhu majetku, jemuž hrozí nebezpečí vloupání a podle jeho atraktivity, dále podle hodnoty majetku v areálu, poškození a nebezpečí zneužití. Také ji ovlivňuje celková cena, kterou je majitel investovat do zabezpečení areálu. V objektu I. a ve skladu I., se nacházejí zabezpečené místnosti, kde hodnota aktiv je přibližně 50 000 000 Kč. K tomu jsou další budovy v areálu, kde se nalézají různé sklady materiálu, jehož ztráta už ale neohrožuje bezpečnost informací. Jsou to například pneumatiky, přenosné klimatizace, skříně, spojovací materiál a nábytek

6.2.4 Provozní režim areálu

Provozní režim areálu se určuje pracovní dobou zaměstnanců v areálu (například 3x8 hodinový provoz), nepřetržitou přítomnosti ostrahy, možnostech přístupu veřejnosti do areálu, a různých návštěv, exkurzí, a dopravy. Například den otevřených dveří, může způsobit hrozbu, kdy do areálu může proudit dav lidí, které nejsou prověřeny. Tímto by bylo vhodné doplnění vchodu o turnikety a bezpečnostním rámem a termokamerou pro omezení rizika. Pro zaměstnance by bylo vhodné doplnit vstup o turniket s čtečkou RFID karet, pro zajištění bezpečnosti a metod identifikace. Na hlavní vstupní bráně, by bylo vhodné zavedení karet pro automobily s čipem RFID, a automatickou závorou s čtečkou.

6.2.5 Stávající zabezpečení

Ovlivňuje budoucí část modernizace projektu PZTS, u které záleží v jaké kvalitě a rozsahu jsou stávající mechanické zabezpečovací zařízení a poplachové zabezpečovacího zařízení a jak moc velká část se z nich dá použít při budoucí úpravě. To znamená, jestli je potřeba vyměnit stávající čidla a kabeláž, nebo musí být provedena kompletní výměna. Aktuálně je dostatečně zabezpečen jen objekt I. a sklad I., z důvodu uložení důležitých prvků v zabezpečené místnosti. Všechny počítačové prvky ve firemní infrastruktuře, jsou přidělené na určité místnosti a zodpovídají za ně osoby, jejíž jména vždy visí na štítku kanceláře. Na přihlášení do služebních počítačů má vytvořený každý zaměstnanec účet s heslem, které se musí každé tři měsíce měnit. Heslo obsahuje minimálně 10 znaku, minimálně jedno číslo a jeden znak musí být velký. Vždy při odchodu z místnost musí zaměstnanec zamknout účet nebo se ohlásit z počítače, aby zamezil přístupu cizí osoby k místní síti.

6.2.6 Lokalita a historie krádeží

Projektování PZTS také ovlivňuje lokalita umístění areálu, její sousední budovy, nebo také historie předchozích krádeží, které v okolí nebo v daném areálu za určité období nastali. Důležitou položkou v projektu je taky rychlost reakce na signalizaci poplachu, kdy záleží na stráži, jestli je dostupná v areálu nebo se musí spoléhat na externí bezpečnostní agenturu, která ale musí přijet z okolí.

6.2.7 Držitelé klíčů

Držitelé klíčů se určují z řad zaměstnanců, kteří obdrží možnost povolení k přístupu do určených objektů a způsoby, jak se bude zajišťovat evidence osob a klíčů, a jejích vydávaní. Možnosti vydávání a potvrzení má na starost bezpečnostní správce místní lokální správy v areálu, který musí každý rok seznámit všechny zaměstnance pomocí školení a podpisového archu, že absolvovaly školení o bezpečnosti a ochraně pomocí zdravotních pomůcek. Zároveň je zakázáno zapojovat cizí zařízení jako USB klíčenky a pevné disky, neschválené od bezpečnostního správce do místní sítě. Každý půlrok se provádí bezpečnostní audit pro všechny počítače a notebooky, pro případ kontroly.

6.2.8 Prostředí střeženého areálu

Pomocí diagramu příčiny a následku, jsme určily, jaké parametry jsou potřeba pro projektování PZTS, kde se nachází subjekt. V jakém prostředí může být provozován a to buď na venkově, v městské zástavbě a také záleží na typu okolního osídlení. Podle toho se musí řešit zabezpečení areálu například v městské zástavbě je menší šance na krádež, ale zvýšená šance na vandalismus. Problém může nastat i například závadou na elektroinstalaci a následným požárem okolních budov, který se může přenést na zmíněný areál. Každá budova má na přístupném místě nachystané prvky požární ochrany jako hasičské přístroje. K tomu je zpracovaná směrnice pro příjezd Hasičského záchranného sboru a na všech budovách zpracován Požární únikový plán, který je vždy vyvěšen na chodbě.

6.3 SWOT analýza

Tato analýza slouží ke zjištění silných a slabých stránek v zabezpečení objektu. Cílem této analýzy je zjištění všech současných rizik a stavu střeženého objektu. V tabulce č. 7 jsou specifikovány silné a slabé části (interní části) a příležitosti s hrozbami (externí části).

Tabulka 7 – SWOT analýza;

Zdroj: (vlastní zpracování)

SILNÉ STRÁNKY	**SLABÉ STRÁNKY**
❖ Kamerový systém ❖ Prvky PZTS na budovách ❖ Zabezpečení oken a hlavních dveří ❖ Strážní směna ❖ Pult centralizované ochrany	❖ Snadno překonatelné oplocení ❖ Slepá místa ❖ Chybějící detektory na plotu areálu ❖ Nižší citlivost kamer v noci ❖ Omezené metody identifikace
PŘÍLEŽITOSTI	**HROZBY**
❖ Kvalitnější oplocení ❖ Hlídací pes ❖ Slepá místa vykrýt kamerou ❖ Kvalitnější kamerový systém ❖ Vylepšení systému kontroly vstupu	❖ Krádež ❖ Požár ❖ Napadení ❖ Výpadek napájení ❖ Falešné poplachy

Silné stránky

Mezi silné stránky v zabezpečení objektu patří již vybudovaný kamerový systém, který monitoruje objekt I., sklad I. a vnitřní část areálu. Díky nahrávanému záznamu lze zpětné dohledat a přehrát si nedávné události, které byli zaznamenány. Velkou výhodou je přítomná strážní směna v areálu, která se stará nepřetržitě o ochranu areálu. Dále jsou okna v přízemí opatřeny mřížemi na většině budov. Areál obsahuje také pult centralizované ochrany, kde má před sebou na monitorech dohledový pracovník kamerové systémy a systém PZTS s hlavní ústřednou a ovládacími prvky.

Slabé stránky

Mezi slabé stránky patří snadno překonatelné oplocení z přední strany areálu, které má na výšku 2m a není opatřeno aktivní (čidla) ani pasivní (ostnatý nebo žiletkový drát) ochranou. U vchodu a na bráně jsou omezené metody identifikace osob pomocí vstupní identifikační karty a pro auta jsou vystavena povolení k vjezdu. Bylo by vhodné vytvořit turnikety se čtečkou na vstupní identifikační karty pro vstup do areálu z důvodu velkého množství počtu zaměstnanců. Dále jsou v areálu slepá místa, kde nejsou žádné sledovací kamery ani

detektory, čímž zde hrozí riziko neoprávněného vstupu či napadení. Navíc u některých kamer chybí noční přísvit a v noci mají omezené rozlišovací schopnosti.

Příležitosti

Mezi příležitosti patří úprava plotu na kovovou konstrukci s doplněním o aktivní prvky (specifické čidla) a pasivní prvky (ostnatý drát). Ochranné prvky perimetru kontrolují porušení či pohyb v blízkosti monitorované oblasti. Dále by bylo vhodné zřídit kvalitnější kamerový PTZ systém, který umožnuje natočit, sklonit a přiblížit na neidentifikovaný subjekt podle potřeby i se zaostřením, a také kvůli vykrytí slepých míst. Dále je třeba vzít v potaz vylepšení systému kontroly vstupu jako např. turnikety se čtečkami karet a termo kamery pro měření teploty.

Hrozby

Hrozbami můžou být různé krádeže materiálu ze strany cizích osob nebo z řad vlastních zaměstnanců. Dále může vzniknout požár například při zkratu elektrického napájení nebo nedopalkem z cigarety. Zaměstnavatel by měl zvážit zřízení míst určených ke kouření kde je minimalizované riziko požáru. V případě výpadku elektrického napájení by měly být spotřebiče zajištěné zdroji UPS a celá síť elektřiny by měl být napojena energo-centrálu. Iniciátory tzv. falešných poplachů, mohou být různá zvířata, ptáci či nepříznivé povětrnostní podmínky, které můžou způsobit například poškození oken nebo zařízení budov. V extrémních případech může dojít zaplavení sklepních prostor budov. Je třeba také vzít v úvahu možné riziko výtržnictví a vandalismu ze strany civilního obyvatelstva.

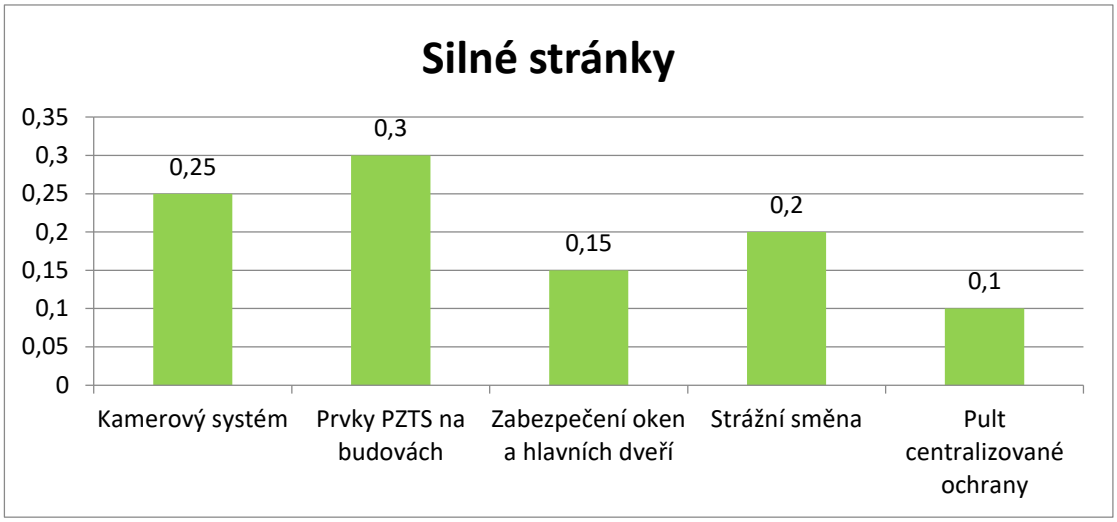
Vyhodnocení SWOT analýzy

Pro správné vyhodnocení je určena stupnice, podle které máme ohodnoceny všechny části. U silných stránek a příležitostí jsou ohodnoceny podle stupnice od čísel 1 až 5. Kde číslo 1 znamená nejnižší hodnocení a číslo 5 nejvyšší hodnocení. U slabé stránky a hrozeb jsou čísla -1 do -5. Podle důležitosti jednotlivých položek je jim přirazena váha, kdy její součet je vždy 1.

Tabulka 8 – Hodnocení SWOT analýzy;

Zdroj: (vlastní zpracování)

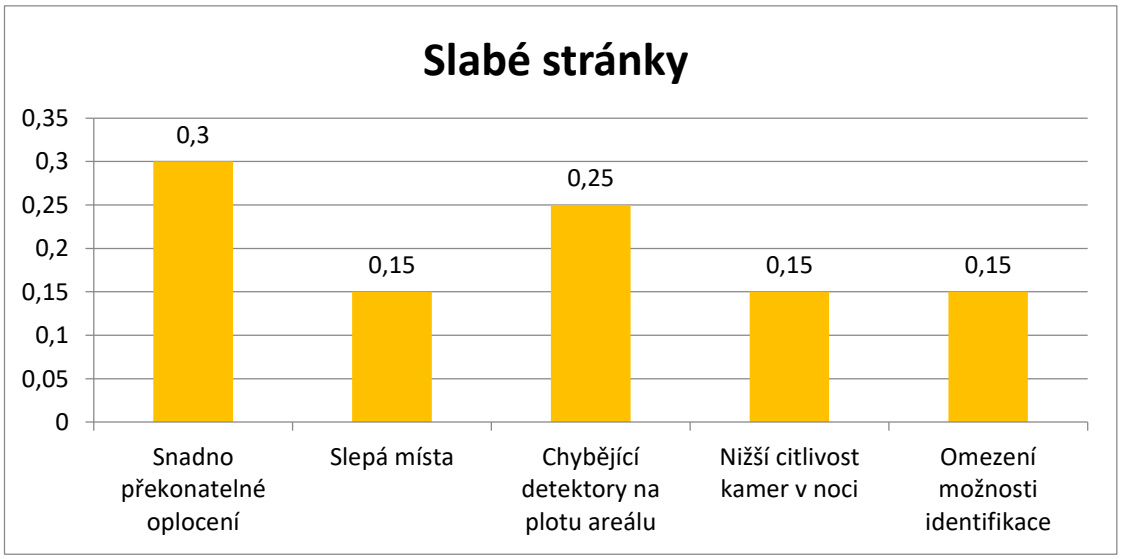
Faktory	**Váha**	**Hodnocení**	**Celkem**
Silné stránky			
Kamerový systém	0.25	4	1
Prvky PZTS na budovách	0.3	4	1,2
Zabezpečení oken a hlavních dveří	0.15	4	0,6
Strážní směna	0.2	3	0,6
Pult centralizované ochrany	0.1	2	0,2
		Celkový součet	**3,6**
Slabé stránky			
Snadno překonatelné oplocení	0,3	-3	-0,9
Slepá místa	0,15	-3	-0,45
Chybějící detektory na plotu areálu	0,25	-3	-0,75
Nižší citlivost kamer v noci	0,15	-2	-0,3
Omezení možnosti identifikace	0,15	-2	-0,3
		Celkový součet	**-2,7**
Příležitosti			
Kvalitnější oplocení areálu	0,3	5	1,5
Hlídací pes	0,1	2	1
Slepá místa vykrýt kamerou	0,15	3	0,45
Kvalitnější kamerový systém	0,2	3	0,6
Vylepšení systému kontroly vstupu	0,25	4	1
		Celkový součet	**3,55**
Hrozby			
Krádež	0,3	-3	-0,9
Požár	0,2	-2	-0,4
Napadení	0,2	-3	-0,6
Výpadek napájení	0,2	-5	-1
Falešné poplachy	0,1	-3	-0,3
		Celkový součet	**-3,2**



Obrázek 18 – Silné stránky areálu;

Zdroj: (vlastní zpracování)

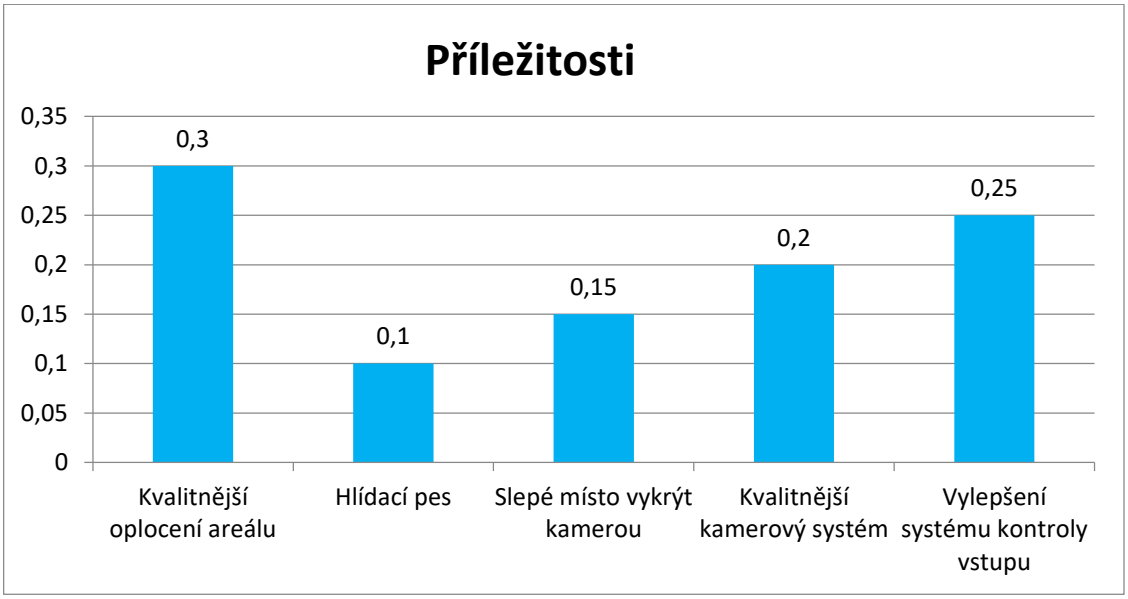
Nejsilnější stránkou zabezpečení objektu v rámci areálu jsou prvky PZTS a kamerový systém. Jak bylo zmíněno výše, mezi silné stránky zabezpečení objektu patří kamerový systém, který byl v nedávné minulosti modernizován a dále prvky PZTS na objektech, které jsou rovněž na velmi vysoké úrovni, co se týká citlivosti pohybu, a to i ve tmě. Zabezpečení oken a hlavních dveří je na funkční úrovni a účinné v přízemí a v 1. NP, kde jsou instalovány kovové mříže. V areálu je také zřízena 24 hodinová monitorovací směna, která provádí předepsané obchůzky ve stanovených časech. Řídící pracovník monitorovací směny má také k dispozici pult centralizované ochrany, ze kterého může pohybovat některými kamerami.



Obrázek 19 – Slabé stránky areálu;

Zdroj: (vlastní zpracování)

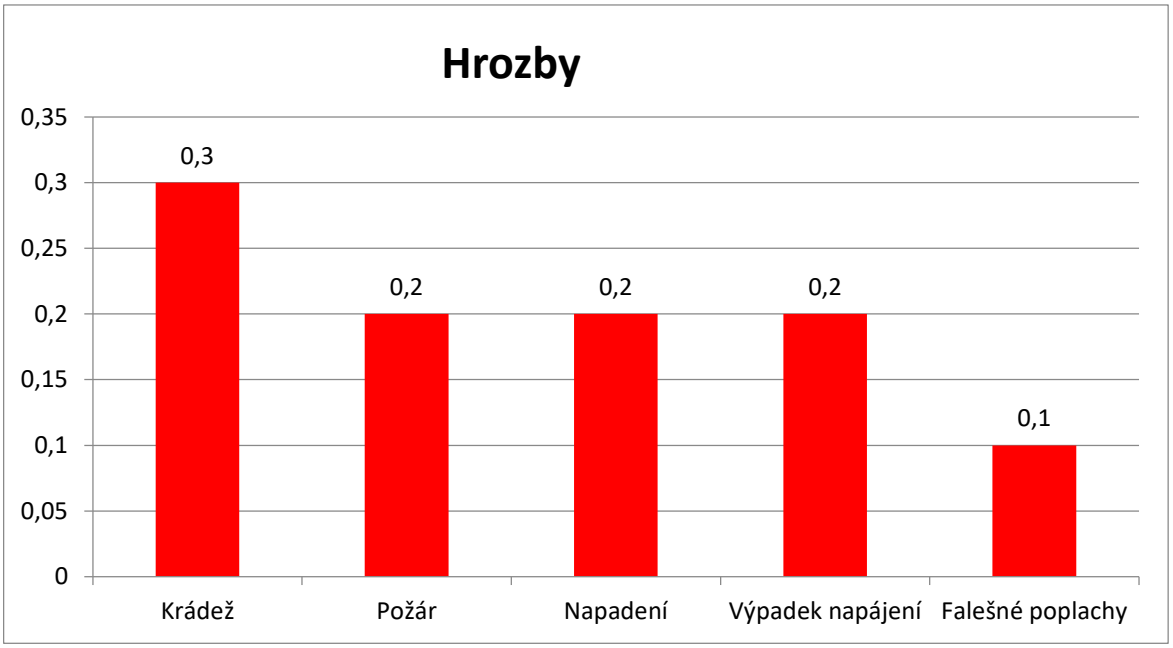
Jak bylo avizováno výše, nejvíce alarmující slabou stránkou je snadno překonatelné oplocení s absencí prvků aktivní (čidla) a pasivní (ostnatý drát) ochrany. Zároveň by se bezpečnostní manažer areálu měl zabývat kamerovým systémem a slepými místy, které nedokáže systém pokrýt. Rovněž je třeba zmínit nižší citlivost kamerového systému ve tmě z důvodu absence infra přísvitu. Při vstupu do areálu chybí identifikační turniket nebo jiná čtečka karet, která by zaměstnance okamžitě autorizovala. Rovněž chybí termo-kamerový systém.



Obrázek 20 – Příležitosti areálu;

Zdroj: (vlastní zpracování)

V rámci investice do zabezpečení areálu se v této SWOT analýze mezi příležitostmi nabízí zřízení kvalitnějšího oplocení areálu, které bude disponovat aktivní i pasivními bezpečnostními prvky. Rovněž je potřeba zřídit identifikační turnikety, jednak pro konkrétní autorizaci zaměstnanců, a také pro identifikaci vozidel vjíždějících do areálu. Mezi příležitosti pro vylepšení monitorovacího systému v areálu je nabízí modernizace kamerového systému, která by zároveň vykryla slepá místa, kde kamery nemonitorují. Za zvážení také stojí pořízení hlídacího psa, který je však náročný jak z časového, tak finančního hlediska.



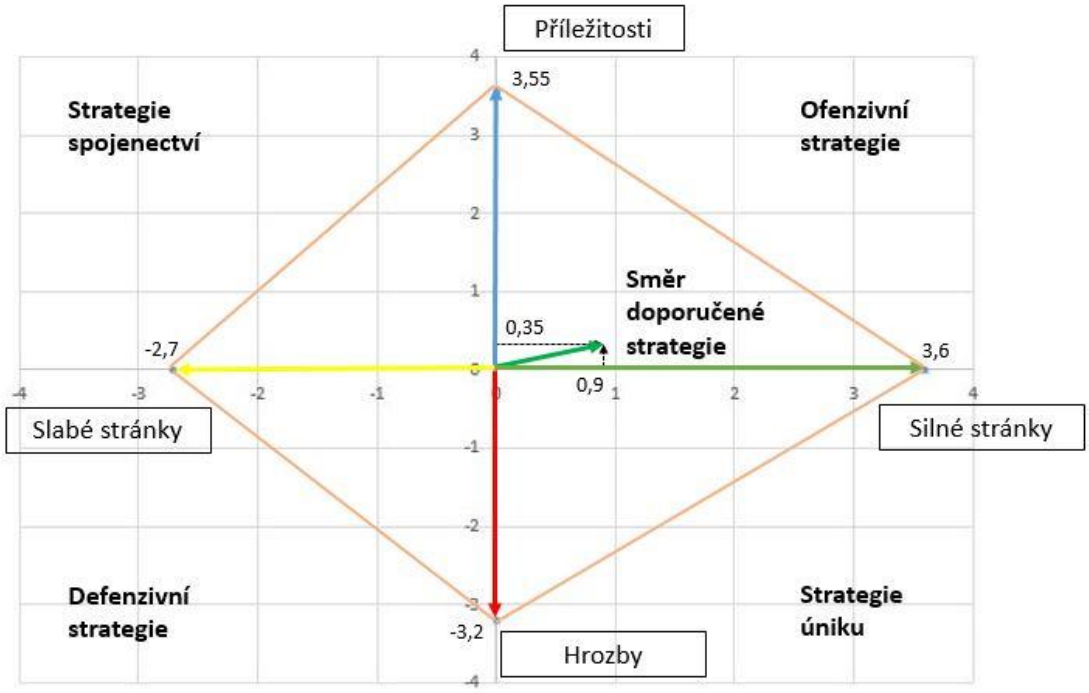
Obrázek 21 – Hrozby areálu;
Zdroj: (vlastní zpracování)

Výše zmíněné příležitosti by mohly za správných okolností zmírnit následující bezpečnostní hrozby, mezi které patří zejména krádeže movitého majetku zaměstnavatele, ať už z řad vlastních zaměstnanců nebo z řad obyvatelstva. Rovněž je potřeba minimalizovat vznik požáru v areálu investicí do elektronických požárních poplachových zařízení. Monitorovací směna by měla dále podstoupit kurzy sebeobrany pro minimalizaci rizika napadení. Výpadky napětí by mohly být eliminovány nákupem záložních energo-centrál a UPS zařízení. Falešné poplachy – viz definice výše, by bylo možno eliminovat periodickým školením zaměstnanců a pravidelné cvičné poplachy, které by prověřovaly monitorovací směnu.

Tabulka 9 – Vyhodnocení SWOT analýzy;
Zdroj: (vlastní zpracování)

Vyhodnocení SWOT analýzy			
Silné stránky – Slabé stránky	3,6	-2,7	**0,9**
Příležitosti - Hrozby	3,55	-3,2	**0,35**

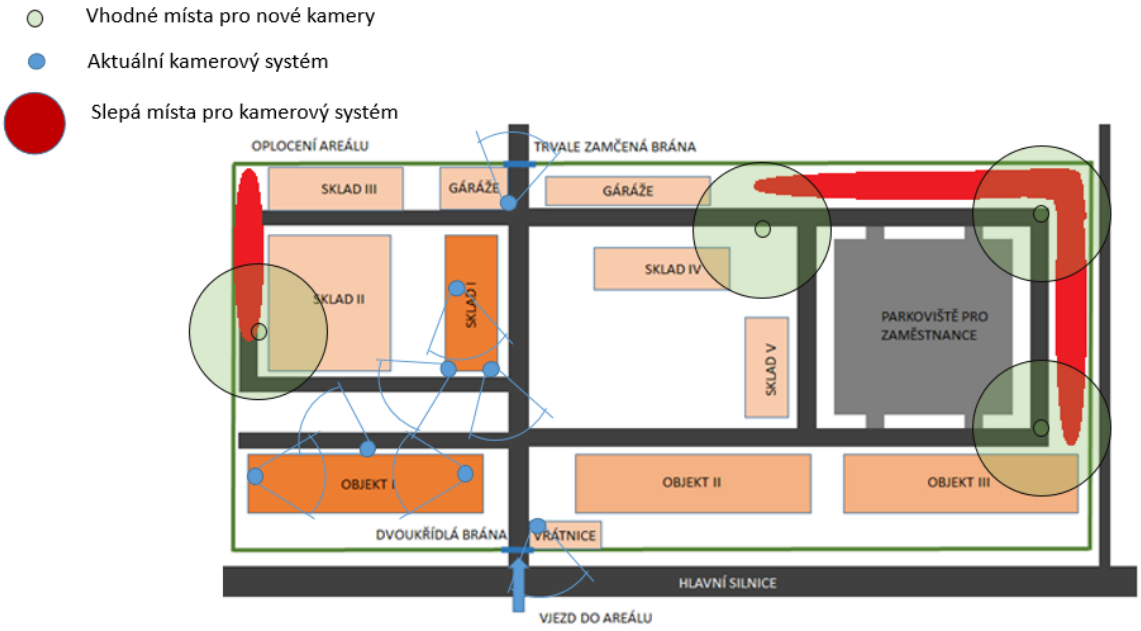
Zadáním hodnot do matice modelových strategií nám určí přesný typ strategie, kterým by se měl areál řídit pro zabezpečení areálu.



Obrázek 22 – Matice modelových strategií v grafu;
Zdroj: (vlastní zpracování)

Vyhodnocením všech parametrů SWOT analýzy je patrné, že silné stránky převažují nad slabými a příležitosti nad hrozbami, jedná se tedy o strategii ofenzivní (SO). Ofenzivní strategie nám říká, že bychom se měli soustředit na příležitosti za pomocí našich silných stránek.

Příležitosti se nalézají v doplnění o kvalitnější oplocení areálu s využitím detektorů narušení perimetru a doplnění o ostnatý drát. Modernizace vstup do areálu s doplněním o turnikety s čtečkou čipových karet. Přitom se využije již existujícího kamerového systému, který bude doplněn o novější VSS zařízení s funkcí PTZ a infra přísvitem pro lepší rozpoznatelnost osob, zvířat a předmětů v noci.



Obrázek 23 Vhodné doplnění PTZ kamer pro vykrytí slepých míst v areálu;
Zdroj: (vlastní zpracování)

I v dalších objektech by byl vhodné pokračovat v doplnění o zabezpečení všech oken, dveří, které se nalézají v přízemi a v 1. patře. Objektech II. a III. by bylo vhodné provést modernizaci prvků PZTS na úroveň v objektu I, ať už na chodbách a místnostech vhodným doplněním o detektory pohybu. Z důvodu velkého množství kanceláří, kde jsou počítače a prvky uzavřené firemní síťové infrastruktury, které můžou narušit bezpečnost informací v areálu. Výhodou je pult centralizované ochrany, která ihned spustí poplach při nesprávné použití čtečky karet a hesla u objektu I. a skladu I., a podle směrnice je ihned vyslána na místo strážní směna, kterou určí centrální dohled. V areálu je 5 členů strážní směny, kteří pracují v 24 hodinových směnách. A disponují technickými prostředky pro sebeobranu a zajištění ochrany areálu.

6.4 Metoda PNH

Metoda PNH je jednoduchá polokvantitativní bodová metoda, která slouží k vyhodnocení rizik, které můžou u daného objektu zájmu nastat. Tato metoda je použita k řešení a vyhodnocení daných rizik k zajištění bezpečnosti informací u areálu kasáren. Vyhodnocení rizik je provedeno v následující tabulce.

Tabulka 10 – Vyhodnocení metody PNH;

Zdroj: (vlastní zpracování)

Druh činnosti	Zdroje rizika	Identifikace nebezpečí	Vyhodnocení závažnosti rizika				Opatření k omezení rizika
			P	N	H	R	
Zaměstnanci	Krádež	Škoda na majetku a ohrožení bezpečnosti informací	4	2	5	40	Doplnění prvků PZTS v celém areálu a kontrola zaměstnanců
	Neodbornost	Škoda na majetku.	2	5	3	30	Pravidelné školení
	Vstup neprověřené osoby	Nebezpečí a ohrožení bezpečnosti informací	4	3	3	36	Přísnější kontrola na vstupu
	Nezamčené okna, vrata a dveře	Ohrožení areálu	4	4	3	48	Kontrola areálu a přidání detektorů
	Ztráta klíčů	Hrozba zneužití	2	3	3	18	Schránka na klíče
Cizí osoby	Krádež	Škoda na majetku a ohrožení bezpečnosti informací	4	4	3	48	Pravidelné kontroly stráže a doplnění prvků PZTS na všechny budovy
	Napadení	Úraz, zranění nebo ohrožení areálu	2	5	4	40	Detektory a prvky pro kontrolu
Obvodová ochrana	Špatný stav oplocení	Možnost napadení, zranění	3	4	3	36	Opravení plotu
	Přelezení plotu	Možnost napadení, krádeže, zranění	3	5	3	45	Doplnění o ostnatý drát
	Plot bez systému PZTS	Možnost napadení nebo krádeže	4	3	4	48	Úprava plotu s doplněním o detektory
Fyzická ochrana	Indispozice strážného	Úraz nebo ohrožení na životě	1	4	3	12	Rádiová kontrola stráže a pravidelné zdravotní prohlídky
	Nepřítomnost stráže	Ohrožení areálu	5	4	3	60	Častější kontrola výkonu stráže
Plášťová ochrana	Překonání dveří	Škoda na majetku a napadení	3	3	3	27	Instalace detektorů na dveře
	Překonání oken	Škoda na majetku a napadení	3	2	3	18	Instalace detektorů na okna
	Překonání zámku	Škoda na majetku	2	3	4	24	Doplnění o kvalitnější zámky
Kamerový systém	Slepé místo	Nebezpečí krádeže nebo napadení	3	2	3	18	Doplnění o kameru nebo detektor
	Nepřítomnost obsluhy	Ohrožení areálu	1	5	4	20	Organizační opatření
Živelné pohromy	Požár	Škoda na majetku a zranění	4	3	3	36	Pravidelné revize elektrických prvků, instalace detektorů kouře a hasicích přístrojů
	Vichřice	Škoda na majetku a vznik poplachu	1	3	3	9	Kontrola zavření oken a stavu stromů
	Povodeň	Škoda na majetku	1	4	3	12	Pročištění kanalizace

Jednotlivé rizika byla ohodnocena podle stupnice v rozmezí 1-5 a navržena opatření k omezení rizika.

Riziko se hodnotí podle tří parametrů.

- P – pravděpodobnost vzniku.
- N – pravděpodobnost následků (závažnost nebezpečí).
- H – názor hodnotitele (hodnoceno kolektivem firmy pomocí metody brainstorming)

- R – celkové hodnocení rizika.

Celkové hodnocení je získáno součinem pravděpodobnosti vzniku, pravděpodobnosti následků a názoru hodnotitele.

$$\mathbf{R = P \times N \times H}$$

Tabulka 11 – Stupnice rizik;
Zdroj: Koudelka – Rizika a jejich analýza, 2006 (upraveno)

Rizikový stupeň	Celková hodnocení rizika	Míra rizika
I.	> 100	Nepřijatelné riziko
II.	Od 51 do 100	Nežádoucí riziko
III.	Od 11 do 50	Mírné riziko
IV.	Od 3 do 10	Akceptovatelné riziko
V.	< 3	Bezvýznamné riziko

Z dat získaných z tabulky 11 vyplynulo, že největší hrozbou je nepřítomnost stráže, která se řadí do kategorie číslo II. Proto je vhodné pravidelná kontrola stráže a výkonu jejich služby. V rizikovém stupni III, tedy v mírném riziku bylo ohodnoceno větší množství rizik. Od krádeže od vlastních zaměstnanců a cizích osob v areálu, kontroly uzamčení oken, dveří a vrat, dále také napadení zaměstnance, přelezení plotu cizí osobou, stavu oplocení, kde by byla vhodné doplnění o ostnatý drát po celém obvodu a chybějící detektory u plotu.

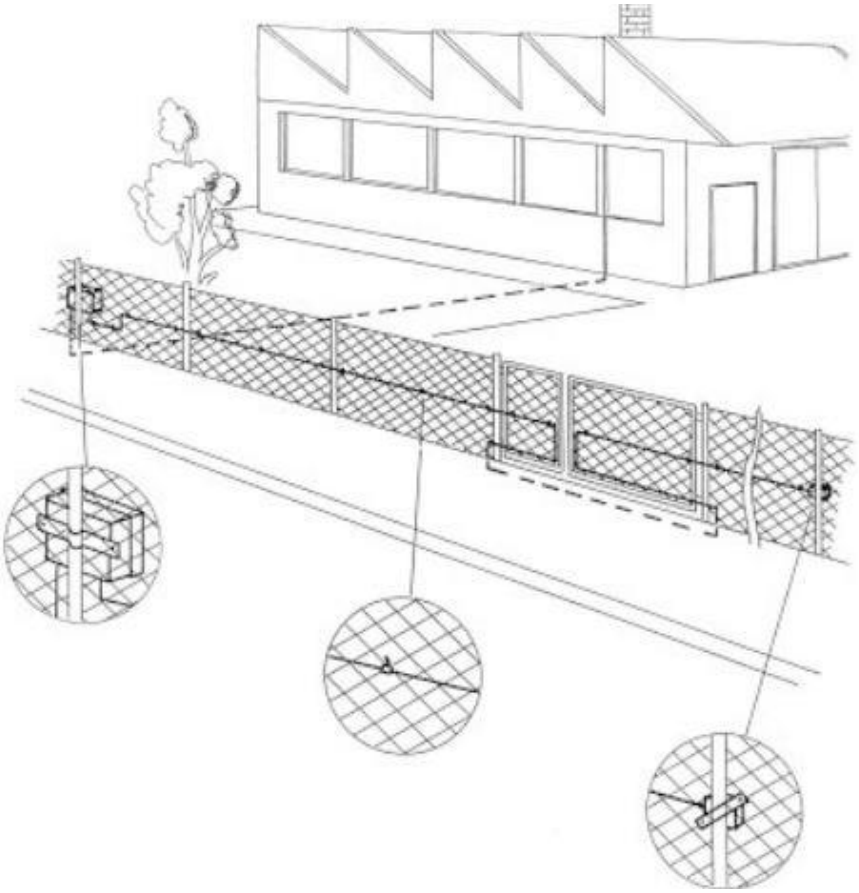
7 NAVRHOVANÁ OPATŘENÍ

V této kapitole budou navržena opatření k zajištění bezpečnosti informací u systému PZTS, které byli zjištěny u střeženého areálu. Navrhovaným vylepšením zabezpečení areálu budou zmenšeny a eliminovány hrozby, které byli zjištěny. V kombinaci se SWOT analýzou a PNH metodou se pokusíme soustředit na slabé stránky a hrozby.

Obvodová ochrana

Pomocí SWOT analýzy vyplynulo, že největší slabina v areálu je jeho oplocení, kde podél pozemku společnosti vede hlavní silnic. Zde se nachází oplocení, které nese známky mnohaletého použití a chybí mu aktivní a pasivní ochranné prvky. Dle mého názoru se jedná o bezpečnostní mezeru, kudy může případný zkušený narušitel vniknout do areálu společnosti. V rámci nákladů, které budou vynaloženy pro zlepšení PZTS doporučuji zahájit rekonstrukci plotu a doplnit jej o detekční systém a ostnatý drát. Například FP 300 (až 300m) nebo FP 600 (2x 300m). (*Plotový systém FP 300 a FP 600: Manuál*, 2020)

O skutečných nákladech při rekonstrukci plotu a doplnění o prvky detekčních systému se v této práci, nechci zmiňovat z důvodu časové a normativní náročnosti. Jen upřesním aktuální cenu jednoho prvku FP 300, která je 28394 Kč a FP 600 44 366 Kč. (HTV-HODINA, 2020)



Obrázek 24 – FP 600;
Zdroj: *Plotový systém FP 300 a FP 600: Manuál*, 2020

Další slabou stránkou je přítomnost slepého místa v areálu, u kterého chybí pokrytí kamerovým systémem a detektory. Na vyřešení tohoto problému by bylo vhodné zakoupit PTZ kameru s režimem den/noc a infračerveným přísvitem na vzdálenost 200 m. Přenos z kamery by byl přenášen do nahrávacího zařízení v administrativní budově. Pokrytím tohoto místa kamerou by došlo ke kompletnímu střežení areálu. Pro případnou modernizaci navrhuji koupit a nainstalovat na vysoký sloup, aby dokázala pokrýt co největší prostor. Například kameru DS-2DF8425IX-AEL - IP PTZ kamera 4MPix; 25x ZOOM; Hi-PoE; ICR+3D-DNR+IR do 200m od firmy HIKVISION. (Viakom.cz, HIKVISION, 2018)

O skutečných nákladech pro doplnění kamerových VSS prvků se v této práci, nechci zmiňovat z důvodu časové a normativní náročnosti. Jen upřesním aktuální cenu jedné zmiňované PTZ kamery, je 55699 Kč.

Obrázek 25 – Otočná kamera se zoomem a přísvitem;
Zdroj: (Viakom.cz, HIKVISION, 2018)

Plášťová ochrana

Nejslabším místem v zabezpečení plášťové ochrany je, že ne všechny budovy obsahují detektory PZTS. Pro plánovanou modernizaci je vhodné doplnit na budovách čidla pro detekci rozbití skla, a PIR čidla na chodbu a i do každé místnosti.

Pro doplnění prvků PZTS je vhodný do každé místnosti detektor JS-25 COMBO, který kombinuje detektor rozbití skla a PIR pohybové čidla. Toto čidlo bude zajišťovat, aby mimo pracovní dobu nikdo nemohl vstoupit do budov ani místností. A rovnou funguje jako detektor rozbití skla, takže zahlásí do systému PZTS i vnitřní napadení pomocí roztříštění

skla v místnosti. Celkový počet by záležel na přesném počtu místností a chodeb, které by bylo vhodné zabezpečit a to v rozsahu 30 až 70 místností a doplněním na sklady.

O skutečných nákladech pro doplnění prvků PZTS do místností a chodeb se v této práci, nechci zmiňovat z důvodu časové a normativní náročnosti. Jen upřesním aktuální cenu jedné zmiňované jednoho kombinované čidla JS-25 1264 Kč. (Jablotron, 2020)

Obrázek 26 – Detektor JS-25 COMBO;
Zdroj: *Jablotron, 2020*

Technická ochrana

Pro kontrolu vstupu a odchodu osob by bylo vhodné vybudovat v hlavních vchodu turniket se snímači čipových karet, který by sloužil k identifikaci osob, které vstupují do areálu a díky čtečce RFID karet, by bylo možné vést statistiky o celkovém počtu zaměstnanců pohybujících se v areálu, jestli přicházejí do zaměstnání včas a neopouští areál bez povolení mimo vyhrazenou dobu. K tomu by bylo vhodné pro vjezd vozidel do areálu, mít dálkově ovládanou závoru po akceptaci čipové karty řidiče, tak vozidla.

Instalací turniketu automatického, včetně signalizace potvrzení identifikace oprávněné osoby s pomocí RFID karty, zamezíme vstupu nepovolaných osob do areálu. Výhody

turniketu jsou funkce jako obousměrný průchod, indikátor povolení a zamezení vstupu, možnost dálkového ovládání přes externí tlačítko. (Turniket, AZ pohony, 2020)

O skutečných nákladech pro instalaci turniketů se v této práci, nechci zmiňovat z důvodu časové a normativní náročnosti. Jen upřesním aktuální cenu zmíněného plně automatického turniketu bez připojené čtečky RFID karet a to je 31 720 Kč. (AZ Pohony, 2020)

Obrázek 27 – Plně automatický turniket;
Zdroj: (Turniket, AZ pohony, 2020)

Fyzická ochrana

Největší hrozbou podle metody PHN, byla zhodnocena nepřítomnost stráže. Tomu se můžeme vyhnout, pomocí určení pravidelná kontroly stráže a výkonu jejich služby a přenosnou osobní radiostanicí s GPS prvky.

ZÁVĚR

Bakalářská práce si kladla za cíl analyzovat a zhodnotit poplachové zabezpečovací a tísňové systémy k zajištění bezpečnosti informace. Čerpal jsem při ní převážně z knih Bezpečnostní technologie, systémy a management, dílů I. až V.

V první teoretické části jsme si na úvod představili prvky PZTS, VSS a jejich normy.

Další teoretická část objasnila bezpečnost informací od identifikace hrozeb, fyzické bezpečnosti po použité metody analýzy rizik, jako je Ishikawa diagram či SWOT analýza.

Následně jsem v této práci na konkrétním příkladu prakticky znázornil daný areál s popisem současných prvků zabezpečení. Identifikoval jsem problematiku projektování PZTS pro zajištění bezpečnosti informací pomocí Ishikawa diagramu a popsal možné bezpečnostní riziko. Pro volbu strategie postupu pomocí SWOT analýzy jsem zjistil silné a slabé stránky nynějšího zabezpečení areálu, metodou PNH jsem zhodnotil rizika, které můžou nastat v areálu, a pro zlepšení a zefektivnění tohoto stavu jsem navrhl technická opatření k zajištění bezpečnosti informací pomocí prvků poplachových zabezpečovacích a tísňových systémů. V rámci obvodové obrany je navrhnuto doplnění pomocí systému detektorů na oplocení areálu a na v místech, kde se nachází slepá místa je navrženo výstavba PTZ kamer. U plášťové ochrany bylo předloženo vhodné doplnění duálními detektory do většiny místností v areálu. Na zlepšení technické ochrany je vhodné doplnění turnikety se čtečkou RFID karet pro identifikaci osob vstupujících do areálu.

Cíl bakalářské práce si dovoluji, s přihlédnutím k výše zmíněným výstupům, považovat za splněný.

SEZNAM POUŽITÉ LITERATURY

[1] *Biometrie je více než otisk prstu.* [online]. [cit. 4. 7. 2018]. Dostupné z: https://ictrevue.ihned.cz/c3-65967870-0ICT00_d-65967870-biometrie-je-vice-nez-otisk-prstu

[2] ČSN CLC/TS 50131-7: *Poplachové systémy - Elektrické zabezpečovací systémy - Část 7: Pokyny pro aplikace.* 2011. Třídící znak 33 4591.

[3] ČSN EN 1627 *Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání - Požadavky a klasifikace*. 2012. Třídící znak 746001.

[4] ČSN EN 1630+A1 *Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání - Zkušební metoda pro stanovení odolnosti proti manuálním pokusům o vloupání.* 2017. Třídící znak 746004.

[5] ČSN EN 50131-1 ed. 2: *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky*. 2007. Třídící znak 33 4591.

[6] ČSN EN 62676-1-1. *Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 1-1: Systémové požadavky – Obecně*. 2014. Třídící znak 33 4592.

[7] HART, Jan. *Poplachové zabezpečovací a tísňové systémy* [online]. [cit. 2020-07-15]. ISBN 978-80-213-2962-1. Dostupné z: https://katedry.czu.cz/storage/7579_Poplachove-zabezpecovaci-a-tisnove-systemy.pdf

[8] *HTV-Hodina: FF 600* [online]. 2020 [cit. 2020-08-05]. Dostupné z: http://www.htv-hodina.cz/product-details/669-venkovni-detekce-fp-600-0909-002/#skip

[9] Ishikawa diagram. *MANAGEMENTMANIA.* [online]. 2015 [cit. 2020-06-25]. Dostupné z: https://managementmania.com/cs/ishikawuv-diagram

[10] *Jablotron: Jablotron 100* [online]. [cit. 2020-06-15]. Dostupné z: https://www.jablotron.com/cz/katalog-produktu/alarmy/jablotron-100/

[11] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015, 240 s. ISBN 978-80-7251-436-6.

[12] KINDL, Jiří. *Projektování bezpečnostních systémů. [I. díl, EPS, EZS].* Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7318-554-1.

[13] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. , 100 s. ISBN 978-80-88168-31-7.

[14] KOUDELKA, Ctirad a Václav VRÁNA. RIZIKA A JEJICH ANALÝZA [online]. Ostrava, 2006 [cit. 2020-06-28]. Dostupné z: https://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf

[15] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky.* Blatná: Cricetus, 2003. 351 s. ISBN 80-902-9382-4.

[16] LOVEČEK, Tomáš, Andrej VEĽAS a Martin ĎUROVEC. *Bezpečnostné systémy: poplachové systémy.* Žilina: Žilinská univerzita v Žiline, EDIS-vydavateľské centrum ŽU, 2015. Vysokoškolské učebnice, 230 s. ISBN 978-80-554-1144-6.

[17] LUKÁŠ, Luděk., a kolektiv. *Bezpečnostní technologie, systémy a management I.* Zlín: VeRBuM, Zlín, 2011, 316 s. ISBN 978-808-7500-057.

[18] LUKÁŠ, Luděk., a kolektiv. *Bezpečnostní technologie, systémy a management II.* Zlín: VeRBuM, Zlín, 2012, 387 s. ISBN 978-80-87500-19-4.

[19] LUKÁŠ, Luděk., a kolektiv. *Bezpečnostní technologie, systémy a management III.* VeRBuM. Zlín, 2013, 456 s. ISBN: 978-80-87500-35-4.

[20] LUKÁŠ, Luděk., a kolektiv. *Bezpečnostní technologie, systémy a management IV.* VeRBuM. Zlín, 2014, 390s. ISBN: 978-80-87500-57-6.

[21] LUKÁŠ, Luděk., a kolektiv. *Bezpečnostní technologie, systémy a management V.* VeRBuM. Zlín, 2015, 368 s. ISBN: 978-80-87500-67-5.

[22] *Otočná kamera se zoomem a přísvitem: HikVISION* [online]. [cit. 2020-08-01]. Dostupné z: https://www.viakom.cz/fileshare/products/later/hik-prf/datasheet_of_ds-2df8425ix-ael(w)_(c)_20180522(14259).pdf

[23] *Plotový systém FP 300 a FP 600: Manuál* [online]. [cit. 2020-07-01]. Dostupné z: http://www.htv-hodina.cz/soubory/plotovy-system-fp-mana4.pdf

[24] AZ Pohony, Turniket: Plně automatický turniket (tripod). *AZ Pohony* [online]. [cit. 2020-07-30]. Dostupné z: http://azpohony.cz/turniket-02-plne-automaticky-turniket-tripod-p-1595.html

[25] VARGOVÁ, Slavomíra. *Analýza rizik: Přednášky, konzultace, materiály pro výuku kombinovaného studia.* Uherské Hradiště, Univerzita Tomáš Bati, 2018. [cit. 2020-06-25].

[26] ZELENÁ, Michaela. *Systém řízení bezpečnosti informací ve vybraném subjektu* [online]. Zlín, 2019 [cit. 2020-08-05]. Dostupné z: https://theses.cz/id/83itla. Diplomová práce. Univerzita Tomáš Bati. Vedoucí práce Ing. Petr Svoboda Ph.D.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AIR Active Infra Red (aktivní infračervená bariéra)

CCTV Closed Circuit Television (uzavřený televizní okruh)

CLC/TS (CENELEC CENELEC - European Committee for Electrotechnical Standardization - Evropský výbor pro normalizaci v oblasti elektrotechniky)

ČSN Česká státní norma

DPPC Dohledové a poplachové příjímací centrum

NVR Digital video recorder (digitální videorekordér)

ICT Information and Communication Technologies (Informační a komunikační technologie)

I&HAS Intruder and Hold-up Alarm Systém (Poplachové zabezpečovací a tísňové systémy)

ISO International Organization for Standartization

MW Microwave (mikrovlnný)

MZS Mechanické zábranné systémy

PCO Pult centrální ochrany

PIR Passive infra red (pasivní infračervené)

PTZ Pan, Tilt, Zoom (natočit, naklonit, přiblížit)

PZTS Poplachové zabezpečovací a tísňové systémy

RFID Radio Frequency Identification (radiofrekvenční identifikace)

SKV Systém kontroly vstupu

US Ultrasound (ultrazvuk)

VSS/VDS Video Surveillance Systém (Video dohledový systém)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK