Komplexní návrh zabezpečení Economy centra ve Zlíně

Bc. Lukáš Votava

Diplomová práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2015/2016

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Lukáš Votava**
Osobní číslo:	**A14796**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Komplexní návrh zabezpečení Economy centra ve Zlíně**
Téma anglicky:	**A Comprehensive Security System Proposal for the Economy Centre in Zlin**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na téma Technické prostředky a prvky zabezpečovací techniky.**
2. **Analyzujte aktuální legislativní prostředí v oblasti ochrany majetku.**
3. **Popište současný stav zabezpečení vybraného objektu.**
4. **Pro daný objekt navrhněte modernizaci stávajícího zabezpečovacího systému.**
5. **Zhodnoťte ekonomickou náročnost navrhovaného systému.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LUKÁŠ, Luděk a kolektiv: Bezpečnostní technologie, systémy a management I, 1. vydání, Zlín: VeRBuM, 2011, 316 str., ISBN 978-80-87500-05-7.**
2. **LUKÁŠ, Luděk a kolektiv: Bezpečnostní technologie, systémy a management II, 1.vydání, Zlín: VeRBuM, 2012, 387 str., ISBN 978-80-87500-19-4.**
3. **LUKÁŠ, Luděk a kolektiv: Bezpečnostní technologie, systémy a management III, 1.vydání, Zlín: VeRBuM, 2013, 456 str., ISBN 978-80-87500-35-4.**
4. **LAUCKÝ, Vladimír.: Technologie komerční bezpečnosti I, 3. vydání, Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 81 s. ISBN 978-80-7318-889-4.**
5. **LAUCKÝ, Vladimír.: Technologie komerční bezpečnosti II, 1. vydání, Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 123 str., ISBN 80-7318-231-9.**
6. **VALOUCH, Jan.: Projektování bezpečnostních systému. Skriptum. Zlín: UTB, 2012. 152 str., ISBN 978-80-7454-230-5.**

Vedoucí diplomové práce: **Ing. Martin Hromada, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **5. února 2016**

Termín odevzdání diplomové práce: **16. května 2016**

Ve Zlíně dne 5. února 2016

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně, dne …….

podpis diplomanta

ABSTRAKT

Cílem diplomové práce je vypracování návrhu na posílení zabezpečení objektu Economy centra ve Zlíně. Toto centrum je složeno ze tří samostatných firem, sídlících ve dvojpodlažní budově v centru města. V současné době jsou zde, mimo mechanické zábranné systémy, jen tři PIR detektory v přízemním podlaží. Tato diplomová práce zahrnuje návrh zabezpečení perimetru objektu, kde se nachází samostatně stojící garáž a stání pro kola zaměstnanců, dále návrh zabezpečení pláště budovy a nejobsáhlejší částí diplomové práce je pak návrh zabezpečení interiéru objektu a to včetně suterénu. Zabezpečení vnitřního prostoru se bude skládat z elektronických zabezpečovacích systémů i elektrické požární signalizace. Celý návrh je posílením stávajícího zabezpečení, které je značně nedostačující.

Klíčová slova:

Poplachový, zabezpečovací a tísňový systém, kamerový systém, mechanický zábranný systém, bezpečnostní analýza.

ABSTRACT

This thesis deals with the security systems proposal of the Economy Centre Zlín. This center is composed by three separate companies and it´s located in downtown Zlín. Currently there are only mechanical safety systems and a few PIR detectors in first floor. This thesis includes a proposal for a recommendation of the perimeter security, where is the deteched garage and bikes standings. The next step is about recommendation of the security systems for the object of Economy centre. The security will consist of electronic security system, electronic fire alarm system and video surveillance systém. The entire proposal is strenghtening the existing securiy systém, that is highly inadequate.

Keywords:

Security systém, electronic fire alarm, video surveillance systém, mechanical safety systems, safety analysis.

Děkuji tímto svému vedoucímu diplomové práce ing. Martinovi Hromadovi, Ph.D. za odborné vedení a rady, které mi poskytoval během tvorby práce.

Dále chci poděkovat svým rodičům a blízkým, kteří mě podporovali po celou dobu mého studia.

OBSAH

ÚVOD

Jedním z problémů 21. století je rychlé rozmáhání kriminality a násilí ve společnosti. Čím dál více lidí dává přednost „jednoduššímu“ způsobu obohacení se, než typickým zaměstnáním. Tento problém vzniká hlavně upadající morálkou občanů, migrací osob, nezodpovědnou výchovou dětí a mnohými dalšími aspekty. Mnozí mají možná pocit, že platí příliš vysoké daně státu, který pro ně na oplátku nic nedělá a chování dnešních představitelů národa k tomu svým chováním značně přispívá. Obyčejný jedinec pak lehce může nabrat dojem, že se s poctivostí se dneska člověk moc daleko nedostane a že dobré mravy jsou na ústupu.

V dnešní době je otázka bezpečnosti velice aktuální téma. Vytvořit pocit vnitřního bezpečí se stává složitějším problémem, než tomu bylo dříve. A přitom je bezpečnost jako taková prioritní zájem všech subjektů moderní doby. Každý si chce hájit vlastní zájmy, ochránit sebe, svoji rodinu (popř. firmu) a svůj majetek. Ovšem vždycky se najdou jedinci, kteří se budou chtít obohatit na úkor jiných. Nestačí spoléhat na orgány veřejné moci a na opatření samotného subjektu, kde hrozí nějaké riziko, ale je minimálně vhodné připojit do procesu třetí složku. A to jsou zejména složky průmyslu komerční bezpečnosti. Tyto složky, většinou se jedná o právnické osoby, jsou dnes jedním z hlavních pilířů bezpečnosti. Teprve privatizace bezpečnosti umožňuje ji naplňovat v rozsahu, v jakém je to dnes potřeba. Je to dáno hlavně tím, že státní orgány nejsou schopny zabezpečit každého tak, jak potřebuje a hlavně na to nejsou ani finanční prostředky. Proto se každý musíme, v případě potřeby zvýšení bezpečnosti, obrátit na komerční bezpečnostní služby a připlatit si za dnes už potřebný „nadstandart“. Každému navíc vyhovuje něco jiného a pocit bezpečí si taktéž každý představuje jinak. Proto je každý zabezpečovaný subjekt v podstatě jedinečný a musí se k němu přistupovat individuálně.

Bezpečnost je dneska nadstandartní záležitost, za kterou si lidé rádi připlatí. To je další důvod, proč je dnes takový boom v průmyslu komerční bezpečnosti. Průmysl komerční bezpečnosti kombinuje použití moderních technologií a fyzickou ostrahu, kdy v celku jde v podstatě nepřetržité střežení, ať už fyzicky, nebo technicky s napojením na dohledové, poplachové a přijímací centrum, odkud se dále problémy řeší a to non-stop. Kromě mechanických zábranných systémů se jedná spíše o preventivní opatření, ale i ty mnohdy rozhodují o tom, jestli se pachatel rozhodne to zkusit, či nikoliv.

I. TEORETICKÁ ČÁST

1 OCHRANA OBJEKTŮ

Tato kapitola seznámí čtenáře s obecnou problematikou zabezpečování objektů. Cílem je, aby se čtenář dozvěděl o základních principech a praktikách služeb komerční bezpečnosti a o legislativní stránce této problematiky. Bezpečnost je stav, kdy jsou na maximální možnou míru potlačena rizika plynoucí z hrozeb. Bezpečnost jako taková se dá rozdělit na více sektorů, které jsou níže dále specifikovány. Základní bezpečnostní opatření jsou v první řadě mechanické zábranné systémy. Například každý obyčejný plot tvoří případnému pachateli nějakou překážku, kterou musí překonat a která ho při výkonu neoprávněné činnosti zpomalí. Pokud se ve střeženém objektu nachází například i fyzická ostraha, je daleko pravděpodobnější, že pachatele odhalí, když bude po cestě za svým cílem zpomalován překážkami. Dalším důležitým pilířem zabezpečení objektů i fyzické ostrahy jsou elektronické poplachové systémy. Tyto prvky nepřetržitě monitorují danou lokalitu a vyhodnocují její stav. V případě narušení bezpečnosti vyhlásí nouzový stav.

1.1 Legislativa v oblasti ochrany osob a majetku

Právní úprava v oblasti ochrany osob a majetku obsahuje široké spektrum zákonů, nařízení a norem. Pro účel této práce je zde uveden jen jejich úzký výběr, který je nezbytný pro návrh zabezpečení objektů.

Pro všechny občany České republiky jsou společná zákonná ustanovení, jako je Ústava České republiky, Listina základních práv a svobod, trestní řád a trestní zákoník a další zákony.

- **Ústava České republiky** byla schválena 16. 12. 1992**.** Ústava ČR je nejdůležitější právní listinou v České republice, Protože upravuje základní práva a povinnosti týkající se občana a České republiky a jejich vzájemný vztah. Z pohledu Ústavy mají lidé právo na ochranu svého majetku, života a zdraví. Musí tak ale činit v souladu s příslušnými zákony.

- **Listina základních práv a svobod**, jakožto součást Ústavy vymezuje vztahy mezi občany. Lidská práva a svobody jsou všeobecnou a nedotknutelnou hodnotou. Tyto práva a svobody mají všichni lidé bez ohledu na vyznání, barvu pleti, politického smýšlení, nebo sociálního původu. Hlavním principem je to, že každý člověk má svá práva a že tato práva jsou nezadatelné, nezcizitelné a nepromlčitelné a že nikomu nesmí být způsobena újma na právech pro uplatňování jeho základních práv a svobod. Veškerá právní omezení musí být postavena na základě stanoveného zákona.

    - Účelem **trestního zákona** je pak chránit zájmy společnosti. Pro náš účel (ochrana osob a majetku) bereme v potaz především §13 (Nutná obrana), §14 (Krajní nouze) a §15(Oprávnění použití zbraně). Trestní zákon také charakterizuje trestné činy majetkového charakteru, které tvoří objektů hrozby. Trestní zákon definuje např.:
    - *Trestný čin loupeže - §173: Kdo proti jinému užije násilí, nebo výhrůžky bezprostředního násilí v úmyslu zmocnit se cizí věci, bude potrestán odnětím svobody na dvě léta až deset let*
    - *trestný čin krádeže - § 247: Kdo si přisvojí cizí věc tím, že se jí zmocní, a*
        - *a) způsobí tak škodu nikoli nepatrnou,*
        - *b) čin spáchá vloupáním*
        - *c) bezprostředně po činu se pokusí uchovat si věc násilím nebo výhrůžkou bezprostředního násilí,*
        - *d) čin spáchá na věci, kterou má jiný na sobě nebo při sobě, nebo*
        - *e) byl za takový čin v posledních třech letech odsouzen nebo potrestán, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty [10]*

Zákon o PČR č. 283/1991 Sb. stanoví náplň činnosti a úkoly policie. Zároveň upravuje její strukturu a organizaci řízení a povinnosti a prostředky policistů.

1.2 Legislativa v oblasti bezpečnostních systémů

Při návrhu PZTS i při výrobě jednotlivých prvků je nutné se řídit platnými normami a vyhláškami. V této kapitole je vypsána vybraná legislativa pro bezpečnostní systémy a jejich aplikace. Vše musí být v souladu s ustanovením ČSN CLC/TS 50398 (Poplachové systémy – kombinované a integrované systémy – všeobecné požadavky).

Požadavky jsou klasifikovány do následujících skupin:

- Systémové požadavky
- Aplikace technických norem
- Pokyny k použití, montáži a spolehlivosti PZTS
- Požadavky na dokumentaci a školení

Tyto ustanovení by měly napomáhat ke správnému použití konkrétních aplikačních norem a k naplnění požadavků a pokynů na prvky PZTS

V první řadě je ale nutné zmínit obecné zákony pro veškeré výrobky.

Jedná se o následující zákony:

- Zákon č. 22/1997Sb. o technických požadavcích na výrobky a o změně a doplnění některých zákonů.
- Zákon č. 59/1998 Sb. o odpovědnosti za škodu způsobenou vadou výrobku.
- Zákon č. 64/1986 Sb. o České obchodní inspekci.
- Zákon č. 102/2001 Sb. o obecné bezpečnosti výrobků.

Dále je třeba uvažovat s nařízením vlády, k provedení zákona č. 22/1997Sb o technických požadavcích na výrobky, kterými se stanovují technické požadavky na konkrétní zařízení.

V případě PZTS se jedná převážně o elektrická zařízení, takže je nutné, aby tyto zařízení byly vyhovující těmto nařízením:

- Nařízení vlády č. 17/2003Sb., které stanovuje technické požadavky na elektrická zařízení nízkého napětí.
- Nařízení vlády č. 616/2006Sb., kde jsou dány technické požadavky na výrobky z hlediska jejich elektromagnetické kompatibility.
- Nařízení vlády č. 426/2000 Sb., které stanovuje technické požadavky na rádiová a na telekomunikační koncová zařízení.

1.2.1 Normy v oblasti MZS

Pro instalaci prvků MZS se vychází zejména z následujících norem. Opět se nejedná o výpis veškerých norem týkajících se oblasti MZS. Jde o stručný seznam norem, které je potřeba brát v úvahu pro vypracování návrhu, který je zpracován v praktické části diplomové práce.

Označení normy	***Obsah***
ČSN P ENV 1627	Okna, dveře, uzávěry - Odolnost proti násilnému vniknutí Požadavky a klasifikace
ČSN P ENV 1628	Okna, dveře, uzávěry - Odolnost proti násilnému vniknutí Zkušební metoda pro stanovení odolnosti při statickém zatížení
ČSN P ENV 1629	Okna, dveře, uzávěry - Odolnost proti násilnému vniknutí Zkušební metoda pro stanovení odolnosti při dynamickém zatížení
ČSN P ENV 163	Okna, dveře, uzávěry - Odolnost proti násilnému vniknutí Zkušební metoda pro stanovení odolnosti proti manuálním pokusům o násilné vniknutí
ČSN EN 1303	Stavební kování - Cylindrické vložky pro zámky - Požadavky a zkušební metody
ČSN EN 1906	Stavební kování - Dveřní štíty, kliky a knoflíky - Požadavky a zkušební metody

Tabulka 1: Vybrané normy v oblasti MZS

1.2.2 Normy v oblasti PZTS

Pro PZTS se většinou uvažuje používání elektrotechnických prvků. Tyto prvky taktéž musí splňovat určité požadavky. Jedná se především o normy:

Označení normy	*Obsah*
ČSN 33 1500	Elektrotechnické předpisy. Revize elektrických zařízení
ČSN 33 1600	Revize a kontroly elektrických zařízení během používání
ČSN 33 2000	Elektrické instalace budov
ČSN 33 2000-1	Elektrické instalace budov - Rozsah platnosti, účel a základní hlediska
ČSN 33 2000-3	Elektrotechnické předpisy. Elektrická zařízení. Část 3: Stanovení základních charakteristik
ČSN 34 2300	Předpisy pro vnitřní rozvody sdělovacích vedení
ČSN 33 4000	Elektrotechnické předpisy. Požadavky na odolnost sdělovacích zařízení proti přepětí a nadproudu
ČSN 33 4010	Elektrotechnické předpisy. Ochrana sdělovacích vedení a zařízení proti přepětí a nadproudu atmosférického původu
ČSN 33 0165	Elektrotechnické předpisy. Značení vodičů barvami nebo číslicemi. Prováděcí ustanovení
ČSN EN 60445	Základní a bezpečnostní zásady pro rozhraní člověk-stroj, značení a identifikaci
ČSN EN60529	Stupně ochrany krytem (krytí -IP kód)

Tabulka 2: Vybrané elektrotechnické normy

Co se týče samotných prvků PZTS, všechny musí splňovat požadavky z daných norem.

Označení normy	***Obsah***
ČSN EN 50131-1	Systémové požadavky pro PZTS
ČSN EN 50131-2-2	Požadavky na pasivní infračervené detektory
ČSN EN 50131-2-3	Požadavky na mikrovlnné detektory
ČSN EN 50131-2-4	Požadavky na kombinované detektory (pasivní infračervené a mikrovlnné detektory)
ČSN EN 50131-2-5	Požadavky na kombinované detektory (pasivní infračervené a ultrazvukové detektory)
ČSN EN 50131-2-6	Požadavky na detektory otevření
ČSN EN 50131-2-7	Požadavky na detektory narušení – detektory rozbití skla
ČSN EN 50131-3	Požadavky na ústředny PZTS
ČSN EN 50131-4	Požadavky na Výstražná zařízení
ČSN EN 50131-5	Požadavky na bezdrátová zařízení
ČSN EN 50131-6	Požadavky na napájecí zdroje
ČSN EN 50132-1	CCTV – uzavřené televizní okruhy - systémové požadavky
ČSN EN 50133-1	ACS – přístupové systémy - systémové požadavky
ČSN EN 50134-1	SAS – systémy přivolání pomoci - systémové požadavky
ČSN CLC/TS 50131-7	Pokyny pro aplikace

Tabulka 3: Vybrané normy v oblasti PZTS

Každá aplikace musí splňovat požadavky technických norem a zároveň i její instalace do systému musí být v souladu se specifickými požadavky pro integraci.

Požadavky pro EPS upravují následující zákony a vyhlášky:

- Zákon č. 133/1985 Sb., o požární ochraně
- Zákon č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon).
- Zákon 360/1992 Sb., o výkonu povolání autorizovaných architektů a o výkonu povolání autorizovaných inženýrů a techniků činných ve výstavbě.
- Vyhláška č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci).
- Vyhláška č. 23/2008 Sb., o technických podmínkách požární ochrany staveb.
- Vyhláška č. 268/2009 Sb. o technických požadavcích na stavby.
- Nařízení vlády č. 163/2002 kterým se stanoví technické požadavky na vybrané stavební výrobky

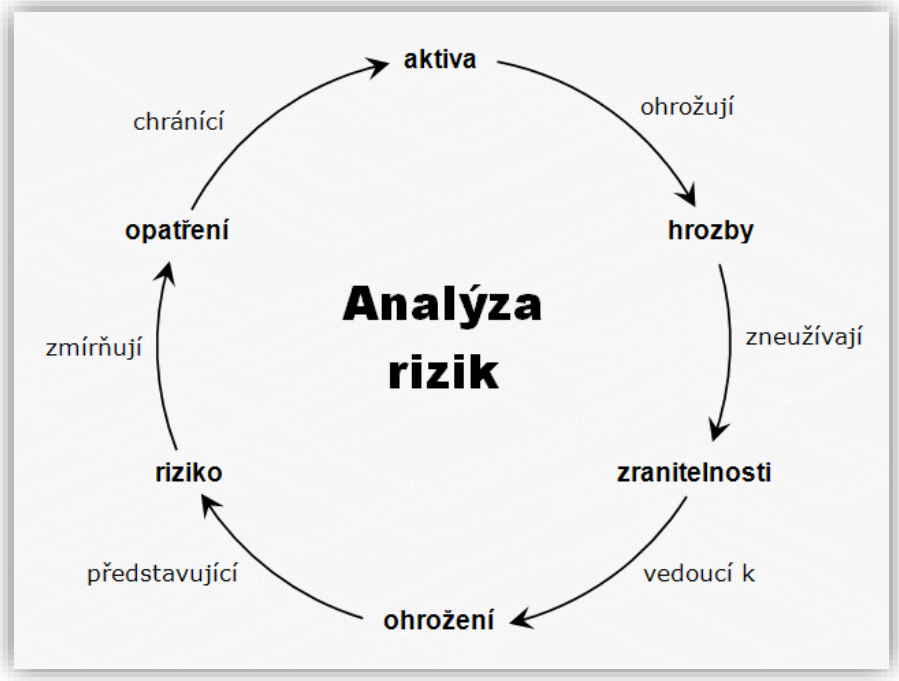
Projektování těchto systémů je pak normováno především:

- ČSN 73 0875 - Požární bezpečnost staveb - Stanovení podmínek pro navrhování elektrické požární signalizace v rámci požárně bezpečnostního řešení.
- ČSN 34 2710 - Elektrická požární signalizace - Projektování, montáž, užívání, provoz, kontrola, servis a údržba.
- ČSN 34 2300 - Předpisy pro vnitřní rozvody sdělovacích vedení

Dá se říci, že veškerá činnost v oblasti bezpečnosti osob, jejich zdraví a majetku je upravena nějakým zákonem nebo normou. Zákony jsou povinni všichni dodržovat, kdežto normy by se daly nazvat jakýmsi „doporučením“ pro používání daných prvků. Pokud se ale něco stane, a vyšetřování odhalí, že se nepostupovalo dle normy, neznamená to, že nikdo neponese následky.

1.3 Analýza rizik

Analýza je obecně charakterizována jako metoda poznání, jejíž podstatu tvoří rozložení problému na dílčí části, a u těch pak hledat jejich příčiny a jejich odstranění. Aby analýza splnila svůj účel, je nutné přesně stanovit vazby mezi jednotlivými částmi. Pro analýzu nebyly stanoveny žádné konkrétní postupy, protože každá analýza je v podstatě jedinečná. Jsou stanoveny pouze doporučené postupy. Každý objekt se musí analyzovat individuálně, protože faktory ovlivňující jeho bezpečnost se mění.



Obrázek 1: Znázornění analýzy rizik [6]

Analýza rizik představuje nejdůležitější část správného návrhu PZTS, známe-li hrozící rizika, dokážeme se na ně adekvátně připravit. Událost, která způsobí ztrátu nebo poškození majetku, je právně nazývána hrozbou. Analýza rizik je tedy zpracována za účelem zjištění, jakým hrozbám bude objekt čelit a je nezbytná pro správný návrh systému ochrany objektu.

1.4 Stupně zabezpečení

Stupně zabezpečení vyjadřují schopnost objektu odolat případnému narušiteli. Zabezpečení rozlišujeme na čtyři stupně. *Kvalitativní schopnosti činnosti narušitele vyjadřují jeho znalosti, dovednosti a technické vybavení, jímž disponuje při překonávání systému fyzické bezpečnosti. [7]*

Při pořizování jakéhokoli bezpečnostního prvku je nutné předem zhodnotit, jaká rizika hrozí, a na základě toho pak zvolit příslušný stupeň zabezpečení, pro který budeme tyto prvky pořizovat. Celý objekt má pak takový stupeň zabezpečení, jako jeho nejslabší článek. To znamená, že pokud je požadavek na zabezpečení druhého stupně, nesmí se v objektu vyskytovat jediný zabezpečovací prvek s nižším stupněm bezpečnosti.

Úrovně zabezpečení jsou zpracovány s využitím ČSN P CEN/TS P 14383-3, ČSN P CEN/TS P 14383-4. Pro visací zámky a petlice jsou stanoveny základní požadavky v ČSN EN 12320. Podle těchto technických norem je definováno 5 úrovní zabezpečení pro dané úrovně rizika.

Úroveň zabezpečení	Úroveň rizika	Preventivní opatření
1	Velmi nízké	Jednoduché MZS
2	Nízké	Složitější MZS
3	Střední	Složitější MZS a minimální úroveň PZTS
4	Vysoké	Rozsáhlé MZS a střední úroveň PZTS
5	Velmi vysoké	Rozsáhlé MZS a vysoké úroveň PZTS

Tabulka 4: Úroveň rizika a způsob zabezpečení [9]

Tyto úrovně jsou určovány na základě odolnosti jednotlivých zabezpečovacích prvků a hodnotě chráněného majetku.

Stupně zabezpečení PZTS

Tyto stupně jsou definovány v normě ČSN EN 50113-1, kde jsou dána kritéria pro funkce jednotlivých prvků zabezpečení. Jednotlivé kategorie jsou definovány podle ČSN 50121-1.

- **Stupeň 1: Nízké riziko**
  Jedná se narušení objektu člověkem, který má jen malé znalosti poplachových, zabezpečovacích a tísňových systémů (dále jen PZTS). Dále se předpokládá, že tento narušitel disponuje pouze omezeným základním vybavením, které lze pořídit z obecně dostupných zdrojů.
  Tento stupeň zabezpečení se nejčastěji uplatňuje pro rodinné domy, byty nebo garáže.

- **Stupeň 2: Nízké až střední riziko**
  Jedná se narušení objektu člověkem, který má už určité znalosti PZTS. Dále se předpokládá, že narušitel disponuje pouze běžným nářadím a základními přenosnými přístroji.
  Tento stupeň zabezpečení se nejčastěji uplatňuje pro komerční objekty, jako jsou například ochody, výrobní prostory, kanceláře apod.

- **Stupeň 3: Střední až vysoké riziko**
  Jedná se narušení objektu člověkem, který má dobré znalosti PZTS. Tento narušitel má k dispozici úplný sortiment nástrojů a přenosných elektronických zařízení.
  Tento stupeň zabezpečení se nejčastěji uplatňuje pro peněžní ústavy, směnárny, obchody s vysoce cenným zbožím apod.

- **Stupeň 4: Vysoké riziko**
  Tento bezpečnostní stupeň se používá jen ve výjimečných případech a to zejména tehdy, má-li zabezpečení objektu nejvyšší prioritu. U takových objektů musí mít pachatel už přesně zpracovaný plán pro vniknutí. Počítá se i s tím, že narušitel má přesný plán prvků PZTS a kompletní sortiment nástrojů pro jeho překonání.
  Tento stupeň zabezpečení se nejčastěji uplatňuje pro důležité prvky kritické infrastruktury. Zde patří např. jaderná zařízení, státní instituce apod.

Hlásící zařízení musí rovněž odpovídat příslušnému stupni zabezpečení podle ČSN EN 50131-1 a přenosové cesty dle v ČSN EN 50136-1.

Stupeň zabezpečení	Výstražná a hlásící zařízení
1	Nezávisle napájená siréna
2	Přenosový systém s intervalem kontrolních hlášení 30 min
3	Hlavní přenosový systém s intervalem kontrolních hlášení 3 min. Doplňkový přenosový systém s intervalem kontrolních hlášení 30 min
4	Hlavní přenosový systém s intervalem hlášení 90 s. Doplňkový přenosový systém s intervalem hlášení 3 min nebo hlavní přenosový systém s intervalem kontrolních hlášení 20 s

Tabulka 5: Požadavky na výstražná zařízení [9]

Pokud má být jakýkoli objekt maximálně zabezpečen, musí se v první řadě co nejpřesněji určit hrozící rizika. Na základě analýzy těchto rizik se pak navrhuje zabezpečení daného objektu. Nejde jen o mechanické zábranné systémy, elektronické poplachové systémy a třeba kamerový systém. K tomu aby se dal objekt označit za bezpečný je třeba daleko víc, než jen jej vybavit nějakým zabezpečovacím systémem. Vždy je nutné nastavit a poctivě dodržovat daná režimová opatření a celkově dbát na bezpečnost. S nadsázkou lze říci, že i nejlepší dveře půjdou relativně snadno otevřít, když je zapomeneme zamknout a i nejkvalitnější sejf půjde vykrást, když je na nástěnce v místnosti napsán kód k jeho otevření. Jinými slovy při nedodržení režimových opatření se i nejsilnější zabezpečení může stát neúčinným.

Můžeme tedy říci, že ochrana objektů zahrnuje režimová opatření, činnost fyzické ostrahy a technické prostředky systému fyzické bezpečnosti. Pouze vhodná kombinace a sladění těchto prvků vede k tíženému cíli, a tím je snaha o maximální možnou eliminaci rizik pro daný objekt.

1.5 Režimová bezpečnostní opatření

Režimová opatření představují souhrn zásad a pravidel, kterými se musí všichni v daném objektu řídit. Neplatí jen pro zaměstnance, ale i pro veškeré návštěvy objektu. Tato pravidla napomáhají k zajištění chodu celého systému a bez jejich dodržování se stává systém znatelně zranitelnějším.

Režimová opatření jsou procesní naplnění bezpečnostní politiky organizace (instituce, firmy). Cílem režimových opatření je stanovit zásady, pravidla, oprávnění při pohybu zaměstnanců a dalších osob v prostorách organizace, způsob nakládání s bezpečnostně důležitými prvky, kontroly přinášeného a odnášeného materiálnu apod. [1]

K režimovým opatřením patří i pravidelná kontrola technické ochrany, Jedná se o odzkoušení všech technických prvků v objektu. Každý prvek, ať už se jedná o pohybový detektor, nebo požární detektor je vyzkoušen, jestli funguje tak jak má a jestli předá poplašnou zprávu. Kontrolují se i poplašná zařízení jako jsou například sirény. A v neposlední řadě i přenos informací na pult centralizované ochrany.

Tato opatření musí být navržena tak, aby na jednu stranu co nejméně omezovala personál a nezdržovala jeho pohyb v objektu. A na stranu druhou musí být režimová opatření nastavena tak, aby se zabránilo nežádoucím situacím a byl zajištěn požadovaný stupeň bezpečnosti. Proto se pro každý objekt navrhuje individuálně. Důležitou součástí režimových opatření je kontrola vstupu. Nejedná se pouze o vstup do objektu, nebo do areálu, ale to i do jednotlivých sekcí objektu, nebo areálu. Nemusí se kontrolovat jen samotné osoby, které přichází, ale někdy se kontroluje i obsah zavazadel popř. se kontrolují zavazadlové prostory automobilů.

Režimová opatření jsou, i když se to možná na první pohled nezdá, stejně důležitá, jako zbylé části zabezpečovacího systému. Ne nadarmo se říká, že příležitost dělá zloděje. Je proto důležité tyto opatření cílevědomě a svědomitě dodržovat.

1.5.1 Fyzická ostraha objektů

Jedná se o ostrahu objektů živou silou. To znamená, že ji vykonává člověk, nebo skupina lidí. Fyzická ostraha je vhodná pro její včasnou rekci na vzniklé hrozby. U menších objektů se může jednat pouze o kontrolu u vstupu do areálu, u větších objektů se mohou provádět pravidelné obchůzky. Při provádění obchůzek je vyšší pravděpodobnost odhalit případného pachatele a zadržet jej. Členové fyzické ostrahy jsou adekvátně vycvičení a vybaveni pro řešení mimořádných událostí a jejich přítomnost je proto často vyžadována. Kvůli včasné reakci, z důvodu jejich působení přímo v místě mimořádné události, se mohou snížit dopady vzniklé touto událostí. Největší nevýhodou fyzické ostrahy je jejich přílišná finanční náročnost. Fyzická ostraha může být prováděna komerčními bezpečnostními službami, nebo policisty.

Kynologická ostraha.

Pro zkvalitnění obchůzek kolem přísněji střežených objektů je může provádět kynologická ostraha. Jedná se o pracovníka ostrahy (psovoda) a psa. Tato kombinace dává kvalitě obchůzky zcela nový rozměr. Psi mají totiž podstatně lepší smysly než člověk a případného pachatele snadněji najdou. Při setkání s agresivním útočníkem pes zároveň psovodovi velmi ulehčí přemožení pachatele.

Obrázek 2: pracovníci kynologické ostrahy [11]

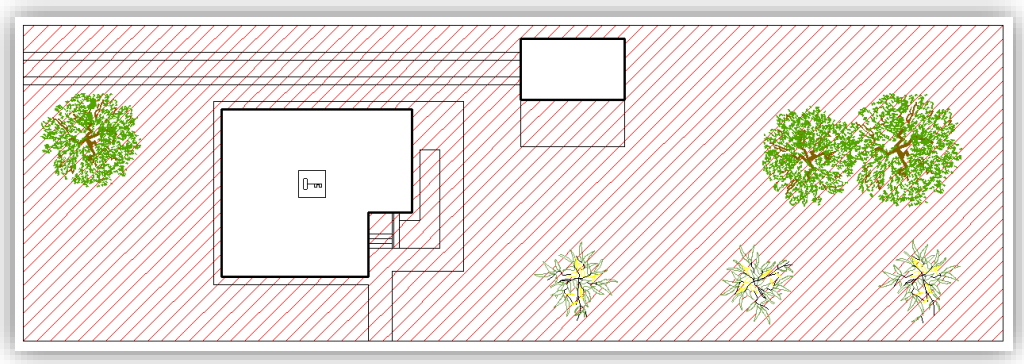
1.5.2 Technické bezpečnostní prostředky

V první řadě je nutné si rozčlenit střeženou oblast na dílčí části. Jedná se o oblasti, které musí pachatel překonat při pokusu o získání předmětu jeho zájmu. Úroveň zabezpečení by měla odpovídat stupni zabezpečení, které se odvíjí mimo jiné i od hodnoty chráněných aktivit. Technické prvky PZTS neplní funkci zabránit pachateli v jeho jednání, ani jej zpomalit, nýbrž jen upozornit na jeho přítomnost.

Základní rozdělení prostoru je tedy:

- **Perimetrická ochrana**

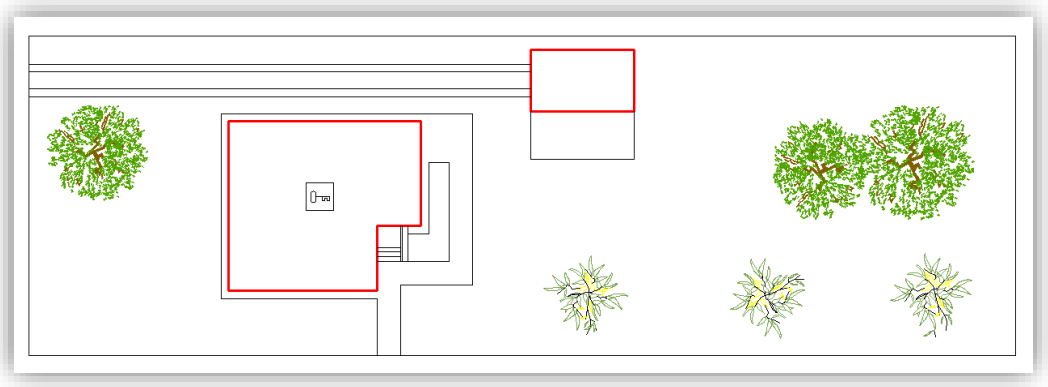
  Jedná se o ochranu celého pozemku objektu. V první řadě jde většinou o ochranu obvod pozemku. V případě zabezpečení větších areálů se nezabezpečuje jen plot kolem areálu, ale často se přidává i ochrana volného prostoru. Tato se provádí například použitím štěrbinových kabelů, nebo s různými typy infračervených závor nebo bariér. Snahou je zajistit celý perimetr a nejen jeho obvod. Hranice pozemku bývá nejčastěji ohraničena umělou bariérou (např. plotem, zdí, nebo třeba přilehlou budovou) nebo bariérou přírodní (např. řekou, či jiným přírodním útvarem, který zabrání přechodu osob).



Obrázek 3: Perimetrická ochrana [Zdroj: Autor]

- **Plášťová ochrana**

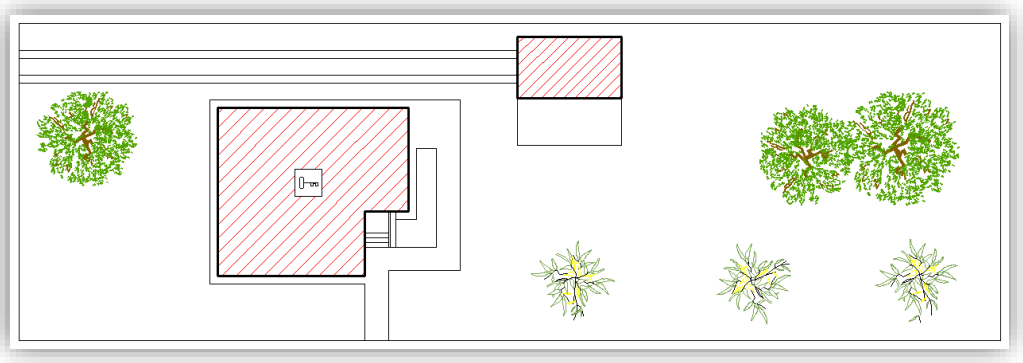
Jedná se o ochranu pláště budov. Jejím cílem je maximální možné ztížení průchodu z perimetru objektu do objektu samotného. Nejčastěji se jedná o zabezpečení oken a dveří. Tato ochrana je realizována např. zámky, mřížemi, bezpečnostními dveřmi a okny s magnetickými kontakty pro detekci otevření apod.



Obrázek 4: Plášťová ochrana [Zdroj: Autor]

- **Prostorová ochrana**

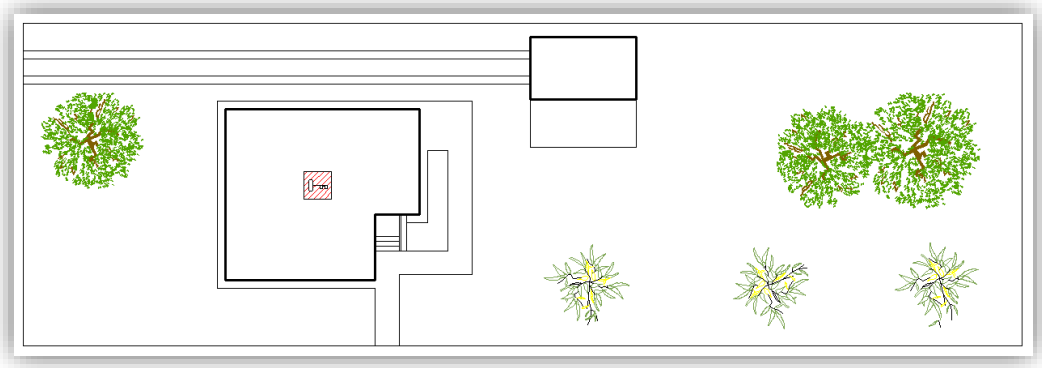
Prostorová ochrana je ochrana interiéru budov. Jejím cílem je detekovat a zpomalit narušitele pohybujícího se uvnitř objektu. Mezi klasické prvky prostorové ochrany patří např. vnitřní dveře, pohybové detektory, kamerové systémy apod.



Obrázek 5: Prostorová ochrana [Zdroj: Autor]

- **Předmětová ochrana**

Pojem předmětová ochrana charakterizuje ochranu konkrétních aktiv, která jsou pro majitele hodnotná. Tyto aktiva jsou různě veliká i cenná, takže se k jejich zabezpečení musí přizpůsobovat individuálně. Detektory sloužící k předmětové ochraně musí nejen detekovat narušitele poblíž, ale i manipulaci pachatele s předmětem jeho zájmu. Prvkem předmětové ochrany může být například tlakové čidlo, na kterém leží (popř. visí) aktivum, nebo třeba trezor, ve kterém jsou aktiva uložena.



Obrázek 6: Předmětová ochrana [Zdroj: Autor]

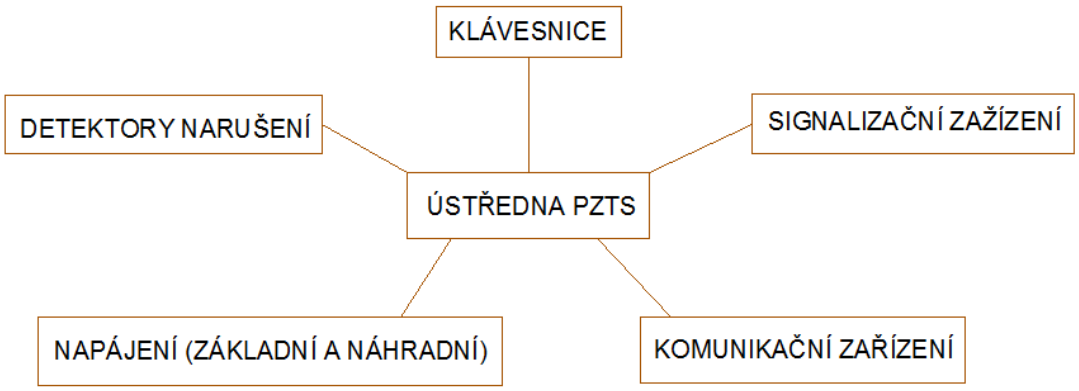
1.6 Shrnutí

Při zabezpečování se používají různé bezpečnostní prvky a různá bezpečnostní opatření. Při použití těchto prvků samostatně nemůžeme nikdy docílit optimálního řešení bezpečnostní situace. Optimální bezpečí vychází ze správně nastavené kombinace všech zabezpečujících prvků a opatření postavených na dané bezpečnostní třídě, zvolené na základě pečlivě provedené analýze bezpečnosti. Pouze vhodná kombinace technických prvků, mechanických zabezpečujících prvků a režimových opatření může střežený objekt ochránit.

2 POPLACHOVÉ, ZABEZPEČOVACÍ A TÍSŇOVÉ SYSTÉMY

PZTS (dříve EZS) jsou primárně určeny k tomu, aby rozpoznali narušitele pohybujícího se ve střeženém prostoru a tuto informaci dále nahlásili na příslušná místa. Dalším účelem může být například pachatelovo zastrašení pomocí výstražných zařízení, jako jsou majáky a sirény. Pachatel je tudíž obeznámený s tím, že se o něm ví, a že zásahová jednotka, nebo policie je už na cestě.

Středem celého systému PZTS je ústředna, která celý systém řídí a vyhodnocuje stavy posílané z detektorů. Nesmí chybět signalizační zařízení, které upozorní na přítomnost pachatele. Pro samotnou činnost systému je pak zapotřebí umístění nějakého ovládacího zařízení, kterým je nejčastěji klávesnice a v neposlední řadě se jedná o kabeláž (nejedná-li se o bezdrátový systém). Základní schéma těchto základních prvků je znázorněno na obrázku č. 6.



Obrázek 7: Základní schéma PZTS [Zdroj: Autor]

Detektor je zařízení, které slouží k detekci neoprávněného vniknutí do střeženého prostoru. Základní principem všech detektorů je snímání fyzikálních jevů (konkrétně jejich změn) a na základě těchto změn vyhodnotit neoprávněné vniknutí. Detektory, po jejich aktivaci, snímají prostředí nepřetržitě. Po detekci narušitele pak tyto detektory vyšlou poplachový signál nebo zprávy. Detektory mají ovšem pouze informativní charakter, pachatele nezastaví, nezpomalí a ani nedají žádné další informace o charakteru narušení.

Detektory narušení se dají dělit podle různých kritérií.

Základní kritéria pro rozčlenění detektorů narušení jsou:

- Dělení detektorů dle napájení:
  - Napájené
  - Nenapájené

- Dělení detektorů dle jejich vyzařování signálu do prostoru:
  - Aktivní
  - Pasivní

- Dělení detektorů dle oblasti, kterou střeží:
  - Prostorové
  - Směrové
  - Bariérové
  - Polohové

- Dělení detektorů dle fyzikálního principu, ze kterého vychází:
  - Elektromagnetické
  - Elektroakustické
  - Elektromechanické

Existují další způsoby, dle kterých se dají detektory dělit. U nenapájených detektorů může jít o detektory destrukční nebo nedestrukční. Napájené detektory se dají dělit např. i podle snímací charakteristiky (kruhové, širokoúhlé, bariérové, atd.), nebo podle jejich dosahu. Detektory se samozřejmě dělí i dle prostředí, ve kterém budou pracovat (vnitřní a venkovní) a také podle zóny ve které budou umístěny (perimetrická, plášťová, prostorová, nebo předmětová)

Při výběru detektoru je třeba brát v potaz hlavně prostředí, ve kterém bude pracovat a preferovanou bezpečnostní třídu. Každý detektor má trochu jiné funkce a vlastnosti a ty je třeba zvážit. Mimo základní funkce mohou mít některé detektory i další doplňkové funkce.

Důležité doplňkové funkce jsou ty proti sabotáži. Každý detektor by měl být odolný vůči případnému narušiteli, který se jej bude pokoušet vyřadit z provozu, nebo jeho provoz aspoň omezit. Důležitou vlastností detektorů je tedy odolnosti a detekce proti neoprávněnému přístupu do detektoru nebo k jeho součástkám popř. nastavovacím prvkům. Pouzdro detektoru by tedy mělo být vybaveno tamperem (spínacím kontaktem), který po otevření krytu detektoru automaticky vyhlásí poplach. Dalším důležitým prvkem je schopnost detektoru rozpoznat s jeho manipulací, i pouhé otočení detektoru musím být vyhodnoceno jako sabotáž a musí být vyhlášen poplach. Detektor musí být rovněž odolný proti omezení jeho funkce zakrytím čočky. K tomu slouží funkce antimasking, která v případě zaclonění výhledu rovněž spustí poplach.

Mezi další časté doplňkové funkce patří autotest, který kontroluje funkčnost detektoru a to jak místně, tak i dálkově. Detektory by měl testovat svoji funkci minimálně jednou denně, ale po dobu maximálně půl minuty, aby prostor nebýval dlouho nestřežený. Dále jde o snahu výrobců a odolnost proti falešným poplachům. Mezi další časté funkce moderních detektorů patří např. i funkce pet, která rozpozná, že se před ním pohybuje domácí mazlíček a nevyhlásí poplach.

2.1 Ústředny PZTS

Ústředna je klíčovou součástí celé soustavy PZTS. Je to část, kde se vyhodnocují veškeré data z detektorů, požárních hlásičů nebo tísňových spínačů. Je nutné zajistit její nepřetržitý chod.

Za hlavní funkce ústředen považujeme:

- Příjem a vyhodnocování stavů z komponentů PZTS
- Napájení komponentů PZTS
- Kontrola nepřetržitého provozu systému
- Indikace funkčních stavů systému.
- Obsluha celého systému

Požadavky na instalaci a zapojování ústředen PZTS a její základní funkce vyplývají z ČSN EN 54-2, ČSN 34 2710 a ČSN 54-4 ve smyslu napájení systému elektrickou energií, kde jsou uvedeny požadavky na hlavní, záložní nebo náhradní zdroje napájení apod.

Ústředny se dají rozdělit na ústředny analogové, sběrnicové nebo koncentrátorové a nebo bezdrátové.

Analogové ústředny pracují na principu předávání informací z detektorů do ústředny pomocí změny napětí nebo proudu. Každá poplachová smyčka je tedy připojena samostatně a je ukončena zakončovacím odporem. Nevýhodou je samozřejmě rozsah kabeláže a s tím i náklady na provedení.

Sběrnicové ústředny jsou v současnosti nejčastěji používané. Pracují na principu komunikace po sběrnici mezi ústřednou a detektorem. Ústředna periodicky generuje adresu detektoru s datovým dotazem na jeho stav a přijímá odezvy. Výhodou tohoto systému je relativně jednoduchá kabelová síť (na každý detektor stačí 2 páry vodiče, jeden je sběrnicový, druhý napájecí) a možnost připojovat detektory v libovolném pořadí. Nevýhodou může pak být omezený počet detektorů, což je ve dnešní době málo častá záležitost, protože sortiment těchto ústředen je obrovský.

Koncentrátorové ústředny rovněž pracují na principu datové komunikace, ale na rozdíl od sběrnicových ústředen probíhá komunikace mezi ústřednou a koncentrátorem (sběrnicový modul popř. expandér).

Bezdrátové ústředny můžou být často vhodné pro snadnou instalaci do objektu. Ale na druhou stranu mají i množství nevýhod. Tou největší je asi to, že signál těžce projde železobetonem a tudíž je pro řadu objektů tento systém nepoužitelný. Baterie u jednotlivých komponentů vydrží relativně dlouho, takže to za nevýhodu nepovažuji. Navíc se jedná převážně o tužkové baterie (baterie AAA, které nejsou drahé). Je možné používat baterie dobíjecí

2.2 Detektory narušení

Elektromechanické detektory lze definovat jako zařízení, které slouží k identifikaci pohybu ve střeženém prostoru. Obecně pracují na principu změny určitého fyzikálního, nebo chemického jevu. Může se jednat o přerušení elektrického obvodu, nebo světelného paprsku, nebo jiného parametru (například změnu amplitudy vlivem mechanických vibrací apod.). Tuto změnu jsou schopny detektory rozpoznat a převézt ji na elektrický signál, který je poslán do ústředny. Detektory tak hlásí ústředně svůj aktuální stav, který ústředna vyhodnotí a na základě nastavené dané zóny například vyhlásí poplach. .

Základní stavy detektorů jsou:

- **Stav střežení**

  Detektory jsou v provozu a střeží chráněný prostor. V tomto stavu detektory předávají ústředně signály o jejich stavu (poplach, sabotáž, porucha). Používá se v momentě, kdy je prostor střežen a pohyb po něm je nežádoucí.

- **Stav klid**

  V tomto stavu je detektor zapnutý, funkční, ale nehlásí ústředně stavy poplach, sabotáž či porucha. Používá se v době, kdy je v prostoru povolen pohyb a poplachy jsou tím pádem zbytečné

- **Stav poplach**

  Detektory indikují narušení, nebo pokus o jejich zastínění, či jiné pokusy o jejich vyřazení z provozu

- **Stav sabotážní poplach**

  Detektor hlásí přesušení obvodu, nebo neoprávněnou manipulaci

- **Stav porucha**

  Detekce poruchy (autotest je dnes základní doplňková funkce detektorů)

- **Stav test**

  V tomto stavu je detektor v podobném stavu jako v režimu střežení, jen dává ústředně pouze signál sabotáže, ostatní signály jsou blokovány.

Detektory narušení mají nezastupitelnou roli v moderním zabezpečení domů. Jsou jedním z hlavních prvků, který detekuje přítomnost osoby v místech, kde tyto osoby nemají povolen přístup. Detektory můžeme rozdělit dle místa, kde se umísťují

Detektory perimetrické ochrany

- infračervené závory a bariéry
- mikrovlnné bariéry
- štěrbinové kabely
- zemní tlakové hadice
- perimetrické PIR detektory

Detektory plášťové ochrany

- magnetické kontakty
- mechanické kontakty
- detektory tříštění skla
- poplachové fólie, tapety, polepy a poplachová skla

Detektory prostorové ochrany

- PIR detektory
- ultrazvukové detektory
- mikrovlnné detektory
- kombinované detektory

Detektory předmětové ochrany

- otřesové detektory
- závěsné detektory
- kapacitní detektory

Pozn.: Nejsou zde vyjmenovány všechny typy detektorů. Na trhu je podstatně větší množství zabezpečovací techniky. Zde jsou vypsány pouze ty nejčastěji používané typy.

2.2.1 Magnetické kontakty

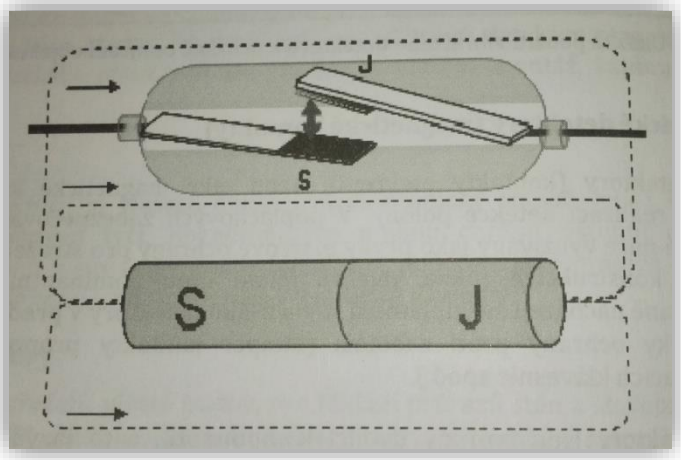
Magnetické detektory (někdy označované jako magnetické spínače) patří mezi nejčastěji používané detektory pro plášťovou ochranu objektů. Nejčastěji slouží k detekci otevření dveří či oken. Mimo to se dají tyto kontakty použít například jako prvky předmětové ochrany, nebo jako protisabotážní kontakty (tampery), například pro detekci otevření boxu ústředny (častější je ovšem spínací mechanický kontakt).

Jejich princip je velice jednoduchý. Magnetické kontakty se primárně skládají ze dvou částí. Základním prvkem je jazýčkový kontakt, který buď obvod uzavírá, nebo jej otevírá v závislosti na tom, jestli je v dosahu druhá část, kterou tvoří permanentní magnet. Jazýčkový kontakt je uložen ve speciální buňce z olovnatého skla (může se setkat i s plastovými buňkami). Tyto buňky jsou naplněny inertním plynem. Ve většině případů se jedná o dusík nebo argon. Kontaktní vrstvy jazýčků jsou pak pro jejich maximální možnou vodivost galvanicky pokryty vrstvou zlata, platiny, wolframu nebo stříbra. Při správném umístění do blízkosti permanentního magnetu se jazýčky zmagnetizují a přitáhnout se k sobě. Tím vznikne vodivý spoj, který uzavře obvod. Při oddálení permanentního magnetu se jazýčky opět odpojí.

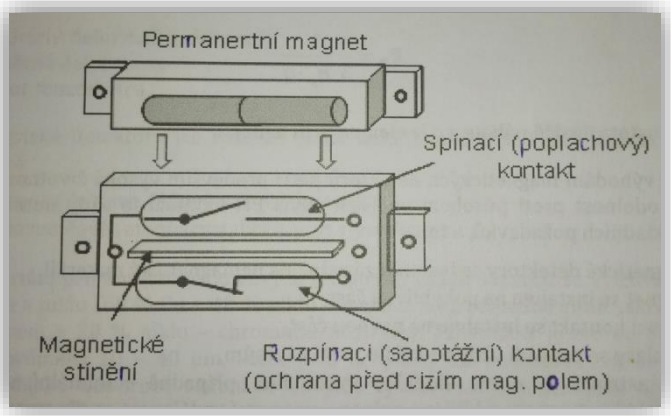
Magnetické kontakty můžeme rozdělit do více skupin:

- s jedním nebo s více jazýčkovými kontakty
- kontakty spínací, nebo rozpínací
- s vestavěným ochranným odporem
- s vestavěnou ochrannou smyčkou nebo bez ní

Pro připojení těchto magnetů do ústředen se používají 4vodiče. Dva jsou pro samotný magnet (pro jazýčkové kontakty) a druhý pár pak slouží jako sabotážní smyčka.



Obrázek 8: Princip magnetického kontaktu [1]



Obrázek 9: Magnetický kontakt s ochranou proti vlivům vnějšího magnetu [1]

Běžné provedení magnetických kontaktů jsou většinou pro zabezpečení prvního a druhého stupně. Pro vyšší stupně zabezpečení se už používají magnetické kontakty kombinované s jinými vlastnostmi (např. odolnost proti vnějším magnetům – Obr. 9)

2.2.2 PIR detetory

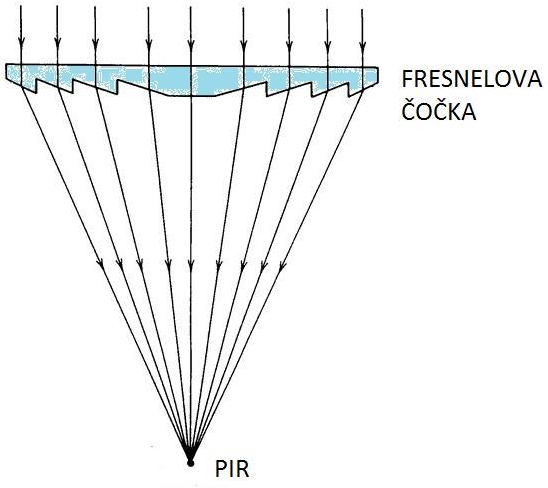
Pasivní infračervené detektory (PIR) jsou nejčastějším prvkem moderních PZTS. Tyto detektory jsou instalovány ve většině případů. PIR detektory vyhodnocují změny záření v infračerveném spektru a elektromagnetického vlnění. Pro zachycení tohoto vlnění slouží základní prvek každého PIR detektoru, pyroelektrocký snímač. Jedná se o element, který dokáže detekovat změny záření, které na něj dopadají a tyto změny převést na elektrický náboj. S pomocí tohoto elementu dokáže PIR detektory rozpoznat pohybující se těleso, které má odlišnou teplotu než jeho okolí. Většinou je detektor nastavený na oblast záření, kterou je typická pro teplotu lidského těla.

Základní části PIR detektoru jsou:

- Pyroelektrický snímač
- Optický systém
- Elektronika pro zpracování snímaného signálu
- Tamper kontakt
- Indikační LED diody

Při konstrukci PIR detektoru jsou používány speciální optické systémy, které slouží převážně k tomu, aby se signál zesílil a aby se docílilo zvýšení citlivosti detektoru. Další neméně důležitou funkcí této optiky je rozdělení střeženého prostoru do více zón. Toto rozdělení nám zaručuje zachycení pohybujícího se tělesa tím, že se přesouvám mezi jednotlivými zónami. Proto je PIR detektor nejvíce účinný, když se objekt pohybuje kolmo k optické ose detektoru. Při pohybu tělesa po ose detektoru se jeho detekční citlivost snižuje a to i přesto, že se prostor dělí i v tomto směru (ale na méně zón než ve směru kolmému k ose detektoru).

PIR detektory jsou vybaveny Fresnelovou a vypuklou čočkou.



Obrázek 10: Fresnelova čočka [12]

Typ a uspořádání čoček pak tvoří detekční charakteristiky detektorů. Mezi základní typy patří:

- Standartní
- Vějířovitá (širokoúhlá)
- Kruhová (stropní)
- Záclona (bariéra)
- Chodbová (s dlouhým dosahem)
- Zvířecí

Mezi hlavní výhody PIR detektorů patří jejich nenáročnost jak na spotřebu, tak na cenu pro vlastní koupi zařízení. I jejich instalace je snadná, protože se vzájemně neruší a jejich detekční zóny se mohou libovolně překrývat.

Jako hlavní nevýhodu se dá považovat jejich časté plané poplachy, které mohou být vyvolány slunečním zářením, stoupajícím teplým vzduchem z radiátorů, nebo např. automobilovými světly. Planý poplach může vyvolat i zvíře.

2.2.3 Mikrovlnné detektory

Mikrovlnné detektory jsou aktivní detektory, které pracují na principu Dopplerova jevu. Dopplerův jev změna vlnění, kdy se při pohybu vysílače mění vlnová délka elektromagnetických vln u přijímače. To znamená, že těleso pohybující se k přijímači bude mít vyšší frekvenci odraženého signálu a naopak u tělesa, které se oddaluje od přijímače, bude vlnová délka odraženého signálu klesat. Mikrovlnné detektory tento jev využívají. Jedná se o aktivní detektory, to znamená, že vysílají signál (9 -11GHz) a měří jeho frekvenci v momentě, kdy se odražený od překážky vrátí zpět.

Tento princip se využívá třeba i v radarech nebo sonarech. Vysílač i přijímač jsou v těle detektoru společně.

Mikrovlnné detektory se často používají v kombinaci například s PIR detektory. Tyto detektory nazýváme duální detektory.

2.2.4 Ultrazvukové detektory

Jedná se o pohybový detektor. Nepohybující se předmět je pro tento detektor tedy neviditelný. Ultrazvukové detektory pracují na stejném principu jako detektory mikrovlnné, jen používají jiný kmitočet (vlnová délka 20 – 60 kHz). Vysílač vysílá signál na stálém kmitočtu a přijímač přijímá odražené vlnění. Pohybuje-li se ve střeženém prostoru nějaký objekt, mění se fáze přijímaného signálu a detektor vyhlásí poplach.

Detektor opět obsahuje vysílač i přijímač, které jsou většinou v jednom těle. Ultrazvukové detektory jsou úmyslně nastaveny mimo slyšitelný rozsah lidského ucha.

SHRNUTÍ

PZTS tvoří jeden ze tří hlavních pilířů zabezpečení objektů (PZTS, MZS, režimová opatření) a proto je třeba při jejich návrhu postupovat obezřetně a profesionálně. Při výběru prvků je třeba brát ohledy nejen na zvolenou bezpečnostní třídu, ale hlavně na prostředí, ve kterém se systém a konkrétně jeho prvky nachází.

2.3 Elektronická požární signalizace

Systémy elektrické požární signalizace (EPS) jsou významným prvkem v moderních bezpečnostních aplikacích. Jejich úkolem je identifikovat požár a nahlásit tento stav na příslušná místa. V některých případech může systém sám začít požár hasit.

Základní systém EPS je tvořen:

- Ústřednou EPS s komunikačním modulem
- Hlásiči požáru
- Signalizací

EPS můžeme integrovat do systému jako samostatný prvek, nebo je možné některé hlásiče implementovat do systému PZTS. Vlastní ústřednu pro EPS nemusíme mít u menších objektů (např. rodinné domy), kde se nachází malé množství hlásičů.

2.3.1 Hlásiče požáru

Hlásiče požáru slouží k identifikaci, lokalizaci a nahlášení požáru při jeho vzniku. V zásadě můžeme hlásiče rozdělit na dva základní typy, které se dále dělí. Prvním typem jsou automatické hlásiče požáru a typem druhým jsou hlásiče tlačítkové. Ten hlavní rozdíl je v potřebě přítomnosti člověka pro vyhlášení požárního poplachu.

Automatické hlásiče pak můžeme dělit na základě fyzikální veličiny, kterou měří. Dle tohoto kritéria můžeme hlásiče rozdělit na:

- Kouřové hlásiče (optické nebo ionizační)
- Teplotní hlásiče
- Hlásiče plamene
- Hlásiče plynu
- Multisenzorové hlásiče

Kouřové hlásiče ionizační

Detekce požáru je u těchto hlásičích založena na změně vodivosti plynného prostředí v detekční komůrce hlásiče. Změna vodivosti nasává kvůli přítomnosti nezoxidovaných pevných částic kouře. Plyny jsou obecně nevodivé, proto je potřeba je ionizovat. Toho se v hlásičích dosáhne radioaktivním zářením typu α. Ionizační komůrka je tvořena α zářičem a dvojicí elektrod. Po přivedení napětí do elektrod hlásiče začne komůrkou procházet proud. Pokud se do ionizační komůrky dostane i kouř, hlásič rozpozná snížení proudu (zvýšení odporu vlivem pevných částí obsažených v kouři) a vyhlásí poplach.

Kouřové hlásiče optické

Optické kouřové hlásiče mohou pracovat na dvou principech. V první řadě se může vyhodnocovat rozptyl optického paprsku, nebo v případě druhém pohlcování optického paprsku způsobeného kouřem.

Hlásiče pracující na principu rozptylu paprsku světla jsou většinou konstrukčně řešeny jako hlásiče bodové. Detekční část těchto hlásičů je tvořena komůrkou, ve které se nachází jak zdroj světla, tak i jeho přijímač. Komůrka je z důvodu zvýšení spolehlivosti izolována od okolního světla a je konstruována tak, aby bez výskytu kouře nemohl paprsek světla z LED diody dopadnout na přijímač. To může způsobit až výskyt kouře, který rozptýlí světelný paprsek.

Hlásiče pracující na principu zeslabení paprsku jsou naopak konstruovány ze dvou oddělených částí, které se umísťují naproti sobě tak, aby mezi nimi byla přímá viditelnost. Jsou dvě konstrukční metody těchto hlásičů. V prvním případě je zdroj světla v jedné části a v části druhé je přijímač. Druhy typ má zdroj i přijímač v jednom těla a druhou číst tvoří jen odrazová plocha. Hlásič měří intenzitu dopadajícího světla, a pokud se tato intenzita sníží na 50 – 70% (100% je bráno jako porucha nebo sabotáž), detektor vyhlásí poplach.

Teplotní hlásiče

Teplotní hlásiče pracují na velice jednoduchém principu. Jsou nejstaršími hlásiči požáru. Princip je založen na vyhodnocování teplotních změn v místě hlásiče. Tyto hlásiče vychází z měření teploty a jeho vyhodnocování pomocí termistoru. Vyhodnocení může spočívat v překročení jisté teplotní hranice (statický hlásič), nebo rychlosti nárůstu teploty diferenciální hlásič).

Hlásiče plamene

Hlásiče plamene jsou bodové hlásiče, vyhodnocující specifické vlastnosti radiace plamene při požáru. Hodnotí se charakteristika intenzity vyzařování plamene, jeho spektrální charakter a časová proměnlivost (oscilace) plamene. Hlásiče plamene můžeme rozdělit na hlásiče infračervené, ultrafialové, nebo kombinované. Tyto hlásiče se skládají z optické sestavy, která slouží k usměrnění toku světla na detekční prvek, pásmového interferenčního filtru pro odstranění nežádoucího záření (např. slunečního), a samotného detekčního prvku. Z něj se signál zesílí a následně vyhodnocuje.

SHRNUTÍ

EPS jsou dnes běžnou součástí zabezpečení objektů. Požáry každoročně způsobují obrovské ztráty nejen na majetku ale i na životech. Proto se dnes prevence proti požárům stává prakticky běžnou součástí zabezpečení objektů a instaluje se automaticky do každé novostavby. Včasné ohlášení požáru je nezbytné pro včasnou evakuaci osob a zachránění majetku. Pro menší objekty nemusíme integrovat celý systém EPS. Systémy PZTS nabízí možnost připojení požárních detektorů, které mohou systém EPS v malých objektech nahradit. Existují i autonomní hlásiče požáru (někdy označovány jako bytové hlásiče požáru), které pracují bez ústředny EPS.

3 KAMEROVÉ SYSTÉMY

Tato část diplomové práce se zabývá kamerovými systémy a jejich použitím. Jelikož je kamerový systém součástí návrhu v praktické časti diplomové práce, nachází se zde krátký teoretický rozbor těchto systémů s vypsanou platnou legislativou.

Obecně se dá říct, že CCTV (Close circuit television) je systém užití kamer ke sledování prostor, k zobrazování záběrů z kamer na monitorech a archivaci natočených záběrů. Systém může rovněž sloužit k verifikaci příčiny poplachu PZTS. CCTV slouží jako dohledový systém, kde vyhodnocovací zařízení představuje záznamové zařízení DVR (Digital Video Recorder) nebo NVR (Network Video Recorder) a jednoúčelová zařízení představují kamery.

3.1 Základní rozdělení kamerových systémů

Základní rozdělní je možné například z hlediska obslužnosti systému. Dle tohoto kritéria můžeme CCT rozdělit na:

- Systémy s plnou obsluhou
  - Sledovací centra s operátory
  - Střežený prostor se sleduje na monitorech
  - Při incidentu operátor rychle reaguje
  - Vysoká úroveň zabezpečení
- Systém s částečnou obsluhou
  - Operátor nesleduje trvale dění na monitorech
  - Hrozí riziko propásnutí kritické události
  - Událost se případně dohledává v záznamu, který může být nekvalitní
- Systém bez dozoru
  - Videosystém bez lidské obsluhy
  - Střežená plocha musí být vykrytá fixními kamerami
  - Nutná vysoká rozlišovací schopnost kamer

Kamery dále můžeme klasifikovat dle dalších kritérií, jako jsou například

- Zpracování obrazu
  - Analogové kamery
  - Digitální kamery

- Prostředí
  - Vnitřní kamery
  - Venkovní kamery

- Snímání obrazu
  - Černobílé kamery
  - Barevné kamery
  - Kombinované kamery

- Konstrukční řešení:
  - Standartní kamery
  - Kompaktní kamery
  - Dome kamery
  - PTZ kamery
  - Bezdrátové kamery
  - Deskové kamery
  - Speciální a skryté kamery

3.2 Legislativa v oblasti CCTV

Norma ČSN EN 50132-1 platná od 1.11.2010 se vztahuje na systémy CCTV užívané pro sledování soukromých a veřejných prostor. Revize nově definuje čtyři stupně zabezpečení a čtyři třídy vlivu prostředí. Je určena výrobcům, systémovým integrátorům, montážním firmám, konzultantům, majitelům, uživatelům, pojišťovacím společnostem a společnostem zajišťujícím prosazování práva v dosažení kompletní a přesné specifikace sledovacího systému. Tato norma nespecifikuje typ technologie nebo požadavky na kvalitu obrazu pro konkrétní úlohy sledování.

Další normy, které je třeba zohlednit při instalaci kamerového systému jsou:

- **ČSN CLC/TS 50398** Poplachové systémy- Kombinované a integrované systémy- Všeobecné požadavky
- **ČSN EN 50 132-x-y** Poplachové systémy- CCTV sledovací systémy pro použití v bezpečnostních aplikacích
- Dále pro CCTV platí všechny zákony, nařízení a požadavky pro za řízení nízkého napětí,
    - NV 168 – organizace práce a pracovních postupů
    - NV 169 – EMC
    - NV 176 – nebezpečná prostředí
- Obecné normy pro zařízení nízkého napětí doplňující příslušná nařízení
    - ČSN EN 60065, 60950 – požadavky na bezpečnost,
    - ČSN EN 50081 – EMC

SHRNUTÍ

Pro bezpečnostní aplikace se většinou CCTV používá v kombinaci s prvky PZTS, které na pohyb pachatele pouze upozorní, ale už o pachateli nepřináší žádné další informace. S použitím kombinace PZTS a CCTV lze na poplachové přijímací centrum poslat i snímek či videosekvence pachatele. A celý incident může být zaznamenán a archivován pro pozdější přezkoumání či identifikování pachatele. Kamerové systémy mohou monitorovat jak interiér, tak i perimetr objektu. Z technického pohledu je možné je umístit víceméně kamkoli.

4 MECHANICKÉ ZÁBRANNÉ SYSTÉMY

Mechanické zábranné systémy tvoří základní stavební kámen celého systému zabezpečení objektů. Je to jediná součást zabezpečení, která může pachatele zastavit, popř. jej zdržet než přijede zásahová služba nebo policie.

Mezi MZS se řadí veškeré mechanické prvky, které jakýmkoli způsobem ztěžují případnému pachateli cestu. Patří sem ploty, obvodové zdi a s nimi okna a dveře. Okna a dveře jsou nejčastější místa pro překonání mechanických zábranných systémů a pro vniknutí do objektu. Proto se často zabezpečují nejvíce (mechanickými zábrannými systémy jako bezpečnostní mříže či rolety, bezpečnostní vrstvená skla atd.). Dále sem patří veškeré zámky či jiné uzamykatelné systémy (trezory apod.).

Průlomová odolnost

Správně zvolené MZS musí zajistit, že doba trvání jejich překonání je kratší, než příjezd policie, nebo zásahové služby. I samotná délka prolomení MZS může pachatele odradit. Tento čas je nazýván průlomovou odolností a je závislý na kvalitě prvků MZS, na jejich umístění a zpracování. Tato průlomová odolnost se také odvíjí od vybavení, jímž se pachatel snaží MZS prolomit a jeho znalostmi o konstrukci daného zabezpečení. Každý mechanický zábranný systém je překonatelný, tudíž se liší jen v čase, ve kterém je možné jej prolomit. Tento vztah jde matematicky definovat jako:

$$\Delta t = t_2 - t_1 \quad [\text{min}], \qquad [7]$$

Kde: Δt … časový interval potřebný k překonání překážky
t_1 … čas zahájení útoku
t_2 … čas úspěšného ukončení útoku (překonání překážky) *[7]*

V případě výpočtu průlomové odolnosti u úschovných objektů použijeme definici:

$$T_{vloupání} = [(V_R - B_V) : C_1] \times (2 \div 3) \text{ [min]} \qquad [7]$$

Kde: $T_{vloupání}$ … Doba minimální průlomové odolnosti úschovného objektu
V_R … Hodnota průlomové odolnosti
B_V … Základní ocenění použitého nářadí
C_1 … Koeficient průlomové odolnosti úschovného objektu *[7]*

Výsledek následně vynásobíme koeficientem (2 ÷ 3).

Vychází se z typu úschovného objektu. Hodnota průlomové odolnosti se liší u skříňových a komorových trezorů, které mají odpovídající počet odporových jednotek. Tyto jednotky se udělují na základě testů a fyzických zkoušek a na podkladě použitých přístrojů a podle typu nářadí.

Za obecně kvantitativní ohodnocení překážky považujeme časový interval, který pachatel potřebuje k jejímu přelomení [5]

Tento vztah vyjádříme jako:

$$R = T_{vloupání} / T_i \qquad [7]$$

Kde R je stupeň rizika pro ohrožení objektu, $T_{vloupání}$ zde představuje minimální dobu průlomové odolnosti objektu a Ti je čas, který potřebuje výjezdová skupina SBS, nebo policie ČR na dopravu ke střeženému objektu. *[7]*

SHRNUTÍ

Mechanické zábranné systémy tvoří jedinou fyzickou překážku pro pachatele, tudíž se musí při jejich návrhu zhodnotit čas, který je potřeba pro příjezd jednotek SBS nebo policie ČR. Po tuto dobu by měly MZS odolávat útoku pachatele. Podporou MZS je pak PZTS, která detekuje přítomnost narušitele a než dotyčný překoná MZS, přijede pomoc (policie ČR, zásahová jednotka SBS, atd.). MZS se proto navrhují tak, aby průlomová odolnost systémy byla výrazně delší, než je dojezd pomoci, jedině pak může být střežený objekt uchráněn.

5 ZÁVĚR

V teoretické části diplomové práce se čtenář seznámil se základní problematikou zabezpečování objektů a s tím spojenou legislativou.

V první kapitole teoretické části se čtenář seznámí s právními aspekty pro ochranu zdraví a života osob a jejich majetku. Je nutné podotknout, že výčet právních předpisů je vzhledem k rozsahu práce značně omezený. Další částí první kapitoly je pak teorie analýzy bezpečnostních rizik a zvolení stupně zabezpečení objektu. Dále jsou zde popsány základní důvody režimových opatření a jejich popis. K závěru první kapitoly je výpis prostředí, které se obvykle zabezpečuje. Ve druhé kapitole je teoreticky rozepsán systém PZTS. Je zde popsáno z jakých částí se tento systém skládá, a tyto části jsou popsány a jsou zde vysvětleny jejich primární funkce. Jedná se ústředny PZTS a detektory narušení. Tato kapitola je zaměřená i na systémy EPS. Tato část ale není příliš obsáhlá, protože v praktické čísti jsem samostatný systém EPS nepoužil. Pro detekci jsou použity požární detektory připojené k PZTS. Třetí kapitola rozebírá prvky kamerového systému. Je zde základní rozbor CCTV s vypsanými typy těchto systémů i samotných kamer. Součástí této kapitoly je stručný výběr legislativních aspektů pro CCTV. Teoretickou část pak uzavírá kapitola o mechanických zábranných systémech. Je zde popsána i průlomová odolnost jednotlivých prvků

Teoretická část diplomové práce neobsahuje veškeré poznatky pro zabezpečován objektů. Jejím cílem je pouze teoretický rozbor problematiky řešené v praktické časti diplomové práce, tedy pro konkrétní návrh zabezpečení vybraného objektu.

II. PRAKTICKÁ ČÁST

6 ANALÝZA OBJEKTU

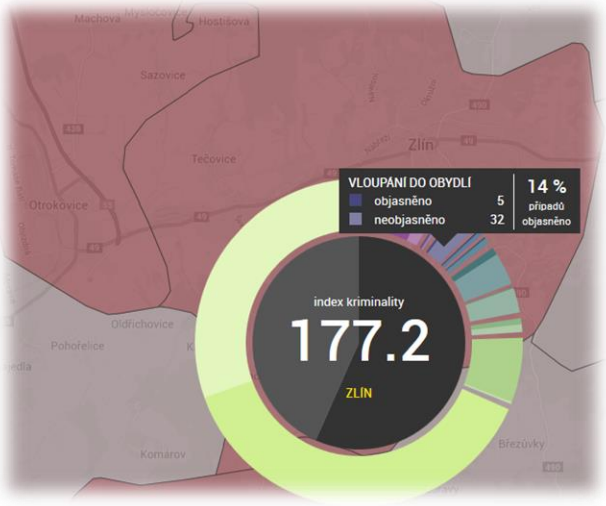
Tato kapitola v první řadě seznámí čtenáře se zabezpečovaným objektem a jeho okolím. Poté je zde provedena základní analýza rizik, na jejímž základě se stanoví bezpečnostní třída pro zabezpečení objektu. Poté jsou zde navrženy dvě varianty zabezpečení. Jedna varianta je bezdrátová a druhá klasická drátová. Závěrem práce je celý návrh zabezpečení tohoto objektu ekonomicky vyhodnotit.

6.1 Bezpečnostní analýza

Bezpečnostní analýza v podstatě znamená seznámit se s veškerými možnými riziky, které danému objektu hrozí. Základem funkčního návrhu zabezpečení objektu je správě provedená analýza rizik. Z této analýzy a z hodnoty chráněných aktiv se pak vychází při volbě bezpečnostní třídy a samotného návrhu zabezpečení.

Kriminalita ve Zlínském kraji

Ve Zlínském kraji bylo v letošním roce (1.1.2016 až 31.3.2016) evidováno zatím 2079 trestných činů. Z toho bylo nahlášeno 24 krádeží vloupáním do domů a 88 činů souviselo s poškozením cizí věci. Tyto údaje pochází ze statistik policie ČR veřejně dostupných na internetu. Ze statistik jde soudit, že těchto trestných činů přibývá a že pouze 14% případů je objasněných.



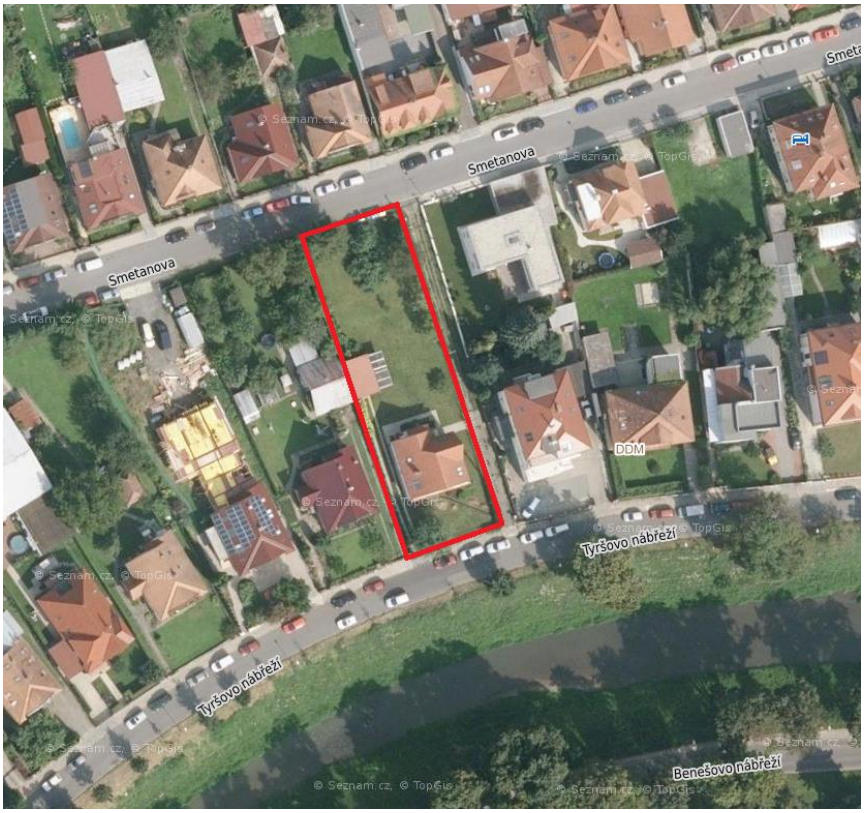
Obrázek 11: Vloupání do obydlí ve Zlíně v roce 2015 [13]

6.1.1 Základní informace o objektu

Jedná se o dvojpodlažní, částečně podsklepený dům, nacházející se v klidné oblasti Zlína. Na pozemku objektu je i samostatně stojící garáž, u které je pergola se stáním pro kola zaměstnanců. Celý perimetr je oplocený. Je zde jedna branka pro pěší a jedná brána pro automobily. Tato brána neslouží pro průjezd zaměstnanců ani klientů. Všichni tudíž parkují mimo pozemek objektu, takže je tato brána povětšinu času zamčená.

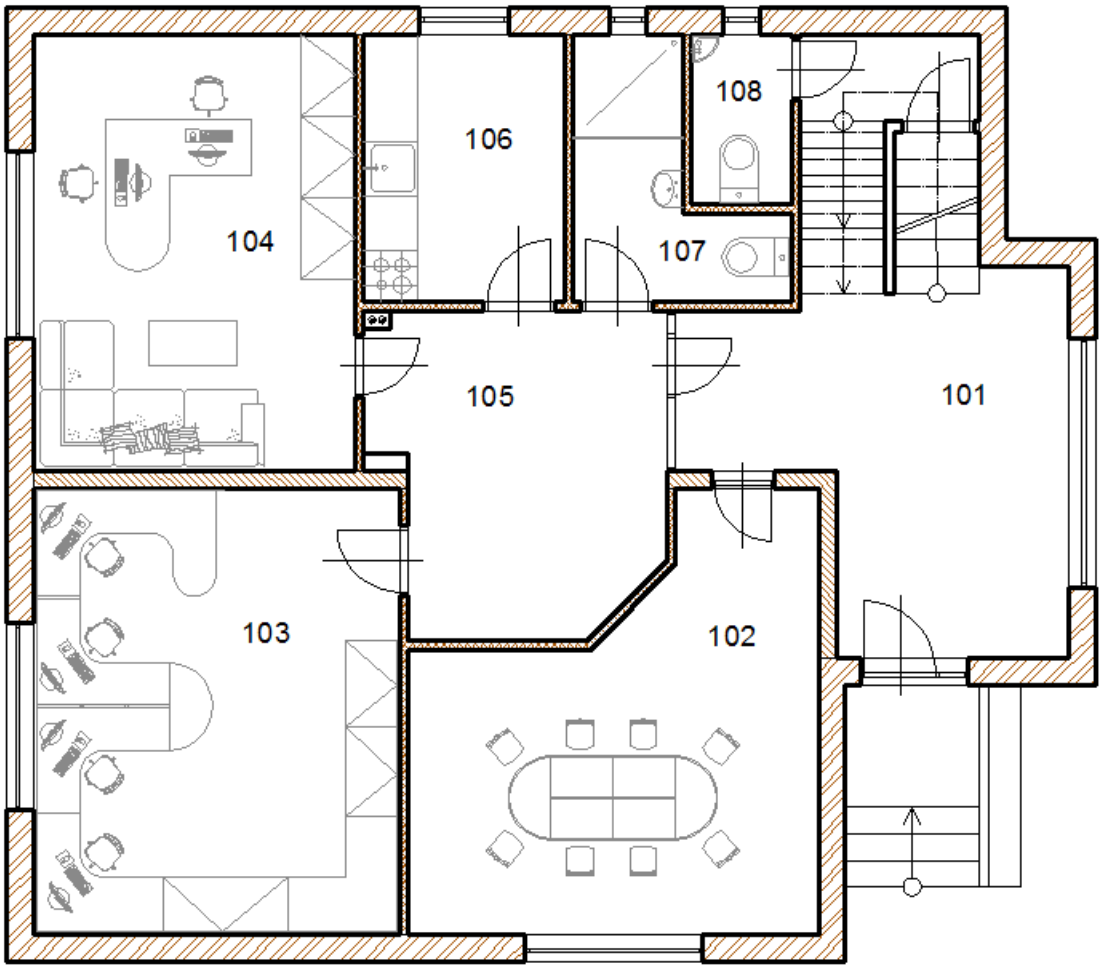
V okolí domu jsou pouze rodinné domy a pár menších firem, sídlících v podobných sídlech. Celkově je tato lokalita většinou velice klidná. Nevýhodou je blízkost fotbalového stadionu a s tím zvýšené riziko vandalismu. I tuto skutečnost zohledňuji pří návrhu PZTS

Objekt bude o víkendech, státních svátcích i po nocích prázdný, tudíž je tu zvýšené riziko napadení. V objektu se taktéž nachází větší množství elektroniky a výpočetní techniky. Zároveň je v objektu archiv s citlivými daty klientů.



Obrázek 12: Situace objektu [14]

PŮDORYS 1.NP



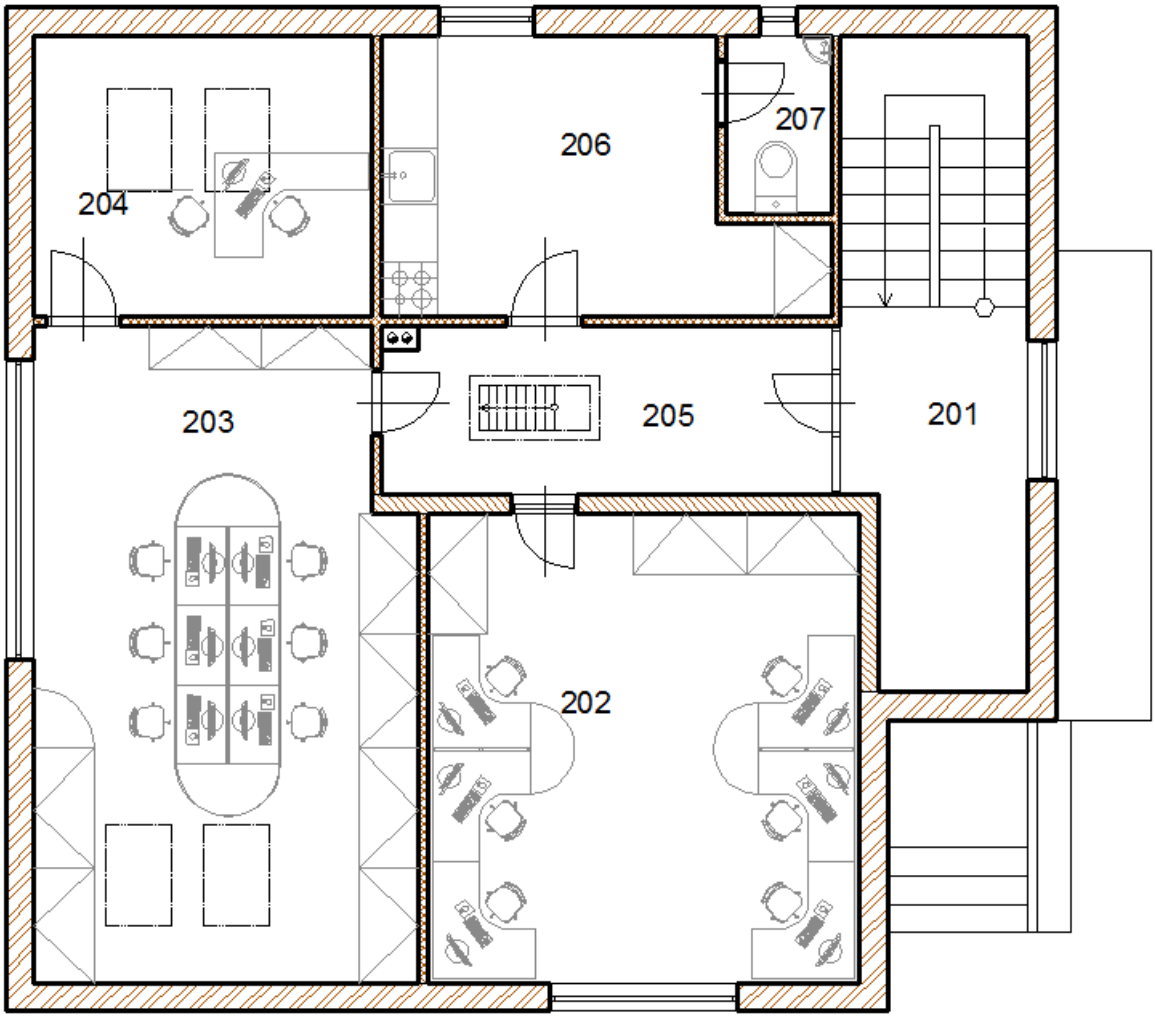
Obrázek 13: Půdorys 1.NP [Zdroj: Autor]

LEGENDA MÍSTNOSTÍ

MÍSTNOST	ÚČEL	ROZLOHA (m^2)
101	VSTUPNÍ HALA	14,1
102	ZASEDACÍ MÍSTNOST	18
103	KANCELÁŘ	20,5
104	KANCELÁŘ	17,6
105	CHODBA	11,2
106	KUCHYŇKA	6,7
107	KOUPELNA	4,9
108	WC	2,1

Tabulka 6: Legenda místností - 1.NP [Zdroj: Autor]

PŮDORYS 2.NP



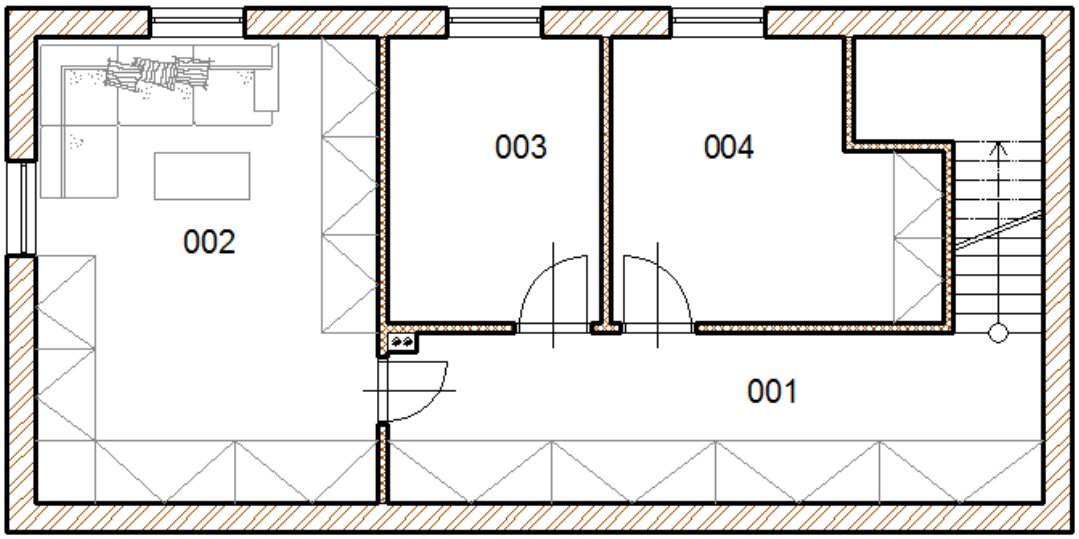
Obrázek 14: Půdorys 2.NP [Zdroj: Autor]

LEGENDA MÍSTNOSTÍ

MÍSTNOST	ÚČEL	ROZLOHA (m²)
201	CHODBA	7,4
202	KANCELÁŘ	23
203	KANCELÁŘ	27,7
204	KANCELÁŘ	10,8
205	CHODBA	14,1
206	KUCHYŇKA	12
207	WC	2,1

Tabulka 7: Legenda místností - 2.NP [Zdroj: Autor]

PŮDORYS 1.PP

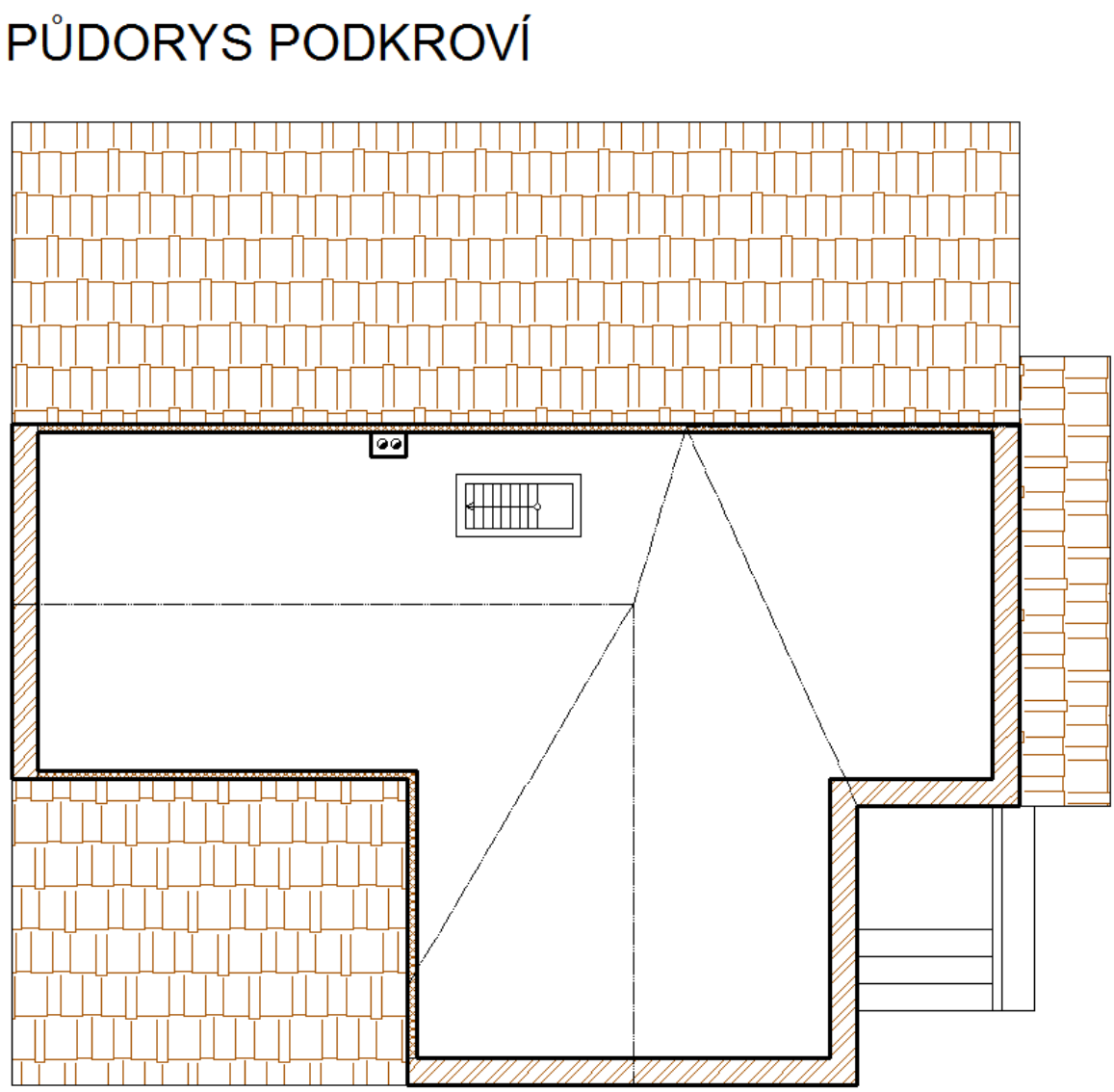


Obrázek 15: Půdorys suterénu [Zdroj: Autor]

LEGENDA MÍSTNOSTÍ

MÍSTNOST	ÚČEL	ROZLOHA (m²)
101	CHODBA _ ARCHIV	12,4
102	ARCHIV	17,6
103	KOTELNA	6,8
104	SERVEROVNA + SKLAD	9,2

Tabulka 8: Legenda místností – suterén [Zdroj: Autor]



Obrázek 16: Půdorys podkroví [Zdroj: Autor]

6.1.2 Stávající zabezpečení objektu

Stávající zabezpečení objektu je silně nedostačující. Byla sice navržena obnova MZS (plánovaná 1. fáze zabezpečení objektu), ale ta se ještě nerozběhla. V této první fázi zabezpečení zde byly navrženy nové dveře a bezpečnostní rolety s parametry splňující systémy pro zabezpečení druhé bezpečnostní třídy. Dalším prvkem první fáze zabezpečení byla výměna garážových vrat za nová od firmy Lomax, které taktéž splňují požadavky pro bezpečnostní třídu 2. Okna jsou plastová, osazená v roce 2007 při rekonstrukci objektu.

Druhá fáze zabezpečení proběhne dle projektu vycházejícího z této diplomové práce. První fáze se pozastavila z finančních důvodů, ale toto léto by měla být zahájena. Obě fáze zabezpečení Economy centra nakonec pravděpodobně proběhnou současně, a to hlavně z toho důvodu, aby práce neprobíhaly zbytečně dlouho a zaměstnanci mohli pracovat.

Perimetr objektu je oplocený. Na pozemek se dá dostat brankou, nebo příjezdovou bránou (visací zámek splňující požadavky druhé bezpečnostní třídy). V prvním podlaží je starý systém PZTS s jednou klávesnicí. Tento systém obsahuje pouze tři PIR detektory u vchodu do budovy a ve dvou místnostech. Zabezpečení je pravděpodobně z doby před přestavbou z rodinného domu na firemní objekt, která se konala v roce 2007. Systém PZTS není napojený na DPPC v případě poplachu pouze odešle varovné sms zprávy zástupcům firem.

Co se týče provozního režimu v objektu tak zde pracuje celkem 11 zaměstnanců. Každý má vlastní klíče od budovy. Další klíč má paní uklízečka, která sem chodí jeden den v týdnu. Klíče od garáže a od brány jsou pouze tři a mají je ředitelé firem sídlících v objektu. Pro vstup do objektu je mimo odemčení zadat bezpečnostní heslo na klávesnici u dveří. Vzhledem k tomu, že je „zabezpečený v podstatě jen vstup, tak je heslo jen jedno a znají ho všichni.

6.1.3 Analýza hrozeb

Pro tento objekt je zpracována pouze neformální analýza. Ta představuje spíše pragmatickou analýzu rizik. Tento přístup není založen na strukturovaných, předem určených metodách, ale na zkušenostech projektanta a na jeho znalosti dané lokality.

Z hlediska zabezpečovaných aktiv uvažujeme s majetkem v hodnotě přibližně 1 500 000 Kč. Majetek je tvořen moderní elektronikou, výpočetní technikou a firemním vozem. Ten je zamčený v garáži na pozemku. Tyto předměty by se mohly stát zájmem pachatele.

V této oblasti se nejčastěji jedná o vandalské trestné činy. Posprejované zdi, vysypané popelnice na zahradách a místy rozbité okno nějakým kamenem. Většinu těchto činů mají na svědomí fotbaloví fanoušci vracející se v podnapilém stavu ze stadionu na vlakové nádraží.

Co se týče krádeží, hrozí riziko zcizení výpočetní techniky, které je v objektu velké množství. Jedná se především o počítače, notebooky, tiskárny a projektor.

V objektu je rovněž archiv s citlivými osobními a daňovými údaji klientů firem co v objektu působí. Nejsou zde klientská know-how, ale spíše osobní data, kopie daňových přiznání a další účetní data, které se musí archivovat po dobu několika let. Riziko bude hrozit nejčastěji v noci nebo o víkendech, kdy se v objektu, až na výjimečné případy, nikdo nevyskytuje.

Katalog hrozeb

Aktiva	*Zdroje*	*Způsob zabezpečení*
Majetek	Budova Economy centra, garáž, stání pro bicykly	PZTS, kamerový systém
Informace o zákaznících	Archiv, PC a notebooky	PZTS, hesla na PC

Tabulka 9: Katalog hrozeb

Analýza rizik

Pro daný objekt je největším rizikem majetková kriminalita. Je nutno počítat jak s odcizením majetku, tak i s jeho zničením či s jinými projevy vandalismu z důvodu situace objektu v blízkosti fotbalového stadionu. Hrozí zde kromě zničení majetku nebo krádeže i zneužití citlivých informací o klientech Economy centra.

6.1.4 Stanovení stupně zabezpečení

Pro tento objekt byl na základě bezpečnostního posouzení objektu i jeho prostředí zvolen **stupeň zabezpečení 3** (střední riziko). To znamená, že případní pachatelé budou mít určité znalosti o PZTS a že použijí základní sortiment nástrojů a přenosných přístrojů.

Tento stupeň byl zvolen na základě přibližně vyčíslené hodnoty majetku a citlivosti archivovaných dat. Dalším důvodem je umístění objektu přímo v centru města. Jedná se sice o klidnou oblast, ale z hlediska vloupání může působit vilová čtvrt lukrativně. Navíc je zde večer a přes noc minimální pohyb osob což může být pro případné pachatele rovněž bráno jako výhoda.

7 NÁVRH PZTS

Projektování PZTS vyžaduje soubor tvůrčích i technických znalostí a dovedností projektanta. Zároveň je nutná jistá míra předvídavosti a znalosti dané lokality aby se daly co nepřesněji odhadnout případná rizika. Tvůrčí dovednosti projektanta jsou potřeba k vhodnému a účinnému umístění komponentů PZTS tak, aby byly střeženy všechny rizikové oblasti v objektu a zároveň tak, aby jich bylo co nejméně a ušetřily se peníze. Rovněž technické znalosti projektanta a montážního technika jsou nezbytně nutné pro správně nainstalování a nastavení všech komponentů PZTS. Často se zabezpečovací prvky integrují do nějakého systému PZTS, takže technické znalosti stávajícího systému jsou nezbytností pro tuto integraci.

Je nutné, aby celý systém byl nepřetržitě funkční a bezporuchový a navíc pokud možno bez výskytu planých poplachů.

Při návrhu jsem vycházel v první řadě z požadavků zákazníka. Ten kromě standartního spolehlivého chodu systému a požadavků přímo na tento systém nechtěl narušit chod objektu ani jeho vzhled. Proto jsem zvolil jako první variantu návrhu bezdrátový systém Magellan.

Dále jsem vycházel ze své zkušenosti s ústřednami Paradox Security Systems, konkrétně s řadou Digiplex, takže pokud by z jakýchkoli důvodů (slabý signál kvůli přechodu betonovými stropy apod.) nebylo do objektu možné nainstalovat bezdrátovou ústřednu, zvolil jsem jako druhou variantu drátovou ústřednu Digiplex Evo48. Poměr ceny a výkonu je u těchto ústředen velice výhodný a jejich instalace je jednoduchá a přehledná. Proto jsem tento systém zvolil i v následujícím případě.

Celý návrh PZTS je proveden plně v souladu s platnými zákony, vyhláškami a normami. S těmi základními jsme se seznámili v teoretické části diplomové práce.

7.1 Konfigurace systému – Varianta 1

Přání klienta je, aby prvky PZTS nezasahovaly do objektu po stavební stránce, proto je první varianta bezdrátová. Pokud by tento systém kvůli betonové konstrukci objektu nebyl možný, bude použita druhá konfigurace (varianta 2).

Dalším požadavkem je mít objekt rozdělený na dva podsystémy s tím, že veškeré kanceláře, společné prostory, plášťová ochrana a zasedací místnost budou tvořit jeden podsystém, a sklep bude tvořit podsystém druhý.

Tento celý systém obsahuje celkem 27 zón. Z toho důvodu jsem navrhl ústřednu PARADOX MAGELAN MG6250-868. Jedná se o bezdrátový zabezpečovací systém. Velkou výhodou je jeho kompaktnost. Systém tvoří integrovaný ovládací panel (ústředna, klávesnice a bezdrátová nadstavba v jednom).

Nastavení jednotlivých zón

V následujících tabulkách je přehled zón s jejich konfigurací a způsobem zapojení

- pro podsystém 1

Číslo zóny	*Název zóny*	*Typ zóny*	*Název detektoru*
Zóna 1	MG 101	Zpožděná, 30s	MG-DCT10
Zóna 2	PIR 101	Zpožděná, 30s	MG-PMD1P
Zóna 3	GB 101	Okamžitá	G550-868
Zóna 4	MG 102-1 MG 102-2	Okamžitá	MG-DCT10
Zóna 5	PH 102	Okamžitá	SD-738
Zóna 6	PIR 102	Okamžitá	MG-PMD1P
Zóna 7	MG 103-1 MG 103-2	Okamžitá	MG-DCT10
Zóna 8	PH 103	Okamžitá	SD-738
Zóna 9	PIR 103	Okamžitá	MG-PMD1P
Zóna 10	MG 104-1 MG 104-2	Okamžitá	MG-DCT10

Zóna 11	PH 104	Okamžitá	SD-738
Zóna 12	PIR 104	Okamžitá	MG-PMD1P
Zóna 13	MG 106	Okamžitá	MG-DCT10
Zóna 14	PH 105	Okamžitá	SD-738
Zóna 15	PH 202	Okamžitá	SD-738
Zóna 16	PIR 202	Okamžitá	MG-PMD1P
Zóna 17	PH 203	Okamžitá	SD-738
Zóna 18	PIR 203	Okamžitá	MG-PMD1P
Zóna 19	PH 204	Okamžitá	SD-738
Zóna 20	PH 206	Okamžitá	SD-738
Zóna 21	PIR 205	Okamžitá	MG-PMD1P
Zóna 22	PH 301	Okamžitá	SD-738

Tabulka 10: Prvky PZTS v podsystému 1 _ varianta 1

- pro podsystém 2

Číslo zóny	***Název zóny***	***Typ zóny***	***Název detektoru***
Zóna 23	PIR 001	Okamžitá	MG-PMD1P
Zóna 23	PH 001 PH 002	Okamžitá	SD-738
Zóna 24	MG 002-1 MG 002-2	Okamžitá	MG-DCT10
Zóna 23	PIR 002	Okamžitá	MG-PMD1P
Zóna 24	PIR 003	Okamžitá	MG-PMD1P
Zóna 25	MG 003-1 MG 003-2	Okamžitá	MG-DCT10
Zóna 26	PIR 004	Okamžitá	MG-PMD1P
Zóna 27	PH 003 PH 004	Okamžitá	SD-738

Tabulka 11: Prvky PZTS v podsystému 2 _ varianta 1

7.2 Komponenty systému PZTS _ Varianta 1

Pro první variantu jsem zvolil bezdrátový systém Magellan od výrobce Paradox security systems. Předpokládám, že by tato varianta měla být pro daný účel více než dostatečná.

7.2.1 Ústředna Magellan MG6250-868

Jedná se o integrovaný systém PZTS. Hlavní výhodou tohoto systému je kromě jeho bezdrátového provedení i jeho kompaktnost. Ústředna totiž obsahuje integrovaný panel, který je složený ze samotné ústředny, klávesnice a bezdrátové nástavby. To vše je v jednom těle. To jsou hlavní důvody, proč jsem tuto ústřednu zvolena i pro tento objekt. Tato ústředna je kompatibilní se všemi bezpečnostními prvky, potřebnými pro požadované zabezpečení daného prostředí. Tato ústředna je osazena vnitřní sirénou o 90dB. Z toho důvodu nebude v tomto případě použita siréna venkovní. Nebude zde ani atrapa sirény.

Tato ústředna je programována buď přímo z klávesnice nebo pomocí softwaru Babyware.

Technické parametry:

- Maximální počet zón 64
- Maximální počet PGM 8x bezdrátově, 2x na desce
- Maximální počet událostí 256
- Podsystémy 2
- Záložní akumulátor 7 ,2 V, 1,5 Ah, NiMH – integrován v ústředně
- Napájecí výstup 7,5 V, 1A trvale (elektronická pojistka 1,1A)
- Výstup na sirénu 1A (elektronická pojistka 3A)
- Proudový odběr 110 mA
- Integrovaná siréna 90 dB
- Dosah antény 40 m

Obrázek 17: Ústředna Magellan MG6250-868 [15]

Obrázek 18: Vestavěná klávesnice Magellan [15]

7.2.2 Komunikační modul GPRS14

Tento modul slouží ke komunikaci ústředny s DPPC a s uživateli. Je možné jen používat s použitím jedné, nebo dvou SIM karet. Jedna slouží k samotné komunikaci a druhé je pro zálohování komunikace. Tento modul se instaluje přímo do ústředny MG6250-868.

Technické parametry:

- Komunikace: GSM, SMS, GPRS
- Kompatibilita: MG6250-868
- Napájení: z desky ústředny
- Počet tel. Čísel (občanský telefon): 8 (volání nebo SMS)
- Anténa: Externí
- Tys SMS zpráv: poplach / porucha / zapnuto / vypnuto

Obrázek 19: Komunikační modul GPRS14 [16]

7.2.3 PIR MG-PMD1P

Pro detekci pohybu ve vnitřních prostorách objektu jsem zvolil PIR detektor MG-PMD1P. Jedná se o analogový bezdrátový detektor. Detektor MG-PMD1P využívá patentovaný systém zpracování signálu (auto pulse signal procesing) a je vybaven automatickou teplotní kompenzací. Další důležitou doplňkovou funkcí je pak indikace stavu baterií a samozřejmě tamper kontakt, který hlídá sundání detektoru ze zdi, nebo otevření jeho krytu.

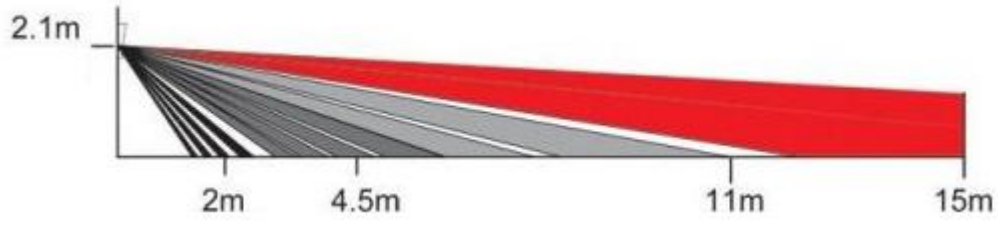
Tento detektor je napájeny třemi AA alkalickými bateriemi a jeho velkou předností je software „Alive“ sloužící k maximalizaci výdrže baterií. Tento software funguje tak, že pokud detektor přenese dva signály porucha v rozmezí asi pěti minut, přepne se detektor do úsporného režimu. Po dalších pěti minutách se přepne zpět do klasického režimu a tím šetří baterii.

Parametry detektoru:

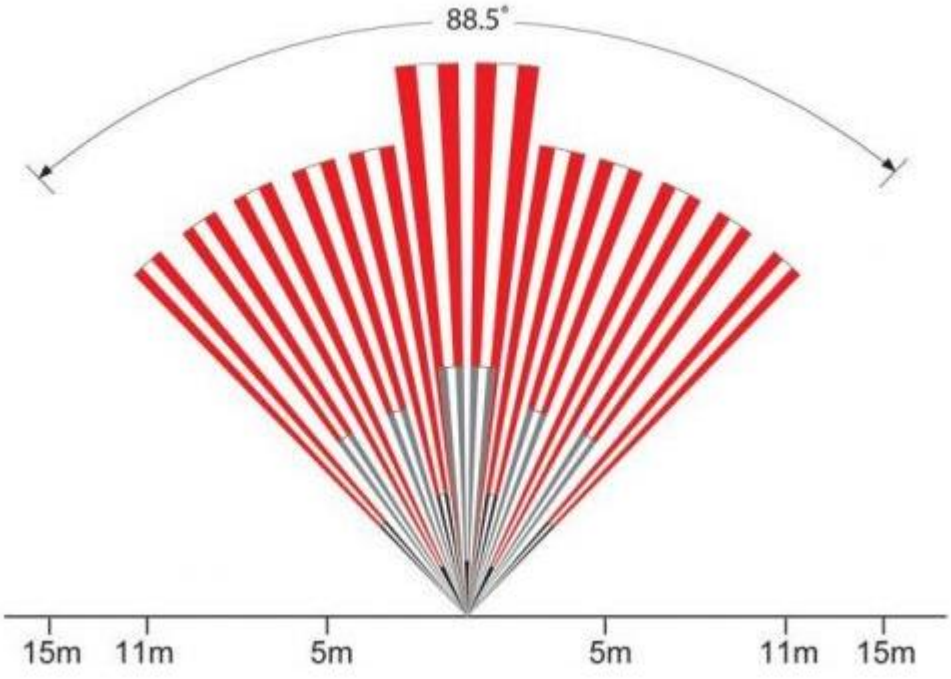
Zpracování signálu	Analogový
Montážní výška	2,1 – 2,7 m
Baterie	3x AA alakalická baterie
Výdrž baterie	Až 4 roky
FR frekvence	433MHz nebo 868MHz
Čočky	2. generace Fresnelových čoček LODIFF
Přenosový dosah	35m

Tabulka 12: Parametry detektoru MG-PMD1P

Detekční diagramy:



Obrázek 20: Detekční diagram PIR detektoru MG-PMD1P [17]



Obrázek 21: Detekční diagram PIR detektoru MG-PMD1P [17]

PIR detektor MG-PMD1P:

Obrázek 22: MG-PMD1P [17]

7.2.4 Magnetický kontakt MG-DCT10

Pro zabezpečení detekce otevření (zavření) oken či dveří jsem vybral magnetické kontakty MG-DCT10. tyto magnetické kontakty jsou taky bezdrátové a jsou napájeny Alkalickými bateriemi typu AAA. Tělo detektoru je obsahuje tamper kontakt pro detekci jeho otevření

Parametry detektoru:

Vstup	NC
FR frekvence	433MHz nebo 868MHz
Indikace stavu baterie	LED diody
Přenosový dosah	35m
Rozměry	124 x 45 x 33 mm

Tabulka 13: Technické parametry magnetického detektoru MG-DCT10

Obrázek 23: Magnetický kontakt MG-DCT10 [18]

7.2.5 Kouřový detektor SD-738

Kouřový detektor SD-738 je vysoce citlivý opticko-kouřový bezdrátový detektor. Tento detektor zároveň obsahuje vlastní sirénu pro akustickou indikaci požáru. Tento výrobek není od firmy Paradox, ale je pro ni exkluzivně vyráběn společností EVERday Technology Co. Ltd. Tím, že je vyráběn přímo pro ústředny od Paradox security systems, je zaručená kompatibilita s ústřednou MG6250-868.

Parametry detektoru:

FR frekvence	433MHz nebo 868MHz
Indikace stavu baterie	LED diody
Přenosový dosah	30m
Vlhkost	10 až 85%
Životnost baterií	18 měsíců
Rozměry	10 cm (průměr) x 3,2cm (výška)

Tabulka 14: Parametry opticko-kouřového detektoru SD-738

Obrázek 24: Opticko-kouřový detektor SD-738 [19]

7.2.6 Detektor tříštění skla G550-868

Pro detekci rozbití skleněné desky ve vstupní hale uvažuji s použitím detektoru tříštění skla. Pro tyto účely jsem zvolil bezdrátový detektor Paradox G550-868. Tento detektor se umísťuje před chránění sklo, nebo na protější zeď (v dosahu detektoru). Tento detektor má kruhovou charakteristiku snímání okolí a detekuje rozbití skla až na vzdálenost šesti metrů. Pouzdro tohoto detektoru je osazeno tamper kontaktem pro detekci vniknutí do detektoru.

Parametry detektoru:

Typ detektoru	Digitální audio, elektretový senzor
FR frekvence	868MHz
Indikace stavu baterie	LED diody
Přenosový dosah	35m
Úhel záběru, dosah	Kruhová charakteristika, 1 až 6 m
Napájení	3x AAA alkalické baterie
Životnost baterií	Až 2 roky
Rozměry	95 x 60 x 35 mm

Tabulka 15: Detektor tříštění skla Paradox G550-868

Obrázek 25:
Paradox G550-868 [20]

7.3 Konfigurace systému _ Varianta 2

Celý systém PZTS v této variantě bude rovněž obsahovat 27 zón a bude rozdělen do dvou podsystémů, stejně jako u varianty č. 1.

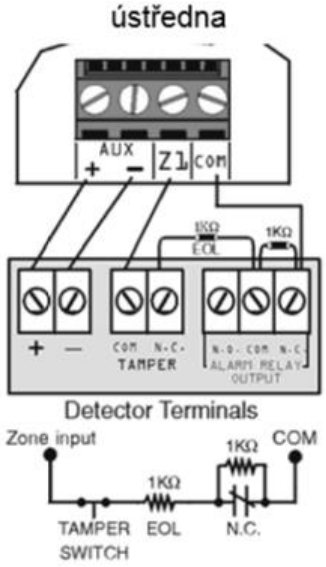
Na tento systém budou použity 3 rozšiřující moduly ARP-ZX8,. Samotná ústředna má jen 8 svorek. Ty budou využity na zabezpečení hlavního vstupu a svorka Z8 zůstane pro tamper boxu ústředny. Zbytek prvků PZTS bude zapojen přes již zmíněné expandéry.

Ústředna bude umístěna v podsystému 2 a bude napájena pomocí kabelu CYKY-J 3×1,5 (3Cx1,5). Kabel bude natažen z ústředny přímo do rozvaděče a bude mít samostatný jistič. Záložní akumulátor ústředny je umístěn přímo v boxu s ústřednou, a tudíž je dobře ochráněn. Jedná se o Akumulátor Alarmguard CJ 12-18 (12V/18Ah) až s dvanáctihodinovou výdrží.

Detektory budou připojeny 6-žilovým kabelem (W-6x0,22+2x0,5) k ústředně nebo k expandérům. Expandéry se k ústředně připojí taktéž 6-žilovým kabelem.

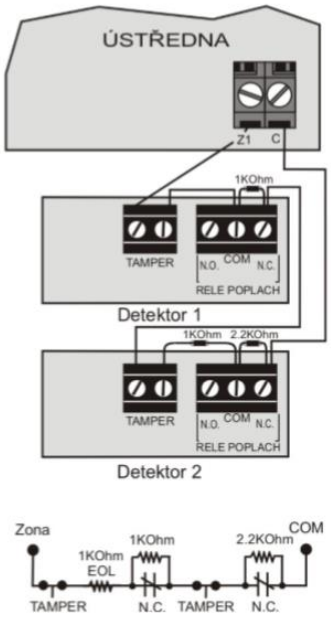
Zapojení komponentů

Většina komponentů bude mít samostatnou svorku v ústředně nebo v expandéru. Tyto smyčky budou normálně zavřené (NC) se zakončovacím odporem – EOL a hlídaným tamperem proti sabotáži. (obrázek č. 15)



Obrázek 26: NC kontakty s EOL, s hlídáním tamperu [21]

Jiné prvky (např. magnetické kontakty v oknech, kde jsou po dvou) budou zapojeny za pomocí NC smyček s EOL s ATZ a s tamperem



Obrázek 27: NC kontakty s EOL, s ATZ s tamperem [21]

Nastavení jednotlivých zón

V následujících tabulkách je přehled zón s jejich konfigurací a způsobem zapojení

- pro podsystém 1

Číslo zóny	***Název zóny***	***Typ zóny***	***Název detektoru***	***Zapojení***
Zóna 1	MG 101	Zpožděná, 30s	P3G SM60	EVO (Z1), EOL
Zóna 2	PIR 101	Zpožděná, 30s	Optex RXC-ST	EVO (Z2), EOL
Zóna 3	GB 101	Okamžitá	Glasstrek 457	EVO (Z3), EOL
Zóna 4	MG 102-1 MG 102-2	Okamžitá	P3G SM60	EVO (Z4), EOL s ATZ
Zóna 5	PH 102	Okamžitá	VAR-TEC FDR 26-S	EVO (Z5), EOL
Zóna 6	PIR 102	Okamžitá	Optex RXC-ST	EVO (Z6), EOL

Zóna 7	MG 103-1 MG 103-2	Okamžitá	P3G SM60	EXP. 2 (Z1), EOL s ATZ
Zóna 8	PH 103	Okamžitá	VAR-TEC FDR 26-S	EXP. 2(Z2), EOL
Zóna 9	PIR 103	Okamžitá	Optex RXC-ST	EXP. 2(Z3), EOL
Zóna 10	MG 104-1 MG 104-2	Okamžitá	P3G SM60	EXP. 2 (Z4), EOL s ATZ
Zóna 11	PH 104	Okamžitá	VAR-TEC FDR 26-S	EXP. 2(Z5), EOL
Zóna 12	PIR 104	Okamžitá	Optex RXC-ST	EXP. 2(Z6), EOL
Zóna 13	MG 106	Okamžitá	P3G SM60	EXP. 2(Z7), EOL
Zóna 14	PH 105	Okamžitá	VAR-TEC FDR 26-S	EXP. 2(Z8), EOL
Zóna 15	PH 202	Okamžitá	VAR-TEC FDR 26-S	EXP. 3(Z1), EOL
Zóna 16	PIR 202	Okamžitá	Optex RXC-ST	EXP. 3(Z2), EOL
Zóna 17	PH 203	Okamžitá	VAR-TEC FDR 26-S	EXP. 3(Z3), EOL
Zóna 18	PIR 203	Okamžitá	Optex RXC-ST	EXP. 3(Z4), EOL
Zóna 19	PH 204	Okamžitá	VAR-TEC FDR 26-S	EXP. 3(Z5), EOL
Zóna 20	PH 206	Okamžitá	VAR-TEC FDR 26-S	EXP. 3(Z6), EOL
Zóna 21	PIR 205	Okamžitá	Optex RXC-ST	EXP. 3(Z6), EOL
Zóna 22	PH 301	Okamžitá	VAR-TEC FDR 26-S	EXP. 3(Z7), EOL

Tabulka 16: Prvky PZTS v podsystému 1

- pro podsystém 2

Číslo zóny	*Název zóny*	*Typ zóny*	*Název detektoru*	*Zapojení*
Zóna 23	PIR 001	Okamžitá	Optex RXC-ST	EXP. 1(Z1), EOL
Zóna 23	PH 001 PH 002	Okamžitá	VAR-TEC FDR 26-S	EXP. 1(Z2), EOL
Zóna 24	MG 002-1 MG 002-2	Okamžitá	P3G SM60	EXP. 1 (Z3), EOL s ATZ
Zóna 23	PIR 002	Okamžitá	Optex RXC-ST	EXP. 1(Z4), EOL
Zóna 24	PIR 003	Okamžitá	Optex RXC-ST	EXP. 1(Z5), EOL
Zóna 25	MG 003-1 MG 003-2	Okamžitá	P3G SM60	EXP. 1 (Z6), EOL s ATZ
Zóna 26	PIR 004	Okamžitá	Optex RXC-ST	EXP. 1(Z7), EOL
Zóna 27	PH 003 PH 004	Okamžitá	VAR-TEC FDR 26-S	EXP. 1(Z8), EOL

Tabulka 17: : Prvky PZTS v podsystému 2

Poznámka: Všechny prvky PZTS jsou zapojeny jako NC s EOL s hlídaným tamperem. Rozdíl je při zapojení dvou prvků do jedné svorky. Pro tento účel používám typ s ATZ. Tyto typy zapojení vychází přímo z manuálu ústředny.

Ústředna bude připojena na DPPC vybrané společnosti. Tato soukromá bezpečnostní firma zatím nebyla vybrána, podkladem pro výběrové řízení bude tato práce. Bezpečnostní agentura bude vybrána na základě jejího dojezdového času v momentě vyhlášení poplachu a samozřejmě na základě jejich cen za nabízené služby. Nejedná se za cenu pouze za práci při montáži, ale také za paušální cenu napojení na pult a veškeré další servisní, revizní a výjezdové služby.

7.4 Komponenety PZTS _ Varianta 2

7.4.1 Ústředna Digiplex EVO48

Pro PZTS jsem vybral ústřednu od firmy Paradox Security Sysems, která je určena pro střední a velké objekty. Paradox je kanadská firma, která je na trhu přes 20 let a za tu dobu vyvinula vysoce sofistikovaný systém. Celý tento systém je možné rozdělit do čtyř podsystémů.

Digiplex Evo48 je sběrnicová ústředna, u které lze připojit detektory přímo na sběrnici, nebo přes expandéry.

Ústřednu jsem zvolil z důvodu možnosti výhodného poměru cena/nabízené služby a z důvodu její relativně snadné instalace a nastavení. Ústřednu zle rozšířit až do počtu čtyřiceti osmi zón a to také skrze bezdrátovou nástavbu.

Technické parametry:

- Střídavé napětí: 16V, 20/40 VA, 50-60 Hz
- Zálohovací akumulátor 12Vss – 4hod minimálně
- Napájecí výstup 12Vss, 600mA trvale (elektronická pojistka 1,1A)
- Výstup na sirénu 1A (elektronická pojistka 3A)
- Proudový odběr 110 mA

Základní vlastnosti:

- 8 zón (16 při zdvojení zón, ATZ technologie)
- Integrované vlastnosti přístupového systému
- Programování pomocí systému Winload nebo NEware
- 2 pevné PGM
- Paměť na 1024 událostí
- 96 uživatelských kódů
- Podpora až 127 rozšiřujících sběrnicových modulů
- Umožňuje navolit až 4 podsystémy
- Zabudovaná baterie reálného času

- Sledovaný okruh sirény, výstupu a telefonní linky
- Mechanické tlačítko pro nastavení továrních hodnot
- Podsvícení klávesnic dle času (automatická úspora)
- Možnost bezdrátové nástavby pomocí RTX3

Obrázek 28: Digiplex EVO48 [21]

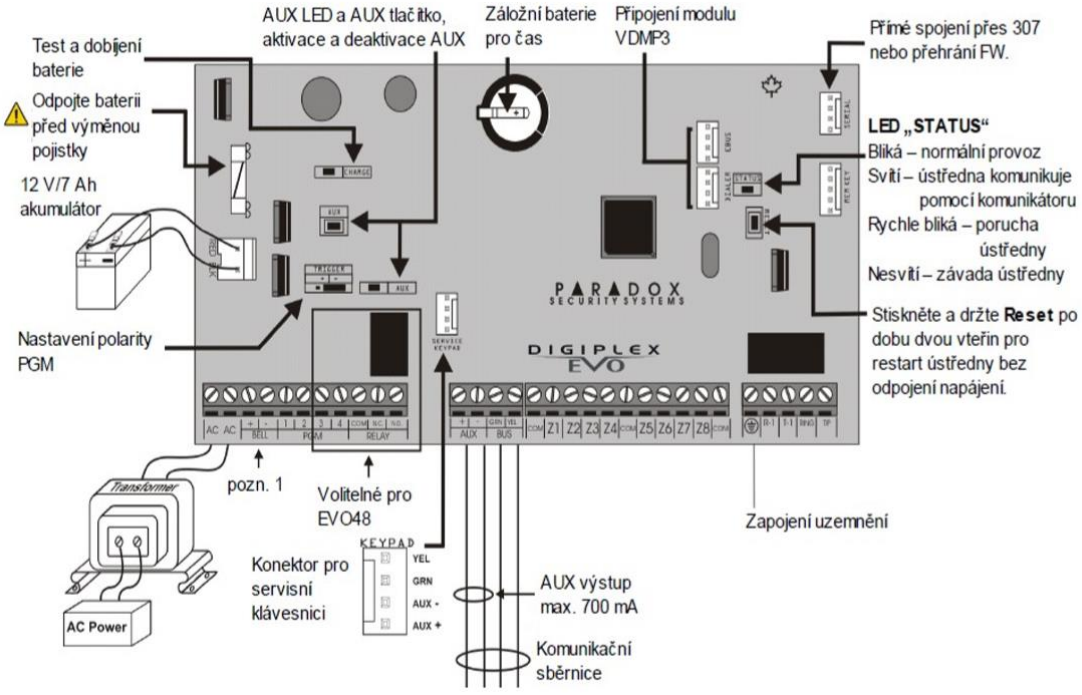
Programování ústředny se provádí nejčastěji pomocí programu Winload. Počítač se připojí pomocí speciálního Direct Connect Interface 307USB-TI08 (viz obrázek 12). Druhá možnost programování prvků je pomocí klávesnice. To je vhodné spíše pro rychlé úpravy nastavení. Pro první instalaci se doporučuje použití počítače (Winload). Je to hlavně z důvodu přehlednosti a rychlosti a to i případě, když zkušený technik umí velice rychle a obratně pracovat se systém i přes klávesnici.

Obrázek 29: 307USB
[Zdroj: Autor]

Prostor kolem ústředny bude následně střežen PIR detektorem pohybu (mimo MZS)

Konkrétní nastavení jednotlivých zón a umístění prvků PZTS do jednotlivých expandérů bude uvedeno v samostatné kapitole. Pro návrh jsem použil SW Winload.

Schematické zapojení ústředny:



Obrázek 30: Schéma základního zapojení [21]

Technické parametry ústředny EVO48:

Střídavé něpětí	16V, 20/40 VA, 50-60 Hz
Zálohovací akumulátor	12Vss – 4 hod minimálně
Napájecí výstup	12Vss, 600mA trvale (elektronická pojistka 1,1A)
Výstup na sirénu	1A (elektronická pojistka 3A)
Proudový odběr	110 mA

Tabulka 18: Technické parametry ústředny Digiplex EVO48

Základní vlastnosti ústředny EVO48:

- 8 zón (16 při zdvojení zón, ATZ technologie)
- Integrované vlastnosti přístupového systému
- Programování pomocí systému Winload nebo NEware
- 2 pevné PGM
- Paměť na 1024 událostí
- 96 uživatelských kódů
- Podpora až 127 rozšiřujících sběrnicových modulů
- Umožňuje navolit až 4 podsystémy
- Zabudovaná baterie reálného času
- Sledovaný okruh sirény, výstupu a telefonní linky
- Mechanické tlačítko pro nastavení továrních hodnot
- Podsvícení klávesnic dle času (automatická úspora)
- Možnost bezdrátové nástavby pomocí RTX3

7.4.2 Komunikační modul PCS200

Komunikační modul PCS200 poskytuje EZS ústřednám Paradox možnost bezdrátové komunikace, přenos systémových událostí prostřednictvím GPRS nebo GSM sítě na DPPC (dohledové a poplachové přijímací centrum). Modul PCS200 lze nakonfigurovat tak, aby posílal události koncovému uživateli prostřednictvím SMS a vzdáleně komunikoval (upload / download) se softwarem Winload přes GPRS. To vše je dosaženo pomocí jednoduchého 4-vodičové sériové spojení mezi ústřednou a modulem PCS200. Modul PCS200 lze instalovat až 2m od EZS ústředny. Anténu na modulu lze nainstalovat až do vzdálenosti 18m od zařízení, pomocí volitelného anténní prodloužení v závislosti na síle signálu. *[Eurosat]*

Technické parametry komunikátoru:

Výstupní výkon	Class 4 (2W) @ 850 / 900 MHz Class 2 (1W) @ 1800 / 1900 MHz
Šířka pásma	70 / 80 / 140 / 170 MHz Automatická detekce pásma
Anténa	Zisk 3dBi, impedance 50 Ohm, příkon 2W max.
Odběr	80 mA, max. 600 mA při GPRS / GSM přenosu
Provozní teplota	0 - +50 °C
Kódování	128-bit (MD5 a RC4) nebo 256-bit (AES)
SMS protokol	8-bit (IRA: ITU-T.50) nebo 16-bit (UCS2 ISO/IEC10646)

Tabulka 19: Technické parametry komunikačního modulu PCS200

7.4.3 Rozšiřující modul APR-ZX8

Ústředna Digiplex EVO48 má sama o sobě jen 8 svorek pro připojení jednotlivých prvků. Pro rozšíření počtu střežených zón použijeme tento modul. Pomocí expandérů je možné systém rozšířit až na 48 zón.

Pro tento systém budou tyto moduly použity celkem 3.

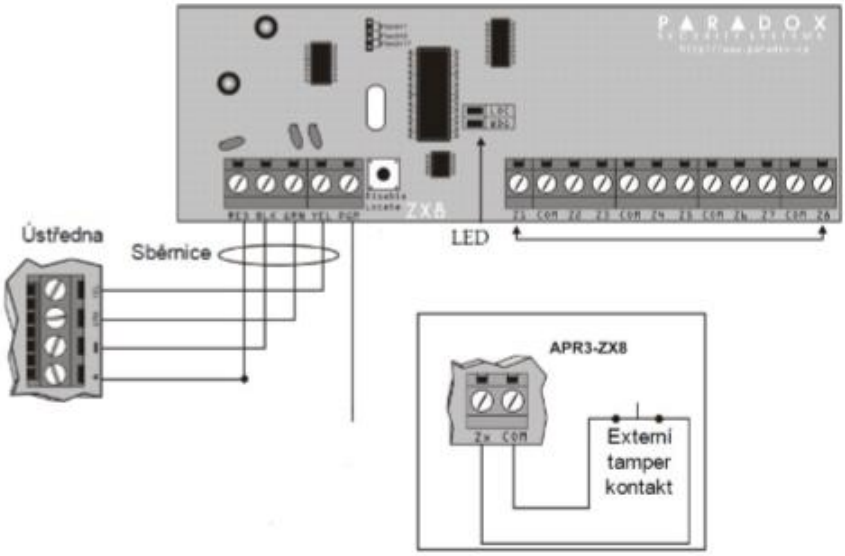
Technické parametry modulu:

Napájení	9 – 16 Vdc
Proudový odběr	28 -31 mA
Pracovní teplota	-10 až +50 °C
Vlhkost	max. 95%
Typy zón	NC, s detekcí tamperu na smyčce
Rozměry	140 x 46 mm
Vyhodnocení	Digitálně
Max. zatížení PGM výstupu	50 mA
Metody zpracování	Automatické pulsy, dvě úrovně, teplotní kompenzace
Optická indikace	Červená, zelená

Tabulka 20: Technické parametry expandéru APR-ZX8

Rozšiřující modul a schéma jeho zapojení do ústředny

Obrázek 31: Rozšiřující modul APR-ZX8 [22]



Obrázek 32: Schéma zapojení modulu [21]

Ústředna Pradox EVO48 je sběrnicová ústředna, do které se prvky řadí sériově. To znamená, že BUS sběrnice jde nejprve do klávesnice, pak do expandérů a až pak se vrací zpět do štředny.

7.4.4 Klávesnice Digiplex K641

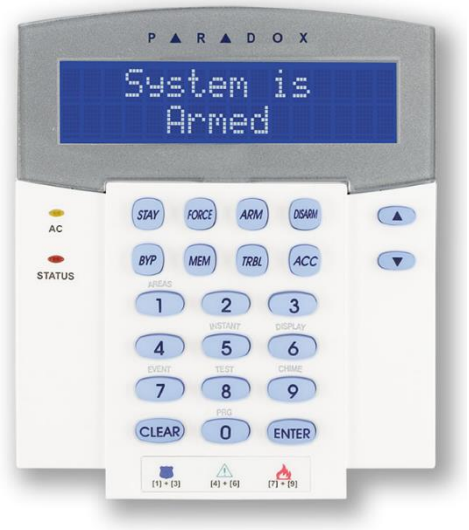
Klávesnice Digiplex K641 je od stejného výrobce jako ústředna EVO 48, tedy firmy Paradox Security Systems. Tato klávesnice je uživatelsky velice příjemná. Její jednoduché prostředí je vhodné i pro techniky pro nastavení ústředny, i pro kódování budovy či jednotlivých zón v běžném provozu.

Klávesnice je vybavena dvouřádkovým displejem se 32 znaky pro zobrazování zpráv, instrukcí, nebo stavu PZTS. Tento displej má samozřejmě nastavitelný kontrast, osvětlení a dokonce lze korigovat rychlost přepínání jednotlivých zpráv dle přání zákazníka.

Ústředna Digiplex EVO je vybavena hlídaným výstupem pro připojení klávesnice.

Základní vlastnosti:

- 32 znaků (2x16)
- Modře podsvícený LCD displej
- Možnost českého jazyka
- 1 zóna a 1 PGM (omezená tabulka PGM událostí)
- 14 tlačítek
- Nezávislé nastavení zvonkohry
- Možnost přiřazení jedné, nebo více skupinám



Obrázek 33: Klávesnice K641 [23]

Základní parametry klávesnice K641

Napájení	9 – 16 Vss
Proudová spotřeba	110 mA
Proudové omezení PGM	50 mA
Počet vstupů	1
Indikace napájení	Žlutá LED (svítí)
Indikace umístění	Zelená a žlutá LED (společně blikají)
Indikace chybné komunikace	Červená a žlutá LED (blikají střídavě)

Tabulka 21: Parametry klávesnice Digiplex K641

7.4.5 PIR Optex RXC-ST

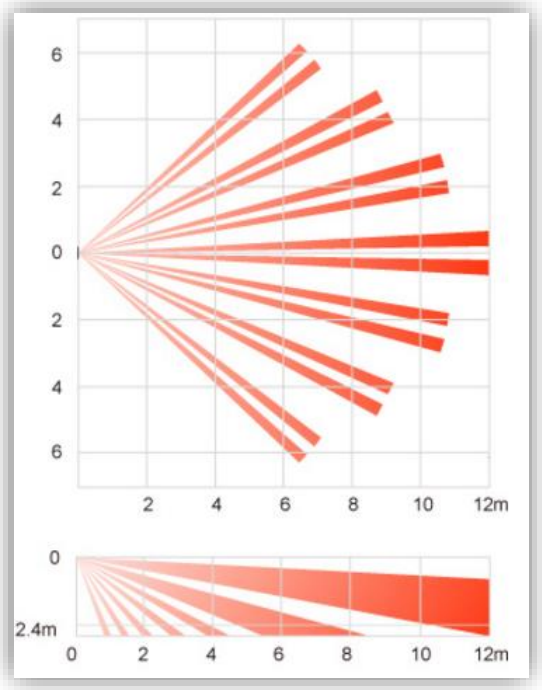
Pro detekci pohybu jsem zvolil PIR detektory od firmy Optex. Jedná se o model RXC-ST. Tento detektor je vhodný pro zastřežení vnitřních prostor komerčních i nekomerčních objektů. V balení nalezneme i sadu pro uchycená na zeď, která je velice prakticky koncipována. Detektor se většinou kvůli jeho detekční charakteristice umisťuje do rohu místností do výšky v rozmezí mezi 2200 a 2400 mm od podlahy. Výrobce sice udává, že montážní výška je už od 1500mm, ale pro jeho náročnější sabotování se doporučuje jej dávat mimo dosah běžného člověka. Tato klávesnice je opatřena odklápěcím krytem. Toto řešení vyhovuje požadavkům klienta (působí reprezentativněji než klávesnice s odkrytými tlačítky). Tento detektor je samozřejmě plně kompatibilní s ústřednou Paradox EVO 48.

Obrázek 34: Optex RXC-ST
[Zdroj: Autor]

Základní parametry detektoru:

Zpracování signálu	Digitální
Montážní výška	1,5 – 2,4 m
Napájení	9,5 – 16 Vss
Odběr (nominální/maximální)	8mA / 11mA
Poplachový výstup	Polovodičový NC, 24Vss / 0,2 A
Sabotážní výstup	NC
Poplachová perioda	30s
Třída prostředí	II – vnitřní všeobecné
Pracovní teplota	-20 - +50 °C
Rozměry (výška / šířka / hloubka)	93,4 mm / 61,4 mm / 46 mm
Hmotnost	70 g

Tabulka 22: Základní parametry detektoru OPTEX RXC-ST

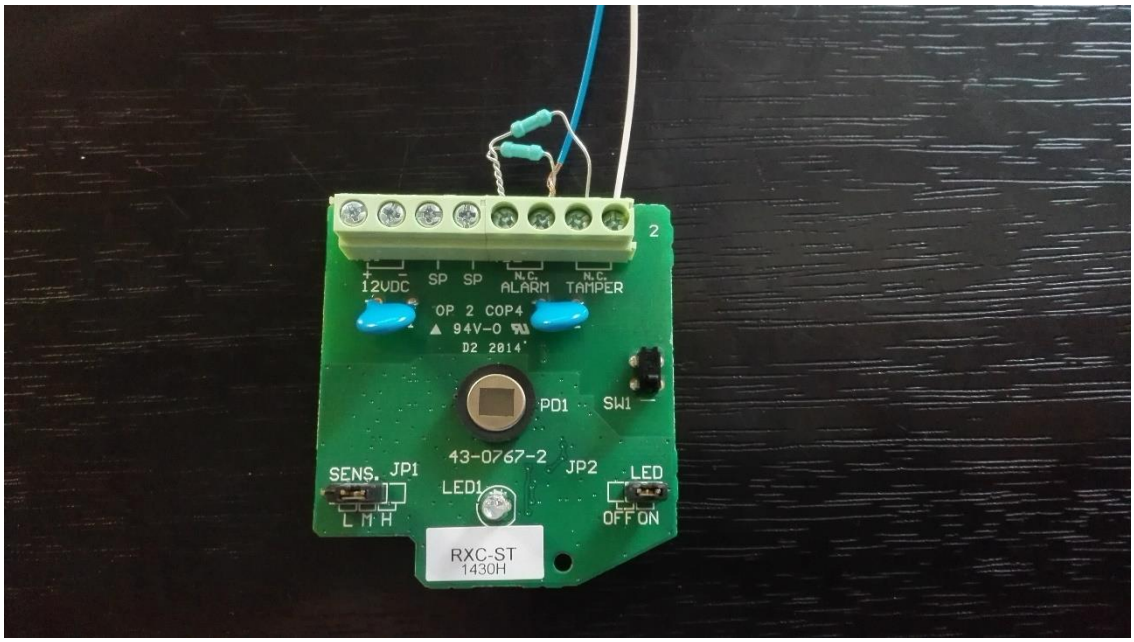


Obrázek 35: Detekční diagram detektoru OPTEX RXC-ST [24]

Ústředna Paradox EVO 48 je nastavená daná hodnota pro odporové vyvážení smyček. V případě EOL vyvažujeme s použitím rezistorů o velikosti 1kΩ a v případě 2EOL kombinací 1kΩ a 2,2kΩ.

Každá zóna má v tomto konkrétním případě samostatnou svorku (v ústředně nebo v expandéru). Například zóna 1 se zapojí do svorky Z1, pak projde do detektoru, a pak jde zpět do ústředny do svorky COM.

Při instalaci je není vhodné umísťovat detektor naproti ventilačním šachtám či klimatizaci (nebo jakýchkoli jiných předmětů, které rychle mění teplotu). Není vhodné umísťovat detektor ani i infračerveným zdrojům světla. Plané poplachy může vyvolat dokonce i lednice nebo sporák, které vyvolá proudění vzduchu, na které může detektor reagovat. V neposlední řadě se rovněž nedoporučuje umístění naproti lesklým a průhledným stěnám.



Obrázek 36: Odporové vyvážení detektoru - EOL s tamperem [Zdroj: Autor]

7.4.6 Magnetické kontakty Paradox 3G SM60

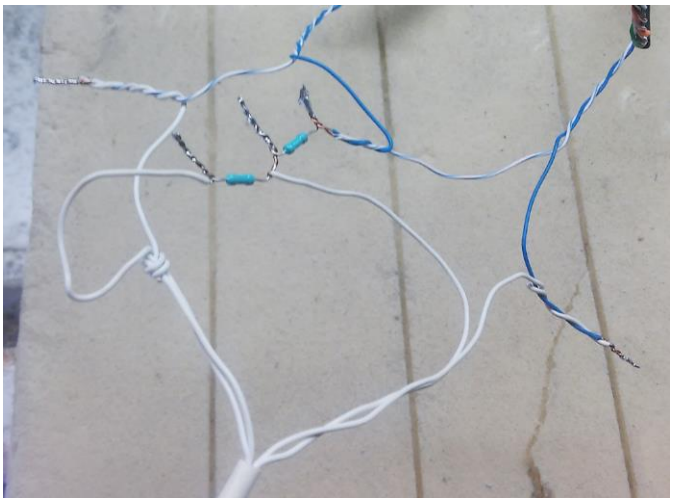
Vysoká bezpečnost magnetického kontaktu díky polarizování. Tento magnetický kontakt nelze vyřadit jiným magnetem.

Jedná se o 4 vodičový magnetický kontakt

- smyčka pracovní,
- 2. smyčka samotážní.

Magnetický kontakt je plastový a má otvory pro přišroubování. Jeho maximální pracovní vzdálenost je 30mm.

Obrázek 37: Magnetický kontakt PARADOX [25]

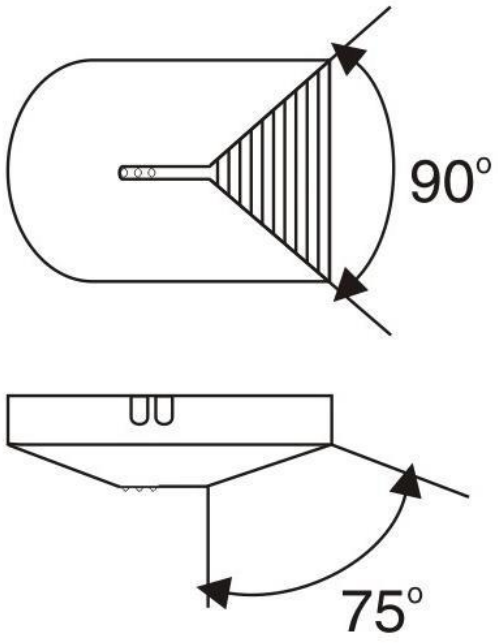


Obrázek 38: Odporové vyvážení s EOL s tamperem [Zdroj: Autor]

7.4.7 Detektor tříštění skla Glasstrek 457

Detektor tříštění skla Glasstrek 457 je klasický akustický detektor. Tříštění skla má charakteristický zvuk, který tento detektor rozpozná a vyhodnotí a v případě shody může vyvolat poplachový stav. Pro tuto detekci používá dvou frekvencí. V první řadě se jedná o nízkofrekvenční vlnu nárazu a v řadě druhé vysokou frekvenci tříštění skla. Pro vyhlášení poplachu je třeba zachytit obě frekvence, jinak se poplach nevyhlásí. Tento detektor splňuje požadavky pro druhou třídu prostředí a je certifikován pro třetí stupeň zabezpečení.

Obrázek 39: Glasstrek 457 [26]



Obrázek 40: Detekční charakteristika [26]

Vlastnosti detektoru:

- Analýza slyšitelného zvukového pásma i infrazvuku
- Nastavitelná citlivost (4,5 – 9 m)
- Nepodléhá vysokofrekvenčnímu rušení
- Tamper kontakt proti sabotáži

Technické parametry detektoru:

Napájení	9 – 16 Vdc
Proudový odběr	20 – 37 mA
Pracovní teplota	-10 až +50 °C
Krytí	IP 50
Poplachové relé / tamper	28 Vdc, 150 mA
Rozměry	90 x 67 x 25

Tabulka 23: Technické parametry Glassbreak detektoru

Instalace detektoru:

Základní zásadou pro instalaci tohoto detektoru je jeho umístění přímo před skleněnou tabuli, které hrozí rozbití a to na pevný podklad. Je vhodné si před montážní každého takového detektoru zjistit z manuálu jeho detekční dosah a následně detektor umístit dle pokynů. Pro všechny případy v tomto objektu je dosah vyhovující, i když je detektor umístěn na protější zdi. Kdyby tomu tak nebylo, musí se umístit doprostřed místnosti.

Tento detektor není vhodný do hlučných prostor, kde hrozí vyhlašování planých poplachů.

Co se týče zapojení do ústředny tak se tento detektor zapojuje a vyvažuje stejně jako PIR detektory. Vyvážení se provádí rezistory o velikosti 1kΩ

7.4.8 Požární detektor VAR-TEC FDR 26-S

Tento opticko-kouřový detektor je určen jako doplňkový detektor k systémům PZTS. Nepotřebuje tedy vlastní ústřednu EZS. Detekce kouře je u tohoto detektoru založena na principu vniknutí kouře do vyhodnocovací komory, která je prosvětlována IR diodou a tento svit je zpětně vyhodnocován. Kouř změní vlastnosti IR paprsku a detektor vyhodnotí poplach. K ukončení poplachu dojde až po „vyvětrání“ detekční komory v čidle od kouře.

Technické parametry detektoru

Napájení	10,5 -14VDC
Proudový odběr	klid 0,032 mA, poplach 55 mA
Pracovní teplota	-10 až +50 °C
Krytí	IP 42
Výstup	NO/NC, relé max. 1A, 30V SS
Optická indikace	Červená LED dioda
Detekční plocha	Max. 40 m^2
Montážní výška	Max. 7 m

Tabulka 24: Technické parametry detektoru FDR 26-S

Obrázek 41: VAR-TEC FDR 26-S [27]

7.4.9 Siréna TEKNIM-720WR

Venkovní siréna VAR-TEC FDR 26-S je vybavena akustickou i optickou signalizací. Pro akustickou signalizaci siréna používá piezoměnič a pro optickou signalizaci stroboskop. Je to zálohovaná siréna s tamper kontaktem proti jejímu otevření nebo sundání ze zdi. K zálohování je součástí dodávky i akumulátor (konkrétně Ni-MH akumulátor). Tato siréna splňuje požadavky pro čtvrtý stupeň zabezpečení a pro čtvrtou třídu prostředí. Tato siréna se připojuje do ústředny do speciální hlídané svorky BELL.

Technické parametry sirény

Napájení	9 – 16 V dc
Proudový odběr	450 mA
Detekce napájení	2 červené LED diody
Akustický výkon	118 dB/m
Akustická signalizace	piezo siréna
Optická signalizace aktivace sirény	červený blikač stroboskop 1Hz
Tamper	sejmutí ze zdi, otevření sirény
Venkovní krytí	IP 44
Rozměry	212mm / 300mm / 60mm

Tabulka 25: Technické parametry sirény

Obrázek 42:
Siréna Teknim [28]

7.5 CCTV

Pro kamerový systém jsem zvolil sestavu Evolveo Detective S4CIH7D. Tato sestava se skládá ze 4 IP kamer pro vnitřní i venkovní použití, rekordéru s dálkovým ovládáním, myší i kabeláží. Ke každé kameře je 18m dlouhý kabel, který je pro tyto účely plně dostačující. Výhodou tohoto systému je jeho snadná instalace. Vzhledem k tomu, že se jedná o předem sestavený set, je vše v podstatě nachystané a to je i jeden z důvodů, proč jsem zvolil celý systém uzavřeného televizního okruhu v jednom kuse od jednoho prodejce.

Technické parametry kamer:

Záznamový senzor	0,25" CMOS čip s rozlišením 700TVL
Průměr čočky	3,6 mm
Viditelný úhel	62,2°
Rozlišení	PAL: 976 x 582 NTSC: 976 x 494
Video výstup	1.0 Vp-p750Ohm
S/N poměr	Přes 52 dB
Gamma charakteristika	0,45
Rychlost uzávěrky	1/50-1/100000 sec
IR dosah pro noční vidění	20 – 25 m
Provozní teplota	-10 až +45 °C
Spotřeba	12Vdc, 260mA (se zapnutým IR přísvitem)
Krytí	IP 65

Tabulka 26: Technické parametry kamer Evolveo

Technické parametry sestavy a rekordéru:

• DVR jednotka
• video komprese: H.264
• video systém: NTSC/PAL
• k dispozici SW pro Windows/Android/Symbian/MAC OS kompatabilní zařízení
• možnosti zobrazeni záznamu: samostatná kamera, 4 kamery, střídavé
• záznamové módy: určený čas/ detekce pohybu/spuštění senzorem
• HDD rozhraní: 1 x SATA HDD 2.5" nebo 3.5", max. kapacita 4TB
• vyhledávání záznamu podle času a data, nebo podle událostí
• SW možnost ovládání pohybu kamer
• síťové rozhraní: RJ45 10/100Mbit/sec
• síťové protokoly: TCP/IP, UDP, DHCP, DNNNS, PPPoE
• přístup přes internet: přístup v reálném čase prostřednictvím Internet Exploreru a přes mobilní telefony
• zálohování: AVI soubory přes USB flash, USB externí disk, USB CD/DVD
• přehrávání: Normální rychlost/Rychlé/rychlé zpět, po jednotlivých snímcích
• záznam po zvoleném časovém úseku: 15/30/45/60 min
• dálkový ovladač je součástí balení
• myš je součástí balení
• napájecí zdroj: DC12V/3A
• VGA/HDMI rozhraní: ano
• datový tok: při střední kvalitě záznamu přibližně 225MB na 1 kameru za hodinu [ALZA]

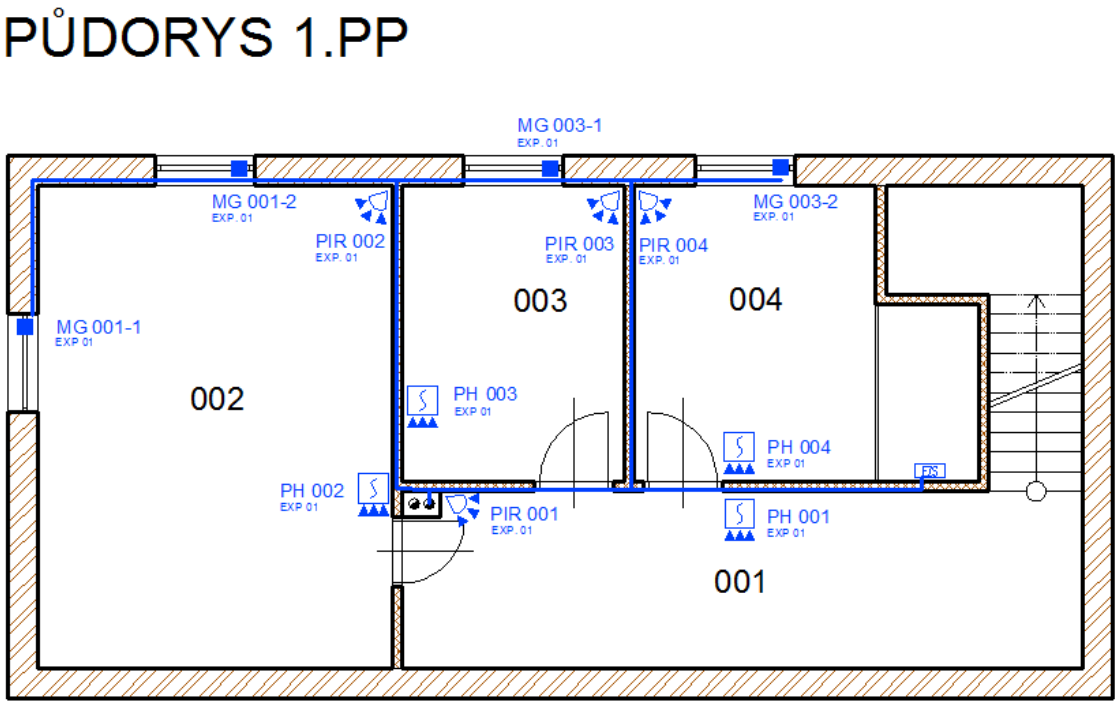
7.5.1 Umístění kamer

V tomto systému Evolveo Detective jsou celkem 4 kamery, což je přesný počet požadovaný pro tento objekt. První kamera zabírá vstupní branku do perimetru objektu a zároveň i prostor před hlavním vchodem. Kamera druhá je namířena na garáž a sleduje jak samotné vrata do garáže, tak i altánek spojený s garáží, kde zaměstnanci nechávají svá kola a odkud už byly několikrát odcizeny. Třetí kamera snímá prostor hlavní brány a cestu ke garáži. Poslední kamera zabírá prostor před průčelím objektu, kde je umístěna siréna a hranici perimetru, kde je HUP, který byl v minulosti opakovaně poničen vandaly.

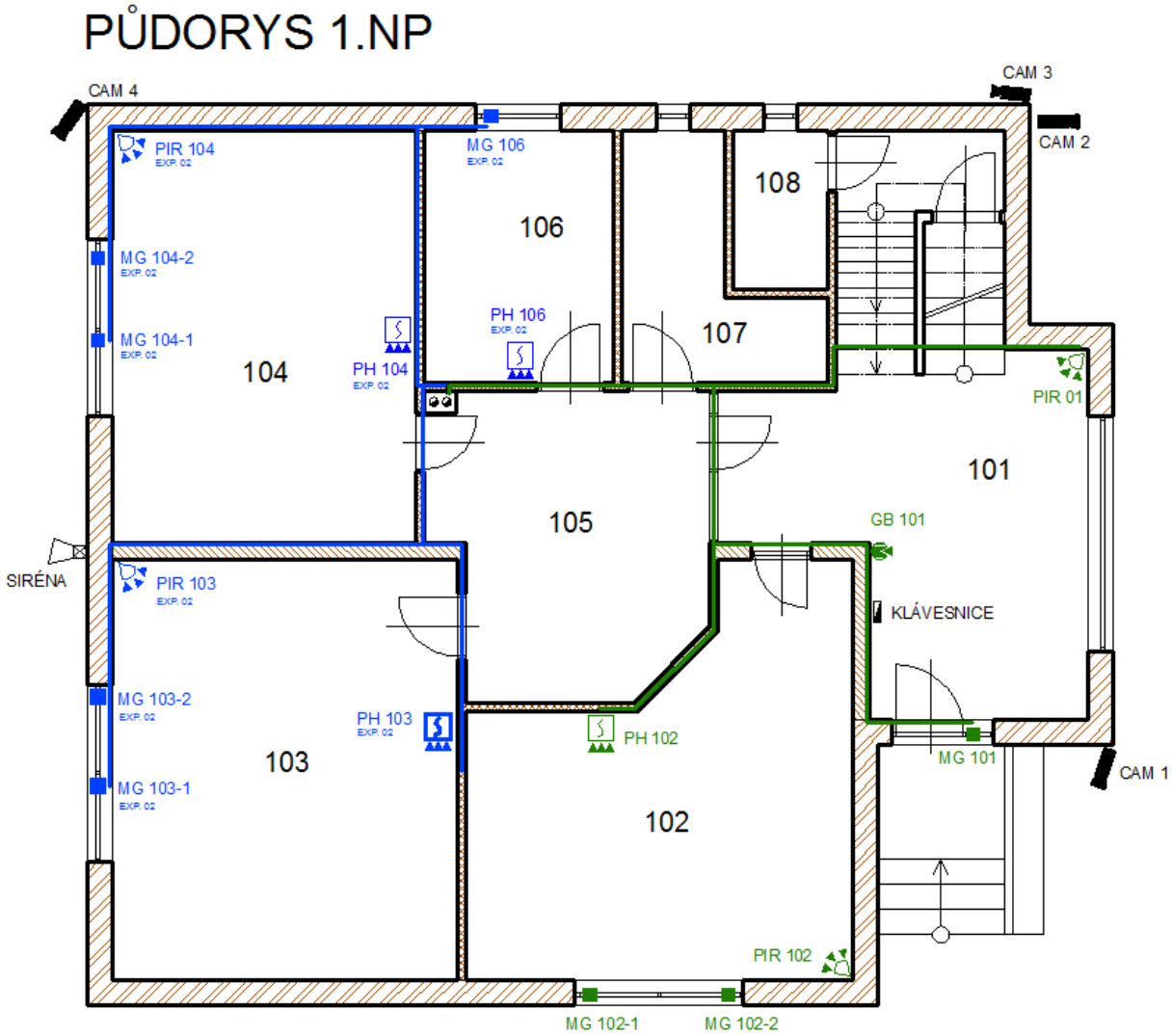
7.6 Umístění komponentů PZTS a CCTV

Komponenty PZTS jsou umístěny dle platných norem. Celý systém je navržený tak, aby maximálně eliminoval hrozící rizika. To znamená, že prvky PZTS jsou navrženy se správně zvoleným rozsahem a způsobem jejich fungování. Dalším kritériem bylo zvolit komponenty kvalitní, ale pokud možno relativně laciné. Nejedná se tedy o celý systém od jednoho výrobce, nýbrž o kombinaci prvků od různých výrobců tak, aby se cena snížila. Při návrhu se samozřejmě počítalo se vzájemnou kompatibilitou jednotlivých prvků.

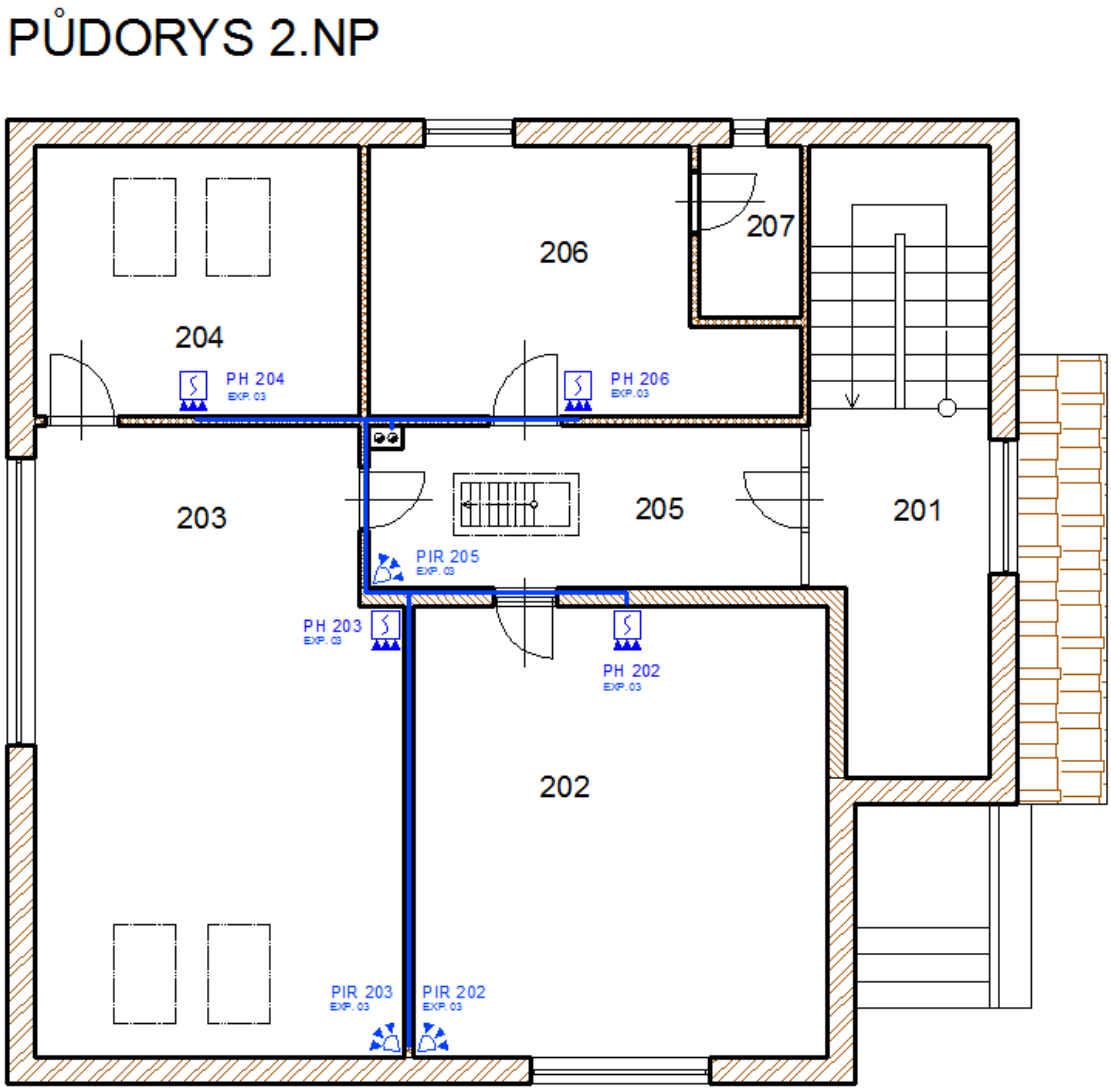
Do každé místnosti byl umístěn kouřový detektor značky VAR-TEC. Dosah tohoto hlásiče je až 40m^2, takže není třeba jej umístit doprostřed místnosti, jak bylo přáním zákazníka. Toto přání měli hlavně z estetických důvodů.



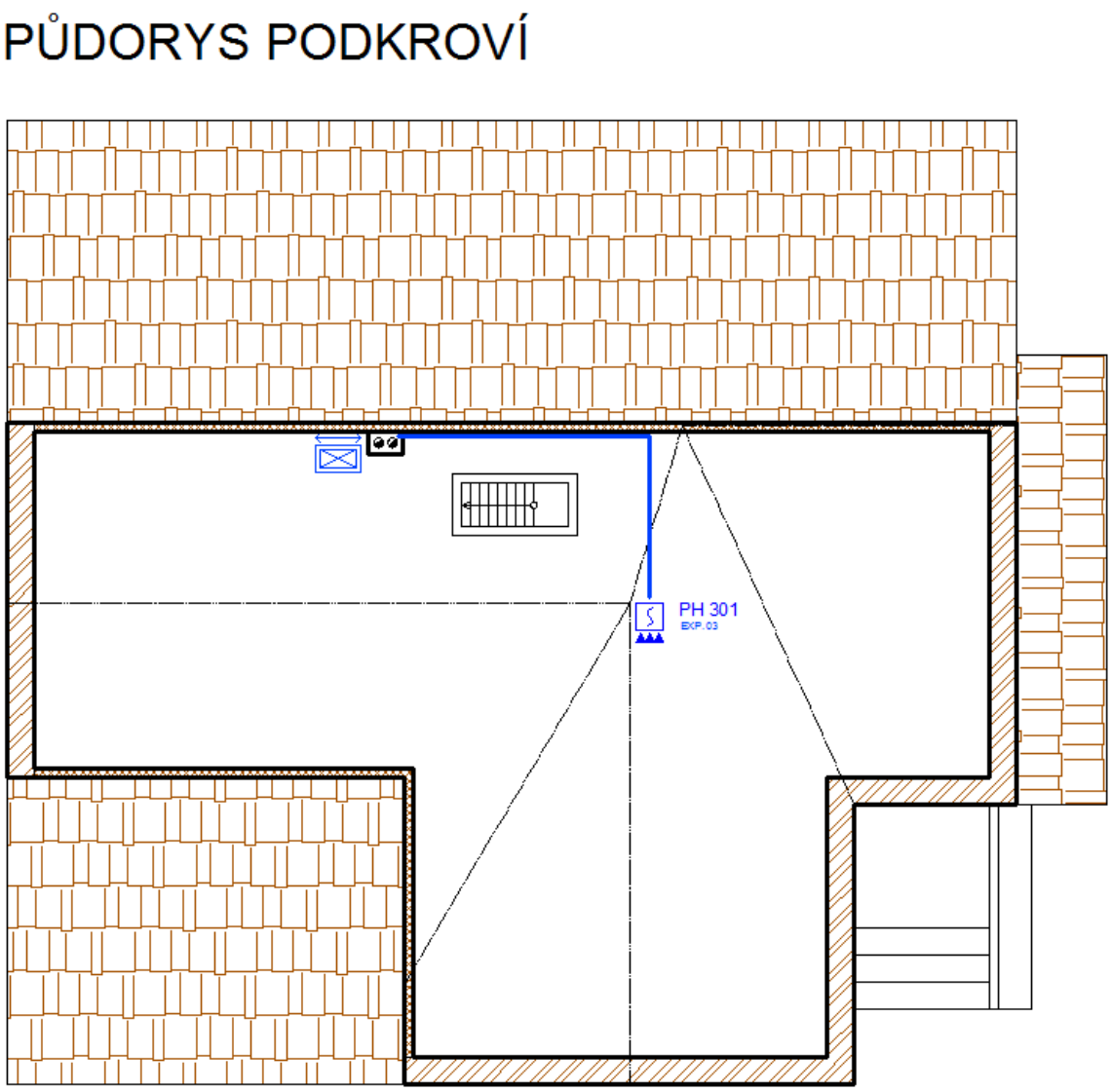
Obrázek 43: Návrh na umístění prvků PZTS - 1.PP [Zdroj: Autor]



Obrázek 44: Návrh na umístění prvků PZTS a CCTV - 1.NP [Zdroj: Autor]



Obrázek 45: Návrh na umístění prvků PZTS - 2.NP [Zdroj: Autor]



Obrázek 46: Návrh na umístění prvků PZTS – podkroví [Zdroj: Autor]

8 EKONOMCKÁ NÁROČNOST ZABEZPEČENÍ

Ekonomická náročnost systému PZTS bude hrát velkou roli při výběru z navržených variant. Požadavek investorů bylo vejít se s celkovou cenou na implementaci PZTS do 100.000,-Kč. Tento požadavek byl s přehledem splněn.

8.1.1 Náklady na zabezpečení objektu

V následující tabulce jsou vypsány prvky PZTS a kamerového systému včetně jejich pořizovací ceny.

Prvek PZTS	Počet	Cena (Kč) - jednotková	Cena (Kč) - celková
Ústředna Magellan MG 6250-868	1 ks	4.200,-	4.200,-
Komunikátor GPRS14	1 ks	2.610,-	2.610,-
PIR MG-PMD1P	8 ks	1.550,-	12.400,-
Magnety MG-DCT10	12 ks	1.110,-	13.320,-
Požární detektor SD-738	13 ks	2.440,-	31.720,-
Glass break G550-868	1 ks	2.820,-	2.820,-
Evolveo Detective S4CIH7D	1 ks	5.990,-	5.990,-

Tabulka 27: Ceny zabezpečovacích prvků – varianta 1 (ceny uvedeny včetně DPH)

V tabulce druhé jsou obsaženy veškeré komponenty PZTS a kamerového systému s jejich cenami pro druhou variantu

Prvek PZTS	Počet	Cena (Kč) - jednotková	Cena (Kč) - celková
Ústředna Digiplex EVO 48	1 ks	3.500,-	3.500,-
Expandér Digiplex APR-ZX8	3 ks	1.440,-	4.320,-
Klávesnice Digiplex K641	1 ks	2.880,-	2.880,-
Komunikátor Paradox PCS200	1 ks	5.890,-	5.890,-
PIR Optex RXC-ST	8 ks	400,-	3.200,-

Magnety Paradox 3G SM60	12 ks	280,-	3.360,-
Požární detektor VAR-TEC FDR 26-S	13 ks	1.060,-	13.780,-
Glassbreak Glasstrek 457	1 ks	720,-	720,-
Siréna TEKNIM-720WR	1 ks	1.300,-	1.300,-
Box pro ústřednu	1 ks	800,-	800,-
Evolveo Detective S4CIH7D	1 ks	5.990,-	5.990,-
Akumulátor Alarmguard CJ 12-18	1 ks	900,-	900,-
Kabeláž W-6x0,22+2x0,5	200 m	16,-	3.200,-

Tabulka 28: Ceny zabezpečovacích prvků – varianta 2 (ceny uvedeny včetně DPH)

Musíme připočítat cenu za montáž a nastavení systému, s tím že kabeláž je potřeba klást do drážek ve stěnách (kromě podkroví a suterénu) a poté je zasádrovat, aby nebyly vidět. Zákazník si přeje, aby tyto práce co nejméně narušily reprezentativní vzhled objektu.

Budeme-li uvažovat s cenou za práci 10.000,- za práci na první (bezdrátové variantě) a 15.000,- Kč za variantu druhou a s cenou za komponenty 49.840,- Kč za variantu 1 a 73.060,- Kč za variantu 2, vyjde nám celková pořizovací cena na toto zabezpečení pro první variantu kolem **88.000,-Kč** a pro druhou kolem **65.000 Kč.** Jedná se pouze o pořizovací cenu. Po celou dobu provozu se bude platit paušál za DPPC. Jeho cena bude pro obě varianty stejná a bude určena SBS.

Spolu s prvky MZS, které byly navrženy v první fázi zabezpečení objektu a jejichž cena byla vyčíslena celkem na 83.500,- Kč (bezpečnostní rolety 35.000,-Kč, garážová vrata 25.000,-Kč, vstupní dveře 10.000,-Kč atd.). I s prací bude celková cena za zabezpečení objektu činit v obou variantách do 170.000,-Kč. Tato cena je úměrná kvalitě zabezpečovacích prvků.

ZÁVĚR

Cílem této diplomové práce bylo navrhnout komplexní zabezpečení daného objektu. Vzhledem k tomu, že MZS byly navrženy již dříve, více jsem je v práci nerozebíral a soustředil se spíše na PZTS. Pro tento byla provedena bezpečnostní analýza objektu i jeho okolí a na základě této analýzy byla zvolena patřičná bezpečnostní třída, pro kterou se pro tento objekt pořizovaly jednotlivé prvky PZTS. Komponenty PZTS jsou popsány, je k nim uvedeno na jakém fyzikálním principu fungují, jaké mají technické parametry a jaké jsou jejich detekční charakteristiky. Všechny prvky tedy splňují požadavky minimálně pro druhou bezpečnostní třídu Veškeré prvky PZTS jsou v práci popsány včetně způsobu jejich zapojení. Součástí návrhu je nejen výběr prvků, ale i jejich umístění a nastavení. Objekt byl rozdělený do dvou subsystémů. Toto rozdělení je z důvodu bezpečnosti. Klient si nepřeje, aby uklízecí firma chodila do sklepa a do technických místností a archivů. A vhledem k tomu, že sem chodí uklízet o víkendu, nebo po pracovní době, bylo nutné, aby při odstřežení zbytku objektu byl sklep stále zabezpečen. Pro znázornění rozmístění komponentů PZTS jsem vypracoval výkresy v programu AutoCAD, kde jsou znázorněny jak jednotlivé komponenty systému s kabeláží. Dalším cílem diplomové práce bylo seznámit čtenáře s legislativní problematikou zabezpečování objektů. Této problematice se věnuje celá kapitola. Jedná so však pouze o výběr zákonů, předpisů a norem pouze pro tento případ zabezpečení. Kompletní výčet zákonů, předpisů a norem by vystačil na další diplomovou práci. Legislativa nebyl hlavní zájem pro tuto práci. V závěru práce je zhodnocena ekonomická náročnost navrženého řešení. Cena za práci je odhadovaná, ale počítá se s tím, že by se měly PZTS vejít i s pracemi do 90.000,- Kč pro první variantu a do 65.000,- Kč pro variantu druhou. Vzhledem k chráněným aktivům je i cena dražší varianty přiměřená.

Vzhledem k přání zákazníka vyhnout se nevzhledné kabeláži v lištách a tím pádem náročnější instalaci prvků spojené se stavebními úpravami (sekání drážek, tahání kabeláže, sádrování drážek a následné malování), což se promítne do pracovního tempa zaměstnanců, si investor pravděpodobně vybere bezdrátovou variantu i přes její vyšší cenu. Druhá varianta je navržena z toho důvodu, kdyby dané prostředí bylo pro bezdrátový systém nevyhovující.

CONSCUSION

The aim of this thesis was to design a comprehensive security for the building of Economy centre in Zlín. Given that mechanical bariers has been proposed previously, so it is not elaborate to much at this work and thesis focus mainly on alarm systems. For this purpose it was made a security analysis of the object and its divided on the basic of this analysis was chosen appropriate safety class for which this object acquiring. Alarm system components are described with their physical principle on which they works, also there are any technical parameters and detection characteristics. All the elements have to meet the requirements for at least the third safety class alarm systém. All elements are described in the thesis, including the way their wireing. The proposal includes not only the selection of elements, but also their location and setting. The building was partitioned into two subsystems. This is mostly for security reasons. The client doesn´t want a cleaning company went to the basement, technical rooms and archives. And whereas they are just cleaning up the weekend or after hours, it was necessary to disarm while the rest of the basement of the building was still secured. To illustrate the deployment of components alarm system I worked out any drawings in AutoCAD, which show where are every components and its wireing. Another aim of the thesis was to acquaint readers with the legal issues of security objects. This issue is discussed in another chapter. That´s only choice of laws, regulations and standards for this case. A complete listing of laws, regulations and standards would be enough for a further thesis. Legislation is not the main concern of this work. The conclusion evaluates the economic aspects of the proposed solution. The price for the works is estimated. It is calculated, that alarm system would be fit well with the price lower than 90.000, - CZK for the first option and lower than 65.000, - CZK for the second option. Due to the protected assets, the price is reasonable.

Due to the customer wish to avoid unsightly wiring in the rails and thus demending instalation of elements associated with building modifications (cutting grooves, putting wires, plaster-off the grooves and painting), which is reflected in the pace of work of employees, the investor is likely to choose wireless0technology despite its higher price. The second variant is designed from the case if the environment was unsuitable for a wireless system.

SEZNAM POUŽITÉ LITERATURY

[1] LUKÁŠ L. a kolektiv - Bezpečnostní technologie, systémy a management I, 1. vydání, Zlín: VerBuM, 2011, 316 s. ISBN 978-80-87500-07-7.

[2] LUKÁŠ L. a kolektiv - Bezpečnostní technologie, systémy a management II, 1. vydání, Zlín: VerBuM, 2011, 387 s. ISBN 978-80-87500-19-4.

[3] LUKÁŠ L. a kolektiv - Bezpečnostní technologie, systémy a management III, 1. vydání, Zlín: VerBuM, 2011, 456 s. ISBN 978-80-87500-35-4.

[4] LAUCKÝ, JUDr. V. – Technologie komerční bezpečnosti I. Zlín: Univerzita Tomáše Bati ve Zlíně, 2003, 64 s. ISBN 80-7318-119-3.

[5] LAUCKÝ, JUDr. V. – Technologie komerční bezpečnosti II. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 122 s. ISBN 978-80-7318-231-9.

[6] SMEJKAL, V. a RAIS K. – Řízení rizik ve firmách a jiných organizacích. 4. aktualizováno a rozšířeno. Vyd. Praha: Grada, 2013. ISBN 978-80-247-4644-9.

[7] IVANKA, J. – Systematizace bezpečnostního průmyslu II Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 86 s. ISBN 978-80-7318-863-4

[8] VALOUCH, J. – Projektování bezpečnostních systému. Skriptum. Zlín: UTB, 2012. 152 s. ISBN 978-80-7454-230-5.

[9] *www.gremiumalarm.cz* [online]. ©2013 [cit. 2016-05-01] Dostupné z: http://www.gremiumalarm.cz/wp-con tent/uploads/DEF_TNI-2-A4-pro-www.pdf

[10] *www.zakony.centrum.cz* [online]. [cit. 2016-05-01] Dostupné z: http://zakony.centrum.cz/trestni-zakonik/cast-2-hlava-2-dil-1-paragraf-173

[11] *www.bambi215.wordpress.com* [online]. [cit. 2016-05-01] Dostupné z: https://bambi215.wordpress.com/2015/02/26/policie-ceske-republiky/

[12] *www.vutbr.cz* [online]. [cit. 2016-05-01] Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=37984

[13] *www.mapakriminality.cz* [online]. [cit. 2016-05-01] Dostupné z: http://www.mapakriminality.cz/

[14] *www.mapy.cz* [online]. [cit. 2016-05-01] Dostupné z: https://mapy.cz/zakladni?x=17.6333892&y=49.2179610&z=12&source=muni&id=3045

[15] *www.stasanet.cz* [online]. [cit. 2016-05-01] Dostupné z: https://www.stasanet.cz/Paradox-a-ostatni-EZS/System-EZS-akcni-sety/MG6250-868-integrovany-bezdratovy-system-EZS-Paradox-Magellan.html

[16] *www.abalarm.cz* [online]. [cit. 2016-05-01] Dostupné z: http://www.abalarm.cz/ishop/cs/elektronicke-zabezpecovaci-systemy/925-paradox-magellan-gprs14-modul-gprs-pro-mg6250-.html

[17] *www.eurosat.cz* [online]. [cit. 2016-05-01] Dostupné z: http://www.eurosat.cz/415-mg-pmd1p.html

[18] *www.eurosat.cz* [online]. [cit. 2016-05-01] Dostupné z: http://www.eurosat.cz/418-mg-dct10.html

[19] *www.eurosat.cz* [online]. [cit. 2016-05-01] Dostupné z: http://www.eurosat.cz/420-mg-sd738.html

[20] *www.variant.cz* [online]. [cit. 2016-05-01] Dostupné z: http://www.variant.cz/zbozi/1202-015-g550-868

[21] *www.eurosat.cz* [online]. [cit. 2016-05-01] Dostupné z: http://www.eurosat.cz/3033-evo48.html

[22] *www.atisgroup.cz* [online]. [cit. 2016-05-01] Dostupné z: http://www.atisgroup.cz/show_product.php?id=017+12000

[23] *www.eurosat.cz* [online]. [cit. 2016-05-01] Dostupné z: http://www.eurosat.cz/217-k641-dgp2-641bl.html

[24] *www.adiglobal.cz* [online]. [cit. 2016-05-01] Dostupné z: https://www.adiglobal.cz/iiWWW/cz/produkty110.nsf/web_category_list1_cenik_asc/2521197D3B897B8FC1257A0C005498F8

[25] *www.variant.cz* [online]. [cit. 2016-05-01] Dostupné z: http://www.variant.cz/zbozi/0701-065-3g-sm-60-hneda

[26] *www.eurosat.cz* [online]. [cit. 2016-05-01] Dostupné z: http://www.eurosat.cz/3566-glasstrek-457.html

[27] *www.variant.cz* [online]. [cit. 2016-05-01] Dostupné z: http://www.variant.cz/zbozi/0701-028-fdr-26-s

[28] *www.variant.cz* [online]. [cit. 2016-05-01] Dostupné z: http://www.variant.cz/zbozi/0703-031-teknim-720wr

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PZTS	Poplachové zabezpečovací a tísňové systémy.
EPS	Elektrická požární signalizace
CCTV	Uzavřený televizní okruh
PČR	Policie české republiky
SBS	Soukromé bezpečnostní služby
ČSN	Česká technická norma
EN	Evropská norma
mm	Milimetr
cm	Centimetr
m	Kilometr
PIR	Pasivní infračervený detektor
CCTV	Uzavřený televizní okruh
ACCESS	Přístupové systémy
SAS	Systémy přivolání pomoci
MW	Mikrovlnné detektory
US	Ultrazvukové detektory
ISO	Mezinárodní úřad pro standardizaci
MZS	Mechanické zábranné systémy

SEZNAM OBRÁZKŮ

SEZNAM TABULEK