

**Jihočeská univerzita v Českých Budějovicích**

Pedagogická fakulta - Katedra fyziky

Zabezpečovací elektronické zařízení v policejní praxi -  
Pult centralizované ochrany objektů

Bakalářská práce

Vedoucí práce: PaedDr. Josef Voda

Autor: Kateřina Buřičová

## Anotace

Cílem této bakalářské práce je přiblížit elektronické zabezpečovací systémy - Pult centralizované ochrany jež využívá Policie ČR.

V úvodní části je nastíněna historie vzniku prvních zabezpečovacích elektronických systémů, další část se soustředí na soubor jednotlivých druhů ochrany objektů, popis jednotlivých prvků používajících se v zabezpečovacích elektronických systémech a jejich praktické využití v ochraně zboží.

Závěr je věnován podrobnějšímu popisu pultu centralizované ochrany, ekonomickému přínosu a statistika způsobených poplachových událostí.

## Annotation

The purpose of my bachelor theses is to explain the electronic security systems, the Control Panel of Centralized Security, used by the Police of the Czech Republic.

The introduction outlines the history of the initial electronic security systems and the next part is focused on the set of various object security types describing the particular elements used for electronic security systems and their practical use to protect the goods.

The conclusion provides more details of the Control Panel of Centralized Security and its economic benefit as well as the statistics of alarm and emergency events.

Prohlašuji, že předloženou práci jsem vypracovala samostatně, pouze s použitím uvedené literatury.

V Českých Budějovicích dne 20.listopadu 2006

Kateřina Buřičová

Poděkování:

Touto formou děkuji mému vedoucímu práce PaedDr. Josefu Vodovi, za jeho cenné rady, připomínky a za velkou oporu při řešení problémů týkajících se mé práce.

## Obsah

Úvod .....	9
I. Historie zabezpečovacích systémů .....	10
II. Zabezpečovací poplachové systémy .....	14
II.1. Operační hledisko .....	14
II.1.2. Technické hledisko .....	15
II.2. Základní druhy ochrany objektů .....	15
II.2.1. Klasická ochrana .....	15
II.2.2. Režimová ochrana .....	15
II.2.3. Fyzická ochrana .....	16
II.2.4. Technická ochrana .....	16
II.3. Elektronické zabezpečovací systémy .....	17
II.3.1. Pravidla zřizování elektrické zabezpečovací signalizace objektů .....	18
II.3.1.1. Účel elektrické zabezpečovací signalizace .....	18
II.3.1.2. Základní terminologie .....	18
II.3.1.3. Účastníci procesu zřizování .....	19
II.3.1.4. Základní způsobilost vstupů .....	19
II.3.2. Stupně zabezpečení a klasifikace prostředí .....	19
II.3.2.1. Stupně zabezpečení .....	19
II.3.2.2. Klasifikace prostředí pro zařízení .....	19
II.3.2.3. Zařazení zařízení do stupňů zabezpečení .....	20
II.3.2.4. Zařazení objektů do míry rizika .....	20
II.3.3. Postup při zřizování elektrické zabezpečovací signalizace .....	21
II.3.3.1. Bezpečnostní posouzení objektu a posouzení všech vlivů .....	21
II.3.3.2. Návrh k nabídce .....	21
II.3.3.2.1. Druhy ochrany .....	21
II.3.4. Několik obecných zásad pro aplikaci jednotlivých komponentů .....	22
III. Monitorování objektů .....	26
IV. Integrovaná ochrana zboží .....	27
IV.1. Elektronické anténní systémy - ochrana zboží v obchodech .....	28
IV.1.1. RF- radiofrekvenční technologie .....	28
IV.1.1.1. Tvrdé etikety .....	28
IV.1.1.2. Měkké etikety .....	28
IV.1.1.3. Tvrdé etikety na lahve .....	28

IV.1.1.4. Piny na kabely .....	28
IV.1.1.5. Ochranné obaly na MC, CD, video, DVD .....	29
IV.1.1.6. Samolepící etikety .....	29
IV.1.2. EM - elektromagnetická technologie .....	29
IV.1.3. AM – sousto - magnetické technologie .....	29
IV.2. Elektronické anténní systémy - ochrana knihovního fondu .....	30
IV.2.1. Ochrana jednotlivých druhů knihovního fondu .....	30
IV.2.1.1. Knihy, časopisy .....	30
IV.2.1.2. Audiokazety .....	31
IV.2.1.3. CD disky .....	31
IV.2.1.4. Videokazety .....	31
IV.2.1.5. Gramofonové desky .....	31
IV.3. Předmětová ochrana zboží .....	31
IV.4. Kamerové systémy .....	32
IV.5. Bezpečnostní zrcadla .....	33
IV.6. Ochrana nákupních vozíků .....	33
V. Čidla elektronického zabezpečovacího systému .....	34
V.1. Dělení čidel elektronického zabezpečovacího systému .....	34
V.1.1. Čidla napájená .....	34
V.1.1.1. Aktivní čidla .....	34
V.1.1.2. Pasivní čidla .....	34
V.1.1.3. Čidla napájená aktivní a pasivní .....	34
V. 2. Čidla nenapájená .....	33
V. 2.1. Destrukční čidla .....	33
V.2.1.1. Fóliové polepy .....	36
V.2.1.2. Čidla otřesová .....	36
V.2.1.2.1. Čidla otřesová s mechanickým měničem .....	37
V.2.1.2.2. Čidla otřesová s akusticko- mechanickým měničem .....	37
V.2.1.2.3. Čidla na ochranu skleněných ploch .....	37
V.2.2. Nedestrukční čidla .....	38
V.2.2.1. Mikrospínače .....	38
V.2.2.2. Nášlapné koberce .....	38
V.2.2.3. Magnetické kontakty .....	39
V.3. Čidla bariérová .....	39

V.3.1. Čidla infračervené závory .....	39
V.4. Čidla pohybu .....	40
V.4.1. Antimasking .....	41
V.4.2. Dělení čidel pohybu .....	41
V.4.2.1. VKV čidla .....	42
V.4.2.2. Mikrovlnná čidla .....	42
V.4.2.3. Ultrazvuková čidla .....	44
V.4.3. Zpracování signálu čidel pohybu .....	45
V.4.3.1. Analogové zpracování signálu .....	45
V.4.3.2. Digitální zpracování signálu .....	45
V.5. Čidla tísňového hlášení .....	46
V.5.1. Veřejné tísňové hlásiče .....	46
V.5.2. Speciální tísňové hlásiče .....	46
V.5.2.1. Bankovní čidla .....	47
V.5.2.1.1. Bankovní kontaktní čidla .....	48
V.5.2.1.2. Bankovní bezkontaktní čidla .....	48
V.5.2.2. Osobní tísňové hlásiče .....	49
V.5.2.2.1. Systémy ochrany a zabezpečení osob .....	50
VI. Pult centralizované ochrany .....	51
VI.1. Historie pultu centralizované ochrany .....	51
VI.2. Přenosové prostředky .....	52
VI.2.1. Přenos přímou (pevnou) linkou .....	52
VI.2.2. Přenos linkou jednotné telekomunikační sítě .....	53
VI.2.2.1. Přenos po síti ISDN .....	53
VI.2.2.1.1. Přepínaná linka .....	54
VI.2.2.1.2. Přenos v nadhovorovém pásmu .....	54
VI.2.2.1.3. Počítačové sítě .....	54
VI.2.3. Přenos bezdrátový .....	55
VI.2.3.1. Přenos rádiový .....	55
VI.2.3.2. Přenos optický .....	56
VI.3. PCO v podmínkách Policie ČR .....	56
VI.3.1. Praktická činnost .....	58
VI.3.2. Taktika zásahu .....	60
VI.4. Planý poplach .....	61

VII. Statistika způsobených poplachových událostí .....	62
VII.1. Statistika poplachových událostí .....	62
Závěr .....	66
Přílohy .....	67
Poznámkový aparát .....	75
Seznam použité literatury .....	76
Seznam zkratek .....	77



## Úvod:

Pro zvolené téma mé bakalářské práce „Zabezpečovací elektronické zařízení v policejní praxi – Pult centralizované ochrany objektů“ byla pro mě velkou motivací má služba u Policie ČR. Zpracování tohoto tématu mi umožnilo učinit syntézu teoretických poznatků načerpaných studiím na Pedagogické fakultě Jihočeské Univerzity v Českých Budějovicích a z odborné literatury na jedné straně a praktických poznatků získaných při výkonu mé služby na straně druhé. Takto je i má bakalářská práce koncipována. Jistým východiskem se stal pojem „Ochrany“, jako prostoru bezpečí jednotlivce, či skupiny osob. A právě již zde je spojnice - činnost Policie ČR, ochraňující životy, zdraví a majetek osob ke které využívá prostředky dané jí právními normami, neboť nad jejich rámec není ke své činnosti zmocněna. O těchto prostředcích, ne jen v podmínkách služby Policie ČR, hovoří další části předmětné práce, a to elektronické zabezpečovací systémy, monitorování objektů, integrovaná ochrana objektů, čidla elektronického zabezpečovacího systému. Za stěžejní část své práce považuji část nazvanou pult centralizované ochrany, která navazuje na předchozí části, z nichž přebírá technologická východiska, která dále rozvádí v podmínkách Policie ČR.

## I. Historie zabezpečovacích systémů

Pojem OCHRANA nebyl dosud v České republice přesně definován, a proto je nutné vycházet z obecně přijaté terminologie amerických specialistů G. Greena a R.J. Fischera aplikované v práci Introduction to security, U.S.A : Security World Publishing Co., Inc., 1993, citují :

*„Ochrana znamená stabilní, relativně předvídatelné prostředí, ve kterém může jedinec nebo skupina sledovat své cíle bez rušení a ohrožení, bez strachu z vměšování nebo násilí.“<sup>1)</sup>*

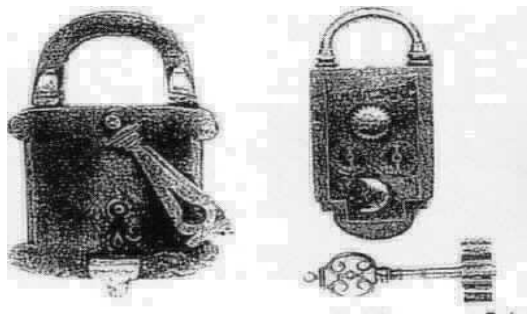
Z historického hlediska je ochrana jedním z tradičních oborů lidské činnosti. První klasické i fyzické ochrany jsou doloženy už v raném starověku a jejich účel se dodnes nezměnil - vždy měly a mají za úkol chránit lidské životy a majetek.

Například visací zámek - výrobek, je sám o sobě obecně znám a používán jistě v každé domácnosti. Stal se nezbytnou součástí a potřebou, jehož opodstatnění nezměnil ani čas uplynulý od jeho vynálezu je zřejmé, že každá provozovna, dílnička, obchod ale i domácnost disponuje alespoň jedním.

Visací zámky prodělaly konstrukční i technologický vývoj v rámci celé zámečnické výroby, která patřila spolu se zbrojířstvím a později i hodinářstvím k nejvyspělejším technickým řemeslům. Naši předkové, zejména pak v době antiky, však vytvářeli v této oblasti výrobky již značně pozoruhodné.

Podle historiků a archeologů začíná historie visacích zámků v českých zemích asi ve 12. století. Podle nalezených jednotlivých klíčů a dalších artefaktů však nelze jednoznačně určovat dobu vzniku a druh zámku. Vlastní nálezy na našem území datují odborníci mezi 13. a 15. století, ale bez seriózních dokladů. Většinou se jednalo se o importované středověké výrobky.

V 18. století vznikají manufaktury, které postupně vytlačují cechovní výrobu. Pravděpodobně první česká manufaktura byla založena na Vrbovském panství v Hořovicích kolem roku 1760.



Obr. č.1 Příklady šáličových visacích zámků jež jsou uloženy v muzeu Saint - Laurent

Postupně se však na místo římských a francouzských konstrukcí prosazují zámky anglické a v 19.století zámky americké.

V 19. a 20. století vznikají první bezpečnostní uzamykající mechanismy. Jejich bezpečnost je odvislá od přesných posunů vložených bezpečnostních prvků, které blokuje závoru. S konstrukcemi těchto mechanismů jsou spojena zejména jména vynálezců např. Barron, Bramah, Cvivelli a další.<sup>2)</sup>

Cesta k vývoji dalších a daleko složitějších mechanismů a nakonec i nejmodernějších zabezpečovacích systémů s využitím elektrické energie je však ještě velmi složitá, což by mělo objasnit i téma této práce.<sup>3)</sup>

Nejmladším oborem ochrany objektů jsou technické prostředky. Není to však novinka posledních desetiletí. Např. prostředky elektrických zabezpečovacích systémů byly druhou prakticky využitelnou aplikací elektřiny vůbec. Roku 1844 byl vynalezen telegraf. Když ale roku Alexandr Graham Bell zkoušel svoji myšlenku dálkového přenosu lidského hlasu „po drátech“, použil k tomu zabezpečovací rozvody pultu centralizované ochrany, vybudovaného již roku 1853 v New Yorku Edwenem Holmesem. Teprve za další tři roky rozsvítil Tomáš Alva Edison svou první žárovku (1879).

Je historickým faktem, že Edwin Holmes, zakladatel Newyorské městské společnosti, která dodnes nese jeho jméno, byl průkopníkem elektrických poplašných zařízení i prvních primitivních telefonních ústředěn. Vynalezl první telefonní kontakt, který vahou sluchátka rozpojuje telefonní okruh. Tento princip je prakticky používán dodnes. On jako první prosazoval komerční využití poplašných a telefonních systémů v době, kdy ještě neexistovali výrobci těchto zařízení. Jako první na světě začal vyrábět izolované elektrické vodiče a instaloval vlastní propojovací okruhy mezi chráněnými objekty a vlastním centrálním úřadem.

Seznam uživatelů Holmesovy centrály elektrické ochrany, založené roku 1958 v Bostonu a New Yorku, brzy obsahoval řadu významných a zároveň i prominentních zákazníků. (Tiffany, Bowery Bank atd.). Roku 1972 Edwin Holmes vyvinul „elektrický sekretář“ pro ukládání klenotů a jiných cenností.

Stěny úložného prostoru byly propletené průběžnou vodivou fólií a dveře opatřeny kontakty, propojenými na centrální stanoviště se 24 hodinovou službou schopnou kdykoliv zasáhnout.

Teprve počátkem 20. století se objevují elektromechanická čidla založená na principu setrvačnosti, popřípadě kyvadla. Jsou to speciální kyvadlová čidla určená pro ochranu trezorových místností, nejrůznější typy vibračních kontaktů, používaných až do začátku osmdesátých let.

Teprve rozvoj elektroniky za druhé světové války a po ní, následná miniaturizace elektronických zařízení a výrazný a náhlý rozmach nových technologií vyvinutý především pro potřeby kosmonautického výzkumu umožnily od šedesátých let vznik nových druhů čidel.

Jde např. o mikrovlnné čidlo, jehož aktivním prvkem je bezkontaktní rozdělovač proti letadlového granátu. S tím to typem se, ale v praxi a běžném životě setkáme velice zřídka.

Když v roce 1973 předložil A.G. Bell a jeho spolupracovníci Holmesovi prototyp telefonu byla již podle Holmesových návrhů vybudována elektrická vedení, spojující centrálu se zákazníky. Toto se ukázalo jako velmi vhodné pro komunikaci se vzdálenými zákazníky.

V květnu 1877 byla vybudována první komerční telefonní ústředna jež byla v New Yorku a nesla jméno BELL TELEPHONE ASSOCIATION.

Roku 1933 v našem Československém státě je popsána a zaznamenána první větší aplikace zabezpečovací techniky. Jednalo se o zřizování poplašných telefonních hlásičů. Rozmach zabezpečovacích systémů se datuje od padesátých let, kdy se bezpečnostní ochrana začala nejvíce využívat i v bankovníctví. V bankách a bankovních domech byly používány elektrické spínací zámky trezorových dveří se světelnou a akustickou signalizací, dále pak systémy kontaktních čidel, trezorových vibračních čidel a zařízení PETEX, i další.

V letech 1950-1960 vyráběla tyto zabezpečovací systémy Tesla Jihlava. Především se jednalo o jednoduché ústředny typového označení SU-1, dálkové signalizace DS-1, dále pak různé druhy kontaktních a vibračních čidel řady WK, více smyčkové ústředny a další sortimenty. Více smyčkové ústředny vyráběné v již zmíněném podniku, se pro jejich větší velikost a pro jejich jednoduché ovládání s malými obměnami vyrábí dosud a používají se jistě i pro jejich spolehlivost.

V roce 1958 bylo v podniku Obchodní zařízení a potřeby státního obchodu Praha započato s vývojem prvních elektrických zabezpečovacích prvků a systémů. Na tomto vývoji se nemalým podílem účastnilo i Ministerstvo vnitra.<sup>4)</sup>

Významným krokem ve využití elektrických zabezpečovacích systémů (dále jen „EZS“) v tomto období byla centralizace ochrany objektů soustředěná na Službu ochrany objektů veřejné bezpečnosti (dále jen VB) a byly zřizovány systémy centralizované ochrany .

V letech 1971-1975 se v naší republice začal vyrábět nový EZS, jehož širšímu využití napomohlo usnesení vlády ČSSR č. 73 z roku 1982 a centralizace zabezpečených objektů. Citované vládní usnesení určovalo do jaké kategorie a jaké důležitosti spadají jednotlivé objekty a z toho vyplývaly i nároky na jejich zabezpečovací a technickou vybavenost jednotlivých systémů. To vedlo k významnému zvýšení bezpečnosti při manipulaci s velkými finančními prostředky zejména v bankách, spořitelnách a.j. Na základě tohoto nařízení vznikly řady organizací, jež se zabývaly projekcí, montáží a i servisem těchto systémů.

V roce 1986 byla vydána ČSN 334590 Zařízení elektrické zabezpečovací signalizace. Touto normou byl vnesen určitý řád do projektování a montáže zavedením homologačních podmínek a stanovením konkrétních pravidel.

EZS byly budovány jen na bázi kontaktních a destruktivních čidel. Používali se různé druhy kontaktů spínacích i rozpínacích, často ve spojení s nástražným drátem.

Tyto obdobné principy se používají dodnes, avšak v sofistikovanější podobě. Rozmach a především rozvoj výpočetní techniky velice pomohl k tomu, že určité lidské činnosti lze nahrazovat technickými prvky.

Významného zlomu bylo dosaženo v období po roce 1989, kdy dochází ke zvýšení dovozu dokonalejších elektronických zabezpečovacích systémů.<sup>5)</sup>

## II. Zabezpečovací poplachové systémy

Jedná se o soubor organizačních a technicko-taktických opatření, která zajišťují požadovanou bezpečnost objektů, jenž vedou k zefektivnění ochrany majetku. Je však zapotřebí vytvoření určitého modelu na němž budou ověřovány a uskutečňovány tyto zkušenosti a poznatky v praxi.

Při rozboru problematiky zabezpečovacích systémů je zapotřebí dvou různých pohledů na tyto systémy jež se vzájemně výrazně ovlivňují.

Jedná se o : - *Operační hledisko,*  
- *Technické hledisko.*

### II.1.1. Operační hledisko

Pro různé zabezpečovací systémy z pohledu operačního hlediska je cílová funkce různá. To především proto, že každý subjekt, na němž je umístěn zabezpečovací systém, bude mít jiný rozsah a jiný způsob provedení.

Tato skutečnost vyplývá především z hlediska ekonomického, technické efektivity a v případě překonání zabezpečovacího systému i na míře škod způsobené nezákonným jednáním narušitele.

Pomineme-li pouze společenský požadavek na zabránění zcizení, zničení či poškození chráněného zájmu a budeme-li brát i tyto aspekty z policejního hlediska, zjistíme, že zabezpečovací poplachové systémy a některé jejich doplňující požadavky mohou výrazně ovlivnit boj proti kriminalitě v kladném slova smyslu např.:

- *vytvoření podmínek pro bezprostřední dopadení pachatele na místě činu nebo v jeho nejbližším okolí,*
- *poskytnutí „nenapadnutelných“ usvědčujících důkazů ( videozáznam),*
- *v případě zcizení historicky cenných předmětů možnost jejich znovunalezení a navrácení.<sup>6)</sup>*

## **II.1.2. Technické hledisko**

Zásadní rozdíl mezi těmito dvěma hledisky tkví v tom, že technické prostředky slouží především k získání informací o stavu chráněného objektu. Charakteristické rysy nebezpečí v okolí chráněného zájmu jsou zdrojem informací, které je nutno transformovat na elektrické signály. Tuto funkci zajišťují v zabezpečovacích systémech *čidla (detektory)*. Technické prostředky pracují s fyzikálními jevy a s jejich charakteristikami. Proto je nutné převést bezpečnostní pojmy (např. narušení prostoru, krádež apod.) na podněty s charakteristickými rysy nebezpečí, které lze pak pomocí technických prostředků detekovat.

## **II.2. Základní druhy ochrany objektů**

Řešení skutečných problémů týkajících se ochrany objektů musí být vždy prováděno komplexně. Jednotlivé druhy ochrany jsou velice specifické. Zabezpečovací systém je tvořen zejména z těchto druhů ochran :

- *Klasická,*
- *Režimová,*
- *Fyzická,*
- *Technická.*

### **II.2.1. Klasická ochrana**

Jedná se o vývojově nejstarší typ ochrany. Slouží k zajištění příslušného objektu použitím takových (mechanických) zařízení, jež umožní spolehlivou ochranu (vytvoření určitých zábran znemožňujících odcizení či poškození zboží, výrobků či cenných předmětů). Takovéto zábrany odpovídaly samozřejmě technické úrovni doby v níž byly a jsou použity, např.: kovové truhlice, různé typy zámků, ploty apod. Klasická ochrana je základem každého zabezpečovacího systému, (je využívána na každém kroku), na každém objektu, např. vysoké zdi, ploty, v dřívějších dobách i vodní příkopy, atd.

### **II.2.2. Režimová ochrana**

Je souborem organizačně administrativních opatření a postupů směřujících k zajištění požadovaných podmínek pro správnou funkci zabezpečovacího systému a jeho sladění s provozem chráněného objektu. Ve své podstatě zajišťuje možnost řádné funkce ostatních druhů ochrany. Snižuje zranitelnost chráněných zájmů z hlediska dalších forem páchaní trestných činů, např. : loupež<sup>7)</sup>, vloupání<sup>8)</sup>, apod. Základním problémem režimové ochrany je převedení souboru určitých bezpečnostních směrnic do každodenního režimu objektu. (tzv. režimová opatření )

*Bezpečnostní směrnice:* opatření jež se týkají vstupních a výstupních podmínek, vstup do objektu, jež je předmětem ochrany, pohyb zaměstnanců u konkrétního daného objektu, možnost a podmínky vjezdu vozidel, dále pak např. bezpečnostní zajištění teplovodního potrubí, případně výtahů, atd.

### **II.2.3. Fyzická ochrana**

Je ochranou prováděnou fyzickými osobami jako např.: vrátnými, hlídači, hlídací službou či příslušníky Policie České republiky (v textu dále pak jen „policisty“). Tato forma ochrany je z ekonomického hlediska nejdražší. Na rozdíl od ostatních druhů ochrany, u kterých nejvyšší investice na počátku a pak nadále se náklady pohybující v nízkých finančních rovinách, zde je na počátku investice nízká, ale pozdější náklady jsou dosti značné (mzdy zaměstnanců).

### **II.2.4. Technická ochrana**

Jedná se o relativně nový druh zabezpečení objektu. Tyto prostředky jsou z hlediska současných požadavků i technických možností a v návaznosti na rychlost zákroku (zásahové jednotky či policie) nejspolehlivější a nejhůře ze všech zmiňovaných ochrany překonatelné. Proto jsou velmi účinným doplňkem dosavadních systémů klasické ochrany.

Hlavní funkce spočívá v tom, že velmi rychle reagují na změny vyvolané pachatelem v okolí chráněném objektu. Na základě těchto změn, indukovaných i na dosti značné vzdálenosti, dávají do činnosti složky jež jsou schopné v další činnosti pachateli jež se nachází na tomto objektu zamezit a dopadnout jej při činu.

Technická ochrana sama o sobě není ochranou v pravém slova smyslu, ale je ve směru k pachateli psychologickým prostředkem. Jde o detekční systém, který zajišťuje a předává informace o situaci na daném objektu jež je předmětem ochrany.<sup>9)</sup>



### II.3. Elektronické zabezpečovací systémy

EZS jsou soubory prvků schopných na základě optického nebo akustického signálu zpracovat a vyhodnotit na určitém místě vstup či pokus o vstup, případně přítomnost neoprávněné osoby ve střeženém objektu či prostorách.

EZS jsou složeny z několika základních částí jež každá sama o sobě plní specifické funkce a zároveň v tzv. zabezpečovacím řetězci vytváří celek.

Základní části : - *čidlo* (podrobněji v kapitole V ),  
- *ústředna*,  
- *přenosové prostředky*,  
- *signalizační zařízení*,  
- *doplňková zařízení*.

*Ústředna* - přijímá a zpracovává informace z čidel podle stanoveného programu a požadovaným způsobem je realizuje. Dále umožňuje ovládání a indikaci zabezpečovacího systému, zajišťuje jeho napájení a inicializaci následného přenosu informací.

*Přenosové prostředky* - zajišťují přenos výstupních informací z ústředny do místa signalizace, případně povelů opačným směrem.

*Signalizační zařízení* - zajišťuje převedení předaných informací na vhodný signál ( vyhlašuje poplach nebo výstrahu).

*Doplňková zařízení* - usnadňují ovládání systému nebo umožňují realizovat některé speciální služby.

Tyto základní prvky nacházíme v nejrůznějších podobách, ve vzájemných kombinacích a také v různých stupních složitosti. Existují jednodušší zařízení, v nichž jsou jednotlivé prvky sdruženy v jednom, pouzdře. Zřizována jsou ale také zařízení obsahující složitější přístroje, např. počítačové pracoviště jenž zpracovává informace ze stovek i tisíců zabezpečovacích ústředen. Takovéto pracoviště jsou součástí okresních či městských ředitelství Policie ČR .

Všechna spojení elektronického zabezpečovacího systému jsou průběžně kontrolována. Některé objekty jsou kontrolovány denně - zkušebním poplachem, smluveným s obsluhou „PCO “<sup>10)</sup>, jiné jsou kontrolovány nepravidelně v různých časových odstupech.

Tímto dochází k znemožnění vyřazení zabezpečeného systému z provozu, aniž by došlo k informování obsluhy (počítačového střediska - PCO). Průběžná kontrola správnosti a funkčnosti EZS je jedním ze základních faktorů jež ovlivňují zranitelnost systému jako jeho celku.<sup>11)</sup>

Výběr jednotlivých technických prvků vedoucích k zajištění zabezpečení objektů závisí na několika aspektech. A to především na technologii výstavby daného objektu, jeho provozních podmínkách, systémech jež zabezpečují nezbytná režimová opatření. Dále pak také záleží na výši stupni zabezpečení chráněného objektu.

### **II.3.1. Pravidla zřizování elektrické zabezpečovací signalizace objektů**

#### **II.3.1.1 Účel elektrické zabezpečovací signalizace**

Zařízení elektrické zabezpečovací signalizace slouží k signalizaci nebezpečí ve střeženém objektu. Zejména informuje o nežádoucím vniknutí (vloupání) do objektu. Může však být kombinováno i s indikací jiných nebezpečí (např. tísňové hlášení při přepadení či zdravotních obtížích, požární nebezpečí, únik plynu, zaplavení vodou, apod.).

#### **II.3.1.2. Základní terminologie**

*Objekt* je místo, prostor (obvykle dům), ve kterém se systém zřizuje.

*Zřizování EZS* je proces návrhu, instalace systému do objektu a jeho servis.

*Zařízení* je soubor technických prostředků (komplementů) určených k realizaci EZS.

*Objednatel* je ten, kdo instalaci zřizuje a obvykle dále spravuje (např. majitel objektu, správce apod.).

*Dodavatel* je montážní firma, která zakázku realizuje- zřizovatel.

*Uživatel* je ten, kdo zařízení v praxi používá.

*Kompetentní účastník* je další osoba, (fyzická či právnická) která nese částečnou odpovědnost nebo má příslušné pravomoci v oblasti ochrany majetku (pojišťovny, bezpečnostní agentury, policie, apod.), anebo je provozovatelem či garantem určité služby, která je pro EZS využívaná (komunikační sítě, energetické sítě, apod.).

*Výchozí revize* je činnost, která se provádí z hlediska elektrické bezpečnosti podle příslušných norem a týká se napájených zařízení. Provádí se na odpojených obvodech namontovaného zařízení.

*Zkouška funkce* je činnost, při které se prověřuje stav kompletního elektrického zabezpečovacího zařízení.<sup>12)</sup>

### **II.3.1.3. Účastníci procesu zřizování**

Základními účastníky jsou objednatel a dodavatel (zřizovatel). Při zřizování EZS je však často třeba zvážit hlediska a požadavky dalších účastníků, zejména pak pojišťoven (prostudováním pojistné smlouvy či konzultací), bezpečnostních agentur či policie, pokud jim budou předány informace z objektu. Podstatné jsou též podmínky provozovatelů komunikačních a jiných sítí či prostředků, které budou při provozu EZS využívány.

### **II.3.1.4. Základní způsobilost vstupů**

Do procesu zřizování vstupují kromě účastníků též hmotné (zařízení, nářadí atd.) a nehmotné vstupy (znalosti, data, pravidla, atd.). Před zřizováním EZS je žádoucí prověřit způsobilost podstatných vstupů. Zejména pak :

Viz. tabulka č.1 Přílohy

## **II.3. 2. Stupně zabezpečení a klasifikace prostředí**

### **II.3. 2.1.Stupně zabezpečení**

Norma ČSN EN 50131-1 se člení do 4 stupňů zabezpečení (číslovaných v opačném pořadí než kategorie původní zrušené normy ČSN 334590). Stupně zabezpečení uvádí tabulka. Míra rizika je stanovena předpokládanou znalostí a vybaveností narušitele (pachatele). Kategorie původní ČNS se neshodují se stupni zabezpečení platné normy ani v opačném pořadí, neboť nová norma klade technicky rozdílné požadavky.

Viz. tabulka č.2 Přílohy

### **II.3.2.2. Klasifikace prostředí pro zařízení**

Kromě stupně zabezpečení je při výběru vhodného zařízení též třeba zvážit prostředí, do kterého se bude ten který komponent montovat. ČSN EN 50131-1 určuje 4 třídy prostředí I až IV- viz tabulka č.3 Přílohy. Třidu, pro kterou je zařízení určeno udává výrobce v dokumentaci.

### **II.3.2.3. Zařazení zařízení do stupňů zabezpečení**

Stupeň zabezpečení, pro který je zařízení určeno, deklaruje výrobce v technických údajích zařízení. Požadované technické vlastnosti zařízení pro jednotlivé stupně určují normy řady ČSN EN 50131. Stupeň celého systému nebo jeho části určuje podstatný prvek s nejnižším zařazením. Jednotlivé podnikové normy se zaměřují na aplikace systémů stupně 1 až 3 s hlavním důrazem na stupeň 2 (nízké až střední riziko), který je pro potenciální uživatele tohoto dokumentu nejčastější aplikací. Pro EZS vyšších stupňů je nutné respektovat přísnější požadavky příslušných norem a direktiv.

### **II. 3.2.4. Zařazování objektů do míry rizika**

Na rozdíl od klasifikace zařízení do stupňů zabezpečovací normou neexistuje jednotný předpis, který by zařazoval jednotlivé objekty do míry rizika. Při návrhu vhodného stupně EZS je třeba zvážit více aspektů (hodnotu majetku, jeho důležitost, lokalitu, atd.). Zařazení objektu do stupně provádí dodavatel na základě požadavků a upřesnění objednavatele a dalších kompetentních účastníků.

*Poznámky k zařazování objektů do míry rizika:*

- Je-li objekt pojištěn, je vhodné stanovit míru rizika v souladu s požadavkem pojišťovny,
- Obytné objekty (byty, rodinné domky), které nejsou pojištěny na vysoké pojistné částky, obvykle spadají do stupně 1 nebo 2,
- Obchody, restaurace, sklady, kanceláře dílny apod., ve kterých není uložen drahý majetek, jsou ve většině případů zařazovány do stupně 2,
- Místa, kde se nacházejí velké objemy peněz v hotovosti, drahé šperky, omamné látky a podobně, se řadí nejčastěji do stupně 3,
- Do stupně 4 se pak řadí strategicky důležitá místa (tiskárny cenin, zpracování diamantů, zlata, apod.),
- Z uvedeného plyne, že nejvíce objektů v běžné praxi je zařazeno do stupně 2. Česká pojišťovna proto například v pojistných podmínkách pro pojištění movitých věcí specifikuje požadavek na EZS jednotně na stupeň 2.

### II. 3.3. Postup při zřizování elektrické zabezpečovací signalizace <sup>13)</sup>

**Proces realizace zabezpečovacího systému se obvykle skládá z následujících kroků:**

1. *Bezpečnostní posouzení objektu včetně všech vlivů,*
2. *Zhotovení návrhu k nabídce,*
3. *Projednání návrhu a posléze uzavření smluv,*
4. *Zpracování projektu a naplánování instalace,*
5. *Vlastní montáž, kontrola,*
6. *Zkušební provoz,*
7. *Zaškolení obsluhy ( popřípadě jednotlivých zaměstnanců),*
8. *Předání díla, včetně s vyúčtováním,*
9. *Pravidelné kontroly.*

#### II.3.3.1. Bezpečnostní posouzení objektu a posouzení všech vlivů

Před vlastním návrhem je třeba se seznámit s objektem, s přístupovými cestami a ostatními vlivy na budoucí EZS.

Vhodné je získat kopii výkresové stavební dokumentace objektu, případně si pořídit základní nákresy.

#### II.3.3.2. Návrh k nabídce

Při návrhu EZS je třeba objekt hledat „očima případného pachatele“. V závislosti na stupni rizika se volí příslušné zařízení.

##### II.3 3.2.1. Druhy ochran

Podle charakteru objektu, rozmístění majetku v něm, atd. se při návrhu kombinují různé druhy ochran:

*Plášťová* - instalace detektorů pokrývajících plochy vymežující chráněný objekt (celé budova nebo vyčleněný komplex vnitřních prostor) - obvykle se realizuje detektory otevření dveří, oken a detektory rozbití skla.

*Prostorová* - instalace detektorů ve všech prostorách s chráněnými hodnotami včetně klíčových míst. Používají se zejména pohybové detektory.

*Klíčová* - instalace detektorů v místech rozhodující při pohybu osob v objektu ( klíčová místa)

*Předmětová* - ochrana konkrétních předmětů, zpravidla uměleckých děl, trezorů.

*Sabotážní* - ochrana jednotlivých komponentů systému vůči nedovolené manipulaci s nimi.

*Osobní* - ochrana osob při přepadení nebo zdravotních potížích k přivolání pomoci.

*Ostatní* - ochrana proti požáru, úniku hořlavých plynů, zaplavení a jiných nebezpečím.

#### **II.3.4. Několik obecných zásad pro aplikaci jednotlivých komponentů:**

1. *Ústředna a ovládací klávesnice systému* se umísťuje uvnitř střeženého prostoru. Jestliže je EZS dělen do subsystémů o různém stupni zabezpečení, musí být ústředna (klávesnice) v prostoru s nejvyšším stupněm zabezpečení. Ovládací prvky se nemontují do míst, kam má přístup veřejnost.

Má-li být přepnutí ze střežení do klidu realizováno na ústředně, je třeba dbát na takové umístění, aby se co možná nejvíce zkrátila cesta od vchodu k ovládacímu místu. Je třeba dbát, aby se zamezilo možnosti pozorování postupu obsluhy nepovolanými osobami.

2. *Přívodní (propojovací) kabely* - je nutné zvolit propojení odpovídající požadovanému provedení systému a podmínkám okolního prostředí podle specifikace výrobce zařízení.

Pokud je zvoleno kabelové vedení, musí být provozováno uvnitř střeženého objektu. Je nutné věnovat zvýšenou pozornost výběru typu použitého kabelu a s tím i spojené jeho vedení a uchycení.

U bezdrátového vedení je nutné věnovat pozornost vlivu náhodných či úmyslných rádiových přenosů používajících stejný kmitočet, jako u zvolené EZS. Tyto přenosy mohou mít za následek vykazování poruch a nebo stavy narušení střeženého objektu a tím znemožňují správnou funkci spojení.

#### *3. Magnetické detektory otevření oken a dveří*

**a)** patřičně posoudit rozsah otevření pro vstup nebo pro odejmutí předmětů a podle toho umístit snímače (jiná detekce je pro vstup osoby, jiná pro prostrčení ruky či manipulátoru),

**b)** umístění snímačů tak, aby nedošlo k případnému drnčení oken či dveří,

**c)** posouzení dalších faktorů, jež mohou ovlivnit spolehlivou činnost jednotlivých dalších prvků, např. při použití magnetických spínačů při umístění na kovový předmět - plochu použít dielektrických podložek, nebo nemontovat na místa, kde by mohlo dojít k úmyslnému aktivování.

4. *PIR detektory pohybu* pracují na principu pasivní infračervené techniky a jsou náchylné k vlivům :

**a)** předměty umístěné před průzorem čidla, především ty, jež mají za příčinu zvýšení teploty - radiátory, různá topidla aj.,

- b)** průvany před přední částí čidly- vzniklých při špatném utěsnění oken či dveří,
- c)** přímé osvětlení slunečními paprsky,
- d)** turbulence, jež vznikají prouděním teplého či naopak studeného vzduchu a tím zapříčiní rozpořívování např. záclon,
- e)** průnik hmyzu do čidla (čidla musí být dobře utěsněna), apod.

*další detektory :*

*5. Akustické detektory rozbití skla,*

*6. Detektory kouře,*

*7. Detektory úniky plynu,*

*8. Tísňové hlásiče* - tyto hlásiče především slouží k přivolání pomoci. Používají se různé typy. Základní rozlišení :

Pevný tlačítkový typ - hlásič, pevně namontovaný, přenos je po kabelu, případně bezdrátový,

Přenosný tlačítkový typ - klíčenka, přenos signálu je bezdrátový .

*9. Interiérové sirény,*

*10. Vnější sirény a řada dalších.*

### III. monitorování objektů

Siréna zůstává důležitým prvkem zabezpečovacího systému pro objekty s nízkým stupněm rizika. U objektů s požadavkem na vyšší stupně zabezpečení je podmínkou připojení výstupu poplachového systému na pult centralizované ochrany. (viz. kapitola VI.).

*„Nedávný případ opravdu dobrého zabezpečení domu a jeho zahrady se stal v Anglii. Majitelé byli na dovolené ve španělské Malaze. Pachatelé, kteří vnikli do zabezpečeného objektu /nejprve na zahradu /, byli zachyceni zde nainstalovaným systémem, který ve velice malém časovém úseku informoval majitele o vniknutí nežádoucích osob na jeho majetek, a to formou krátké textové zprávy na jeho mobilní telefon o vyhlášení poplachu. Tento majitel díky dalším zabezpečovacím prvkům jež měl zabudovány a o nichž pachatelé neměli vůbec potuchy mohl nerušeně pozorovat na svém „laptopu“ ve stovky km vzdáleném hotelu, pohyb nepovolaných a neoprávněně vniknutých osob a mohl tak přesně pozorovat jejich pohyb tudíž přesně navádět policii, jež vyrozuměl přes telefon. Tím i napomohl k úspěšnému dopadení jež do posledních vteřin neměli potuchy o tom, že policii je na místě a vyčkává na nejvhodnější okamžik k jejich zadržení.“<sup>14)</sup>*

Ještě před několika lety by se tento případ i s jeho průběhem a kladným výsledkem z hlediska dopadení pachatelů trestné činnosti - vloupání a krádeží cizího majetku, zdál jako „sain – fikšn“. I sebemenší nainstalování byt i levného bezpečnostního systému pomáhá k ochraně majetku a tím i policistům k plnění jejich povinností vyplívajících z ustanovení § 2 zákona č.283/1991 Sb., O Policii České republiky.

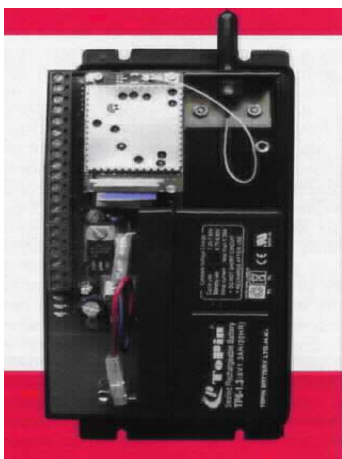
Je nutné brát v úvahu především to, že na střežený objekt působí řada faktorů, které musíme brát v úvahu již při návrhu na způsob zabezpečení, včetně vyhlásování poplachu a přenos informací do monitorovacího centra. „PCO“. Kromě klimatických podmínek, které musejí být jasně definovány u použitých komponentů systému, musí být brán v úvahu i druh majetku jež se má stát předmětem ochrany a jeho hodnota. Atraktivnost pro pachatele loupeží a vloupání se zvětšuje se snadností krádeže a možností zpeněžení.

Ochránit si svůj majetek má být samozřejmou záležitostí každého z nás. Otázky jako : „Co z toho budu mít, když si dobře zabezpečím dům, zahradu či provozovnu?“ nebo „Jaké výhody to pro mne bude mít, od pojišťovny, když si pořídím zabezpečení podle jejich požadavků ?“ nejsou a především by neměly být na zcela místě. V řadě států světa je běžné, že si pojišťovny stanoví určitou standardní úroveň zabezpečení, a kdo jí nebude vyhovovat, toho vůbec nepojistí.



Vzhledem ke stále se navyšujícímu se počtu vloupání a tudíž i ke zvyšování způsobených škod, musí být podmínky pojistné ochrany zpřísněny.

Na základě tzv. „blokované výjimky“<sup>15)</sup> si mohou jednotlivé pojišťovny stanovit stejné podmínky pro zabezpečení. V tomto směru je plně využíván servis Certifikačního institutu ČAP, který poskytuje seznamy technických prostředků, montážních firem a soukromých bezpečnostních agentur s ověřenou kvalitou. Pokud provozovatelé pultů centralizované ochrany vyhoví standardům ČAP, mohou být zařazeni do seznamu doporučených firem.<sup>16)</sup>



Obr. č.2..GSM hlásič poplachu

## IV. Integrovaná ochrana zboží

V České republice došlo po roce 1989 ke zvýšení a vůbec zavedení obchodů s volným přístupem ke zboží neboli samoobslužných prodejen (hypermarketů a supermarketů) a později i jejich obchodních komplexů se začal bohužel i zvyšovat nárůst a počet krádeží.

Ke zvýšené kriminalitě docházelo a dochází nejen v oněch již zmiňovaných obchodních celcích, ale došlo i k podstatně velkému nárůstu krádeží ve veřejných knihovnách. Podle v té době vedené statistiky došlo k nárůstu krádeží i ztát způsobených zloději přicházejících z vnějšku (potenciálních zákazníků) až 40 % z celkového počtu. Tímto bohužel neslavná statistika nekončí, neboť docházelo i k nárůstu počtu krádeží způsobených za strany zaměstnanců a nelze opomenout zpronevěry i ze strany dodavatelských firem. Toto představuje zhruba dalších 56%.

Tato neblahá statistika vedla po delších neblahých úvahách k tomu, že nastal rozmach metod a systémů na ochranu zboží.

Pojem integrovaná ochrana zboží zastřešuje soubor systémů i opatření snižujících při vhodné kombinaci ztráty v obchodech na minimum.

Do komplexu opatření spadá v první řadě Electronic Article Surveillance (EAS),  
- anténní systém včetně příslušenství, který se umísťuje u východu z prodejen nebo k pokladnám.

Dále do komplexu opatření zahrnujeme:

- smyčkovou ochranu* -elektrické zařízení chránící zboží v přímo propojených kabelových smyčkách a s různými typy koncovek,
- kamerové dohledové systémy analogové nebo digitální,*
- mechanické zábrany a zrcadla,*
- bezpečnostní služby.*<sup>17)</sup>

#### **IV.1. Elektronické anténní systémy - ochrana zboží v obchodech**

Anténní elektronické systémy (dále jen „EAS“) jsou založeny na fyzikálním principu narušení elektromagnetického pole, které je vytvořeno mezi anténami-vysílačem a přijímačem. V případě jedno anténních systémů je tato činnost zabezpečena pouze jedním stojanem(anténou) , která funguje jako vysílač a přijímač zároveň.Narušení pole es dosahuje přítomností etikety (laděného obvod -RF, magnetického pásku-Em, dvojice magnetických kmitajících pásků AM)

Systémy EAS dělíme na : - *RF - radiofrekvenční,*  
- *EM –elektomagnetické,*  
- *AM- sousto-magnetické.*

Poslední novinkou v oboru je tzv. RFID , což je radiofrenkvenční systém pracující na frekvenci např. 13,56 MHz.

#### IV.1.1. RF - radiofrenvenční technologie

**RF** - radiofrenkvenční technologie patří ve světě k nejvíce rozšířeným technologiím, hlavně těch jež pracují na frekvenci 8,2 MHz.

Etikety jsou na ochranu zboží se dá říci, že tato zařízení je možné sehnat nejširší sortiment prvků od různých výrobců: - *samolepící bezpečnostní etikety rozměrů 2,5x2,5 až 5x5 cm,*

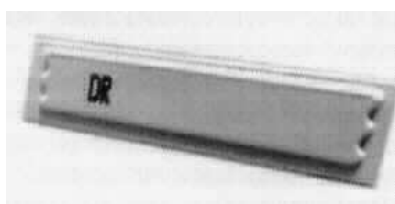
- *tvrdé etikety na textil v mnoha variantách,*
- *etikety na lahve,*
- *etikety na brýle,*
- *etikety na napájecí kabely k elektronickým přístrojům.*



Obr. č. 3. *samolepící bezpečnostní etiketa*

##### IV.1.1.1. Tvrdé etikety

Skládají se ze dvou dílů, z vlastní etikety a z kovového nebo plastového pinu. Připevňují se tak, že pinem je propíchnuto zboží a z druhé strany se nasadí etiketa. Tvrdá etiketa má být instalována viditelně. Doplnit lankem, které je možné použít místo pinu na označení kožené galanterie, elektroniky, obuvi a sportovního náčiní.



Obr. č.4. *tvrdá etiketa*

##### IV.1.1.2. Měkké etikety

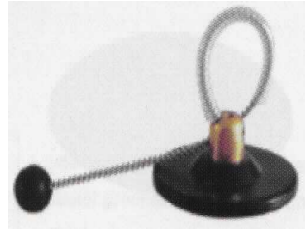
Jsou umístěny v průhledném sáčku. Lze je doplnit jehlou a připevňovacím kloboučkem

##### IV.1.1.3. Tvrdé etikety na lahve

Jsou vybaveny zvláštním lankem, které umožňuje připevnění etikety na hrdlo lahve.

#### **IV.1.1.4. Piny na kabely**

Připevní se na napájecí kabel spolu s etiketou a chrání napojené elektrické zařízení, vrtačku, apod.



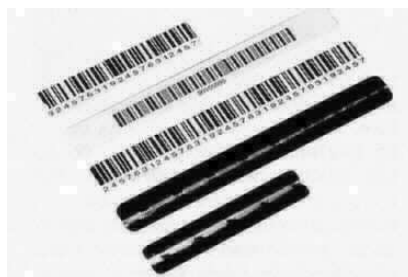
*Obr. č.5 Pin na kabelu*

#### **IV.1.1.5. Ochranné obaly na MC, CD, VIDEO, DVD, apod.**

Jsou vyroben z průhledného plastu a jsou vybaveny zamykatelným systémem. Je možné je vybavit etiketami RF, EM i AM.

#### **IV.1.1.6. Samolepicí etikety**

Jsou de aktivovatelné, na zboží nebo do zboží se nalepují. Cena těchto etiket se připočítává k ceně výrobku.



*Obr. č.6. samolepicí bezpečnostní etiketa jiného druhu*

#### **IV.1.2. EM - elektromagnetická technologie**

**EM** - elektromagnetická technologie se vyznačuje nejméně nápadnými ochrannými samolepicími etiketami velmi malých rozměrů. Systém je založen stejně jako u RF na dvojici antén, mezi nimiž je sledována změna magnetického pole. Velmi zajímavá vlastností

z hlediska např. knižního fondu je možnost opětovné aplikace etikety. Výhodou je malý rozměr samolepicích etiket, možnost zpětné reaktivace samolepicích etiket a možnost ochrany materiálu z hliníku. Nevýhodou jsou poněkud vyšší ceny, možnost vzniku poplachu na podobné materiály jako je etiketa.

#### **IV.1.3. AM – akusto-magnetické technologie**

**AM** – akusto-magnetické systémy jsou unikátní zařízení založená na rozkmitání dvojice magnetických pásků v elektromagnetickém poli, což zaručuje, že systém reaguje pouze na ochranné prvky.

Výhody: jsou v jejich malých rozměrech bezpečnostních samolepicích etiket, velké vzdálenosti mezi anténami- až 2,4 m.

Nevýhody: tloušťka samolepicích etiket, relativně vyšší cenová hladina systémů.

### **IV.2. Elektronické anténní systémy - ochrana knihovního fondu**

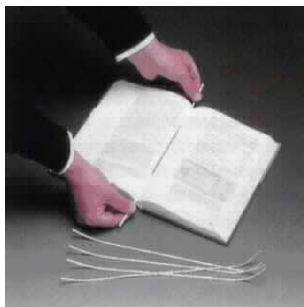
V současné době prudce vzrůstá počet krádeží v půjčovnách knih, což přináší nemalé problémy. Z finančního hlediska jde v celkovém objemu o podstatný zásah do rozpočtu knihoven. Z hlediska kvalitativního pak knihovna nemůže poskytovat služby na takové úrovni, jakou od ní čtenáři právem očekávají.

Veškerý půjčovaný fond knihovny je opatřen speciálními zabudovanými etiketami. Pokud nedojde ke zrušení bezpečnostní funkce těchto etiket personálem půjčovny, je při pokusu o neoprávněné vynesení vyvolán pronikavý poplach sirénou výstupního zařízení, kterým prochází každý návštěvník. Systém chrání veškerý knihovní fond-knihy časopisy, CD disky, apod.

#### **IV.2.1. Ochrana jednotlivých druhů knihovního fondu**

##### **IV.2.1.1. Knihy, časopisy**

U vázaných knih se vlepuje pásková etiketa do hřbetu knihy pomocí magnetického vkládacího nože. Do brožurovaných knih a časopisů se pásková etiketa vlepuje mezi stránky co nejbližší ke hřbetu knihy, resp. časopisu. Vhodné jsou rovněž transparentní etikety s názvem knihovny, které se lepí na zadní stranu obalu. Má-li knihovna k dispozici systém automatické evidence pomocí čárového kódu, používá etikety s předtištěným čárovým kódem a s označením knihovny.



*Obr. č.7. ukázka vlepování ochranné páskové etikety do knihy*

#### **IV.2.1.2. Audiokazety**

Ochrana audiokazet se provádí nalepením etikety přímo na kazetu (způsob obdobný knihám). Deaktivace a reaktivace kazety probíhá na de aktivátoru/re aktivátoru pro audio kazety. Další způsob ochrany audiokazet představuje uzavření kazety do speciálního plastového obalu se zabudovanou etiketou. Z toho obalu je audiokazeta vyjmuta za pomoci speciálního otvírače.

#### **IV.2.1.3. CD disky**

Ochrana CD disků je zabezpečena nalepením etikety na CD disk. K deaktivaci a reaktivaci se používá de aktivátor/re aktivátor pro knihy. Druhá možnost je uzavření CD disku do plastového obalu, obdobného jako u audiokazet i s stejnou manipulací obsluhy.

#### **IV.2.1.4. Videokazeta**

Tyto se chrání nalepením etiket na videokazetu. K manipulaci s videokazetami je určený speciální de aktivátor-re aktivátor. Další způsob je obdobný jako u audiokazet i se stejnou manipulací obsluhy.

#### **IV.2.1.5. Gramofonové desky**

Používají se etikety vlepované do vnitř obalu desky a nebo na střed gramofonové desky. Deaktivace - reaktivace probíhá na zařízení pro knihovny.

### **IV.3. Předmětová ochrana zboží**

Pod pojmem předmětová ochrana se skrývají elektronická zařízení tzv. Loop alarms - smyčkové alarmy a různé zábrany, které jsou v přímém styku s chráněným zbožím.

Smyčkové alarmy jsou malé elektronické systémy, které se skládají z malé ústředny, centrály řídicí jednotky, apod., která je kabely propojena přímo se zbožím. Na oděvy se

přichytávají speciální klipsy, které při nedovolené manipulaci s úmyslem zboží odcizit dají informaci do ústředny jež vyhlásí akustický poplach. Většina zařízení pracuje na baterie nebo akumulátory dobíjené za sítě.

Tyto smyčkové alarmy jsou velice cenově výhodné, neboť jimi lze zabezpečit především, mobilní telefony, elektrické nářadí ale i např. koženou galanterii, další méně rozměrné zboží (To především z důvodů velké nabídky senzorů.).



Obr. č.7 ukázka smyčkových alarmů

#### **IV.4. Kamerové systémy**

K velmi často používaným způsobům zabezpečení patří kamerové dohledové systémy. V oblasti ochrany zboží se používají především kamerové systémy a to hlavně proti zlodějům z řad zaměstnanců. Je nutné však použít kombinaci otočných kamer a kamer skrytých. V těchto případech je zapotřebí vybavení takového objektu velínem se stálou obsluhou. Kamerové systémy se v oblasti ochrany zboží a prevence využívá ve dvou hlavních režimech:

- s obsluhou,
- bez obsluhy.

V případě větších obchodů či obchodních center je nutné použití kamerového systému s *obsluhou*, jež vyhodnocuje potenciální zloděje z řad zákazníků, zaznamenává jednotlivé krádeže a informuje bezpečnostní pracovníky jež mají stanoviště u vchodu do tohoto obchodu (obchodního centra.).

Kamerový systém je vhodný doplněk k jinému zabezpečení zboží např. pomocí EAS nebo již zmíněných smyčkových alarmů. Některé firmy používají a nechávají nainstalovat jako doplněk nefungující kamery.



#### **IV.5. Bezpečnostní zrcadla**

Dalším zabezpečovacím prvkem jsou bezpečnostní zrcadla, jež jsou především umístována u pokladen a nebo v místech kam by jinak obsluha špatně viděla. Používají se jako doplněk z široké škály bezpečnostních systémů.

#### **IV.6. Ochrana nákupních vozíků**

S nástupem velkých obchodních řetězců a sítí hyper-supermarketů se objevil problém, který souvisí se ztrátami . Jedná se o úmyslné krádeže nákupních vozíků. Tyto krádeže jsou sice ojedinělé, bohužel se však vyskytují. Z hledem k tomu, že některé řetězce měli tuto zkušenost již několikrát, přišli s řešením tohoto problému.

Je to novinka na trhu u nás ještě minimálně rozšířena. Je založena na principu vysílače a přijímače jež je umístěn do každého vozíku. Aby se zabránilo odcizení těchto nákupních vozíků je onen již zmiňovaný vysílač umístěn do středu parkovací plochy. Jakmile vozík opustí vymezený okruh vysílačem, kolečka vozíku se zablokují a nekalý záměr je přerušen. Některé obchodní řetězce ještě vybavují ony vozíky akustickým signálem.

Nejvíce je tento systém využíván ve Spojených státech amerických v jejich obchodech, kde představují ztráty těchto nákupních vozíků až 15 kusů týdně což je nezanedbatelná částka. <sup>18)</sup>

## V. ČIDLA ELEKTRONICKÉHO ZABEZPEČOVACÍHO SYSTÉMU

**Čidlo** - (detektor) je zařízení bezprostředně reagující na fyzikální změny, jevy, které souvisejí s narušením střeženého objektu či prostoru nebo na nežádoucí manipulaci se střeženým předmětem. Při indikování stavu narušení reaguje čidlo vysláním poplachového signálu nebo zprávy.

### V.1. Dělení čidel EZS

Čidla elektronického zabezpečovacího systému je rozdělit do dvou základních skupin a to dle toho zda vyžadují či nevyžadují napájení elektrickou energií :

- čidla napájená,
- čidla nenapájená.

#### V.1.1. Čidla napájená

Čidla napájená se dělí z hlediska toho, zda do zabezpečeného prostoru vyžadují nebo nevyžadují využitelnou energii: - *aktivní*  
- *pasivní*<sup>19)</sup>

##### V.1.1.1 Aktivní čidla

Při zjištění charakteristických rysů pro nebezpečí vytvářejí své pracovní prostředí aktivním zásahem do okolního prostoru (např. vysláním elektromagnetického nebo ultrazvukového vlnění).

Díky tomuto lze velice snadno tyto čidla detekovat a určovat jejich, mrtvé zóny. Jsou schopna porovnávat vstupní signály s předem definovanými kritérii (rychlost, frekvence, amplituda), před vysláním poplachového signálu či zprávy.

##### V.1.1.2 Pasivní čidla

Tyto čidlo reagují pouze pasivně na fyzikální změny ve svém okolí, např. pasivní infračervené čidlo reaguje jen na změnu teplotního gradientu, magnetický kontakt pak na změnu polohy. Pasivní čidla lze jen obtížně identifikovat běžnými technickými prostředky.

##### V.1.1.1.1 Čidla napájená aktivní / pasivní

Čidla napájená ať už se jedná o napájená o aktivní či pasivní provedení, jsou nejvíce rozšířenými co se týče použití v EZS. Vzhledem k tomu, že na trhu je jich veliké množství a

provedení lze je dále dělit především podle :

*A) charakteru střežené oblasti:*

- *prostorová čidla* - reagují na jevy související s narušením střeženého prostoru,
- *směrová čidla* - reagují jen v definovaném směru ,
- *bariérová čidla* - reagují na narušení bariéry, která je vytvářena vyzařovací či snímací charakteristikou čidla,
- *polohová čidla* - reagují na změnu polohy chráněného předmětu.

*B) dosahu - pro vnitřní ( vnější ) použití:*

- *s krátkým dosahem* do 15 m (do 50m),
- *se středním dosahem* do 50 m (do 150 m),
- *s dlouhým dosahem* nad 50 m (nad 150 m).

*C) tvaru vyzařovací nebo snímací charakteristiky:*

- *se standardním rozsahem,*
- *se širokouhlým rozsahem - s kruhovým dosahem,*
- *se svislou bariérou ( záclonovou),*
- *s vodorovnou bariérou,*
- *s dlouhým dosahem.*

## **V. 2. Čidla nenapájená**

Vzhledem k tomu, že na trhu je omezený sortiment čidel nenapájených, používaných v elektronických zabezpečovacích systémech, lze je rozdělit podle aktivní činnosti na :

- *destrukční čidla,*
- *nedestrukční čidla.*

### **V.2.1. Destrukční čidla**

Tyto čidla jsou schopna pouze jednofázové funkce - při vyhlášení poplachu dojde k jejich zničení (fóliové polepy, poplachové fólie, tapety, skla).

### V.2.1.1. Fóliové polepy

Fóliové polepy jsou známy již dosti dlouhou dobu zabezpečování, neboť byly používány a využívány i pro viditelnou formu střežení. Umožňují indikaci stavu porušení křehkých a tříštivých ploch jako jsou okna, výkladní skříně, skleněné výplně dveří, ale i tenké neskleněné plochy. Jedná se o pásy z vodivého hliníkové fólie o tloušťce kolem 0,08 mm a šířce 8-12 mm a zpravidla dvou meardů (kontaktních plošek), které se lepí pomocí lodního laku na skleněnou plochu ve vzdálenosti 50 -100 mm od okraje rámu.

Tato vzdálenost, hlavně vzdálenost od horního okraje je velice důležitá a je nutné ji zachovat, neboť tím zabraňujeme minimálnímu vzniku planých poplachů způsobených vodními parami jež se na skleněných plochách srážejí. Tím se mimo jiné prodlužujeme životnost a spolehlivost bezpečnostních fóliových polepů.

Instalací fóliového polepu vytváříme na chráněné ploše tenkou vodivou vrstvu, která je součástí zabezpečovací smyčky. Při rozbití skla zpravidla vždy dojde k přetržení polepu a tím k přerušení průchodu klidového proudu v zabezpečovací smyčce a tak dojde k vyhlášení poplachu. Fóliové polepy se umísťují i na tenké dřevotřískové, případně dřevěné desky - přepážky. Lepí se vždy ze strany opačné než by mohlo dojít k napadení .

Tento druh zabezpečovacích systémů je velice spolehlivý a v poslední době bylo prokázáno, že je spolehlivějším jak čidla vibrační, neboť tyto čidla potřebují neustálou kontrolu a vyžadují časté seřizování.

V zahraničí se vyrábějí i fóliové polepy samolepicí, které jsou však dražší. Do zabezpečovací smyčky se zapojují pomocí kontaktního náběhu, což je plastový výlisek s kovovými plíškami a upevňovacími šrouby.<sup>20)</sup>

### V.2.1.2. Čidla otřesová

Patří do skupiny prvků plášťové ochrany a jedná se o čidla jež reagují na otřes (vibrace), Tyto vibrace vznikají při pokusech o narušení chráněných ploch. Je nutné dávat pozor na jejich citlivost a patřičně je nastavit, neboť se často stává, že jsou - li nastavená na značnou citlivost, je to spíše ku škodě majitelů chráněného objektu. Často se stává, je-li objekt blíže frekventované silnici či jakékoliv komunikaci po níž mohou přejíždět nákladní vozidla, způsobují značné množství planých poplachů. Tato nákladní vozidla bývají dosti často přetížena a pak již stačí maličko rychleji projed okolo zabezpečeného objektu a vlivem chvění - vibračí dochází ke spuštění těchto čidel jež vzniklou situaci vyhodnotí jako poplachovou.

Dále se nedoporučuje umísťovat je na objekty v blízkosti provozu tramvají či letišť.

#### **V.2.1.2.1. Čidla otřesová s mechanickým měničem**

Otřesovým (vibračním) čidlem nazýváme mechanický kontaktní prvek, který lze uvést do stavu rozepnutí nebo sepnutí otřesy jakéhokoliv druhu.

V naprosté většině fungují na principu setrvačnosti pružně uchyceného závaží. Toto závaží při dostatečné rozkmitu podložky se vychýlí a tím se rozpojí zabezpečovací smyčka. Citlivost čidla se nastavuje pomocí justačního šroubku.

Otřesová čidla se umísťují tam, kde k narušení dochází destrukcí provázenou vibrací. A to na objektech se skleněnými výplněmi, skleněné výplně výkladních ploch. Skleněných i neskleněných výplní dveří. Čidlo je schopné chránit plochu cca 3 m<sup>2</sup>.

Při přerušení u vibračních čidel dojde v proudovém okruhu zabezpečovací smyčky pouze během několika milisekund, je nutné k indikaci tohoto přerušení zabezpečovací ústřednou používat rychlé klopné obvody.

#### **V. 2.1.1.2. Čidla otřesová s akusticko-elektrickým měničem**

Tato čidla se instalují na pevný podklad, jehož vibrace snímají prostřednictvím vhodného akustického měniče (uhlíkového, magneto dynamického) a elektronicky vyhodnocují charakteristiky přijetího frekvenčního spektra.

Čidla otřesová s akusticko-elektrickým měničem mají větší šířku pásma vyhodnocovaných kmitočtů, nastavitelnou citlivost a optickou indikaci poplachu s pamětí. Umísťují se podle konstrukčního provedení na riziková místa možného průchodu pláštěm budov, např. zdmi zabezpečeného objektu či na rámy dveří a oken. Nelze je použít pro střežení trezorových skříní a komorových trezorů.

#### **V. 2.1.1.3. Čidla na ochranu skleněných ploch**

Čidla na ochranu skleněných ploch se užívají ke střežení skleněných ploch zabezpečeného prostoru. Jsou známé jako *čidla rozbití skla*. Konstrukčně jsou provedena tak, aby k vyhlášení poplachu vedla již první trvalá mechanická změna střežené skleněné plochy, např. vytvoření otvoru ve výkladní skříní.

Mechanické ovlivnění střeženého skla, jako např. klepání, škrábání, otřesy nebo vhozená hrst písku nevede k vyhlášení poplachu.

### **V.2.2. Nedestrukční čidla**

U těchto čidel při aktivaci dochází ke vratným změnám (vibrační a magnetický kontakt, mikrospínače, apod.).

#### **V. 2.2.1. Mikrospínače**

Mikrospínače jsou miniaturní přepínače, které se používají zejména ke kontrole přístupových cest do chráněného prostoru a zabudovávají se do zárubně proti závoře zámku (zámkové kontakty), čímž střeží uzamčený stav vstupů. Při jejich vhodném vřazení do obvodů ústředny EZS zabrání, aby byla uvedena do stavu střežení v případě, že není některý za stavebních prostupů uzamčen. Užívají se především v případech, má-li prostor více možných vstupů. Mikrospínače jsou používány především jako ochranné kontakty pro jednotlivé prvky EZS. V minulosti se mikrospínače využívaly k indikaci s předmětem. Jejich montáž byla prováděna zpravidla skrytým způsobem.

Nevýhodou je jejich vysoká pracnost montáže, nutnost přesného nastavení pracovního ramene. Další nevýhoda je jejich malá životnost a nutná údržba.

#### **V.2.2.2. Nášlapné koberce**

Jedná se o speciální variantu mechanických kontaktů. Uvádějí se v činnost jestliže pachatel vstoupí na jejich plochu nebo manipulace s předmětem na nich umístěných v době aktivace systému. V ČR se tento systém nepoužívá, ale v zahraničí je rozšířen v některých malých muzeích.

Nášlapné koberce vyrábějí ve dvou základních provedeních:

a) *Fóliové*- bývají menší ( čtverec nebo obdélník o straně 20-50 cm) mají zvýšenou citlivost a menší životnost.

b) *Páskové* - se obvykle dodávají jako obdélník o stranách 0,6-1 m x 4-10 m a jejich délku lze snadno přizpůsobovat.

Nášlapné koberce se používají zásadně skrytě (pod koberce, běhouny, linoleum). Umisťují se především tam kde je zapotřebí signalizace vstupu na určité místo.

Tato čidla lze v některých případech použít jako skryté hlásiče tísňe.

### V. 2.2.3. Magnetické kontakty

V současné době jde o nejrozšířenější kontaktní čidla, vyráběná ve velkém počtu provedení a aplikačních variant.

Magnetické kontakty se liší také podle úrovně jejich odolnosti proti překonání a tak narušení zabezpečeného objektu. Některé lze překonat snadno, jiné jen obtížně. K běžným magnetickým kontaktům stačí přiložit dostatečně silný magnet a pak lze zpravidla chráněné okno či dveře bez vyvolání poplachu otevřít. Jazyčkový kontakt, jež je součástí magnetizačního kontaktu, zůstane sepnutý díky magnetickému poli magnetu přiloženého pachatelem, protože není schopen odlišit magnetické pole jeho „vlastního“ od jakéhokoliv „cizího“ magnetu.

### V.3. Čidla bariérová

Bariérová čidla slouží k vytvoření umělé překohady v chráněných prostorách .

Jde zejména o :

- světelná čidla,
- laserové aktivní záclony,
- pasivní a aktivní infračervená čidla s charakteristikou záclony.

V současnosti se používají světelná čidla s neviditelným světelným paprskem i infračervené části spektra (0,75-10  $\mu\text{m}$  ), proto jsou označována jako infračervená (*Infra - Red -IR* ) čidla a laserová čidla (v oblasti 850 nm.).

#### V.3.1. Čidla infračervené závory

Každá infračervená závora (infra-závora) se vždy skládá z aktivní části - vysílače (V) přijímače (P). Vysílač generuje infračervené paprsky, které pomocí optiky směřují k přijímači, kde jsou zpracovány. Při jejich přerušení (nebo při poklesu detekované úrovně) způsobené vstupem narušitele do dráhy paprsků je vyvolán poplachový stav.

Pokusí-li se někdo oklamat přijímač jiným zdrojem IR záření, jehož modulace neodpovídá modulaci vlastního vysílače, zařízení vyhláší sabotážní poplach. V některých menších prostorách lze jedné infra-závory využít k vícenásobnému blokování prostoru použitím odrazových zrcadel. Při tomto použití světelných závor je IR paprsek vyslaný vysílačem směřován na zrcadlo a odrazem od něj na přijímač nebo na další zrcadlo. v této kombinaci se dosah zkracuje asi na polovinu, v závislosti na počtu odrazných zrcadel. Rizikové faktory vzniku falešných poplachů jsou především v zaprášení nebo orosení odrazových zrcadel nebo jeho i nepatrné vychýlení z nastavené polohy. Bezpečný a

prakticky použitelný dosah těchto infračervených závor je od 20 do 80 m.

#### V.4. Čidla pohybu

Každý druh těchto čidel má určité vlastnosti, kterou jsou výsledkem vývoje zpracování signálu a technologie použité daným výrobcem. Při vlastní aplikaci přenášejí tyto funkce vyšší odolnost proti planým poplachům způsobených především vlivem okolního prostředí umístěného čidla pohybu. (např. proudění vzduchu, osvětlení, vibrace atd.). I pro tyto negativně ovlivňující okolní vlivy, musíme konstatovat, že zaručují vysokou úroveň zabezpečení z hlediska napadení chráněného objektu. Správně nastavené a připojené čidlo jednoduššího technického provedení může uživateli při nižších pořizovacích nákladech zabezpečit stejně dobře a spolehlivě jako kdyby použil dražší provedení.

Z hlediska aplikace nabízejí některé typy čidel pohybu další doplňkové funkce :

- *dálkové odpojení indikační LED diody* - umožní jak montážní firmě tak i uživateli tepování funkce a dosahu čidel v provozu,

- *odpojení mikrovlnné či ultrazvukové vysílací části* - u citlivých osob může při dlouhodobém pobytu v prostorách s ultrazvukovým nebo mikrovlnným polem dojít ke zdravotním potížím ( osoby s kardiostimulátory),

- *paměť poplachových událostí a dálkové nulování (reset) této paměti* - umožňuje identifikaci narušení prostoru či poruchu čidla,

- *další doplňková funkce je antimasking* - jeto funkce aktivní ochrany proti zakrytí a přestříkání čidla.



#### **V.4.1. Antimasking**

Čidla s antimaskingem jsou používána v prostorách s vyšším rizikem napadení a veřejně přístupných, kde hrozí nebezpečí sabotáže systému s cílem upravit si zabezpečený objekt ve stavu střežení na vloupání.

Vyřazení funkce antimaskingu lze provést úmyslně nebo dostatečným zastíněním čidla při přemístění nábytku či pomocí jiného zřízení místnosti. Nemusí jít o úplné zastínění čidla, postačí jen částečné stínění, nebo postříkání vhodným aerosolovým přípravkem, který znemožní propouštění infračerveného, ultrazvukového nebo mikrovlnného záření.

Ochrana antimaskingu spočívá v neustálé důsledné kontrole blízkého prostoru před čidlem samotným.

Základním druhem je vysílání infračerveného záření infradiodou do prostoru před čidlo a jeho následný příjem. Pokud toto záření není přijato přijímací infradiodou, je vše v pořádku. Odrazí-li se infračervené záření od předmětu (tabule skla, kartónová a akrylátová deska), maskující výhled čidla, a následně je toto záření přijato, dochází k vyhlášení sabotážního poplachu.

Další druh antimaskingu využívá mikrovlnného záření o nízkém výkonu. Pokud vyslané mikrovlnné záření odrazí od překážky a je zpětně přijato a vyhodnoceno, čidlo vyhlásí poplach. Takto je hlídán pouze blízký prostor okolí čidla.

#### **V.4.2. Dělení čidel pohybu**

V praxi je možné se setkat s několika druhy čidel pohybu, každé pracující na různém fyzikálním principu. Jednotlivé druhy čidel využívají ke své funkci odlišnou část kmitočtového spektra elektromagnetického vlnění.

Rozdělení čidel pohybu :

- VKV čidla,
- Mikrovlnná čidla,
- Ultrazvuková čidla,
- Infračervená čidla (pasivní, aktivní),
- Kombinovaná (duální) čidla.

##### **V.4.2.1. VKV Čidla**

Tato čidla mají oddělenou vysílací a přijímací část na rozdíl od ostatních čidel pohybu. Mají výkon řádově desítky miliwatt a antény jsou velice podobné malým pokojovým televizním anténám.

Pracují na principu změny homogenity elektromagnetického pole vytvořeného

v chráněném prostoru mezi vysílací a přijímací anténou. Tyto antény jsou umístěny na protějších stranách chráněného prostoru. Na přijímací straně dojde k fázovému posuvu signálů, tzn. kmitočtu přicházejícího přímo u vysílací antény a kmitočtu odraženého od narušitele. Tento fázový posuv je vyhodnocován a při překročení předem nastavené difference dojde k vyhlášení poplachu. Citlivost je v důsledku sčítání fázových posuvů až 50 x větší než u ostatních čidel pohybu. VKV čidla jsou schopna vyzařováním elektromagnetickým polem pokrýt prostor až 50 m dlouhý a 10 m široký. Zvláštní druh VKV čidel - tzv. monolitní využívají Dopplerova efektu .

#### **V.4.2.2. Mikrovlnná čidla**

Stejně jako infračervená tak i čidla mikrovlnná<sup>21)</sup> jsou vedlejším produktem prudkého rozvoje elektroniky.

Úplně první se objevují již počátkem 70tých let minulého století. S postupem rozvoje technologií a poznatků v oblasti mikrovlnné techniky došlo u VKV čidel k přesunutí kmitočtu elektromagnetického vlnění do oblasti mikrovln. Tímto také samozřejmě došlo ke snížení výkonů vysílačů řádově na miliwatty až mikrowatty a tím i ke zvýšení detekční citlivosti mikrovlnných čidel. Anténní systémy těchto čidel jsou plošné, čímž došlo k omezení jedné z negativních vlastností MW čidel a to vyzařování energie „za čidlo“. U nejvyšších stupňů prostorové ochrany se používají tato čidla a při správné instalaci je velice obtížné jejich překonání i pro profesionály (vysoce nízká pravděpodobnost vloupání). Odlišnost mikrovlnných čidel od VKV lze spatřovat především v tom, že jejich elektromagnetické vlnění zpravidla neproniká zdí, dřevem ani sklem, a když, tak velice nepatrně, což má podstatný vliv na jejich praktické použití. Mikrovlnná čidla patří také do skupiny čidel dopplerovských (sama vytvářejí své pracovní prostředí) .

#### Dopplerův jev

Zvláštní jevy nastávají, jestliže se vzájemně pohybují zdroj vlnění a pozorovatel, popř. i prostředí, ve kterém se postupně vlnění šíří. Blíží-li se např. zdroj tónu (automobilová houkačka), slyšíme tón o poznání vyšší, než je-li vzhledem k nám v klidu nebo vzdaluje-li se od nás. Změna pozorované frekvence a její závislost na relativní rychlosti zdroje a pozorovatele, popř. i prostředí se nazývá Dopplerův jev.

Při odvozování kvantitativních vztahů pro Dopplerův jev vycházíme vždy z případu, že zdroj Z a pozorovatel P jsou v klidu jak navzájem, tak vzhledem k prostředí, jímž se vlnění šíří. Při tom pozorovatel zjišťuje, že frekvence  $f$  vlnění, které prochází jeho místem, je

$$f = \frac{c}{\lambda}$$

Kde  $c$  je fázová rychlost vlnění a  $\lambda$  jeho vlnová délka. V tom případě jedna vlnová délka  $\lambda$  projde místem P za periodu

$$T = \frac{1}{f}$$

Jinými slovy, stejné fáze vlnění procházejí místem pozorovatele v časových intervalech  $T$ .

Kvantitativní vztahy pro změnu frekvence, kterou zjistí pozorovatel, odvodíme pro 3 jednoduché případy, při nichž se zdroj vlnění Z a pozorovatel P pohybují po přímce ZP.

1.-Pozorovatel je v klidu vzhledem k prostředí, ale zdroj se pohybuje

a) Jestliže se zdroj pohybuje tak, že se blíží k pozorovateli rychlostí  $v$ , znamená to, že za dobu  $T$  se zdroj Z přiblíží k místu P o dráhu  $v \cdot T$ . Proto doba  $T'$  průchodu dvou sousedních stejných fází místem P je o

$$\Delta T = \frac{vT}{c}$$

Jejich funkce je stejná jako u VKV čidel, ale v jiném kmitočtovém pásmu elektromagnetického vlnění. Jde o pásma 2,5 GHz, 10 GHz nebo 24 GHz. Citlivost MW čidel závisí na velikosti a povrchu odrážejícího tělesa, množství odražené energie, vzdálenosti mezi tělesem a čidlem a rychlosti pohybu tělesa. Pokud se těleso pohybuje pomalu, je frekvenční posun velmi malý, nezávisle na směru pohybu (od nebo k čidlu). Mikrovlnná čidla se musí instalovat tak, aby rušení vlivy mimo střežené zóny nebylo možné, neboť reagují na každý pohybující se předmět úměrný velikosti, vzdálenosti, odraženosti a rychlosti (např. blízko projíždějící vozidla). V blízkosti MW čidel se nesmí nacházet objekty pokovené (např. zrcadla, ochranné fólie) nebo předměty vyrobené z kovu (mříže, sítě, oplechované dveře). Zvláště kritické jsou objekty s rovinným povrchem, od kterého se mikrovlny účinně odrážejí a mění tím výrazně detekční charakteristiku.

### V.4.2.3. Ultrazvuková čidla

Ultrazvuková čidla patří rovněž do skupiny dopplerových čidel aktivních, tzn., že do prostoru vysílají energii. Nevytvářejí však kolem sebe pole elektromagnetické, nýbrž ultrazvukové na frekvenci v pásmu 20-45 kHz.

Aktivním prvkem ultrazvukového čidla je vysílač - akustický zářič (jedná se o obdobu reproduktoru). Ten vysílá do prostoru chráněného objektu vlnění o stálém kmitočtu nad slyšitelný pás zvuku. V chráněném prostoru se tak vytvoří tzv., stojaté vlnění, které reprodukuje klidový stav.

#### **Stojaté vlnění**

Pokud budeme uvažovat, že hadice bude na jednom konci upevněná a na druhém bude kmitat harmonicky, vznikají v podstatě dvě vlnění – přímé a odražené. Složením těchto vlnění vzniká pak vlnění stojaté. V bodech, v nichž je největší amplituda jsou **kmitny** stojatého vlnění, v bodech, které jsou trvale v klidu jsou **uzly** stojatého vlnění.

Mezi postupným a stojatým vlněním je tedy zásadní rozdíl :

Postupné – všechny body kmitají se stejnou amplitudou, ale různou fází (přenáší se energie)  
Stojaté - všechny body kmitají s různou amplitudou, ale stejnou fází  
(energie se nepřenáší, ale jen se periodicky mění potenciální energie pružnosti v kinetickou energii hmotných bodů)

V klidovém stavu elektronika vyhodnotí přijatou vlnu ve stále stejném vztahu k vlně vyslané. Pohybuje-li se v zabezpečeném prostoru libovolné těleso, změní se fáze přijatého vlnění. Tato fáze je vyhodnocena elektronikou a na základě této informace vyhláší poplach. V prostorách, kde jsou uloženy předměty absorbující ultrazvuk (např. koberce, různé druhy pěnových materiálů), že se může citlivost těchto čidel značně změnit oddálením či přiblížením některých předmětů.

Použití více ultrazvukových čidel v jednom chráněném prostoru najednou, realizujeme pouze tehdy, jsou-li vysílače jež obsahují synchronizovány nebo tak kmitočtově stálé, že není možný vzájemný negativní vliv .

Nikdy nesmíme instalovat ultrazvuková čidla za závěsy, nad topná tělesa, v prostorách kde je teplo vzdušné topení. Dále pak se neumisťují v blízkosti zdrojů zvuku se širokým spektrem, v blízkosti telefonu, v prostorách s volně zavěšenými tělesy jako jsou lampy, vývěsní štíty, neboť toto vše má za následek rušení ultrazvukových signálů a tím k vyvolávání planých poplachových událostí.

### **V.4.3. Zpracování signálu čidel pohybu**

Důležitou oblastí čidel pohybu je zpracování získaného analogového signálu. Na kvalitě zpracování těchto informací závisí spolehlivost detekce a odolnost vůči planým poplachům.

Způsoby zpracování signálu : - *Analogové zpracování,*  
- *Digitální zpracování.*

#### **V.4.3.1. Analogové zpracování signálu**

Nejpoužívanějším způsobem zpracování signálu je vyhodnocení jeho prahové úrovně, při jejímž překročení dojde k vyhlášení poplachu. Tento způsob vyhodnocení se používá u většiny čidel ještě s kombinací s tzv. počítadlem pulsů.<sup>22)</sup> To podmiňuje vyhlášení poplachu tím, že při opakovaném překročení prahové úrovně došlo několikrát za sebou během definovaného časového úseku. Avšak i v tomto případě dochází k vyhlášení planých poplachů způsobených především prudkými teplotními změnami či za přispění jiných vnějších vlivů.

Díky těmto vlivům je výhodnější, využívat vyhodnocení nejen prahové úrovně, ale i vyhodnocování celkové amplitudy popř. průběhu signálu.<sup>23)</sup>

Bohužel i přes použití těchto metod a nebo podobných zpracování signálů dochází k výskytu planých poplachů . V poslední době výrobci opouštějí analogové zpracování a přecházejí na využití digitálních technologií.

#### **V.4.3.2. Digitální zpracování signálu**

Digitální signály jsou oproti analogovým mnohem méně náchylné k poruchám. To se ověřilo i při používání kompaktních disků.

Výrobci se tudíž snaží digitalizovat signály po jejich detekování, čímž se eliminují nepřesnosti vzniklé při snímání těchto záznamů signálu. Digitální signály lze mnohem lépe zpracovávat a vyhodnocovat podle různých kritérií a při vyhodnocování algoritmů mikroprocesorem tak v maximální možné míře potlačit výskyt planých poplachů. Dalším nesporným kladem digitálních záznamů signálu je i ten, že takto uložená data nepodléhají stárnutí na rozdíl u analogového uložení záznamů.

## **V.5. Čidla tísňového hlášení**

Čidla tísňového hlášení slouží k ochraně zaměstnanců a veřejnosti přímého ohrožení, a to hlášením do místa odkud může být poskytnuta pomoc. Ať už je to na PCO Policie ČR, nebo městské policie či na bezpečnostní agenturu.

Poplachové hlášení může být vyvoláno za pomoci manuálního aktu, nebo zprostředkovaně při předem určeném postupu manipulace s určitým čidlem.

Podle umístění hlásiče a způsobu vyvolání poplachu je dělíme na :

- *Veřejné tísňové hlásiče,*
- *Speciální tísňové hlásiče.*

### **V.5.1. Veřejné tísňové hlásiče**

Jedná se o magneto - kontakty či mikrospínače, uložené do pouzdra a mající tvar tlačítka. Slouží veřejnosti např. v bankách, pro klientelu k vyvolání tísňového poplachu. Jsou umístěné na veřejných a dobře viditelných místech zabezpečených objektů, na schodištích, v chodbách a halách. Umisťována bývají do výše 120-150 cm od podlahy. Je to z důvodu, aby mohl každý v případě potřeby a nouzové situaci nebo byl svědkem takové nouzové situace, je použit. Dále pak je využívá bezpečnostní agentura případně strážná obchůzková služba. Veřejné tísňové hlásiče jsou opatřeny krycím sklíčkem, aby nedocházelo k bezdůvodnému zneužívání těchto tlačítek tísňového volání a tím k jejich zneužití. Je vhodné, aby tyto veřejné hlásiče byly opatřeny vlastní pamětí, aby v případě vyhlášení poplachové události, se zjistilo z kterého konkrétního tlačítka byl poplach aktivován.

### **V.5.2. Speciální tísňové hlásiče**

Speciální tísňové hlásiče - skryté, jsou určeny k nepozorovatelnému vyvolání tísňového hlášení v případě přímého ohrožení (např. při přepadení v bance, či při přepadení na poště u přepážky). Jsou určeny pro osoby zaměstnané v chráněném objektu a seznámené s jejich účelem, funkcí a způsobem použití. Při jejich umístění je nutno pečlivě zvolit

vhodné místo, neboť nemají ochranný štítek, který by je ochránil před nechtěným vyhlášením tísňového poplachu. Hlásiče tísňového poplachu nesmí být umístěny v dohledu cizích osob, ale musí naopak být co nejvíce přístupné pro zaměstnance, aby v případě ohrožení je mohli snadno a co nejméně nápadně použít. Je jedno zda budou spuštěny nohou, rukou či jinou částí těla (s ohledem na to, v jaké situaci se může obsluha v případě ohrožení nacházet.). Naopak hlásiče musí být zároveň umístěny tak, aby se co nejvíce zabránilo náhodným spuštěním tísňového poplachového hlášení při běžné pracovní činnosti.

Závady spojené s tísňovými hlásiči jsou v naprosté většině způsobeny špatnou manipulací obsluhy a tím k vyvolání plachých tísňových hlášení. Ať už je to způsobeno zaměstnanci z důvodu neznalosti obsluhy či jejich zanedbáním.

Speciální tísňové hlásiče jsou podle způsobu a místa použití vyráběna jako :

1. *Hlásiče lištové* - jsou určeny pro sedící obsluhu, a bývají obvykle umístěny tak, aby mohly být ovládány sešlápnutím, zvednutím nártu či kolenem a to buď do stany či pohybem nahoru.

2. *Hlásiče tlačítkové* - tyto jsou určeny jednoznačně k ručnímu ovládání. Mohou je spíše používat osoby, které nejsou přímo v ohrožení, ale jsou například svědky např. přepadení z vedlejšího pracoviště.

V případě, že je na jednu zabezpečovací smyčku zapojeno několik tísňových hlásičů na jednu je účelné použití prvků s optickou signalizací. Tím se i usnadní identifikace v případě planého tísňového poplachu nesprávné manipulace některého ze zaměstnanců. Základní rozdíl mezi tísňovými hlásiči spočívá v tom, že veřejný tísňový hlásič musí být chráněn před úmyslným vyhlášením poplachu a po použití musí setrvat v poplachovém stavu až do zrušení obsluhou. Zatímco poplachový signál vyvolaný speciálním tísňovým hlásičem trvá jen po dobu trvání podnětu.

Do skupiny speciálních tísňových hlásičů patří též:

- *Bankovní čidla,*
- *Osobní tísňové hlásiče.*

#### **V.5.2.1. Bankovní čidla**

Jedná se o zvláštní hlásiče tísně, známá také pod názvem „poslední bankovky“. Používají se k vyvolání poplachu při neoprávněné nebo vynucené manipulaci s bankovkami (jedná-li se o krádež, přepadení či loupež.<sup>24)</sup>) Umísťují se přímo do peněžních přihrádek .

Bankovková čidla se vyrábějí ve dvou provedeních :

- *Kontaktní (mechanická),*

- *Bezkontaktní (optická).*

#### **V.5.2.1.1. Bankovní kontaktní čidla**

Běžně se používají bankovní kontaktní čidla s mechanickým kontaktem, tzv. bankovní svorka. Jedná se o konstrukční propojení pružinové svorky a svazku bankovek s klasickým magnetickým kontaktem. Při odebrání svazku bankovek, (při loupežném přepadení a na příkaz pachatele), dojde k sepnutí poplachového kontaktu a tím k vyhlášení poplachu.

Nevýhoda : je obtížné je ukryt a jsou zde určité nároky na obsluhu, která při krizové situaci nemusí být schopná správné reakce.

#### **V.5.2.1.2. Bankovní bezkontaktní čidla**

Jedná se o moderní bezkontaktní optická čidla. Pracují na principu bezkontaktního reflexního optického spojení, což je zárukou dlouhodobé spolehlivosti. Jsou vyráběna ve třech provedeních :

- *základní* (bez paměti poplachu),
- *s optickou identifikací* (s pamětí poplachu - adresné).
- *s optickou identifikací a s nastavitelným zpožděním vyhlášení poplachu*

(zde je standardní hodnota zpoždění 6 sekund ).

Akčním členem je optické čidlo, využívající odraz vyslaného infračerveného paprsku, který indukuje přítomnost nebo nepřítomnost průhledné clony, jež je umístěna na povrchu nebo v těsné blízkosti posledních bankovek. Pro správné odstínění a zabránění průchodu nechtěných paprsků světla je zapotřebí umístit do balíčku alespoň 10 bankovek na sebe. Nepatrné rozměry čidla umožňují jeho použití prakticky do všech peněžních přihrádek a slouží k nepozorovatelnému vyhlášení poplachové tísňové události při přepadení. Bankovkové optické čidlo je svou konstrukcí určeno především pro skrytou montáž, a je vhodné i pro použití nejen do banky či jiných bankovních ústavů či objektů kde je větší pohyb peněz, ale i pro použití k ochraně vzácných uměleckých předmětů jako jsou např. gobelíny, tapisérie, obrazy, sochy.



### V.5.2.2. Osobní tísňové hlásiče

Byly vyvinuty zejména pro zajištění bezpečnosti příslušníků ostrahy ve věznicích, pro pracovníky v psychiatrických léčebnách, kde vzhledem k prostředí je největší pravděpodobnost napadení. V dnešní době jsou rozšířeny a jsou jimi vybaveny snad veškerá pracoviště, kde pracují zaměstnanci často osamoceně např. pracovníci benzínových čerpadel, laboratoře, prodejny). V případě přepadení, oloupení či fyzického napadení potřebují rychlou a okamžitou pomoc, kterou si mohou přivolat díky těmto tísňovým hlásičům. Jsou také ideálním technickým prostředkem pro členy závodní stráže, nebo jiné ostrahy.

V současné době se vyrábějí v několika provedeních:

*a) dosahy osobních tísňových hlásičů:*

- *s malým dosahem* (pokryje pouze rozlohu jednoho patra běžné budovy),
- *s velkým dosahem* (pokryje celou budovu, více budov, celý podnik.),

*b) provedení osobních tísňových hlásičů:*

- *jako náramkové hodinky, náhrdelníky, náramky,*
- *volně umístěné v kapse,*
- *s možností zavěšení na opasku,*
- *k připevnění na spodní straně stolu, pultu nebo přepážky.*

*c) způsoby vyvolání poplachu osobních tísňových hlásičů:*

- *ručně* (zmáčknutí tísňového tlačítka na vysílači),
- *pádem* (poplach se vyvolá automaticky pádem nositele vysílače - Po odeslání poplachové informace vysílač automaticky vysílá kód, který usnadní lokalizaci vysílače - napadeného),
- *vytržením* je-li (vysílač nositeli - napadenému) násilně vytržen.

Osobní tísňové hlásiče podle typu provedení využívají různá kmitočtová pásma, nejčastěji pásmo 27 MHz, 300 MHz, 450MHz a řadu dalších předurčených kmitočtů. Poplachové signály (zpravidla po vyhlášení tísňového poplachu tlačítkem na vysílači) lze přijetí a vyhodnocení zobrazit na přijímači. U jednotlivých systémů se poplach hlásí pouze pomocí blikajícího výstražného světla a houkající sirény, u složitějších systémů přijetím signálu do pevné přijímací jednotky a odtud propojením do počítače. O vzniku poplachu je obsluha informována akusticky nebo i na obrazovce PC.

Některé systémy pro zajištění náročnějších požadavků na bezpečnost pracoviště umožňují rozšíření stávajícího systému o tzv. svolávací systém. Poplachová informace v tomto případě prochází přes síť převaděčů k centrálnímu svolávacímu vysílači, který vysílá do kód adresné nouze až ke svolávacím přijímačům, které vlastní členové zásahové jednotky nebo kolegové, kteří mohou ohrožené osobě pomoci.

Poplachové rádiové a infračervené vysílače jsou napájeny litiovými bateriemi s mimořádnou dlouhou životností, je nezbytné pravidelné testování a periodická výměna baterií, i před stanovenou dobou životnosti. Na jejich funkci může záviset mnohdy lidský život. Kromě osobní ochrany mohou uvedené systémy pracovat i jako zabezpečovací zařízení s bezdrátovým přenosem poplachového signálu, protože je na ně možno připojit jednotlivá čidla EZS.

#### **V.5.2.2.1. Systémy ochrany a zabezpečení osob**

Další možnou variantou osobní ochrany jednotlivce je systém ochrany a zabezpečení osob<sup>25)</sup>, který se od osobních tísňových hlásičů obvykle liší tím, že je doplňkem běžných rádio komunikačních systémů. Radiostanice je vybavena tísňovým (nouzovým) tlačítkem a pohybovým čidlem. V případě nenadálé nebezpečné události může pracovník pouhým stisknutím tísňového tlačítka žádat o pomoc.

Radiostanice mohou být rovněž vybaveny speciální zásuvkou, která umožňuje připojení vnějších čidel, například detektor mikrovln, rentgenového a radioaktivního záření nebo plynu. Je také možné připojit kontakt „mrtvého muže“, jehož aktivace závisí na poloze radiostanice. Dojde-li k tomu, že je stanovenou dobu ve vodorovné poloze, vyšle se automaticky tísňový signál, aniž by obsluha musela čímkoliv manipulovat a upoutat tak pozornost pachatele. Tento stav je opět signalizován v řídicím centru.

## VI. PULT CENTRALIZOVANÉ OCHRANY

V dnešní době již většina lidí ví oč jde, ale ne vždy tomu tak bylo. Pokud se někdo domnívá, že PCO se staly součástí našeho života v posledních letech kdy rozmach elektroniky a počítačové techniky byl opravdu obrovský, velice se mylí.

V ČR se PCO budovaly jež v rámci SNB<sup>26)</sup> od poloviny sedmdesátých let. Je zde na místě ještě napsat, že nejprve byly budovány PCO - hlásiče požárů a potop později se vyvinuly a připojily hlásiče zabezpečující ochranu objektů.

### VI.1. Historie pultu centralizované ochrany

Psal se rok 1851, kdy v Bostnu (USA, Massachusetts) byla zahájena výstavba prvního opravdového PCO, sdružujícího výstupy „volacích skříněk“, předchůdců dnešních veřejných hlásičů požáru.

Roku 1856 pan Edwin T. Holmes začal v New Yorku (USA, Stát New York) budovat první PCO, určený pro zabezpečovací aplikace. Z roku 1890 pochází první známá a písemně dochovaná informace o aplikaci veřejného požárního hlásiče vybudovaného v HAMBURKU (Německo).

Poučení o manipulaci s hlásičem požáru, z požárního PCO, uvedeného do provozu 24.4.1864 ukazuje na základní principy činnosti s takovýmto zařízením.

#### **24. dubna 1864 v San Francisko ( CA, USA )**

*„ Po zjištění požáru v blízkosti vaší volací skříňky pomalu a plynule zatočte klikou 25 až 30 krát, potom chvíli vyčkejte, a pokud neuslyšíte tikání ze skříňky nebo požární zvonky, postup opakujte. Jestliže stále nezaznamenáte žádný poplach, přejděte k jiné skříňce a vyhlaste poplachy z ní. Nikdy neotvírejte skříňku a nedotýkejte se kliky, jedině v případě požáru. Nikdy neohlašujte požár, který vidíte z dálky . Před odchodem se ujistěte, že skříňka je uzamčená. “*

Pulty centralizované ochrany se samozřejmě vyvíjely, Nejdříve pomalu, v návaznosti na vývoj telefonu, dálnopisu, a v posledních desítkách let, zejména s příchodem digitální techniky a nových komunikačních prostředků, čím dál tím rychleji.

## **VI.2. Přenosové prostředky**

Má-li zabezpečovací zařízení plnit svůj účel, je nezbytné, aby se informace o poplachu, vyjmutí objektu z ochrany či technické události, přenášely ze střeženého místa do místa, odkud lze zajistit zásah (PCO Policie ČR, městské policie nebo soukromé bezpečnostní agentury).

Přenosové prostředky zajišťují propojení jednotlivých zařízení zabezpečovacího systému a místem, kde je možné bezpečnostní informaci přijmout a odpovídajícím způsobem na ni reagovat.

Tyto přenosové prostředky bývají stále častěji konstrukčně integrovány do zabezpečovacích ústředěn v chráněném objektu a počítačově vyhodnocovány PCO v místě stálé služby, odkud se organizuje zákrok.

***Rozdělení na základní skupiny :***

- *přímá (pevná ) linka,*
- *linka jednotné telekomunikační sítě,*
- *bezdrátový přenos.*

### **VI.2.1. Přenos přímou (pevnou) linkou**

Tento přenos je základní a nejstarší způsob přenosu poplachových informací po vlastním nebo pronajmutém pevném, dvou nebo čtyř vodičovém vedení. Ve většině případů se jedná o vedení sloužící výhradně pro poplachovou signalizaci, nebo vedení, na němž je část přenosové kapacity vyhrazena těmto informacím.

Tato trasa může být řešena několika způsoby :

- zabezpečovací smyčka stejnosměrná,
- zabezpečovací smyčka digitální s obousměrným přenosem.

Přenosové prostředky jsou pak součástí běžně používaných zabezpečovacích systémů. Nevýhodou tohoto přenosu, jsou vysoké náklady na zřízení či pronájem linky, a tak se s tímto způsobem setkáváme pouze v autonomních systémech. Další nevýhody jsou přímo spojené s nevýhodami pevných linek, nevyjímaje organizační a také časově náročné na zřízení těchto přímých linek.

### **VI.2.2. Přenos linkou jednotné telekomunikační sítě**

V současné době představuje tento způsob velmi kvalitní přenosovou cestu. Výhodou je obousměrný přenos informací a tuto linku lze využít i pro běžný telefonní provoz (přenos hovorů, internet, fax, e-mail, atd.). Další výhodou je, že nelze tak jednoduše rušit přenos poplachových zpráv, tak jak tomu je v případě použití rádiového přenosu. Aby byly porušeny tyto přenosy muselo by dojít ke vniknutí do střeženého objektu nebo do zařízení provozovatele telekomunikační sítě. Spojení mezi objektem a PCO je navazováno pouze v případě potřeby, tedy v případě poruch, telefonního rozhovoru a nebo při vyhlášení poplachu. Kontrola linky nebývá příliš častá - obvykle se volí interval 24 hodin, výjimečně kratší, vzhledem k tomu, že každý takovýto přenos je zpoplatněn stejně jako obyčejná telefonní hovor.

Předpokladem správného a bezchybného fungování tohoto přenosu je samozřejmě využití kvalitní techniky - automatický telefonní komunikátor musí být schopen uskutečnit uvolnění linky a zajistit tak, že v případě poplachu dokáže poplachovou zprávu odeslat i při obsazení telefonní linky. V dnešní době moderních digitálních ústředí, jimiž je vybavena většina telekomunikačních sítí, není problém. Splnění tohoto požadavku je jedním ze základních podmínek pro bezpečnost přenosu a přenos poplachů.

Nevýhody : při použití tónové volby - přeslechy a poruchy na lince.

#### **VI.2.2.1. Přenos po síti ISDN**

Je to nejmodernější způsob přenosu poplachových zpráv. *ISDN* v překladu znamená integrovaná síť digitálních služeb. Umožňuje přenos hlasu, obrazu, dat, faxů, apod. Hlavní předností proti analogové telefonní síti je rychlost navázání spojení. Spojení z jakéhokoliv místa je do 2 sekund, přenosová rychlost informace je 64kb/s, vysoká spolehlivost a možnost trvalého dohledu nad spojením. Přenos veškerých informací probíhá u ISDN v digitální formě.

Využití linek ISDN pro přenos poplachových informací znamená významný kvalitativní skok v porovnání s analogovou formou přenosu. Od vzniku poplachu do jejího příjmu na PCO uplynou max. 4 sekundy bez ohledu nato, odkud a kam se volá. Poplachová zpráva je přenášena v digitální podobě s velmi vysokým stupněm zabezpečení. Soudobé technické prostředky umožňují přenášet po linkách ISDN také kvalitní digitální obrazový signál rychlostí až 25 snímků za sekundu. Tohoto se využívá především v případě, že je na objektu nainstalován kamerový systém a za pomoci tohoto zařízení je možno instruovat a přesně navádět zasahující hlídku k zadržení pachatelů jež vnikly do střeženého objektu. V kvalitní digitální telefonní síti s dobře provedenými rozvody lze získat možnost

spolehlivého plošného přenosu na PCO.

Jednotnou telekomunikační síť je možno pro zabezpečovací účely využít i jako:

- *přepínanou linku,*
- *přenos v nad hovorovém pásmu,*
- *počítačové sítě atd..*

#### **VI.2.2.1.1. Přepínaná linka**

V místě stálé obsluhy je dispečerské zařízení, které slouží jako informační jednotka a současně jako dálkové ovládání výkonového dílu, nainstalovaného na městské automatické telefonní ústředně. V pracovní době slouží jako běžná telefonní linka, po jeho přepnutí na konci pracovní doby se z něj stává klasická zabezpečovací smyčka.

#### **VI.2.2.1.2. Přenos v nad hovorovém pásmu**

Přenos v nad hovorovém pásmu umožňuje trvalý dohled nad spojením, je však realizovatelný pouze se souhlasem a za spolupráce provozovatele telefonní sítě. V tomto případě, je nutno počítat s relativně vysokými náklady a nutností spolupráce s provozovatelem sítě. Základní organizace systému je stejná jako u předchozí formy přenosu (přepínané linky). Zabezpečovací informace jsou však přenášeny nosnou frekvencí v nad hovorovém pásmu. Výhodou je, že objekt takto napojený může být střežen i v pracovní době. Jednoduché PCO tohoto typu jsou využívány Policií ČR, ale i městskou policií Policie ČR však používá i složitější systémy. Koncové zařízení v tomto případě obsahuje řídicí počítač.

#### **VI.2.2.1.3. Počítačové sítě**

Jedná se o moderní způsob přenosu informací (o přenos dat, obrazů z kamer či fotografií nebo poplachových událostí), který se velice rychle rozšířil a umožňuje spojení po celém světě (v závislosti na propojení příslušné sítě) tzv. globální spojení.

Základní rozdělení počítačových sítí:

- *veřejné* - např., Internet,
- *neveřejné* - intranet - např. LAN, sítě v rámci organizace (policejní intranet či v bankách, pojišťovny atd.),
- *kombinované* - využití obou typů - např. propojení lokální sítě jedné organizace přes síť Internet s lokální sítí organizace jiné.

Podle způsobu propojení těchto sítí:

- *Klasická telefonní linka*- pracuje tak převážná většina připojení na internetových sítích v České republice,

- *síť ISDN* - jde o digitální síť integrovaných služeb, která se v poslední době velmi rozšiřuje. Tato síť je určena mimo jiné pro vysokorychlostní přenos dat a obrazových informací a rychlou komunikaci faxu,

- *síť GSM* - v souvislosti s prudkým vývojem technologií došlo i k možnosti propojení počítačových sítí jejich prostřednictvím,

- *rádiové sítě* - poslední dobou nabývá toto propojení počítačových sítí pomocí radiového přenosu, zejména pro potřeby řešení zabezpečovacích systémů (připojení PCO).

### **VI.2.3. Přenos bezdrátový**

Používá se v případech, kdy nelze využít metalického vedení (vedení přes kabely) Velkým přínosem jsou nejen pro využití pro přenos poplachových událostí, ale i pro aplikace jež vyžadují přenos širšího spektra informací pro mobilní zařízení.

Rozdělení tohoto přenosu :

- *přenos radiový,*
- *přenos optický.*

#### **VI.2.3.1. Přenos rádiový**

Jde o další možnost přenosu poplachových událostí na PCO. Jde o speciálně vybudované rádiové sítě jednorázové. Největší jejich rozvoj byl v roce 1992 na povolených kmitočtech 300-345 MHz. Se vstupem České republiky do řad NATO, bylo nutné, aby civilní uživatelé tyto frekvence opustili a bylo jim vyhrazena pásma 425-430 MHz a 459-470 MHz. Výhodou radiového přenosu je jeho nezávislost na jednotné telefonní síti nebo nákladných telefonních linkách. Další výhodou je, že celé zařízení je vlastnictvím provozovatele. Nevýhodou tohoto zařízení spočívá v jeho poměrně vysoké pořizovací ceně, za další tyto sítě jsou budovány jako jednosměrné. Další stinnou stránkou je, že lze takovýto přenos relativně snadno rušit a to není ani za potřebí vstupu do takto zabezpečeného objektu. Případnému pachateli postačí pouze umístit do blízkosti přijímací antény širokopásmový rozmítaný vysílač s dostatečným výkonem a dochází k výpadku příjmu.

### **VI.2.3.2. Přenos optický**

V případě, že je zapotřebí zabezpečit některé výrobní haly s velkým výskytem širokopásmových rušivých signálů (např. elektrárenské stanice apod.) se využívá infračervené přenosové trasy. Tento přenos se využívá opravdu jen ojediněle. Výhodou je dobrá odolnost proti rušení. Nevýhody - požadavek na přímou viditelnost, možnost náhodného přerušení infra paprsků okolními objekty např. manipulací ramenem jeřábu.

### **VI.3. PCO v podmínkách Policie ČR**

V zásadě lze rozdělit přijímané události na PCO do dvou kategorií, které jsou dle svého charakteru a přijímaných dat i různě akusticky i opticky hlášeny. Méně závažné události, kterým je přesto nutno věnovat zvýšenou pozornost, se zobrazují modrou barvou a zvukovým signálem, který není tak výrazný, přes to však nepřeslechnutelný. Jedná se zejména o ztrátu spojení, výpadek elektrického proudu či závadu na bateriích, které jsou nedílnou součástí zabezpečovacího systému.

Jsou-li však předaná data z předmětného objektu vyhodnocena jako poplachová událost, je na monitoru tato událost provedena v červené barvě a akustický signál je velice ostrý a pronikavý. Tato situace nastane vždy, když dojde k fyzickému napadení objektu. Dle rozmístění poplachových čidel je pak možno určit jaká část střeženého objektu byla napadena i možný pohyb případného pachatele po objektu. Tedy nejprve narušení pláště (okna, dveře), po té pohyb osoby střeženým prostorem (chodby, kanceláře, aj.) a konečně prostory nejvyšší důležitosti (trezor, vzácný obraz aj.). Tímto způsobem je tedy možno sledovat pohyb nežádoucí osoby (možného pachatele) střeženým objektem a přesně instruovat zasahující policisty. Celý tento systém má ještě jednu výhodu. Provádějí-li určení pracovníci jakoukoliv činnost na tomto zařízení, je tato činnost monitorována jako poplachová událost a jsou-li tyto pracovníci v telefonickém spojení s operátorem na PCO, mohou se sami přesvědčit o včasnosti příjmu zprávy na PCO a její úplnosti. Služba na PCO je zajištěna po 24 hodin denně, čímž je zajištěna nepřetržitá kontrola střežených objektů.



Nyní přejdeme k podrobnějšímu popisu programu a jeho činnosti, později pak k popisu praktických ukázek. Z pochopitelných důvodů zde nelze uvádět do detailu popisy jednotlivých objektů a dalších skutečností, které musí být z taktického hlediska utajené.

Program SensorEd, je speciálně vytvořen pro tvorbu objektů, které jsou využívány programem KLIENT s nímž obsluha PCO pracuje.

Dříve než vůbec dojde k ukládání data do tohoto programu, je zapotřebí mít projekt připravený. Ten není ničím jiným než souborem - souhrnem fotodokumentace, plánek objektů, půdorysů budov či jiných objektů jež jsou předmětem pro připojení na PCO, různých náčrtků v nichž je naznačeno (zakresleno) kde v jakém místě jsou jaká čidla zabezpečovacího systému použitých na tomto objektu. Nelze opomenout, že v první řadě je již EZS připojena a chybí pouze její připojení na PCO. Je lhostejné zda se jedná o přenos dat formou přímou (pevnou) telefonní linkou, či použitím počítačové sítě nebo případně radiovým přenosem.

Zabývejme se tímto problémem v době, kdy se tento souhrn je již hotov, připraven a vše s tímto související již máme připravené. Díky programu SensorEd můžeme do nakreslených a naskenovaných či do digitálních fotografií vkládat různé druhy čidel elektronického zabezpečovacího systému, tak aby s nimi mohl program KLIENT pracovat. Tato čidla jsou součástí programu SensorEd a umožňují nám zobrazení plánu přesně tak jak tomu je ve skutečnosti a umožňuje lepší vedení zásahu policejní hlídkou v případě vyhlášení poplachové události. Program SensorEd pracuje se vstupními programy ve formátu \*.gif nebo \*.jpg. Pro lepší barevné rozlišení a zachování barev je optimálnější soubory s koncovkou \*.gif. Toto je velice vhodné je-li zapotřebí pro zachování detailů jež jsou důležité pro obsluhu PCO neboť tyto detaily mohou přispět k včasnému a přesnému zásahu v případě vykazování poplachové události - narušení objektu. (detail: například různá zákoutí v nichž by se případní pachatelé mohli ukrýt a posléze nepozorovaně opustit objekt.). Grafické editory nám umožňují upravovat obrázky (fotografie, půdorysy) dle svých představ tak aby to nejvíce vyhovovalo pro obsluhu jak PCO, tak i taktice zásahu na objektu. Projekt všechny tyto vstupní soubory sdružuje do jednoho „celku“, tedy souboru obrázků které budou přiloženy a budou se zobrazovat u jednoho konkrétního objektu. V tomto „balíku“ jsou přiřazeny jednotlivá čidla, tato jsou součástí programu a programátor či pověřený pracovník pro vkládání a programování jednotlivých objektů, je nainstaluje do jednotlivých obrázků.

Pro každý objekt je vhodné zařadit několik obrázků hlídaného objektu (z několika různých pohledů - pohled čelní, boční, ze zadu). Výhodné je použít snímek přístupové cesty což může být použito jako část mapy okolí objektu se zvýrazněním místa hlídaného objektu, nejlépe označeno šipkou barevné kombinace, aby vynikla na dotyčném obrázku.

Jedná-li se o objekt vícepatrový, je samozřejmostí, že v souboru fotodokumentace jsou půdorysové plánky vnitřního prostoru jednotlivých pater nebo částí objektu. Doporučená velikost souboru je 60 kB (v \* jpg). Jsou ve velice dobré kvalitě (cca 600x550bodů), při zobrazení v měřítku 1:1, který pokryje téměř celou plochu obrazovky monitoru.

### **VI.3.1. Praktická činnost**

Po přihlášení operátora do PC se objeví na monitoru ikona znázorňující program PCO Klient verze 4.1.1. jež používá Policie ČR.

Po otevření ikony a načtení programu se na monitoru PC objeví okno v němž je přehled napojených objektů, z nichž každý z nich má svůj kód (název objektu). Vedle názvu se zobrazuje ikonka jež informuje obsluhu o tom zda je daný objekt zakódovaný, tedy vzat pod ochranu. V daném okně lze na liště nastavit zda se na obrazovce bude zobrazovat jeden či, dva, tři sloupce objektů. V případě, že jde o ztrátu spojení anebo dojde-li k přerušení komunikace mimo jiné (technické události), objekt se zbarví do fialové barvy .

Oběžník zaznamenává veškerou komunikaci mezi jednotlivými objekty a PCO do souboru historie. Jedná-li se o běžnou komunikaci mezi PCO a objektem , zaznamená se událost do historie sama , aniž by o tom nějak informovala obsluhu. To i v případě správného a včasného zakódování či od kódování objektu, do kterého vstupuje oprávněná osoba se svým osobním kódem. To že někdo v určité době vstoupil do objektu, případně jej opustil, je zaznamenáno v historii (např. navázána komunikace subjektem - FA, EZS; vzato pod ochrnu - uživatel 4, vyjmuta z ochrany, atd.).

U jakékoliv události zaznamenané v historii je kód objektu, přesný čas datum, kód události a o jakou událost jde. Toto je velice výhodné je-li potřeba zpětně přesně zjistit co vykazoval daný objekt a jaká a kdy byla poslední komunikace EZS s PCO.

Ohlásí-li firma která prováděla zapojení EZS na daném objektu (tedy její pracovník), že je na tomto objektu a bude vstupovat do zabezpečovacího systému, obsluha pomocí kliknutí myši na lištu pod heslem Objekt, posléze Porucha a vybráním si objekt do poruchy a zadáním patřičného kódu, jež má daná objekt, vloží do poruchy, to znamená, že veškerá

komunikace s daným objektem, veškerý zásah prováděný revizním technikem v EZS se zaznamenává do záložní paměti do níž mají přístup pouze programátoři PCO, v našem případě jsou to pověřeni pracovníci služby kriminální policie a vyšetřování, kteří mají oprávnění pro vstup a údržbu PCO a jeho programování, vkládání a odstraňování jednotlivých objektů, které jsou připojeny k PCO u Policie ČR. Jedná-li se o zájmové objekty policie, např. rodinné domy (do nichž byli opakovaně prováděno vloupání, či novostavby, určité restaurace,) na strategických místech které by mohly být předmětem napadení a provedení vloupání. Tito pracovníci vyjíždějí na tyto zájmové objekty a zajišťují připojení a zkušební provoz objektu na PCO. Občané, majitelé objektů jenž chtějí být připojeni na policejní PCO v daném okresním či městském ředitelství neboť zde jsou PCO umístovány, musejí počítat s počáteční investicí větší a nelze, aby si tito majitelé nainstalovali jakákoliv elektronická zabezpečovací zařízení. Než vůbec se rozhodnou pro zřízení EZS a posléze i připojení na PCO u Policie ČR, musejí mít připravené veškeré podklady a také se musejí písemnou formou dohodnout s příslušným okresním ředitelstvím.



Obr. Č. 8 : Pult centralizované ochrany

### VI.3.2. Taktika zásahu

V případě, že PCO vyhodnotí příchozí události jako poplachové, narušení objektu, obsluha PCO otevře pomocí „myši“ poplachové okno s poplachovou událostí. Otevře se další okno, zruší se akustická signalizace oznamující tuto událost, otevře se další okno v němž obsluha má možnost si přečíst o jaký objekt se jedná a nejen kód, ale i je zde zobrazeno v prvopočátku. Na pravé straně tohoto okna přicházejí upřesnění poplachových událostí, např. v prvopočátku přijde, že poplach - v objektu, může i po několika vteřinách přijít upřesnění odkud, nebo přichází přímo s poplachem počátečním (např. poplach v objektu, další řádek poplach okno 1.patro - dvůr).

Okamžitě obsluha vysílá radiostanicí policejní hlídku na místo. K plnění těchto úkolů je určena zasahující hlídka (či hlídky), která je speciálně školená, má u sebe směrnice (soubor plánek) ke každému objektu pod stejným kódovým označením jako je v PC. Obsluha PCO této hlídce sděluje, o jaký objekt se jedná, kód objektu, místo - adresu a jaké poplachové události byly hlášeny. V případě, že poplachové události přicházejí ve větším množství vysílá další hlídku pro zadržení případných pachatelů v objektu.

Do doby příjezdu hlídky na místo, obsluha má v dnešní době a této verzi programu klient, možnost otevřít si balík s fotodokumentací, tato je jako přílohou a součástí u daného objektu a je-li zde vloženo do plánek rozložení jednotlivých čidel, které obsluze ukazují postupnou aktivaci čidel a tím i pohyb pachatelů po objektu navádět zasahující hlídky co možná neefektivněji. Součástí pod okna ke každému objektu je několik listů. Na jednotlivých listech s názvem Instrukce, má obsluha PCO instrukce zda a od čeho ode všude má hlídka klíče k objektu, (např. od vrat, či od vstupních dveří), dále pak koho vyrozumět či komu předat objekt při poruše (časté vykazování planých poplachů) zda vložit objekt po domluvě s obsluhou do poruchy. Na dalším listě je popsána přístupová trasa, neboť se může stát, že hlídka k tomuto určená se může v rámci silničního provozu někde zdržet. Pro ostatní zasahující hlídky o jaký typ budovy se jedná či její nějaká zvláštnost, např. domovní dveře.

V následující list je-li potřeba je zde zaznamenáno případná taktika policistů v napadeném objektu. Tyto listy mohou, ale nemusejí být vyplněny, ale na dalším listě je seznam osob majících klíče a přístup do objektu. V některých případech jsou zde uvedeny i adresy těchto kontaktních osob, někdy pouze telefonické spojení. To v případě, že je objekt narušen pachatelem či vykazuje-li opakované plané poplachové události a není uvedeno i instrukcích jinak např., vyrozumět BS (dále jen bezpečnostní služba) - ústředí většinou v Praze o převzetí jejich pracovníků a vložení patřičného objektu na PCO do poruchových událostí.

Nelze zapomenout na důležitou věc a to, že každý objekt je popsán určitým typem,

zda jde o soukromý objekt, nebo zda o objekt státní správy, dále pak je samozřejmostí adresa objektu, kde se nachází - poštovní adresa, telefonní spojení na objekt, např. : ředitel, kancelář, případně na vrátného je-li v pracovní době na objektu přítomen. Na další stránce je uvedena zodpovědná osoba se jménem, adresou a telefonickým spojení.

#### **VI.4. Planý poplach**

Planým poplach je každá signalizace, vyvolaná jakoukoliv příčinou kromě objektivní příčiny. To znamená , že většina je způsobena zaměstnanci, majiteli zabezpečeného objektu - budovy či místností (je-li např. firma mající zabezpečovací systém v pronájmu v budově kde sídlí více firem). Plané poplachy jsou způsobovány především nedbalostí, nepozorností, nesprávným kódováním při vstupech či odchodech ze zabezpečeného objektu. Dále mohou být způsobeny špatným zavřením a zajištěním dveří, oken, nebo může jít o technické plané poplachy , ty jsou způsobené signalizací. Jsou způsobovány převážně čidly a to díky jejich špatnému nastavení (nesouladu čidel s vlastnostmi okolního prostředí). Plané poplachy mohou být také způsobovány elektromagnetickým rušením, vyloučili se bouřkové období, je to ve většině případů způsobeno blízkostí radiových vysílačů.

## VII. Statistika způsobených poplachových událostí

Tato statistika se skládá z několika vybraných objektů jež jsou připojeny na PCO Policie ČR. Z taktických důvodů nebude uveden přesný název, adresa ani bližší popis objektu, uveden bude pouze druh jako např. Restaurace „A“, banka „F“, apod. Tento statistický přehled je utvořen pro přiblížení četnosti poplachových událostí a tím i výjezdů policejních hlídek ať už se jedná o plané, technické či tísňové poplachové události. Ve statistice budou uvedeny jen vybrané měsíce, neboť v období jarních, letních, podzimních a nebo zimních měsících je počet v každém jednotlivém období, lišící se jen několika málo poplachovými událostmi.

### VII.1. Statistika poplachových událostí

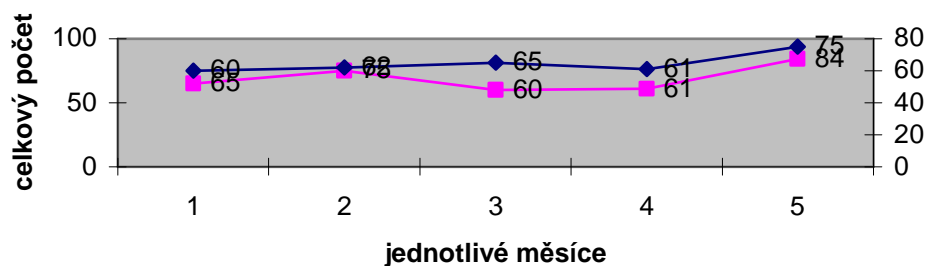
**Tabulka A : Počet poplachových událostí v jednotlivých měsících v roce 2005**

název objektu	březen 2005	duben 2005	květen 2005	Červen 2005	červenec 2005
Restaurace „A“	5	3	4	2	3
Motorest 1	2	4	2	5	2
Rodinný dům „Zavadila“	4	3	4	1	1
Kostel „A“	2	3	1	0	1
Kostel „B“	0	1	2	0	3
Novostavba	1	0	0	2	2
Budova Policie ČR	2	1	3	0	2
Rekreační chata	1	4	0	0	1
Banka „K“	10	8	10	9	4
Banka „R“	6	9	7	10	2
Zdravotní pojišťovna	3	4	5	6	5
Pošta „O“	5	4	7	4	8
Pošta „Q“	6	5	4	3	5
Budova státní správy	2	1	2	3	9
Soukromá firma	0	2	1	0	3
Zlatnictví	1	0	0	1	2
Muzeum	2	2	2	3	5
Hrady a zámky	5	1	7	4	6
Benzínová čerpací stanice	2	8	3	6	9
Základní škola	1	0	1	2	2
<b>Celkový počet</b>	<b>60</b>	<b>62</b>	<b>65</b>	<b>61</b>	<b>75</b>

**Tabulka B : Počet poplachových událostí v jednotlivých měsících v roce 2005**

<b>název objektu</b>	<b>srpen 2005</b>	<b>září 2005</b>	<b>říjen 2005</b>	<b>listopad 2005</b>	<b>prosinec 2005</b>
Restaurace „A“	4	3	5	2	3
Motorest 1	2	2	2	5	2
Rodinný dům „Zavadila“	4	1	4	1	1
Kostel „A“	1	1	2	0	4
Kostel „B“	2	3	0	0	3
Novostavba	0	2	1	2	2
Budova Policie ČR	3	2	2	0	0
Rekreační chata	0	1	1	0	1
Banka „K“	10	4	10	9	5
Banka „R“	7	2	6	10	4
Zdravotní pojišťovna	5	5	3	6	5
Pošta „O“	7	8	5	4	8
Pošta „Q“	4	5	6	3	11
Budova státní správy	2	9	2	3	8
Soukromá firma	1	3	0	0	3
Zlatnictví	0	2	1	1	2
Muzeum	2	5	2	3	5
Hrady a zámky	7	6	5	4	7
Benzínová čerpací stanice	3	9	2	6	8
Základní škola	1	2	1	2	2
<b>Celkový počet</b>	<b>65</b>	<b>75</b>	<b>60</b>	<b>61</b>	<b>84</b>

**Graf č. 1 Porovnání tabulky  
A a B poplachové události**



Legenda : 1 - měsíc *březen, srpen* 2005    4 – měsíc *červen, listopad* 2005  
 2- měsíc *duben, září* 2005    5 – měsíc *květen, prosinec* 2005  
 3 - měsíc *květen, říjen* 2005

\*Do ostatních poplachových událostí je zahrnuto např. porucha čidla na objektu, projetí přetíženého vozidla, přeběhnutí kočky či jiného zvířete.

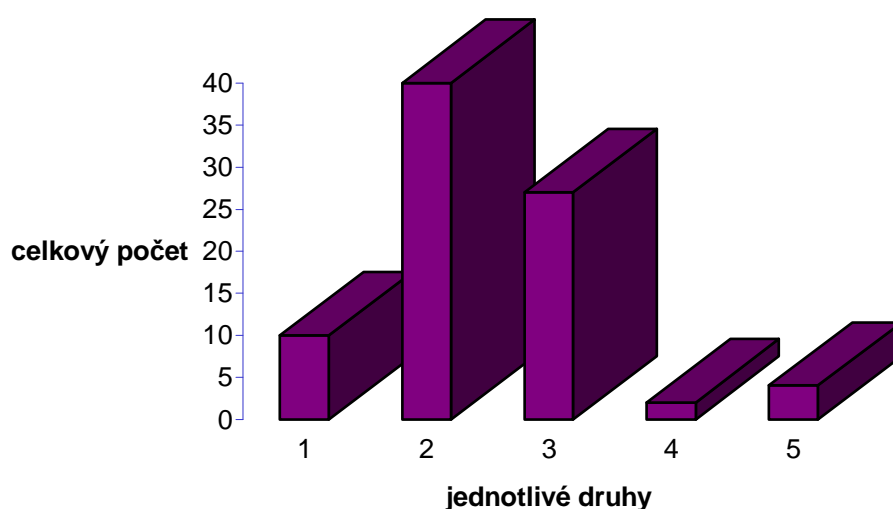
**Hodnoty v této tabulce jsou hodnoty z tabulky B, měsíc prosinec 2005**

název objektu	technické poplachy	revize-zkušební	plané poplachy-zaměstnanci	ostré poplachové události - přepadení	ostatní *
Restaurace „A“	0	1	1	0	0
Motorest 1	0	0	2	0	0
Rodinný dům „Zavadila“	0	1	0	0	0
Kostel „A“	1	2	0	1	0
Kostel „B“	0	1	1	0	1
Novostavba	1	1	0	0	0
Budova Policie ČR	0	0	0	0	0
Rekreační chata	0	1	0	0	0
Banka „K“	1	2	2	0	0
Banka „R“	0	1	3	0	0
Zdravotní pojišťovna	2	3	0	0	0
Pošta „O“	0	3	4	1	0
Pošta „Q“	0	8	3	0	0
Budova státní správy	1	5	1	0	1
Soukromá firma	0	2	1	0	0
Zlatnictví	0	2	0	0	0
Muzeum	2	1	2	0	0
Hrady a zámky	2	2	1	0	2
Benzínová čerpací stanice	0	3	5	0	0
Základní škola	0	1	1	0	0
<b>Celkový počet</b>	<b>10</b>	<b>40</b>	<b>27</b>	<b>2</b>	<b>4</b>



V případě tísňového poplachu, jenž byl vyhodnocen jako „ostrý“ a byl spuštěn na objektu Kostel „A“, se jednalo o bezdomovce jenž obtěžoval kostelníci, která použila tísňové tlačítko. Zasahující hlídka ověřila totožnost muže a jelikož zjistila, že se jedná o osobu po níž bylo vyhlášeno pátrání byl posléze zadržen a nejprve převezen na záchytnou stanici (neboť by v podnapilém stavu), po vystřízlivění byl předán vyšetřujícímu soudci a umístěn do vězeňského zařízení. Důvod pro něhož bylo vyhlášeno pátrání byl, že se nedostavil a vyhýbal se výkonu trestu pro opakované krádeže dle § Tr. zákona a výtržnictví dle § Tr. zákona. V druhém případě, kdy šlo o použití tísňového tlačítka a k vyvolání tísňového poplachu, jenž byl posléze vyhodnocen jako oprávněný, se jednalo o přepadení pracovnice Pošty „O“ neznámým pachatelem s použitím nože. Šlo tedy o loupežné přepadení dle § Tr. zákona .

**Graf č.2 Porovnání poplachových událostí**



Legenda : 1 -Technické poplachy                      3- Plané poplachy - způsobené zaměstnanci  
 2- Revize- zkušební poplach                  4- Tísňové poplachy - ostré  
 5- ostatní poplachové událost

U objektu Muzeum se jednalo o pohyb kočky v prostorách půdy, v případě a Kostel „O“ se jednalo o přítomnost netopýrů (v kopuli, v zákristii) a v objektu Hrady a zámky taktéž šlo o přítomnost a pohyb netopýrů jež se usídlili půdní prostor hradní věže.

## **Závěr :**

Zpracování tématu bakalářské práce mi dalo možnost hlubšího seznámení se s danou problematikou a také s metodami zpracování práce tohoto typu.

Samotná práce může být chápána též jako snaha o zvýraznění důležitosti prevence kriminality a to na podtextu technologických zařízení, která jsou v současné době vyvíjena a stále ve větší míře instalována a využívána nejen právníckými osobami, ale též osobami fyzickými.

Jak vyplývá z úvodních částí bakalářské práce, není to téma blízké lidstvu jen v posledních desetiletích či staletích. A tak závěrem nezbývá, než obrátit pozornost od důmyslných technologických zařízení k samotnému člověku. Vždyť se jedná o prostředky primárně chránící člověka, případně jeho majetek před protiprávní činností další lidské osoby. A tak by tato práce též mohla vést k zamyšlení nad etikou lidského chování a jednání, k zamyšlení nad přístupem k základním lidským právům, právu na život a jeho důstojné podmínky a také na právu na soukromé vlastnictví a jeho ochranu.

**Přílohy :**

Tabulka č. 1

**Základní způsobilost vstupů**

<b>Objednavatel</b>	Ověřit si, že je skutečně oprávněn disponovat objektem a zadávat podobné dílo
<b>Dodavatel</b>	Musí mít registrovanou živnost na Instalaci elektronických zařízení, doplněnou o koncesní listinu.
	Musí být prokazatelně proškolen výrobcem či distributorem zařízení
<b>Zařízení</b>	Prohlášení o shodě, certifikáty, zkušební protokoly
<b>Kompetentní účastník</b>	Oprávnění k provozování služby, kterou do procesu vstupuje
<b>Dokumentace a data</b>	S dokumentací a daty k EZS musí být nakládáno jako s předmětem obchodního tajemství.
<b>Etika</b>	Dodavatel techniky by měl při procesu zřizování jednat eticky. To znamená účtovat přiměřené ceny za výkon, dbát na vysokou profesní úroveň dodávky a na seriózní vystupování vůči objednateli. Nesmí nikde sdělovat žádné informace o objednavateli, které zjistil během procesu zřizování. Výjimku tvoří pouze situace, kdy by zjistil, že se objednatel jedná protiprávně anebo páchá společensky nebezpečnou či kriminální činnost.

Tabulka č. 2.

**Nové označení dle ČSN EN 50131-1**

<b>Stupeň zabezpečení</b>	<b>Název stupně zabezpečení</b>
<b>1</b>	nízké riziko
<b>2</b>	nízké až střední riziko
<b>3</b>	střední až vysoké riziko
<b>4</b>	vysoké riziko

Tabulka č. 3.

**Rozdělení prostředí dle ČSN EN 50131-1**

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

Tabulka č. 4

**Seznam vybraných norem pro poplachové systémy (platnost k březnu 2003)**

<b>Název zjednodušeně</b>	
<b>VŠEOBECNĚ</b>	
ČSN EN 50130-4	Elektromagnetická kompatibilita - Požadavky na odolnost komponentů požárních a poplachových systémů
ČSN EN 50130-5	Metody zkoušek vlivu prostředí
<b>ELEKTRONICKÉ ZABEZPEČOVACÍ SYSTÉMY (EVS)</b>	
ČSN EN 50131-1	Všeobecné požadavky
ČSN EN 50131-1/Z1	Všeobecné požadavky ZMĚNA Z1
ČSN EN 50131-6	Napájecí zdroje
<b>SYSTÉMY PŘENOSOVÉ</b>	
ČSN EN 50136-1-1	Všeobecné požadavky pro poplachové přenosové systémy
ČSN EN 50136-1-2	Požadavky na systémy s rozhlasovými komunikátory využívající veřejnou komutovanou telefonní síť
ČSN EN 50136-2-1	Všeobecné požadavky pro poplachová přenosová zařízení
ČSN EN 50136-2-2	Požadavky na zařízení v systémech využívajících výhradně poplachové přenosové cesty
ČSN EN 50136-2-3	Požadavky na zařízení v systémech s digitálními komunikátory využívající veřejnou komutovanou telefonní síť
ČSN EN 50136-2-4	Požadavky na zařízení v systémech s hlasovými komunikátory využívající veřejnou komutovanou telefonní síť
<b>SYSTÉMY CCTV</b>	
ČSN EN 50132-2-1	Černobílé kamery
ČSN EN 50132-7	Pokyny pro aplikace
<b>SYSTÉMY KONTROLY VSTUPŮ</b>	
ČSN EN 50133-1	Systémové požadavky
ČSN EN 50133-7	Pokyny pro aplikace
<b>SYSTÉMY PŘIVOLÁNÍ POMOCI</b>	
ČSN EN 50134-1	Systémové požadavky
ČSN EN 50134-2	Aktivační zařízení
ČSN EN 50134-3	Místní jednotka a kontrolér
ČSN EN 50134-7	Pokyny pro aplikace

Tabulka č. 5

**Část seznamu s uvedením doporučeného stupně zabezpečení a pojistné třídy\*\***

	ČSN EN 501131-1	
<b>A</b>		
Advokát, notář		A
Antikvariát - obchod bez klenotnického zboží	2	
Ateliér umělecký	1-2	B
Aukční výstava	4	
Autobazar		B-C
Autogaráže (bez čerpání PH a bez oprav)		A
Automobilové kino		B
Autobazar		B-C
Autoškola	1-2	B
<b>B</b>		
Baletní škola		A
Banka	3-4	E
Bankovní úschovna	3-4	E
Bar	2	
Bednářství	1	
Benzinová čerpací stanice	3	C-D
Betonárna/štěrkovna	1-2	A
Bistro		B
Botanická/zoologická zahrada	1	O
Brusírna drahých kamenů	3-4	F
Butik s klenotnickým zbožím	3	C
<b>C-Č</b>		
Cestovní kancelář	1	B
Cukrárna	1	B
Čerpací stanice vody	3-4	A
Čistírna odpadní vody	1	A
Čistírna peří	1	A
<b>D</b>	1	
Dálková výtopy	1	
Dětský domov	1-2	
Diskotéka	1.II	
Divadlo	1-3	A
Domácnosti včetně rodinných domů		
Drogerie/parfumerie/kosmetický salón		B-C
Drůbeží farma	1	
Dům nábytku	1-2	
Dům s ošetrovatelskou službou		B
<b>E</b>		
Elektrárna oblastní	2-4	B-C
Elektrárna strategická	2-4	E
Elektrotechnická dílna	1	B

Expreso	1	
Pokračování tabulky č. 5		
<b>F</b>		
Farma kožešinové zvěře	2	
Farmaceutické/lékařské zboží	3	C
Filmové /nahrávací studio s video	2-3	
Finanční úřad	3	
Fitcentrum	1	B
Fotoateliér	1.II	B-C
Fotoateliér	1-2	B-C
Fyzikální laboratoř	2-4	
<b>G</b>		
Galerie	2-4	O
Galvanizovna	1	
Garáž ) bez čerpání PH a bez oprav)		O
Grafický závod/tiskárna		B
<b>H</b>		
Hasiči		A
Herna		C-D
Hotel/penzion	1-3	B
Hrací sál	2	
Hrad/zámek	2-4	O
Hrnčířství	1	
<b>CH</b>		
Chemická laboratoř	2-3	
Chladírna	1	
<b>I</b>		
Internát	1	
<b>J</b>		
Jatka	1	
Jezdecká škola/stáj/ jízdárna	1	O
Jídelna	1	B
<b>K</b>		
Kancelář /úřad	1-3	
Kaple	2-3	
Klášter	1-3	O
Knihovna s archivními fondy	2-3	
Kostel	1-3	O
Koncertní síň	1.II	A
Koželužství	1	
<b>L</b>		
Lanová dráha	2	
Lékárna	2-3	C
Lékařská praxe/ laboratoř	2	
Lisovna	1	
<b>O</b>		





















































Obchod s automobily včetně příslušenství	2	C-E
Pokračování tabulky č. 5		
Obchod s ceninami	2	
Pokračování tabulka č.5		
Obchod s elektrickým zbožím bez zab. elekt.	2	B
Obchod s elektrickým zbožím se zab. elekt.		C-D
Obchod s chemikáliemi	2	
Obchod s obrazy/uměleckými předměty	1-2	O
Obchod s počítači		C-D
Obchod se sklem		B
Obchod se zbraněmi	3-4	D-E
Obytné budovy	1	
<b>P</b>		
Peněžní ústav	3-4	E
Pivovar	1	
Pošta	2-3	
Pohřební ústav	2	A
Přístaviště		O
Půjčovna filmů/videotéka	1	C
<b>R</b>		
Radiový vysílač	2	
Radnice/ obecní správa	2	B
Restaurátor		
<b>S-Š</b>		
Sanatorium	1	
Sbírka umění		
Starožitnictví včetně klenotnického zboží		O
<b>T</b>		
Tapiserie	1	
Tiskárna cenných papírů		
<b>U</b>		
Umělecký atelier	1	C
<b>Z-Ž</b>		
Zahradnictví	1	
Železářství		A

**\*\*Přesný a úplný seznam objektů obsahuje Oborová norma AGA 50131-1 až 7**



Tabulka č. 6 :

Projekční Schématické značky EZS \*

	MG magnetické čidlo otevření		MW mikrovlnné čidlo		EXP expander, link. modul, koncentrátor
	MGT magnetické čidlo otevření odolné		PIR/MW dušňní čidlo		TAB tablo EZS
	DTS čidlo rozbití skla		PIR/MWS dušňní čidlo stropní		ATS přenosové zařízení – komunikátor
	DTS AM čidlo rozbití skla antimask		VIB otřesové čidlo		TR trafo TR 220/16 V
	PI čidlo kontaktní PIEZO		MC čidlo poslední bankovky		Z modul zdroj PS
	PIR PIR vějíř		TH tlačítkový hlásič tlačítkový		AKU záložní akumulátor
	PIR V PIR vějíř venkovní		TL tlačítkový hlásič tláka		WLV bezdrátový vysílač
	PIR AM PIR vějíř antimasking		TC technologický hlásič		WLP bezdrátový přijímač
	PIR D PIR dlouhý dosah		GH hlásič úniku plynu		KS klíčový spínač
	PIR Z PIR záclona		PH hlásič požáru		ZE propouštěcí zámek
	PIR ZAM PIR záclona antimasking		SG signálizace optické		KL ovládač EZS
	PIR ID čidlo s vlastní adresou		SZ signálizace opt. a akus.		PCO poplachové přijímací centrum
	UZ ultrazvukové čidlo		SI výstražné zařízení siréna vnitřní s blikáčem		WM vstupně-výstupní modul
	PIR DV PIR záclona dveří		SS výstražné zařízení siréna vnitřní		REL releový modul
	PIR S PIR stropní čidlo		SE výstražné zařízení siréna vnější s blikáčem		
	PIR/DTSS PIR stropní komb. s DTS		SB výstražné zařízení siréna vnější bez blikáče		
	IZ IR infrazvuk		MJ výstražné zařízení mojžák		
	IZV IR infrazvuk - vysílač		EVS ústředna EZS		
	IZP IR infrazvuk - přijímač		PS napájecí zdroj		

**Názvosloví pro elektrické zabezpečovací systémy \*\*\***

<b>Pojmy</b>	<b>Vysvětlení pojmů</b>
<b>Adresa</b>	Kódové číslo identifikující prvek v adresném systému.
<b>Adresná sběrnice</b>	Vedení procházející střeženým objektem (obvykle dvou , tří nebo čtyřvodičové), na než se připojují jednotlivé adresné prvky.
<b>Akreditace</b>	Pověřený k výkonu určité činnosti, např. hodnocení vlastností prvků zabezpečovací techniky. Akreditace platí vždy pouze pro přesně vymezené činnosti a podle předem stanovených postupů.
<b>Bezdrátový systém</b>	Systém nepoužívající pro spojení mezi prvky systému metalické ani optické spojení. Zpravidla pracuje na principu přenosu rádiovými vlnami.
<b>Blokovací zámek</b>	Zámek určený k zapínání zabezpečovacího zařízení, mající elektromechanické blokování proti uzamčení, není-li zabezpečovací zařízení ve stavu umožňující zapnutí do stavu střežení.
<b>By-pass</b>	Anglický výraz pro překlenutí zabezpečovací smyčky (vyřazení ze střežení)
<b>Certifikace</b>	Postup, při němž oprávněný orgán ( certifikační místo) vydává potvrzení o tom, že určitý výrobek prvek( splňuje nároky, které certifikační orgán vyžaduje.).
<b>Čidlo</b>	Nepříliš šťastně zvolený termín pro prvek zabezpečovací techniky sloužící k detekci nějaké formy narušení nebo napadení. V angličtině i němčině se používá výraz "detector".
<b>Detektor pohybu</b>	Zařízení pro detekci pohybu, pracující zpravidla na principu mikrovlnném nebo ultrazvukovém.
<b>EZS</b>	Zkratka pro elektrický zabezpečovací systém (podle ČSN EN 50131-1 Poplachové systémy - Elektrické zabezpečovací systémy část 1.)
<b>Falešný poplach</b>	Poplach způsobený chybnou funkcí systému (kupříkladu následkem elektromagnetického rušení apod. ) nezaviněný obsluhou.
<b>ISDN</b>	Nejmodernější veřejná spojovací síť pracující na principu digitálního přenosu informace po běžném telefonním vedení. Tato síť umožňuje vytvoření virtuální pevné datové linky.
<b>Klid</b>	Stav, kdy je zabezpečovací systém EZS napájen, není však aktivní ( v angličtině "unset", v němčině " unschart").
<b>Kompatibilita</b>	Slučitelnost ( prvků a systémů ) je schopnost navzájem spolupracovat.
<b>Komunikátor</b>	Zařízení určené k přenosu poplachových zpráv z místa instalace EZS do místa příjmu poplachových zpráv, zpravidla na pult centralizované ochrany.
<b>Komutovaná linka</b>	Telefonní linka sítě, u níž je spojení mezi účastníky navazováno na základě volby jednoho z účastníků pouze na dobu hovoru nebo přenosu zprávy.
<b>Monitorování</b>	Dohled; tento výraz může být použit jak ve smyslu dohledu nad funkcí systému, tak ku příkladu sledování stavu střeženého objektu.
<b>Napájecí zdroj</b>	Část EZS, zajišťující napájení celého systému a všech jako

	komponentů.
Pokračování tabulky č. 7	
<b>Narušení</b>	Neoprávněný postup do zabezpečeného prostoru.
<b>Otřesový detektor</b>	Detektor reagující na otřes. Speciálním případem jsou tzv. trezorové detektory, u nichž se uskutečňuje analýza druhu otřesů s cílem zachytit pouze otřesy vyvolané pokusy o proniknutí do trezoru.
<b>PCO</b>	Pult centralizované ochrany- zařízení pro příjem poplachových zpráv ze zabezpečených objektů.
<b>PIR</b>	Zkratka používaná pro pasivní infračervený detektor pohybu -Passive Infra Red detector
<b>Planý poplach</b>	Poplach způsobený normální činností systému, ale nezpůsobený vloupáním či jiným narušením . Příčinou může být chyba obsluhy ( vstup do zabezpečeného prostoru před jeho vypnutím) nebo vnější vlivy(průvan, nedovřené okno apod.).
<b>Poplachový stav</b>	Stav, kdy je detektor (čidlo) aktivován. Je to stav EZS nebo jeho komponentů, který je výsledkem odezvy na přítomnost nebezpečí.
<b>Reset</b>	Nastavení zabezpečovacího systému do základního stavu( poplachu, po údržbě, revizi apod.)
<b>Sabotážní poplach</b>	Poplach způsobený narušením sabotážní ochrany ( např. otevření krytu prvků apod.)
<b>Stupeň zabezpečení</b>	Kategorizace rizikivosti chráněných objektů a zařízení podle normy ČSN EN 50131-1 stanový zabezpečení, od nejnižšího stupně 1 do nejvyššího stupně. Většina objektů patří do stupně 1 a 2, čtyři stupně, ve stupni 3 se předpokládají jen objekty typu bank, klenotnictví a objekty s přísně tajnými dokumenty a skutečnostmi podle kategorizace NBU.
<b>Tíseň</b>	Stav při násilném pokusu o vydání majetku, hotovosti nebo jiné hodnoty.
<b>Tísňový hlásič</b>	Mechanický prvek realizovaný ve formě tlačítka nebo tíšňového spínače, slouží k ohlášení poplachu při přepadení nebo jiném tíšňovém stavu.
<b>Tónová volba</b>	Způsob volby v telefonní síti, při němž jsou jednotlivé číslice rozlišeny kombinací různých kmitočtů.
<b>Ústředna</b>	Hlavní část elektronického zabezpečovacího zařízení. Hlavními znaky jsou způsob činnosti (analogová-smyčková nebo sběrníková-adresná), počet samostatně střežitelných prostorů, počet smyček, případně počet adresných bodů.
<b>Vloupání</b>	Neoprávněné vniknutí do uzavřeného prostoru.
<b>VdS</b>	Zkratka pro německou asociaci pojišťoven, tato organizace vydává předpisy pro zabezpečovací zařízení , má vlastní zkušebnu a certifikační místo. Předpisy VdS jsou uznávány jako nejlépe zpracované normy pro zabezpečení objektů.
<b>Zámkový kontakt</b>	( v němčině Riegelkontakt) Prvek umožňující kontrolu uzamčení oken nebo dveří. Montuje se proti závoře zámku. Výhodou je kontrola skutečného uzamčení naproti

magnetickému kontaktu, který je sepnut i při otevření okna či dveří.

Pokračování tabulky  
č.7

<b>Zóna</b>	Tento výraz se doporučuje nepoužívat, protože není jednoznačný - v některých případech jím je míněna zabezpečovací smyčka, jindy DURNFELDERE samostatně zapínatelný střežený prostor.
<b>Zrcadlová optika</b>	Optická část infrapasivního detektoru pohybu, využívající k soustředění paprsků k pyoelementu parabolickou optiku. Užívá se u kvalitnějších detektorů.

\*\*\* Úplné znění názvosloví, je uvedeno : Security Magazín, Ročník VII, Leden/únor 2000, str. 55-57

## **Poznámkový aparát**

- 1) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str. 5
- 2) srv. Časopis zabezpečení a kriminalita, 6. ročník , březen 1997, Ing. Ladislav Toms – Zabezpečení vstupů , prostor a objektů visacími zámky
- 3) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str. 6
- 4) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str. 6
- 5) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str. 7
- 6) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str. 9-10
- 7) §
- ) §
- 9) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str. 17
- 10) PCO – Pult centralizované ochrany viz. Zkratky
- 11) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str. 24
- 12) Magazín Security, Ročník XI, červenec/srpen 2004
- 13) Magazín Security, Ročník XI, červenec/srpen 2004
- 14) Reportáž na televizním programu Prima, pořad Extra
- 15) Vyhláška ÚOHS č. 202/2001 Sb.
- 16) Magazín Security, Ročník X, květen/červen 2003
- 17) Magazín Security, Ročník XI, červenec/srpen 2004
- 18) Magazín Security, Ročník XI, červenec/srpen 2004
- 19) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str.25
- 20) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str.26
- 21) MW- mikrowale – viz. Zkratky
- 22) Počítadlo pulsů – pulse count – viz. Zkratky
- 23) Systémy APSP – Auto pulse Signal Processing – viz. Zkratky
- 24) znění § ..
- 25) Personál Security Systém – viz. Zkratky
- 26) SNB – Sbor národní bezpečnosti – viz. Zkratky

## Seznam použité literatury

### Odborná literatura:

- Křeček, S.: Příručka zabezpečovací techniky. Cricetus, 2002.
- Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001
- Kindl, J.: Projektování bezpečnostních systémů. 2004
- Dip. Ing.Paták, J., prof. JUDr. Protivinský, M., JUDr. Klvaňa, K.: Zabezpečovací systémy
- Pütz,J. a kol.: Úvod do číslicové techniky. SNTL –Praha 1983.
- Hráčský, J., Anderle, H.: kurz elektronických obvodů pro průmyslovou elektroniku . SNTL Praha 1976
- Limann, O.; Pelka, H.: Elektronika bez balastu. Alfa, Bratislava.
- Syrovátko, M.: Zapojení s polovodičovými součástkami.
- Farský; Prokeš : Elektrické obvody I.
- Šícha, M., tichý, M.: Elektronické obvody II. SNP, Praha 1982.
- Gauner, K.: Základy elektroniky, skriptum. ZČU, Plzeň 2001.
- Frisch, M.: Základy elektroniky a elektronických obvodů. SNTL, Praha 1987.
- Klaus, T. a kol.: Příručka pro elektrotechnika. Europa-Sobotáles cz. Praha 2002

### Časopisy :

- Security magazín. Ročník VII, leden/únor 2000 s.55-57 - názvosloví
- Security magazín. Ročník IX,květen/červen 2003
- Security magazín. Ročník IX, červenec/srpen 2003
- Security magazín. Ročník X , červenec/srpen 2004
- Zabezpečení a kriminalita. Ročník VI, březen 1997
- Katalog produktů pro ochranu majetku a osob (10/2004)

### Internetové zdroje:

[www.fides.cz](http://www.fides.cz)

[www.zabezpečení.netlezs-house](http://www.zabezpečení.netlezs-house)

[www.ambo.cz/index.php?sec=redaction&red\\_id=8&title\\_string=nabídka%20publikací&lang=cz](http://www.ambo.cz/index.php?sec=redaction&red_id=8&title_string=nabídka%20publikací&lang=cz)

**další zdroje :**

trestní zákon a trestní řád ....

Věstník ministerstva vnitra ČR, ze dne 29.května 1997

Oborová norma AGA 50131-1 až 7

Česká technická norma: ČSN EN 50131-1/Z1.Praha: Český normalizační institut. 2000,  
str.84-85

### **Seznam zkratek :**

PCO – Pult centralizované ochrany

EZS – elektronická zabezpečovací signalizace

AGA – Asociace grémium alarm

ČAP - Česká asociace pojišťoven

EM – Elektromagnetické

AM – sousto-magnetické

RF - radiofrekvenční

EAS – Electronic Article Surveillance

ATV – Automatické telefonní vodiče

PSS - Personál Security Systém

SNB – Sbor národní bezpečnosti

VB – Veřejná Bezpečnost (nyní Policie)

MW- Microwave; mikrovlnná čidla

ISDN – Integrated Services Digital Network

APSP – Auto Pulse Signal Processing

GSM – Global Systém Mobile Communication

US – Ultrasonic – ultrazvuková

LED – Light Emission Diode



**Přílohy :**

Tabulka č. 1

**Základní způsobilost vstupů**

<b>Objednavatel</b>	Ověřit si, že je skutečně oprávněn disponovat objektem a zadávat podobné dílo
<b>Dodavatel</b>	Musí mít registrovanou živnost na Instalaci elektronických zařízení, doplněnou o koncesní listinu.
	Musí být prokazatelně proškolen výrobcem či distributorem zařízení
<b>Zařízení</b>	Prohlášení o shodě, certifikáty, zkušební protokoly
<b>Kompetentní účastník</b>	Oprávnění k provozování služby, kterou do procesu vstupuje
<b>Dokumentace a data</b>	S dokumentací a daty k EZS musí být nakládáno jako s předmětem obchodního tajemství.
<b>Etika</b>	Dodavatel techniky by měl při procesu zřizování jednat eticky. To znamená účtovat přiměřené ceny za výkon, dbát na vysokou profesní úroveň dodávky a na seriózní vystupování vůči objednateli. Nesmí nikde sdělovat žádné informace o objednavateli, které zjistil během procesu zřizování. Výjimku tvoří pouze situace, kdy by zjistil, že se objednatel jedná protiprávně anebo páchá společensky nebezpečnou či kriminální činnost.

Tabulka č. 2.

**Nové označení dle ČSN EN 50131-1**

<b>Stupeň zabezpečení</b>	<b>Název stupně zabezpečení</b>
<b>1</b>	nízké riziko
<b>2</b>	nízké až střední riziko
<b>3</b>	střední až vysoké riziko
<b>4</b>	vysoké riziko

Tabulka č. 3.

**Rozdělení prostředí dle ČSN EN 50131-1**

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





















































Tabulka č. 4

**Seznam vybraných norem pro poplachové systémy (platnost k březnu 2003)**

	<b>Název zjednodušeně</b>
<b>VŠEOBECNĚ</b>	
ČSN EN 50130-4	Elektromagnetická kompatibilita - Požadavky na odolnost komponentů požárních a poplachových systémů
ČSN EN 50130-5	Metody zkoušek vlivu prostředí
<b>ELEKTRONICKÉ ZABEZPEČOVACÍ SYSTÉMY (EZS)</b>	
ČSN EN 50131-1	Všeobecné požadavky
ČSN EN 50131-1/Z1	Všeobecné požadavky ZMĚNA Z1
ČSN EN 50131-6	Napájecí zdroje
<b>SYSTÉMY PŘENOSOVÉ</b>	
ČSN EN 50136-1-1	Všeobecné požadavky pro poplachové přenosové systémy
ČSN EN 50136-1-2	Požadavky na systémy s rozhlasovými komunikátory využívající veřejnou komutovanou telefonní síť
ČSN EN 50136-2-1	Všeobecné požadavky pro poplachová přenosová zařízení
ČSN EN 50136-2-2	Požadavky na zařízení v systémech využívajících výhradně poplachové přenosové cesty
ČSN EN 50136-2-3	Požadavky na zařízení v systémech s digitálními komunikátory využívající veřejnou komutovanou telefonní síť
ČSN EN 50136-2-4	Požadavky na zařízení v systémech s hlasovými komunikátory využívající veřejnou komutovanou telefonní síť
<b>SYSTÉMY CCTV</b>	
ČSN EN 50132-2-1	Černobílé kamery
ČSN EN 50132-7	Pokyny pro aplikace
<b>SYSTÉMY KONTROLY VSTUPŮ</b>	
ČSN EN 50133-1	Systémové požadavky
ČSN EN 50133-7	Pokyny pro aplikace
<b>SYSTÉMY PŘIVOLÁNÍ POMOCI</b>	
ČSN EN 50134-1	Systémové požadavky
ČSN EN 50134-2	Aktivační zařízení
ČSN EN 50134-3	Místní jednotka a kontrolér
ČSN EN 50134-7	Pokyny pro aplikace

Tabulka č. 6 :

Projekční Schématické značky EZS \*

	MG magnetické čidlo otevření		MW mikrovlnné čidlo		EXP expander, link. modul, koncentrátor
	MGT magnetické čidlo otevření odolné		PIR/MW duální čidlo		TAB tablo EZS
	DTS čidlo rozbití skla		PIR/MWS duální čidlo stropní		ATS přenosové zařízení - komunikátor
	DTS AM čidlo rozbití skla antimask		VIB otřesové čidlo		TR trafo TR 220/16 V
	PI čidlo kontaktní PIEZO		MC čidlo poslední bankovky		Z modul zdroj PS
	PIR PIR vějíř		TH tiskový hlásič tlačítkový		AKU záložní akumulátor
	PIR V PIR vějíř venkovní		TL tiskový hlásič tlak		WLV bezdrátový vysílač
	PIR AM PIR vějíř antimasking		TC technologický hlásič		WLP bezdrátový přijímač
	PIR D PIR dlouhý dosah		GH hlásič úniku plynu		KS klíčový spínač
	PIR Z PIR záclona		PH hlásič požáru		ZE propouštěcí zámek
	PIR ZAM PIR záclona antimasking		SG signalizace optická		KL ovladat. EZS
	PIR ID čidlo s vlastní adresou		SZ signalizace opt. a akus.		PCO poplachové přijímací centrum
	UZ ultrazvukové čidlo		SI výstražné zařízení siréna vnitřní s blikacem		WM vstupně-výstupní modul
	PIR DV PIR záclona dveřní		SS výstražné zařízení siréna vnitřní		REL reliéový modul
	PIR S PIR stropní čidlo		SE výstražné zařízení siréna vnější s blikacem		
	PIR/DTSS PIR stropní komb. s DTS		SB výstražné zařízení siréna vnější bez blikáče		
	IZ IR infračervená		MJ výstražné zařízení maják		
	IZV IR infračervená - vysílač		US ústředna EZS		
	IZP IR infračervená - přijímač		PS napájecí zdroj		

Tabulka č. 6

**Část seznamu s uvedením doporučeného stupně zabezpečení a pojistné třídy\*\***

\*\*Přesný a úplný seznam objektů obsahuje Oborová norma AGA 50131-1 až 7

	ČSN EN 501131-1	
<b>A</b>		
Advokát, notář		A
Antikvariát - obchod bez klenotnického zboží	2	
Ateliér umělecký	1-2	B
Aukční výstava	4	
Autobazar		B-C
Autogaráže (bez čerpání PH a bez oprav)		A
Automobilové kino		B
Autobazar		B-C
Autoškola	1-2	B
<b>B</b>		
Baletní škola		A
Banka	3-4	E
Bankovní úschovna	3-4	E
Bar	2	
Bednářství	1	
Benzinová čerpací stanice	3	C-D
Betonárna/štěrkovna	1-2	A
Bistro		B
Botanická/zoologická zahrada	1	O
Brusírna drahých kamenů	3-4	F
Butik s klenotnickým zbožím	3	C
<b>C-Č</b>		
Cestovní kancelář	1	B
Cukrárna	1	B
Čerpací stanice vody	3-4	A
Čistírna odpadní vody	1	A
Čistírna peří	1	A
<b>D</b>	1	
Dálková výtopna	1	
Dětský domov	1-2	
Diskotéka	1-2	
Divadlo	1-3	A
Domácnosti včetně rodinných domů		
Drogerie/parfumerie/kosmetický salón		B-C
Drůbeží farma	1	
Dům nábytku	1-2	
Dům s ošetřovatelskou službou		B

<b>E</b>		
Elektrárna oblastní	2-4	B-C
Elektrárna strategická	2-4	E
Elektrotechnická dílna	1	B
Expreso	1	
Pokračování tabulky č. 5		
<b>F</b>		
Farma kožešinové zvěře	2	
Farmaceutické/lékařské zboží	3	C
Filmové /nahrávací studio s video	2-3	
Finanční úřad	3	
Fitcentrum	1	B
Fotoateliér	1-2	B-C
Fotoateliér	1-2	B-C
Fyzikální laboratoř	2-4	
<b>G</b>		
Galerie	2-4	O
Galvanizovna	1	
Garáž ) bez čerpání PH a bez oprav)		O
Grafický závod/tiskárna		B
<b>H</b>		
Hasiči		A
Herna		C-D
Hotel/penzion	1-3	B
Hrací sál	2	
Hrad/zámek	2-4	O
Hrnčířství	1	
<b>CH</b>		
Chemická laboratoř	2-3	
Chladírna	1	
<b>I</b>		
Internát	1	
<b>J</b>		
Jatka	1	
Jezdecká škola/stáj/ jízdárna	1	O
Jídelna	1	B
<b>K</b>		
Kancelář /úřad	1-3	
Kaple	2-3	
Klášter	1-3	O
Knihovna s archivními fondy	2-3	
Kostel	1-3	O

Koncertní síň	1-2	A
Koželužství	1	
<b>L</b>		
Lanová dráha	2	
Lékárna	2-3	C
Lékařská praxe/ laboratoř	2	
Lisovna	1	
<b>O</b>		
Obchod s automobily včetně příslušenství	2	C-E
Pokračování tabulky č. 5		
Obchod s ceninami	2	
Pokračování tabulka č.5		
Obchod s elektrickým zbožím bez zab. elekt.	2	B
Obchod s elektrickým zbožím se zab. elekt.		C-D
Obchod s chemikáliemi	2	
Obchod s obrazy/uměleckými předměty	1-2	O
Obchod s počítači		C-D
Obchod se sklem		B
Obchod se zbraněmi	3-4	D-E
Obytné budovy	1	
<b>P</b>		
Peněžní ústav	3-4	E
Pivovar	1	
Pošta	2-3	
Pohřební ústav	2	A
Přístaviště		O
Půjčovna filmů/videotéka	1	C
<b>R</b>		
Radiový vysílač	2	
Radnice/ obecní správa	2	B
Restaurátor		
<b>S-Š</b>		
Sanatorium	1	
Sbírka umění		
Starožitnictví včetně klenotnického zboží		O
<b>T</b>		
Tapiserie	1	
Tiskárna cenných papírů		
<b>U</b>		
Umělecký atelier	1	C
<b>Z-Ž</b>		
Zahradnictví	1	
Železářství		A

## **Poznámkový aparát**

- 1) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str. 5
- 2) srv. Časopis zabezpečení a kriminalita, 6. ročník , březen 1997, Ing. Ladislav Toms – Zabezpečení vstupů , prostor a objektů visacími zámky
- 3) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str. 6
- 4) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str. 6
- 5) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str. 7
- 6) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str. 9-10
- 7) § 247 /písmeno A) Tr. Zák. č.140/1961 Sb.
- 8) § 247 /písmeno B) Tr. Zák. č.140/1961 Sb.
- 9) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str. 17
- 10) PCO – Pult centralizované ochrany viz. Zkratky
- 11) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str. 24
- 12) Magazín Security, Ročník XI, červenec/srpen 2004
- 13) Magazín Security, Ročník XI, červenec/srpen 2004
- 14) Reportáž na televizním programu Prima, pořad Extra
- 15) Vyhláška ÚOHS č. 202/2001 Sb.
- 16) Magazín Security, Ročník X, květen/červen 2003
- 17) Magazín Security, Ročník XI, červenec/srpen 2004
- 18) Magazín Security, Ročník XI, červenec/srpen 2004
- 19) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str.25
- 20) srv. Skripta: Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001, str.26
- 21) MW- mikrowale – viz. Zkratky
- 22) Počítadlo pulsů – pulse count – viz. Zkratky
- 23) Systémy APSP – Auto pulse Signal Processing – viz. Zkratky
- 24) ) § 234 Tr. Zák. č.140/1961 Sb.
- 25) Personál Security Systém – viz. Zkratky
- 26) SNB – Sbor národní bezpečnosti – viz. Zkratky



## **Seznam použité literatury**

### **Odborná literatura:**

- Křeček, S.: Příručka zabezpečovací techniky. Cricetus, 2002.
- Uhlář, J.: Technická ochrana objektů, II.díl –Elektrické zabezpečovací systémy. PA ČR, Praha 2001
- Kindl, J.: Projektování bezpečnostních systémů. 2004
- Dip. Ing.Paták, J., prof. JUDr. Protivinský, M., JUDr. Klvaňa, K.: Zabezpečovací systémy
- Pütz,J. a kol.: Úvod do číslicové techniky. SNTL –Praha 1983.
- Hráčský, J., Anderle, H.: kurz elektronických obvodů pro průmyslovou elektroniku . SNTL Praha 1976
- Limann, O.; Pelka, H.: Elektronika bez balastu. Alfa, Bratislava.
- Syrovátko, M.: Zapojení s polovodičovými součástkami.
- Farský; Prokeš : Elektrické obvody I.
- Šícha, M., tichý, M.: Elektronické obvody II. SNP, Praha 1982.
- Gauner, K.: Základy elektroniky, skriptum. ZČU, Plzeň 2001.
- Frisch, M.: Základy elektroniky a elektronických obvodů. SNTL, Praha 1987.
- Klaus, T. a kol.: Příručka pro elektrotechnika. Europa-Sobotáles cz. Praha 2002

### **Časopisy :**

- Security magazín. Ročník VII, leden/únor 2000 s.55-57 - názvosloví
- Security magazín. Ročník IX,květen/červen 2003
- Security magazín. Ročník IX, červenec/srpen 2003
- Security magazín. Ročník X , červenec/srpen 2004
- Zabezpečení a kriminalita. Ročník VI, březen 1997
- Katalog produktů pro ochranu majetku a osob (10/2004)

### **Internetové zdroje:**

[www.fides.cz](http://www.fides.cz)

[www.zabezpečení.netlezs-house](http://www.zabezpečení.netlezs-house)

### **Další zdroje :**

- Trestní zákon a trestní řád č.140/1961 Sb.
- Věstník ministerstva vnitra ČR, ze dne 29.května 1997
- Oborová norma AGA 50131-1 až 7
- Česká technická norma: ČSN EN 50131-1/Z1.Praha: Český normalizační institut. 2000, str.84-85

## **Seznam zkratek :**

PCO – Pult centralizované ochrany

EZS – elektronická zabezpečovací signalizace

AGA – Asociace grémium alarm

ČAP - Česká asociace pojišťoven

EM – Elektromagnetické

AM – sousto-magnetické

RF - radiofrekvenční

EAS – Electronic Article Surveillance

ATV – Automatické telefonní vodiče

PSS - Personál Security Systém

SNB – Sbor národní bezpečnosti

VB – Veřejná Bezpečnost (nyní Policie)

MW- Microwave; mikrovlnná čidla

ISDN – Integrated Services Digital Network

APSP – Auto Pulse Signal Processing

GSM – Global Systém Mobile Communication

US – Ultrasonic – ultrazvuková

LED – Light Emission Diode