Česká zemědělská univerzita v Praze

Technická fakulta

Klady a zápory využití PCO pro zajištění objektu

Bakalářská práce

Vedoucí bakalářské práce: Ing. Zdeněk Votruba

Autor práce: Jan Šrámek

PRAHA 2009

Vysoká škola:	Česká zemědělská univerzita	Fakulta:	technická
Katedra:	technologických zařízení staveb	Akademický rok:	2007/2008

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Student: **ŠRÁMEK Jan**

Studijní obor: OPT

Studijní zaměření:

Název práce: Klady a zápory využití PCO pro zajištění objektu

Zásady pro vypracování:

Cíl práce: Zjistit reálný stav v oblasti instalace malých a středních EZS ústředen. Zmapovat služby nabízené bezpečnostními službami směrem k ochraně přes PCO. Posoudit možnosti těchto organizací a vhodnost nabízených služeb. Zhodnotit právní důsledky při použití a při nepoužití této služby při provozu EZS

Osnova práce:

1. Definice EZS a jejich obecný rozbor
2. Systémy instalované v ČR a ve světě
3. Služby související s napojením EZS na PCO v ČR
4. Zhodnocení a rozbor výše uvedených služeb
5. Finanční, právní, uživatelské a bezpečnostní zhodnocení
6. Závěr, doporučení, návrhy

Metodika práce: Zjistit současná stav a trendu v oblasti EZS pro malé a střední objekty. Zhodnotit rozšiřující služby navázané na provoz malých a středních systémů EZS, posoudit je z hlediska právního, technického, uživatelského, finančního. Stanovit globálně použitelná pravidla pro využití těchto služeb a sestavit obecné doporučení.

Prohlášení:

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a že jsem uvedl všechny literární zdroje a prameny, ze kterých jsem čerpal.

Podpis .....

V Praze dne 3. 4. 2009

Anotace:

Tato bakalářská práce má za úkol seznámit s možnostmi použití pultů centralizované ochrany při řešení problematiky zabezpečení majetku a ochrany osob. Legislativa v zásadě odlišuje zabezpečení majetku a osob před narušitelem a vznikem a následnou likvidací požáru. V tomto přehledu se omezím na výčet technických prvků, dodávajících signály o hrozícím nebezpečí, a dále rozvedu metodické a organizační možnosti při ochraně majetku před narušitelem a možnosti sledování technologických stavů.

Klíčová slova: Pult centralizované ochrany, elektrická zabezpečovací signalizace, bezpečnostní agentura, komplexní řešení, inteligentní budova.

Anotation :

The aim of this bachelor work is to present possibilities of using alarm receiving centre at problems solving of people's protection and security of property. The legislation differentiates in principle people's and property's security at intrusion and fire. I provide in this abstract the summary of technical components which supply impulses about the detected danger. Further are described the methodical and organisational possibilities at property securing from the violator and possibilities of monitoring of technological status.

Key words: alarm receiving centre, elektric safety signalisation, security agency, komplex resolution, intelligent building

Obsah:

1. Úvod

Elektronické signalizace dosáhly vysokého stupně vyspělosti a technické úrovně. Pro využití této špičkové technologie se zřizují speciální pracoviště „Pulty centralizované ochrany“. Tato pracoviště využívají dodávané informace ke snižování dopadů negativních stavů na majetek provozovatelů monitorovaných objektů a zařízení a na zdraví obslužného personálu. Cílem této bakalářské práce je podat přehled o možnostech získávání potřebných informací a jejich využívání při monitoringu zabezpečovaných objektů a následných činnostech, které vyplývají z povahy vzniklých kritických stavů. U elektronických signalizací se omezím jen na jejich výčet a používané prvky. Využívání PCO má význam především při provozování malých a středních celků, které nejsou trvale obsluhovány. Kontrolu těchto objektů přejímají bezpečnostní agentury (BA) na základě smluvních vztahů s provozovateli. Tyto agentury dle rozsahu svých služeb dále zajišťují, samostatně či ve spolupráci s policií nebo Hasičským záchranným sborem, potřebné reakce na registrovaná hlášení elektronických signalizací. Dále se budu zabývat především organizační, smluvní, provozní a ekonomickou stránkou problematiky zřizování a používání dohledových a monitorovacích pracovišť a poskytováním návazných služeb.

2. Význam PCO

V současné době je pro ochranu života a majetku používáno mnoho druhů zabezpečení a jejich kombinací. Počínaje mechanickými zábranami, přes fyzickou ostrahu až po sofistikované elektronické systémy. Technický pokrok elektronických, technických a technologických systémů se postupně ubírá směrem k inteligentním budovám a na lidském faktoru bude spočívat stále vyšší rozhodovací zodpovědnost a s tím spojená kontrolní činnost. Jak s dodanými informacemi o různých sledovaných stavech operativně naložit, nelze pro všechny situace jednoznačně naprogramovat.

2.1 Historie

Lidstvo se odnepaměti snaží všemi dostupnými způsoby chránit svůj majetek před nebezpečím. Tato nebezpečí mohou být přírodního původu jako voda, oheň či vzduch (vítr), nebo od nepřátel lidských i zvířecích. Možnosti dostupné ochrany vždy závisely na technické vyspělosti civilizace. S probíhajícím pokrokem se nebezpečí vzniku škod stupňovalo, ale vyvíjela se i opatření na ochranu spolu s možnostmi předcházení škodním událostem. S koncentrací lidí ve městech se koncentrovala i nebezpečí, z nichž nejhorším byl požár. Spolu s preventivními opatřeními se vyvíjel i systém vyhlašování poplachů pro zamezování vznikajících škod. Velká města problém ochrany před požáry řešila zprvu hlídkami na vyvýšených místech či pochůzkovými kontrolami. Tyto hlídky navíc přispívaly i k ochraně soukromého majetku zejména v nočních hodinách. Později vznikaly i sítě hlásek, které si předávaly zprávy o vzniklém nebezpečí prostřednictvím zvukových signálů (zvony, troubení) či pomocí rychlých poslů atd.

Éra elektrických poplachových systémů navázala na různé systémy mechanické a započala s využíváním telegrafu k předávání zpráv. Vznikly i volací skříňky, předchůdce dnešního veřejného hlásiče. Při zatažení za páku hlásiče se roztočilo vroubkované kolo a prostřednictvím elektrického kontaktu vyslalo sérii teček a čárek, ve kterých byl obsažen určitý kód. Na centrálním pultu pak primitivní zapisovač zaznamenal tuto sérii a vytvořil tak záznam o poplachu. První takový systém byl schválen a uveden do provozu v Bostonu (stát Massachusetts) v roce 1851 a o tři roky později ve městě fungovalo již 42 takovýchto hlásičů. Obdobný systém byl nezávisle vybudován koncem 19. století i v Hamburku, kde sloužil až do roku 1976.

První známý elektrický zabezpečovací systém, značně vylepšený proti mechanické verzi nástražného drátu a principu pastičky na myši, si nechal patentovat pan Augustus Pope roku 1853 ze Sommerville (také stát Massachusetts). Používal kombinaci kontaktů, instalovaných na dveřích a oknech, s baterií a zvonkem. Svůj patent prodal roku 1857 Edwinovi T. Holmesovi, novoanglickému obchodníkovi s galanterií a šicími potřebami . Později pan Holmes tento systém zdokonalil tak, že byl schopen adresovat stav každého zabezpečeného uzávěru. Následně doplnil do systému i hodiny pro možnost „programování“ a spínání domovního osvětlení.

Po delší dobu se pak zabezpečovací signalizace rozvíjela na principu spínaných i rozpínaných kontaktů i ve spojení s nástražným systémem. Teprve začátkem 20. století se objevují elektromechanická čidla založená na principu setrvačnosti (kyvadla, vibrační kontakty nebo i inercionální senzory). Zabezpečovací ústředny byly až do poloviny minulého století zásadně reléové. Pro signalizaci se stále používaly převážně zvonky. Rozvoj elektroniky po druhé světové válce se sériovou výrobou polovodičových součástí přispěl k miniaturizaci a vzniku nových technologií. Rovněž intenzivní vývoj pro potřeby výzkumu kosmu a vojenského průmyslu (válka ve Vietnamu), stejně jako komputerizace, umožnily vznik nových technologií a prostředků vhodných pro použití v zabezpečovací technice (akustické snímače, mikrovlnná čidla). V druhé polovině sedmdesátých let se objevuje na trhu nový zabezpečovací prvek – Passive Infrared Detector (PIR).

V současné době je pro ochranu majetku a osob používáno velké množství systémů různých výrobců. Všechny tyto profesionální poplachové systémy pro zabezpečení a řízení objektů jsou samostatně funkční. Součinnost jednotlivých prvků, zabudovaných do systému, ale vyžaduje různé nadstavby, které přebírané výstupy sjednotí a vyhodnotí. Toto je úkolem různých ústředen a podústředen, které navíc mohou pracovat v různých protokolech. Na ně jsou dále napojeny další nadstavbové či vizualizační systémy. Všechna tato zařízení využívají výpočetní techniku typu PC. [5]

2.2 Charakteristika PCO

Pult centralizované ochrany (PCO) je zařízení, které slouží pro příjem, monitorování, záznam a vyhodnocování zpráv z připojených signalizací – elektronické zabezpečovací (EZS), případně požární (EPS) . Zároveň je možné přenášet na PCO i různé technologické stavy ze systému měření a regulace (MaR). Ústředna PCO podporuje

většinu přenosových formátů, s libovolnou překladovou tabulkou zpráv. Řídící aplikace vyhodnocuje informace v nepřetržitém režimu 24 hodin denně. Nedílnou součástí pracoviště PCO je dispečer pracující v nepřetržitém provozu. Tento operátor má potřebné rozhodovací pravomoci a na základě vyhodnocení situace má k dispozici servisní a výjezdovou skupinu. [20]

Připojením objektu na PCO má uživatel zajištěnu službu profesionálního zásahu v případě jakéhokoliv narušení. Operátor PCO ví jakým způsobem a kudy byl objekt narušen – PCO přesně lokalizuje místo narušení objektu podle instalovaných detektorů a dispečer následně stanoví způsob zásahu. PCO monitoruje i technický stav připojených zařízení jako je například vadný zálohovací akumulátor, chyba detektoru, potřeba servisu či výskyt nedefinovaného stavu a tyto informace jsou neprodleně předány uživateli či jím pověřenému servisnímu pracovišti. Všechna komunikace operátora PCO se zákazníkem a výjezdovou skupinou je nepřetržitě nahrávána a archivována po dobu nejméně 2 měsíců. Připojení systému EZS, EPS a MaR na PCO výrazně zvyšuje úroveň ochrany majetku ve střeženém objektu. [27,28]

Obr. 1: Pracoviště PCO

3. Elektronické signalizace

3.1 Druhy signalizací

PCO je moderní dispečerské pracoviště, na které jsou v zakódované podobě přenášeny veškeré relevantní informace, které jsou systémy EPS a EZS a MaR schopny poskytnout. Systémy EPS se řídí odlišnými právními, prováděcími a realizačními předpisy a jsou převážně provozovány na PCO HZS. Předmětem této práce je především zabezpečení z hlediska fyzického narušení či předcházení škodám vzniklým chybnou

funkcí instalovaných technologií, a proto se u EPS omezím jen na technický popis jednotlivých komponent. Systém EZS integruje i návazné podsystémy uzavřených kamerových okruhů (CCTV) a systém kontroly vstupů (SKV). MaR je podpůrný systém kontroly a monitorování technologických stavů sledovaných zařízení. Výběr jednotlivých signalizací a jejich prvků instalovaných ve sledovaných prostorách je závislý na charakteru, návazných provozních předpisech a hodnotách zařízení v objektu provozovaných. ČSN rozlišuje následující 4 stupně zabezpečení:

Elektrická zabezpečovací signalizace a navazující systémy dle současných norem (v závorce kódy použité v katalogu dle starších norem). [23]

stupeň 1 (N) nízká rizika

stupeň 2 (P) nízká až střední rizika

stupeň 3 (V) střední až vysoká rizika

stupeň 4 (V) vysoká rizika

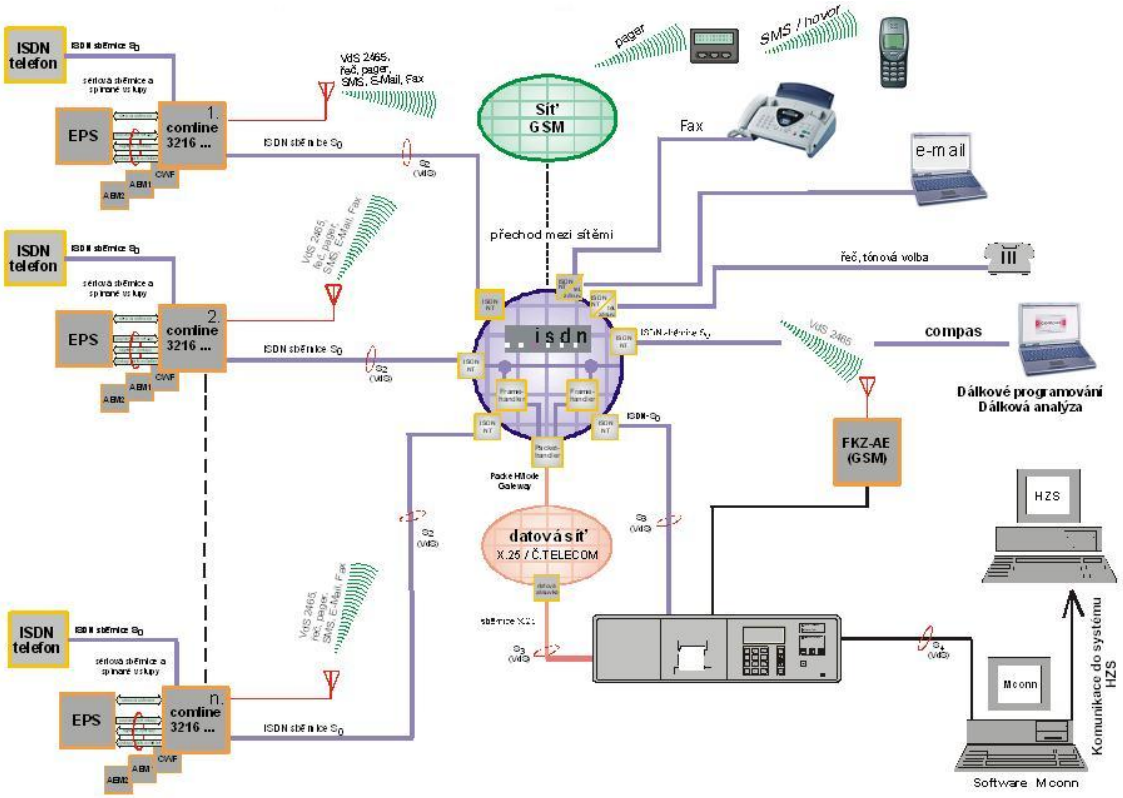
3.1.1 EZS

Elektronická zabezpečovací signalizace je základním druhem zabezpečovací techniky, která přímo navazuje na stavebně konstrukční a mechanické zábranné systémy v objektu. EZS musí být projektována a instalována tak, aby v reálném čase signalizovala pokus nebo nežádoucí vniknutí do chráněného objektu a zaměstnancům umožňovala zvlášť signalizovat stav bezprostředního ohrožení osob a majetku. Signál EZS je následně přenášen na PCO nebo do místa trvalé obsluhy, eventuálně i jako lokální signalizace. Konkrétní požadavky na jednotlivé moduly (prvky) systému, rozsah zabezpečení jsou řešeny na základě platných norem a s ohledem na charakter provozu, míru rizik, případně bezpečnostní posouzení objektu (BPO).

Elektrická zabezpečovací signalizace slouží jako poplachový systém pro zjištění přítomnosti, vstupu nebo pokusu o narušení střežených objektů (viz ČSN EN 50 131 -1). Mezi prvky EZS patří vyhodnocovací ústředny, čidla, hlásiče, prvky poplachové signalizace, přenosová a zapisovací (archivační) zařízení a indikační zařízení, které na

určitém místě signalizuje nepovolený vstup nebo narušení střeženého prostoru, a to jak akusticky, tak opticky.

Hlavním úkolem systému EZS je v co nejkratší době identifikovat, indikovat a následně přenést zjištěný problém na ústřednu EZS, kde jsou provedena vhodná opatření k řešení problému. Zjištěná informace o poplachu musí být zcela přesná a pravdivá, systém EZS by měl být neomylný.



Obr. 2: Schéma možného uspořádání přenosu EZS

Komponenty systémů EZS jsou z větší části složitá elektronická zařízení, která musí splňovat podmínky mnoha technických norem a zákonných předpisů a před uvedením na trh musí projít zákonem stanovenými zkouškami v akreditovaných zkušebnách. Po úspěšném absolvování zkoušek je výrobek systému EZS certifikován do určité kategorie, kterou je dána možnost jeho využití v objektech s odpovídajícími riziky napadení.

Systémy EZS jsou uživateli protokolárně předávány na základě výchozí revize. Pro jejich plnohodnotné užívání a spolehlivou funkci musí být prováděny předepsané periodické kontroly a revize. [10,13]

3.1.2 CCTV

Hlavním cílem uzavřeného kamerového systému je především prevence a dokumentace mimořádných událostí. CCTV by měl být v trvalém provozu, aby se minimalizovala doba odezvy, vhodné je i propojení na EZS pro možnost změny režimu při poplachu a potřebná je i záloha napájení. Umístění jednotlivých kamer musí splňovat požadavky na charakter sledované pracovní činnosti, kvalitu obrazových výstupů podle jejich účelu v návaznosti na normy ČSN, při umístění mimo vnitřní prostory musí být zvláště chráněny proti nežádoucím zásahům a zastřeženy EZS. V provozní době objektu by měl být zajištěn nepřetržitý dohled na monitorovacím pracovišti. [10]

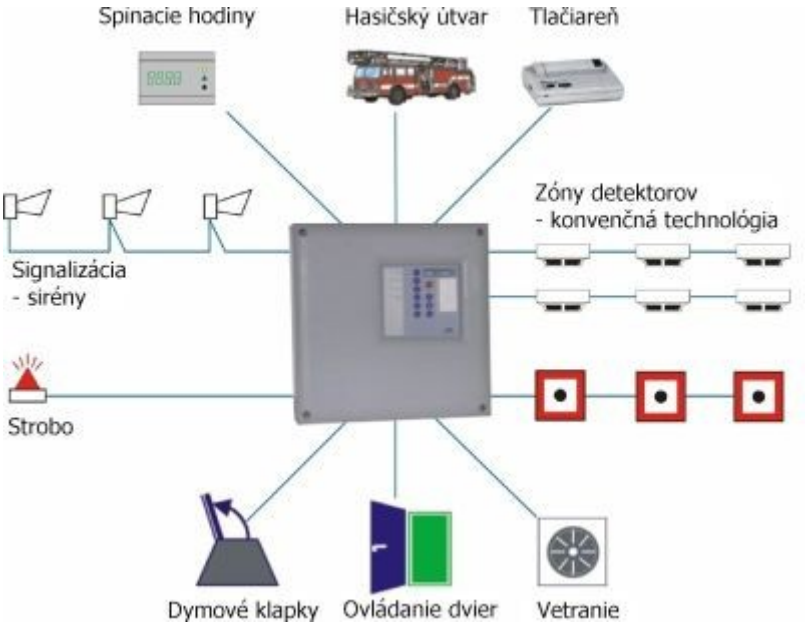
Obr. 3: Kamera s infra přisvícením a nahrávací systém

3.1.3 SKV

Přístupový systém je doplňujícím členem zabezpečovací techniky. Je realizován pomocí čtecích zařízení (schopných pracovat i v autonomním režimu) a magnetických karet či bezkontaktních čipových prvků. Součástí jsou i elektricky ovladatelné dveřní zámky. Umožňuje více režimů v závislosti na časových údajích. Slouží především pro kontrolu a řízení vstupu do vybraných zájmových prostor. Dále může být využit k vyhledávání osob či pro docházkový systém. Pro případy výpadku proudu je doplněn záložním zdrojem a signalizací stavu. [10]

3.1.4 EPS

Elektronická požární signalizace je jedním z druhů celkového zabezpečení, zejména proti nebezpečí zahoření. Slouží k včasnému zpozorování a indikaci vzniklého ohniska požáru a přenesení signálu na ústřednu, kde se buď automaticky nebo prostřednictvím osob provede vhodný zásah ke zlikvidování požáru. Způsobů, jak reagovat na vzniklou situaci je několik. Ústředna, která je napojena na PCO Hasičského záchranného sboru, předá informaci obsluze PCO, vyhlásí současně požární poplach v dotčeném pracovišti a případně uvede v činnost samozhášecí zařízení, pokud je jím objekt vybaven. Při zákroku HZS přebírá velení velitel zásahu.



Obr. 4: Schéma zapojení EPS

3.1.5 Měření a regulace

Měření a regulace je mikroprocesorový systém pro řízení a regulaci technologických stavů používaný i při řízení provozu bezobslužných objektů. Základem systému je centrální jednotka, která obsahuje procesorovou část, aplikační program a komunikační kanály. K centrální jednotce se po rychlé sběrnici připojují periferní jednotky pro styk s logickými a analogovými procesními signály, terminál pro ovládání systému, případně další speciální moduly pro komunikaci atd. V pracovní době se vyhodnocené stavy zobrazují obsluze na velínu, případně alarmové stavy jsou indikovány zvukovou

signalizací či převodem na telefonní přístroj. Mimo běžnou pracovní dobu (případně paralelně) lze zvláště důležité poplachy přenášet standardním způsobem na PCO. Tento systém dokáže vyhodnocovat veškerá hlášení předávaná technologickými zařízeními jako jsou: chlazení centrální i lokální, topení, VZT, elektrorozvaděče, rozvod vody, čerpadla, výtahy, atd. … Dle stavů dodaných na PCO může obsluha informovat pohotovostní servis uživatele například o výpadku mrazících boxů s potravinami, o poruchách provozu automatických kotelen, výpadku čerpadel v lokální kanalizaci a podobně. Včasný zásah následně zabrání vzniku materiálních škod i uvnitř zastřežovaných objektů.

4. Druhy připojení na PCO

Důležitou součástí zabezpečení je komunikace mezi signalizacemi a PCO. Takovéto připojení je možné dle požadovaného stupně zabezpečení různými kanály: po telekomunikační síti, GSM modulem či bezdrátově pomocí vysílače. Na spolehlivost, kvalitu, případně zabezpečení této komunikace jsou kladeny různé požadavky včetně možnosti zašifrování údajů. Kromě rozdílné technické náročnosti zvoleného prostředku je nutné uvažovat i o ekonomičnosti a efektivnosti provozu přenosu ve vztahu na předpokládaná rizika. ČSN rozlišuje následující stupně utajení: [5,27]

Stupně zabezpečení utajovaných skutečností:

"V" stupeň vyhrazené

"D" stupeň důvěrné

"T" stupeň tajné

"PT" stupeň přísně tajné

4.1 Linky JTS

Přenáší na PCO všechny informace, které je instalovaná signalizace schopna poskytovat. U většiny běžně používaných ústředen stačí ke zprovoznění komunikace s PCO pouze naprogramovat, nevyžaduje se dokup dalších zařízení. Sledovaný objekt tedy musí být vybaven telefonní linkou, přenos je pomalejší a závislý na kvalitě této linky. Spolehlivost tohoto přenosu je ovlivňována poruchami na lince, případně jejím přerušením nebo napadením narušitelem. Kontrola spojení je obvykle prováděna 1x za 24 hodin. Výše telefonních poplatků se navyšuje o hovory uskutečněné systémem dle frekvencí zapínání, vypínání i při servisních zákrocích. [5,10]

4.2 Bezdrátové připojení

4.2.1 Rádiové vysílače

Bezdrátově pomocí vysílače

Přenos na PCO funguje bez zpoždění v reálném čase. Interval kontroly spojení s PCO lze provádět až 1x za 30 s. Je proto obtížně napadnutelný narušitelem. Instalovaný systém je nutno dovybavit vysokofrekvenčním vysílačem a zakalkulovat i náklady spojené s jeho instalací. Celkově se navýší poplatky za střežení o náklady na provoz, správu a údržbu radiové sítě.

Obr. 5: Rádiový vysílač

4.2.2 GSM

GSM modul

Zabezpečuje přenos důležitých informací ze střeženého objektu i v případě poruchy telefonní linky (pokud slouží jako záložní spojení). Přenos je jen obtížně napadnutelný narušitelem. Spolehlivost je závislá na momentálním zatížení sítě mobilních telefonů (GSM). Je nutné doplnit ústřednu o modul GSM a provést instalaci. Dále je nutná aktivace SIM karty u některého operátora. V rámci běžně provozovaných operátorských sítí GSM/GPRS lze využít i některou vysoce zabezpečenou síť (například NSG). [27]

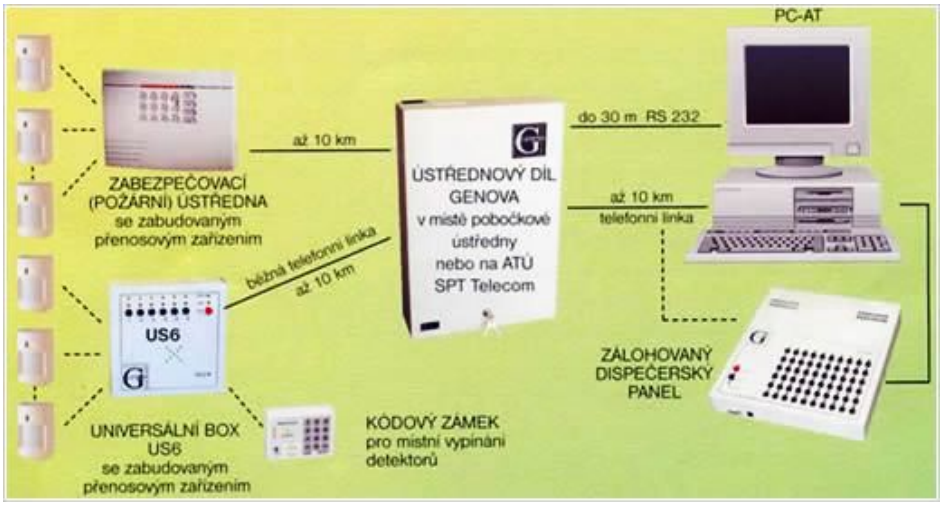
4.3 hodnocení druhu přenosu

Při srovnávacím testování rádiové a GPRS sítě, prováděném největšími dodavateli systémů PCO, se dospělo k závěru, že rádiový přenos na PCO se jeví jako prioritní a GPRS je vhodným doplňkem. Test se zaměřil na porovnání výpadků vysílačů uvedených sítí. Počty výpadků GPRS vysílačů jsou několikanásobně vyšší než u rádiových, navíc jsou i delší. To přináší zejména dispečerům PCO komplikace při posuzování reálnosti výpadku. U rádiového přenosu jde většinou o krátký výpadek, v opačném případě se jedná o poplachový stav. U GPRS vysílače vstupují při rozhodování další aspekty – výpadek sítě u

operátora, oprava základové stanice BTS (Base Transfer Station), zahlcení sítě, použití rušičky a další. Nelze také zapomenout ani na zpoplatňování datových přenosů. U rádia jsou poplatky za datové přenosy nulové, u GPRS řešení je nutné zaplatit poplatky mobilnímu operátorovi. Navíc díky výraznému snížení poplatků za užívání vyhrazené frekvence je provoz rádiových sítí cenově nejvýhodnější na současném trhu. [5,26]

5. EZS a její prvky

5.1 Řídící moduly – zabezpečovací ústředna



Obr. 6: Schéma uspořádání zabezpečovacího systému

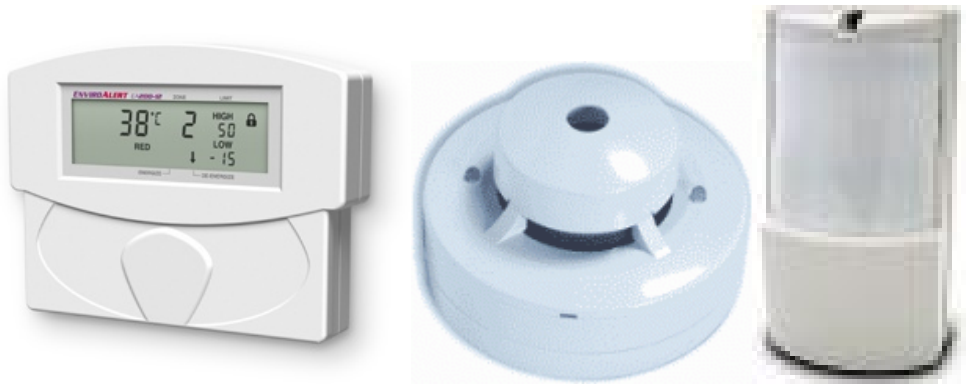
Ústředna umožňuje připojení všech detektorů systému, přijímá a zpracovává informace z čidel podle stanoveného programu a požadovaným způsobem je realizuje. Dále umožňuje ovládání a indikaci zabezpečovacího systému, zajišťuje jeho napájení a inicializaci následného přenosu informací. [10]

Obr. 7: Příklad zabezpečovacích ústředen s klávesnicí

5.2 Detektory

Detektor (čidlo) je zařízení bezprostředně reagující na fyzikální změny (jevy), které souvisejí s narušením střeženého objektu či prostoru nebo na nežádoucí manipulaci se střeženým předmětem. Pracují na různých principech – zaznamenávají pohyb objektů s určitou teplotou, změny kapacity či infrazvukových vibrací, využívají magnetismu, Dopplerova efektu mikrovlnného nebo ultrazvukového pole atd. Prakticky všechny detektory jsou dnes již vybaveny složitou elektronikou, často řízenou procesorem, která umožňuje přizpůsobovat jejich funkci měnícím se vlastnostem prostředí a prakticky eliminovat chybové stavy. Při indikování stavu narušení reaguje čidlo vysláním poplachového signálu nebo zprávy. [10]

Čidla: pohybu
otřesu
tříštění skla
magnetické spínače
infra závory
požární čidla
sirény



Obr. 8: Čidla změny prostředí a pohybu

5.2.1 Aktivní

Aktivní čidla při zjišťování charakteristických rysů nebezpečí vytvářejí své pracovní prostředí aktivním zásahem do okolního prostoru (např. vysíláním

elektromagnetického nebo ultrazvukového vlnění). Proto je možné tato čidla poměrně snadno detekovat a určovat jejich mrtvé zóny. Jsou schopna porovnávat vstupní signály s předem definovanými kritérii (rychlost, frekvence, amplituda, směr) před vysláním poplachového signálu nebo zprávy. [10]

5.2.2 Pasivní

Pasivní čidla, která pouze pasivně registrují fyzikální změny ve svém okolí, např. pasivní infračervené čidlo registruje jen změnu teplotního gradientu. Na rozdíl od aktivních čidel jsou tato obtížně identifikovatelná běžnými technickými prostředky (např. detekce PIR čidla infravizorem). [10]

Koncová zařízení

Umožňují indikaci narušení střeženého objektu. Může být například akustická siréna nebo optická signalizace. Pro dálkový přenos signalizace na pult centralizované ochrany (PCO) se využívá rádiových modemů nebo telefonních komunikátorů.

Ochranné kontakty

Slouží k ochraně vlastního systému EZS před nepovolaným zásahem. Při pokusu o neoprávněné proniknutí do některého zařízení nebo prvku EZS vyhlásí systém sabotážní poplach.

Systém EZS pracuje obvykle ve dvou režimech - v nočním, kdy střeží zpravidla všemi detektory celý objekt, a denním, kdy je budova v normálním provozu a střeží se pouze instalace systému a vybrané předměty (trezory, vystavované předměty apod.).

Zvláštním druhem systému EZS je zařízení pro střežení obvodu rozsáhlých areálů, tzv. perimetrická ochrana. Ta umožňuje zachytit případného narušitele ještě před vlastním vniknutím do střeženého objektu a poskytuje bezpečnostním složkám dostatek času pro zásah. [10,16]

Příklad použití zabezpečovacích prvků podle stupňů rizika :

První stupeň – tvoří magnetické spínače (kontakty), které jsou instalovány na vstupní dveře a okna objektu. Tyto prvky reagují pouze na otevření zajištěné části (např. násilné otevření dveří, oken apod.)

Druhý stupeň – je představován audiodetektory tříštění skla. Detektory slouží k ochraně prosklených ploch oken, dveří a stěn. Jsou vyvinuty pro detekování útoků na prosklené části ze skla jednoduchého, vrstveného, bezpečnostního a temperovaného a jsou instalovány do prostorů místností. Číslicový filtr detektorů reaguje pouze na zvuk vyvolaný tříštěním skla.

Třetí stupeň – tvoří elektronické detektory pohybu. Pohybové detektory jsou určeny pro střežení prostorů místností. Detektory se dále dělí z hlediska principu snímání na infrapasivní – PIR (snímání náhlého rozdílu teploty ve střeženém prostoru), mikrovlnné – MW (snímání pohybu tělesa), ultrazvukové – UZ (reakce na změnu vysílaného a přijímaného ultrazvukového signálu) a kombinované – např. PIR+MW (poplach je vyhlášen při zaregistrování oběma senzory). Nasazení detektorů je dáno typem zabezpečovaného prostoru a použitý typ detektoru je určen projektantem při návrhu systému.

Čtvrtý stupeň – do této kategorie lze zahrnout ostatní prvky, které jsou v systémech EZS používány. Jedná se o tísňové hlásiče, seismické (otřesové) trezorové detektory, závěsné snímače (ochrana obrazů a cenných předmětů v galeriích), snímače úniku plynu, kouře, vody, atd. [23]

5.3 Napájecí zdroje

Napájecí zdroj musí napájet ústřednu a ostatní komponenty EZS nepřetržitě. Požadavky na napájecí zdroj jsou rozděleny na čtyři kvalitativní stupně zabezpečení. Napájecí zdroj splňuje požadavky příslušného stupně, pokud zahrnuje všechny povinné funkce tohoto stupně. Rozlišujeme napájení ze sítě, dobíjených či nedobíjených akumulátorů a baterií a vzájemných kombinací těchto zdrojů. Nejvyšší stupeň zabezpečení je 4 – vysoké riziko. Používá se, má li zabezpečení prioritu před všemi ostatními hledisky. Napájení proto musí být zajištěno ze dvou nezávislých zdrojů, mechanicky zabezpečených a s detekcí přerušení.

Obr. 9: Napájecí zdroje

6. Služby související s napojením na PCO

Základní nabídka služeb PCO obsahuje především dálkový monitoring EZS, EPS, CCTV, SKV, MaR, kontrolu stavu objektu (i výjezdovou skupinou), kontrolu pohybu osob (zaměstnanců) a jejich pobytu ve střeženém objektu. Ostraha objektu provozovaná strážním subjektem pro uživatele je vykonávána na základě smluvního vztahu. V takovéto smlouvě je přesně definován předmět, použitá zabezpečovací signalizace, přenosové zařízení a následné kroky dispečera PCO dle jednotlivých signálů ze střeženého objektu. Dále by měla smlouva obsahovat kontaktní spojení na uživatele a jím pověřené osoby, dobu odezev a finanční ocenění jednotlivých úkonů, případně požadavek na šetrnost a přiměřenost realizovaného zásahu. Předpokladem řádného výkonu ostrahy je i pojištění strážní služby pro případ vzniku škod při zásahu. Součástí smluvních podmínek by mělo být i dodržování kodexu ČKBS, ASBS. [19,21]

Základní nabídka služeb PCO:

- servisní činnosti všech sledovaných připojených systémů
- dálkový monitoring EZS (elektronickou zabezpečovací signalizací)
- dálkový monitoring EPS (elektronickou požární signalizací)
- dálkový monitoring CCTV (kamerovým systémem)
- dálkový monitoring SKV (přehled o pohybu osob v jednotlivých zónách)
- kontrola stavu objektu výjezdovou jednotkou

- zajištění pachatele výjezdovou jednotkou
- monitoring uzamykání objektu (kontrola elektronického zakódování objektu v mimopracovní době nebo u bezobslužného pracoviště)
- zajištění objektu proti vzniku dalších škod
- služba TÍSEŇ – rychlé přivolání pomoci

Využití v dopravě:

- střežení automobilů pomocí sytému GPS
- odstavení odcizeného vozidla z provozu
- navigování zásahové jednotky k vozidlu

Jiná využití (např. v rámci facility managementu):

- dálkové ovládání topení
- hlídání teploty chladicích zařízení
- chod záložních agregátů
- monitoring klimatizace, vzduchotechniky, elektrické, telekomunikační, počítačové sítě

Tvorba cen

Zabezpečované objekty se v Evropě dělí na čtyři kategorie: Nízká rizika, nízká až střední rizika, střední až vysoká rizika a vysoká rizika. Jejich střežení před nežádoucím vniknutím nepovolané osoby se zajišťuje pomocí zařízení elektrické zabezpečovací signalizace (EZS), jejíž složitost a náročnost na instalaci je úměrná kategorii objektu.

Cena připojení jednotlivých objektů na PCO se stanovuje individuálně a je ovlivňována mnoha skutečnostmi, například způsobem volby přenosu signálu nebo tím, je-li již elektronický zabezpečovací systém (EZS) zabudován, či nikoli.

6.1 Provedení zásahu

Důležitou podmínkou efektivní činnosti PCO je spolupráce s útvary zásahových skupin (ÚZS), které provádějí na podnět operátorů PCO výjezdy ke střeženým objektům. Dle charakteru a dostupnosti objektu se příslušníci ÚZS snaží po iniciaci z PCO dorazit k objektu v co nejkratším možném čase.

Ve smlouvě musí být přesně ujednáno, jak postupovat po ověření signálu a zjištění narušení objektu. Některé bezpečnostní agentury nabízejí i zákrok vlastní výjezdovou skupinou. Ta provede nejprve rekognoskaci objektu a v případě zjištění napadení objektu přivolání policie, hasičů, první pomoci. U bezpečnostní služby mohou být uloženy v zapečetěné schránce i klíče od objektu a dojednána kontrola vnitřních prostor pro ověření hlášených stavů. Následně je pak informován uživatel či jeho pověřený servisní pracovník uvedený ve smlouvě. O všech výjezdech či zákrocích je veden písemný záznam. Provozovatelé PCO bývají zapojeni do integrovaného záchranného systému.

Zásahové jednotky

Jejich zaměstnanci procházejí permanentním výcvikem, jehož náplní je zvládání zákroků, fyzická připravenost, ovládání motorových vozidel, střelecký výcvik. Kromě provádění zásahů na objektech střežených prostřednictvím PCO posilují fyzickou ochranu střeženého objektu, pokud ji nestačí strážný vyřešit vlastními silami. Podstatným způsobem tím zvyšují účinnost ostrahy.

6.2 Další nabízené služby

Provozující bezpečnostní služba bývá často i přímým dodavatelem celého zabezpečovacího systému včetně jeho projektu dle zadání uživatele. Při takovémto smluvním vztahu jsou dodávané služby rozšířeny o servis a údržbu, včetně potřebných revizí a předepsaných prohlídek technických zařízení. V případě přenosu informací z MaR na PCO informuje dispečer okamžitě uživatelův HELPDESK, případně servis, o došlých varovných hlášeních.

6.3 Závěry a poznatky ze Setkání výrobců a provozovatelů PCO ze dne 24. 2. 2009 konaném na výstavě Pragoalarm

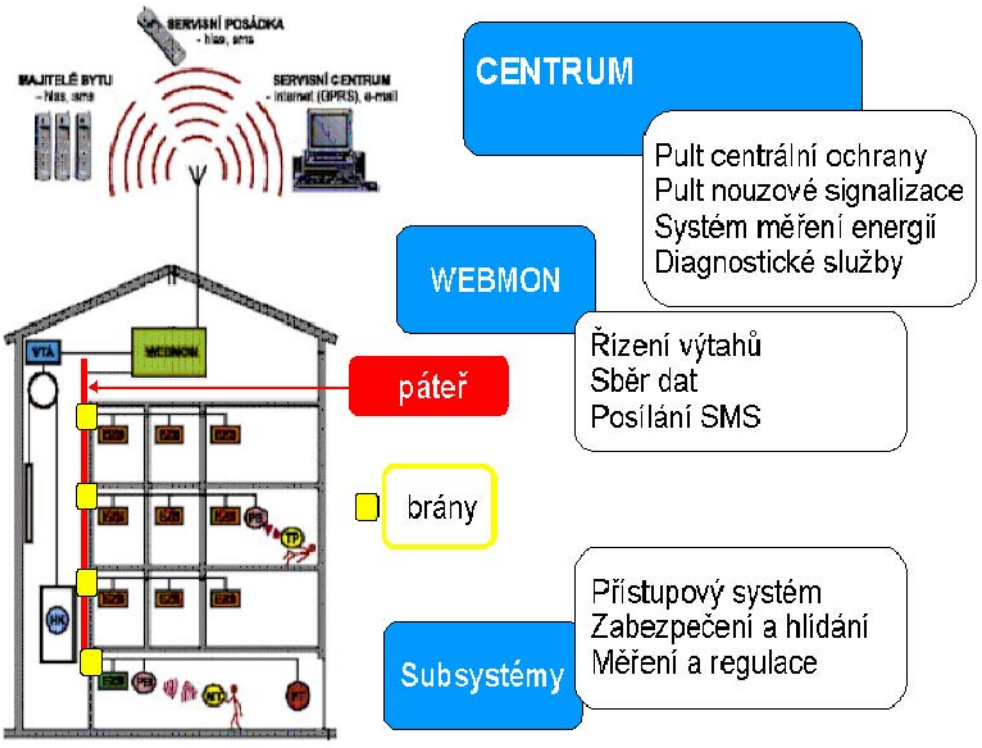
Ve dnech 24.2.-26. 2. 2009 se Český klub bezpečnostních služeb, o.s. prezentoval na 17. mezinárodním veletrhu PRAGOALARM/PRAGOSEC 2009, jehož byl odborným garantem. V rámci doprovodného programu Pragoalarmu proběhl mimo jiné i odborný seminář na téma " SEZNAM PROVOZOVATELŮ A VÝROBCŮ PULTŮ CENTRÁLNÍ OCHRANY". Semináře se zúčastnilo 21 firem z celé ČR, které provozují či se zajímají o PCO. Jako výrobce se prezentovaly dvě firmy, a to NAM SYSTÉM a RADOM. Seminář

doplnili svou přednáškou kolegové a hosté z Polska, kteří jsou stejně jako ČKBS, o.s. členové ESBOCu. [21]

Z jednotlivých prezentací:

V moderních budovách se objevuje množství nových technických systémů, které řeší jednotlivé funkce stavby. Vedle vlastního systému, jenž musí umět danou funkci splnit, je velmi důležité jeho provozování, které musí splňovat ekonomické, energetické, ekologické i legislativní požadavky. Způsob provozování určitého systému je podmíněn možnostmi jeho regulace a řízení. Jednotlivé funkce inteligentní budovy lze rozdělit do skupin podle účelu. Je zřejmé, že pojem inteligentní budova neznamená integraci všech funkcí, ale v jednotlivých typech budov se použijí pouze relevantní funkce. Základní skupiny funkcí inteligentních budov, nazývané služby, jsou energetické a ekologické, komfortní, bezpečnostní, dopravní, sociální, zábavní, komerční.

Právě zde se objevuje velký prostor pro aplikace v oblasti moderních technologií, umožňující přenos a zpracování velkého množství dat. Není velkým technickým problémem algoritmizovat standardní regulační zásahy na jednotlivých systémech a moderní systémy vybavené regulací se tak mohou do jisté míry chovat autonomně na základě podnětů senzorů regulačního systému. Toto chování jednotlivých systémů dalo základ pojmu Inteligentní budova. Inteligentní budova v dnešním pojetí je budova



Obr. 10: Schéma „Inteligentní budovy“

vybavená sjednoceným řízením jednotlivých funkčních systémů – vytápění, větrání, zabezpečení atd. „Inteligence“ budovy se projevuje například tím, že si jednotlivé systémy takto řízené, navzájem nekonkurují. [6,31]

Bezpečnostní služby

Kategorie bezpečnostních služeb je asi nejrozvinutější oblastí v řízení inteligentních budov. Patří sem systémy monitorování vstupu osob do objektu, pohybu osob v objektu, dále pak systémy protipožární ochrany a zabezpečení proti havarijním stavům jednotlivých technických systémů. Díky tomu, že bezpečnostní služby v oblasti ochrany budovy před nezvanými návštěvníky mají, narozdíl od ochrany před technickými poruchami, za soupeře člověka, jenž se snaží tyto systémy obelstít, je to jedna z nejrychleji rozvíjejících se oblastí. Jmenovat lze například systémy pro identifikaci člověka na základě analýzy oka, slin nebo otisku prstu.

V roce 2001 se na trhu objevil systém LATIS, který díky platformě Windows mohl pracovat ve větším rozsahu než předchozí systémy. První velkou výhodou byl přenos dat po různých komunikačních kanálech. LATIS je schopen komunikovat s objekty prostřednictvím různých rádiových sítí (nejen rádiové sítě vlastní produkce), prostřednictvím sítí mobilních operátorů (SMS, GPRS). Využívá také telefonní linky pro komunikaci pomocí veřejných protokolů (4+2, Contact ID) nebo využívá vlastní šifrovaný přenos po telefonních linkách. LATIS komunikuje také prostřednictvím sítí LAN, WAN apod. Další výhodou, zvláště u rozsáhlých objektů, je práce s grafickými podklady. V grafickém prostředí získává operátor nové možnosti a jeho představa o dění v objektu a možnosti ovládání technologií nabývají zcela jiných rozměrů. Další velkou změnou byla modularita systému, kdy se již systém nezabýval jen zabezpečovacími technologiemi. Do systému LATIS se již začaly připojovat systémy pro řízení osvětlení, systémy pro měření vlhkosti, teploty apod. V této etapě se již systém LATIS začal využívat nejen jako pult centrální ochrany, ale také jako lokální nadstavba. Tímto se LATIS® přiblížil k definici pojmu „Inteligentní budova“.

Od roku 2006 je k dispozici systém LATIS SQL, který vzešel ze svého předchůdce LATIS a převzal od něj všechny výhody, které lze využít jak pro PCO, tak pro lokální

nadstavby. Díky novým možnostem využití databází se stává LATIS SQL nástrojem pro rozsáhlé systémy.

Nastupuje další etapa – centralizace systémů ve všech oborech. Na větších objektech se objevuje vedle systémů EZS a EPS také klíčové hospodářství, systém kontroly vstupu (označován zkratkou SKV, EKV nebo ACS), docházka, stravování, rozhlas, řízení parkovacího provozu, kamerové systémy (CCTV), vytápění, klimatizace, vzduchotechnika, výtahy, osvětlení, ovládání žaluzií, čerpadla, obecně systém měření a regulace (MaR) a další speciální technologie, které chce uživatel v co největší míře automatizovat a pod dohledem obsluhy ovládat. Mezi takové speciální technologie patří například perimetrická ochrana. Ta zajišťuje ochranu objektu pomocí speciálních kabelů instalovaných např. na plotových jednotkách. Tyto systémy jsou velmi přesné a dokážou např. identifikovat na plotu o délce několika kilometrů s přesností na jeden metr otřesy způsobené osobou, která se snaží překonat plot. Přitom silný vítr, který „lomcuje“ s plotem, poplach nevyvolá. Do perimetrických systémů lze také zařadit elektrické závory, ty ovšem bývají většinou součástí EZS.

Na trhu je obrovská spousta technologií od různých výrobců. Je těžké se orientovat v této spoustě technologií, a proto jsou v rozsáhlejších komplexech využíváni specialisté, kteří se zabývají pouze problematikou centralizace, monitorování a řízení jednotlivých technologií.

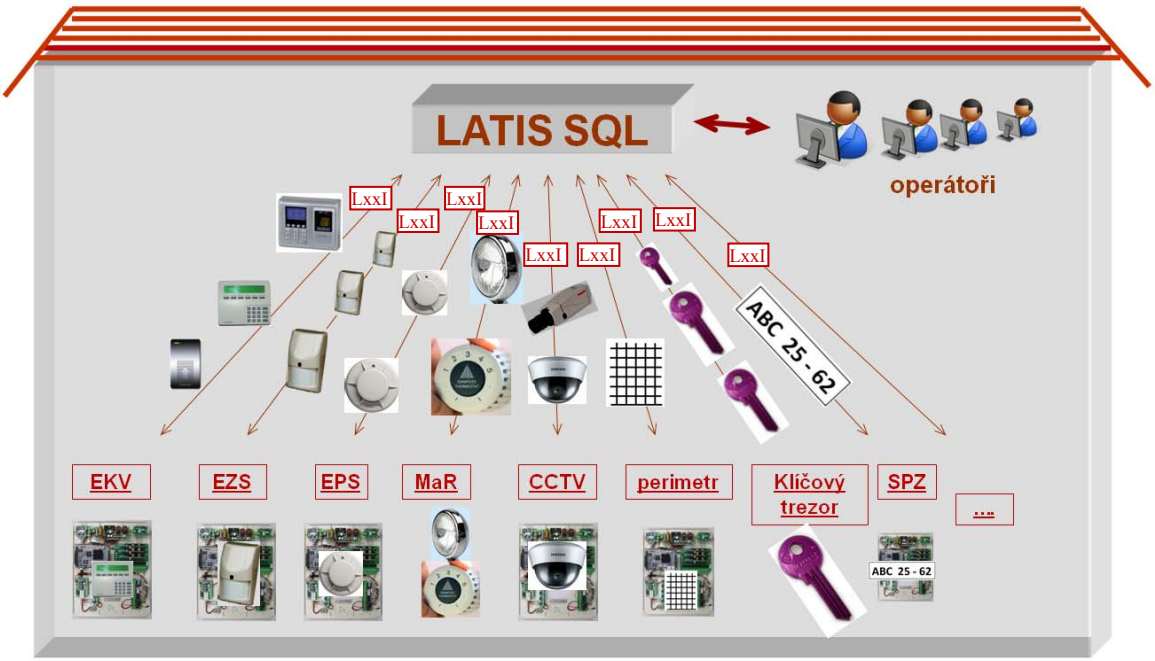
Co je vlastně důležité pro zabezpečení větších komplexů? Velmi důležitým krokem je počáteční rozhodnutí: co všechno chce uživatel monitorovat, řídit, vyhodnocovat a hlavně v jakém rozsahu. Nejedná se jen o typ technologie a o počet připojených prvků v systému, ale také o to, jaké informace je schopna tato technologie předat, v jaké formě a jaké povely může daná technologie přijmout, případně vykonat. U těchto technologií je také velmi důležité, jakým způsobem lze systém zálohovat pro případ výpadku technologie nebo výpadku napájení apod.

LATIS SQL jako pult centrální ochrany

Jádrem systému je Microsoft SQL Server 2005. Software, kterým se definují téměř všechny parametry systému, je zaveden pod názvem LAT – administrační nástroj (Latis Administration Tools). Jde o nástroj síťový a je možné s ním pracovat kdekoli v rámci sítě

LAN. Program pro obsluhu LOW – pracoviště výkonného operátora (Latis Operator Workstation) je opět síťový nástroj, který lze připravit pro operátora podle požadavků uživatele – operátorských pracovišť může být v systému libovolné množství a každé z těchto pracovišť může sledovat stejné nebo různé množství informací. Každý z operátorů může mít přidělena zvláštní práva pro ovládání technologií apod. Služba LAOM – modul automatických činností (LATIS Automatic Operation Module) se stará o všechny automatické operace, které systém musí kontrolovat a vykonávat (hlídání doby střežení, odesílání automatických povelů apod.). Služba LMG – centrum připojení modemů (Latis Modem Gateway) zajišťuje spojení s HW modemy, které komunikují s objekty. Program LDE (Latis Data Export) řeší veškeré exporty z databáze do formátu pdf, csv nebo přímo na tiskárnu.

Velkým plusem systému jsou tzv. zásuvné moduly (pluginy). Tyto moduly mohou být v libovolném množství vloženy do systému podle potřeb uživatele na jakékoli místo v systému. Jádro systému zůstává zachováno jako pevná kostra a uživatelský zásuvný modul se může „vložit“ k operátorskému pracovišti jako speciální aplikace pro práci s technologií, kterou vlastní např. pouze jeden uživatel. Celý systém je postaven jako stavebnice, kterou lze poskládat podle požadavků konečného uživatele a není nutné jej instalovat jako celek se všemi funkcemi. [24]



Obr. 11: Schéma LATIS SQL systému

7. Legislativní rámec provozování PCO

Z důvodu neexistence plnohodnotného zákona o provozování bezpečnostních služeb v ČR se činnosti bezpečnostních agentur a dalších subjektů zabývajících se provozováním koncesované živnosti ostraha majetku a osob řídí především zákonem 455/1991 o živnostenském podnikání, rozvedeném vyhláškou č. 16 ze dne 8. ledna 2009. Podniky, které na základě Přílohy č. 3 k živnostenskému zákonu - Koncesované živnosti, skupiny 314, zajišťují ostrahu majetku a osob, musí splňovat specifické podmínky (odborná způsobilost, bezúhonnost všech zaměstnanců, případně další stanovené v koncesní listině). Odbor pro místní správu zastává právní názor, že v případě napadení objektů zařazených do systému elektronické ochrany musí případný zákrok provést určení zaměstnanci podniků, zajišťující jejich ochranu (nikoliv strážníci obecní policie). Podnik zajišťující ochranu osob a majetku musí být technicky a personálně vybaven tak, aby byl schopen dostát všem závazkům vyplývajícím z předmětu jeho činnosti. Pokud konkrétní situace výjimečně přesáhne kapacitní možnosti daného subjektu, lze se v souladu s platnou právní úpravou obrátit na Policii ČR, eventuálně na strážníky obecní policie.

V souladu se zákonem ČNR č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů (dále jen „zákon o obecní policii“) jsou obecní (městské) policie zřizovány obecně závaznou vyhláškou za účelem zabezpečování místních záležitostí veřejného pořádku. Zákon o obecní policii ve svém ustanovení § 2 uvádí demonstrativní výčet činností strážníků obecní policie při zabezpečování místních záležitostí veřejného pořádku. Z obsahu písm. a) cit. ustanovení sice vyplývá, že strážníci přispívají k ochraně a bezpečnosti osob a majetku, nicméně s odkazem na obsah ustanovení § 35 odst. 2 zákona č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů a s přihlédnutím k ustanovení § 84,85 a 102 cit. zákona, nelze považovat nepřetržitou ochranu majetku právnických či fyzických osob (za úplatu), za plnění úkolů obce v samostatné působnosti, resp. za zabezpečování místních záležitostí veřejného pořádku, neboť obce podle zákona o obcích nenesou odpovědnost za majetek svých občanů.

Provozování PCO a souvisejících služeb tedy musí splňovat zejména požadavky na provozování koncesované činnosti „ostraha majetku a osob“ v následujícím rozsahu :

Ostraha majetku a osob

Koncesovaná živnost ostraha majetku a osob zahrnuje poskytování služeb spojených s ostrahou a ochranou nemovitého a movitého majetku, ostrahou při přepravě peněz a jejich zpracování, cenností či jiného majetku, ochranou osob a právních zájmů, se zajišťováním pořádku v místech konání veřejných shromáždění, slavností, sportovních podniků nebo lidových zábav podle pokynu objednatele, vyhodnocováním bezpečnostních rizik a provozováním centrálních pultů ochrany.

Požadovaná odborná a jiná zvláštní způsobilost podle § 27 odst. 1 a 2 ŽZ

a) vysokoškolské vzdělání nebo vyšší odborné vzdělání právnického, bezpečnostního nebo obdobného zaměření,

b) střední vzdělání s maturitní zkouškou v oboru bezpečnostním nebo právním a 3 roky praxe,

c) střední vzdělání s maturitní zkouškou a osvědčení o odborné kvalifikaci pro příslušnou pracovní činnost vydané s platností na 5 let zařízením akreditovaným podle zvláštních právních předpisů Ministerstvem školství, mládeže a tělovýchovy, za podmínek stanovených zvláštním právním předpisem a 3 roky praxe, za příbuzný obor lze považovat službu u Policie České republiky, obecní policie, Justiční stráže, Vojenské policie atd.

Podmínky, jejichž splnění se vyžaduje podle § 27 odst. 3 ŽZ spolehlivost podnikatele, statutárního orgánu a členů statutárního orgánu, bezúhonnost a odborná způsobilost zaměstnanců (§ 6a odst. 3, § 31a a příloha č. 5 zákona č. 455/1991 Sb., ve znění zákona č. 274/2008 Sb.).

Odbornou způsobilost stanoví Vyhláška ze dne 8. ledna 2009 o obsahu a rozsahu kvalifikace pro výkon fyzické ostrahy a služby soukromého detektiva. Zdravotní způsobilost fyzické osoby zjišťuje a posudek o zdravotní způsobilosti vydává posuzující lékař na základě výsledku lékařské prohlídky, psychologického vyšetření a dalších potřebných vyšetření. Posuzujícím lékařem se pro účely tohoto zákona rozumí praktický lékař, u kterého je fyzická osoba registrovaná k léčebné péči.

Ministerstvo zdravotnictví ve spolupráci s Ministerstvem vnitra stanoví vyhláškou způsob provádění, formu a obsah psychologického a lékařského vyšetření, obsah psychologického posudku a lékařské zprávy a seznam tělesných a duševních vad, nemocí nebo stavů, které vylučují zdravotní způsobilost pro výkon činností podle odstavce 2.

Služby soukromých detektivů

Na udělení koncese se vztahuje § 1 odst. 5 zákona č. 451/1991 Sb. (lustrační zákon).

Podnikatel provozující koncesovanou živnost ostraha majetku a osob nebo služby soukromých detektivů je povinen zajistit, aby tyto činnosti vykonávali zaměstnanci odborně a zdravotně způsobilí.

Všeobecné podmínky provozování živnosti

(1) Všeobecnými podmínkami provozování živnosti fyzickými osobami, pokud tento zákon nestanoví jinak, jsou:

a) dosažení věku 18 let,

b) způsobilost k právním úkonům,

c) bezúhonnost.

Bezúhonným pro provozování koncesovaných živností ostraha majetku a osob, služby soukromých detektivů a poskytování technických služeb k ochraně majetku a osob podle tohoto zákona není ten,

a) kdo byl pravomocně odsouzen pro úmyslný trestný čin nebo byl v posledních 5 letech pravomocně odsouzen pro trestný čin spáchaný z nedbalosti, jestliže jeho jednání, kterým spáchal trestný čin, je v rozporu s předmětem této podnikatelské činnosti,

b) jehož trestní stíhání pro úmyslný trestný čin bylo na základě pravomocného rozhodnutí o schválení narovnání zastaveno a od tohoto rozhodnutí ještě neuplynulo 5 let, je-li jednání, kterým spáchal trestný čin, v rozporu s předmětem této podnikatelské činnosti,

c) jehož trestní stíhání pro úmyslný trestný čin bylo pravomocně podmíněně zastaveno a od uplynutí zkušební doby nebo lhůty, v níž má být rozhodnuto, že se osvědčil, neuplynulo ještě 5 let, nebo bylo v trestním řízení, které bylo proti němu vedeno, rozhodnuto o podmíněném odložení podání návrhu na potrestání a od tohoto rozhodnutí ještě neuplynulo 5 let, je-li jednání, kterým spáchal trestný čin, v rozporu s předmětem této

podnikatelské činnosti,

d) kdo v čestném prohlášení podle odstavce 4 uvede nesprávné údaje nezbytné pro posouzení bezúhonnosti.

(4) Bezúhonnost žadatele o vydání koncesní listiny podle odstavce 3 písm. a) se prokazuje výpisem z Rejstříku trestů 25b), který nesmí být starší 3 měsíců. Bezúhonnost podle odstavce 3 písm. b) a c) prokazuje žadatel o vydání koncesní listiny čestným prohlášením, které nesmí být starší 3 měsíců.

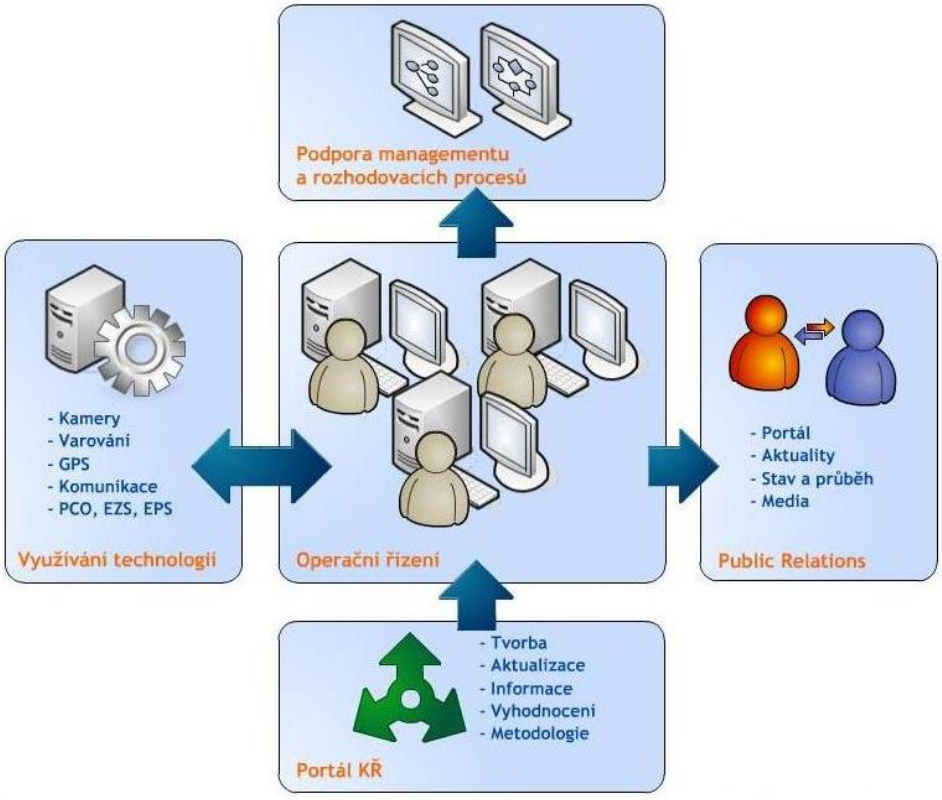
(5) Uchazeč o zaměstnání nebo zaměstnanec je povinen podnikateli nebo osobě, která jedná za podnikatele v pracovněprávních vztazích, do 15 dnů písemně oznámit, že proti němu bylo zahájeno trestní stíhání. K oznámení připojí kopii usnesení o zahájení trestního stíhání nebo v oznámení uvede výrok tohoto rozhodnutí, včetně označení orgánu, který jej vydal. [19,15]

Bezpečnostní agentury, provozující ostrahu objektů a majetku jsou v ČR sdruženy do profesních organizací Český klub bezpečnostních služeb (ČKBS) a Asociace soukromých bezpečnostních služeb (ASBS). Tyto organizace se kromě platné legislativy řídí i vlastními etickými kodexy. V těch jsou obsaženy zejména morální a profesní zásady chování vůči zákazníkům a zásady etiky jednání v dodavatelsko odběratelských vztazích, vztazích mezi sociálními partnery v oboru aj. Kodex zároveň informuje odbornou i laickou veřejnost o zásadách a normách, které společnosti a podnikatelé dobrovolně přijali a hodlají je akceptovat prostřednictvím etické samoregulace.

Obr. 12: Loga profesních svazů

8. Vyhodnocovací aplikace

Nadstavbou koncových zařízení PCO se zabývají programátoři. Převážně pod windows (ale i jinými operačními systémy) vznikají účelově komponované aplikace. Dispečeři a operátoři PCO tak získávají v přehledných formách všechny potřebné informace k řešení kritických situací. K tomuto účelu jsou například vedeny karty objektů, na nichž jsou rozepsány základní potřebné údaje. V další úrovni jsou k dispozici pokyny, jak reagovat na detekovanou situaci. Dalším podpůrným prostředkem je vizualizace objektů. V půdorysných plánech tak mají operátoři k dispozici rozmístění všech instalovaných detektorů. Rovněž jsou vizualizovány instalované technologie včetně jejich ovládacích a regulačních prvků. Takovéto vyhodnocovací aplikace již ovšem kladou i vyšší nároky na obsluhu PCO. Proto bezpečnostní agentury, kromě řešení na klíč, provádějí pravidelné doškolování pracovníků těchto specializovaných pracovišť.



Obr. 13: Přínosy použití PCO

9. Závěr

V dnešní době jsou již na trhu bezpečnosti a ochrany majetku dostupné i zahraniční systémy. Přesto se v ČR více uplatňují domácí dodavatelé komplexních řešení. Je to především z důvodu znalosti prostředí a vývoje tohoto odvětví v závislosti na změně politicko-ekonomických podmínek po roce 1989. Vývoj a aplikace byly podmíněny technickými možnostmi přenosů informací k poskytovatelům služeb. Do roku 1990 převažovala JTS a její spolehlivost nebyla zárukou bezporuchového provozu PCO. Proto značná část provozovatelů upřednostňovala radiovou síť. Linky ISDN se zaváděly pomalu a v tomto druhu přenosu jsme značně zaostali za ostatním světem.

Nyní se již využívají kombinace více druhů přenosů a tím se zajišťuje vysoká spolehlivost.

BA, provozující PCO, rozšiřují nabídku služeb a zejména provozovatelé malých a středních objektů využívají těchto služeb k zefektivnění svých provozů. Ve velkých objektech jsou zřizována bezpečnostní a technologická pracoviště s nepřetržitým provozem (VELÍN). Tato pracoviště bývají zapojena do sítě a tím se zkvalitní a zrychlí nasazení potřebných odborníků v dotčeném objektu. Takovéto celky označujeme pojmem „inteligentní budovy“.

Základním kritériem pro zhodnocení přínosu takovýchto kontrolních a zabezpečovacích pracovišť je doba a kvalita reakce při alarmových situacích. Inteligentní budovy využívají svých „velínů“ pro zajišťování i dalších technologií, potřebných pro celkový chod objektu. Odtud jsou sledovány a mohou být i ovládány provozy výtahů, vzduchotechniky a klimatizací, záložních zdrojů napájení a dalších provozovaných technologií. Rovněž pracovníci útvaru bezpečnosti získávají přehled o pohybu osob, přístupech na pracoviště se zvláštním režimem, obsazenosti garáží atd. Monitorovací pracoviště jsou svým efektivním provozem jednoznačně přínosem pro všechny dohledované celky. Další centralizací monitoringu, specializací poskytovaných služeb a síťovým propojením těchto pracovišť lze dosáhnout vyšší operativnosti a tím i provozních úspor.

Obecným nedostatkem lze snad označit jen skutečnost, že na všech takovýchto pracovištích, provozovaných třetí osobou, jsou k dispozici citlivá data objednatele. Tato skutečnost je však ošetřena smluvně a má oporu i v legislativě.

10. Použitá literatura, zdroje:

[1] BISHOP, O.: *Zabezpečovací zařízení vhodná i ke stavbě svépomocí.* SPN 621.3 Ostrava : 1993

[2] FRÝBA, J.: *Vliv technologií inteligentních budov na zajištění bezpečnosti objeků.* Metodická pomůcka Profesis MP 1.6, IC ČKAIT. Praha : 2008

[3] GUTMAN, J, NĚMEC, P, : *Bezpečný dům Beta Control*. Prezentace Pragoalarm : 2009

[4] HRADECKÝ, Z.: *Řídící systémy objektů*. Diplomová práce. Ostrava : VŠB-TU, 2005

[5] HRADECKÝ, Z.: *Integrace poplachových systémů*. Bakalářská práce. Ostrava : VŠB-TU, 2004

[6] KABELE, K.: *Koncept inteligentních budov.* Prezentace Pragoalarm : 2009

[7] KŘEČEK, S.: *Ochrana majetku systémy průmyslové televize.* GRADA Publishing : 1996. ISBN 80-7169-402-9

[8] PANÁČEK, R.: *Vliv technologií inteligentních budov na zajištění bezpečnosti objektů.* Prezentace Pragoalarm : 2009

[9] UHLÁŘ, J.: *Technická ochrana objektů I. díl.* PA ČR Praha : 2004 . ISBN 80-7251-172-6

[10] UHLÁŘ, J.: *Technická ochrana objektů II. díl.* PA ČR Praha : 2005 . ISBN 80-7251-189-0

[11] UHLÁŘ, J.: *Technická ochrana objektů III. díl.* PA ČR Praha : 2006 . ISBN 80-7251-235-8

[12] VYORÁLEK, R.: *Pulty centralizované ochrany*. Bakalářská práce. Zlín : UTB-FT, 2005

[13] ZAHRÁDKA, J.: *Začínáme s EZS*. Příručka VARIANT plus. Třebíč : 2005

[14] Normy ČSN 50131

[15] Sbírka zákonů ČR

[16] Internetové stránky společnosti ADI : http://www.adi-olympo.cz/

[17] Internetové stránky společnosti AGENCY RS : http://www.agencyrs.cz/cs/

[18] Internetové stránky společnosti AMBO : http://www.ambo.cz/

[19] Internetové stránky společnosti ASBS : http://www.asbs.cz/

[20] Internetové stránky společnosti BARA HK : http://www.barahk.cz/

[21] Internetové stránky společnosti BETACONTROL http://www.betacontrol.cz/

[22] Internetové stránky společnosti ČKBS : http://www.ckbs.cz/

[23] Internetové stránky společnosti EUROSAT : http://www.eurosat.cz/paradox/

[24] Internetové stránky společnosti FENIX : http://www.fenix-security.cz/

[25] Internetové stránky společnosti FIDES http://www.fides.cz/cs/

[26] Internetové stránky společnosti KELCOM http://www.kelcom.cz/novinky.asp

[27] Internetové stránky společnosti NAM system : http://www.nam.cz/

[28] Internetové stránky společnosti PCO VIDOCQ : http://www.pcovidocq.cz/

[29] Internetové stránky společnosti RADOM : http://www.radom.eu/

[30] Internetové stránky společnosti SIEMENS, s.r.o. divize technologie budov http://www.siemens.cz/siemjet/cz/home/sibt/Main/index.jet

[31] Internetové stránky společnosti WIKIPEDIE http://cs.wikipedia.org/

Seznam zkratek:

PCO = pult centralizované ochrany

EZS = elektronická zabezpečovací signalizace

CCTV = (closed circuit television) uzavřený kamerový systém

SKV = systém kontrolovaného vstupu

EPS = elektronická požární signalizace

MaR = měření a regulace

JTS = jednotná telefonní síť

GSM = **G**lobální **S**ystém pro **M**obilní komunikaci

GPRS = (general packet radio service) mobilní datová služba

BTS = (base transfer station) základová stanice

BPO = bezpečnostní posouzení objektu

LAT = (Latis Administration Tools)

Seznam obrázků:

Seznam příloh:

11. Přílohy

Příloha č.1

Etický kodex člena klubu

1. Cíl a působnost Kodexu etiky

1.1.Cíl

Vydání Kodexu etiky sleduje šíření pojmu dobrých obchodních zvyklostí podle Obchodního zákoníku doplněné o specifické požadavky na chování provozovatelů a zaměstnanců soukromých bezpečnostních služeb ve vztahu k zákazníkům, jiným soukromým nebo veřejnoprávním bezpečnostním službám, k sociálním partnerům atd.

1.2.Působnost

Kodex je určen všem subjektům působícím v oboru ochrany majetku a osob a je závaznou normou chování pro členy ČK SBDS a jejich zaměstnance. Kodex zároveň informuje odbornou i laickou veřejnost o zásadách o normách, které společnosti a podnikatelé dobrovolně přijali a hodlají je akceptovat prostřednictvím etické samoregulace.

2. Vztahy k zákazníkům

2.1. Členové Českého klubu SBDS dodržují ve vztazích se zákazníky následující pravidla:

- svojí podnikatelskou činností poskytují zákazníkům formou dodávky výrobků nebo služeb optimální ochranu majetku a osob
- nikdy nezneužijí odborné neznalosti zákazníka, poskytnou pravdivé informace a seznámení jej s možnostmi kvalitního, komplexního a systémového přístupu k zajištění ochrany majetku a osob
- ve svých nabídkách, projektech, výrobcích a službách nabízejí vždy dobrou kvalitu odpovídající potřebě zákazníka a jeho možnostem

2.2. Morální a profesní zásady etického chování zaměstnanců:

- uplatňují zdvořilé jednání, korektní přístup k zákazníkům, jeho zaměstnancům i hostům
- poskytují odborné, nezkreslené informace o bezpečnostní situaci u zákazníka a navrhují opatření k odstranění nedostatků nebo náměty na zvýšení bezpečnosti
- při poskytování služeb se považují za součást podniku a jeho bezpečnost zajišťují s maximální odpovědností
- zachovávají mlčenlivost o všech skutečnostech, se kterými se seznámí u zákazníka, a to i po skončení smluvního vztahu

- plní své povinnosti s vědomím, že jejich profesionální výkon je též vizitkou zákazníka
- nezneužívají svých odborných znalostí a dovednosti ke škodě zákazníka ani jeho zaměstnanců nebo obchodních partnerů

3. Vztahy mezi zaměstnavateli a zaměstnanci

3.1. Zaměstnavatelé, ať společnosti nebo podnikatelé, ve vztahu k zaměstnancům:

- chovají se jako dobrý zaměstnavatel, který respektuje zákonná práva zaměstnanců a dle možností firem řeší jejich opodstatněné požadavky
- vytváří systematicky pracovní podmínky pro odborný a bezpečný výkon pracovní činnosti
- organizují zvyšování odbornosti jako podmínku kvalifikovaného poskytování služeb a zabezpečení jejich kvality
- respektují opodstatněné náměty, připomínky a požadavky sociálního partnera

3.2. Zaměstnanci a jejich zástupci ve vztahu k zaměstnavatelům ctí tyto zásady:

- svědomitě plní pracovní povinnosti s vědomím odpovědnosti za bezpečnost svěřeného majetku, života a zdraví osob
- reprezentují firmu dobrou prací a svým chováním, práci u zákazníka i na veřejnosti chápou jako záruku rozvoje a prosperity firmy, a tím uspokojují i své potřeby
- jsou loajální k zaměstnavateli, zejména nezneužívají firemní prostředky, znalosti související s firmou ani své odborné dovednosti ku prospěchu svému nebo třetí osoby
- vyvarují se jednání, které by jakkoli ohrozilo plnění smluvního vztahu se zákazníkem nebo ohrozilo pověst firmy v očích veřejnosti

4. Vztahy mezi bezpečnostními službami

4.1. Vztahy mezi členskými firmami jsou motivovány příslušností k profesnímu sdružení a z něho vyplývajícími společnými zájmy. V obchodní konkurenci a soutěži platí, že:

- v hospodářské soutěži respektují zákonná pravidla a uznávají dobré obchodní zvyklosti
- vzájemnou soutěž vedou čestnými a poctivými prostředky a zdržují se jednání, která jsou v rozporu s dobrými mravy
- veškerou reklamu vedou pravdivě, nepoužívají metodu srovnávání se s jinými firmami nebo negativního komentování jejich výrobků či služeb
- v hospodářské soutěži preferují vyváženost kvality v porovnání s cenou ve vztahu k potřebám zákazníka a jeho možnostem

4.2. Vztahy členských firem k veřejnoprávním bezpečnostním službám se řídí těmito zásadami:

- ve všech ohledech je respektována úloha a postavení těchto služeb, členové ČK SBDS pracovníkům těchto složek pomáhají v jejich záslužné činnosti
- členové ČK SBDS se cítí být součástí celospolečenského systému prevence kriminality a přispívají k prevenci ve střežených objektech a jejich okolí
- účinnou spolupráci s veřejnoprávními službami na úseku prevence kriminality aj. závadové činnosti považují za svojí občanskou povinnost a otázku profesní cti

V Praze dne 3. 4. 2007 Prezidium ČKBS

Příloha č. 2

Kodex etiky

1. Úvod

Kodex nenahrazuje právní regulaci ochrany majetku a osob, nýbrž na ni navazuje deklarací zásad etiky chování v dodavatelsko odběratelských vztazích, vztazích mezi sociálními partnery v oboru aj..

1.1. Cíl

Vydání Kodexu etiky sleduje šíření pojmu dobrých obchodních zvyklostí podle Obchodního zákoníku doplněné o specifické požadavky na chování provozovatelů a zaměstnanců soukromých bezpečnostních služeb ve vztahu k zákazníkům, jiným soukromým nebo veřejnoprávním bezpečnostním službám, k sociálním partnerům atd.

1.2. Působnost

Kodex je určen všem subjektům působícím v oboru ochrany majetku a osob a je závaznou normou chování pro členy Asociace a jejich zaměstnance. Kodex zároveň informuje odbornou i laickou veřejnost o zásadách a normách, které společnosti a podnikatelé dobrovolně přijali a hodlají je akceptovat prostřednictvím etické samoregulace.

2. Vztahy k zákazníkům

2.1. Členové Asociace dodržují ve vztazích se zákazníky následující pravidla:

Svojí podnikatelskou činností poskytují zákazníkům formou dodávky výrobků nebo služeb optimální ochranu majetku a osob.

Nikdy nezneužijí odborné neznalosti zákazníka, poskytnou pravdivé informace a seznámí jej s možnostmi kvalitního, komplexního a systémového přístupu k zajištění ochrany majetku a osob.

Ve svých nabídkách, projektech, výrobcích a službách nabízejí vždy dobrou kvalitu odpovídající potřebě zákazníka a jeho možnostem.

2.2. Morální a profesní zásady etického chování zaměstnanců:

Uplatňují zdvořilé jednání, korektní přístup k zákazníkům, jeho zaměstnancům i hostům. Poskytují odborné, nezkreslené informace o bezpečnostní situaci u zákazníka a navrhují opatření k odstranění nedostatků nebo předkládají náměty na zvýšení bezpečnosti. Při poskytování služeb se považují za součást podniku a jeho bezpečnost zajišťují s maximální odpovědností.

Zachovávají mlčenlivost o všech skutečnostech, se kterými se seznámí u zákazníka, a to i po skončení smluvního vztahu.

Plní své povinnosti s vědomím, že jejich profesionální výkon je též vizitkou zákazníka. Nezneužívají svých odborných znalostí a dovedností ke škodě zákazníka ani jeho zaměstnanců nebo obchodních partnerů.

3. Vztahy mezi zaměstnavateli a zaměstnanci

3.1. Zaměstnavatelé, ať společnosti nebo podnikatelé ve vztahu k zaměstnancům:

Chovají se jako dobrý zaměstnavatel, který respektuje zákonná práva zaměstnanců a dle možností firmy řeší též jejich opodstatněné požadavky.

Vytváří systematicky pracovní podmínky pro odborný a bezpečný výkon pracovní činnosti.

Organizují zvyšování odbornosti jako podmínku kvalifikovaného poskytování služeb a zabezpečení jejich kvality.

Respektují opodstatněné náměty, připomínky a požadavky sociálního partnera.

3.2. Zaměstnanci a jejich zástupci ve vztahu k zaměstnavatelům ctí tyto zásady:

Svědomitě plní pracovní povinnosti s vědomím odpovědnosti za bezpečnost svěřeného majetku, života a zdraví osob.

Reprezentaci firmy dobrou prací a svým chováním u zákazníka i na veřejnosti chápou jako záruku rozvoje a prosperity firmy a tím uspokojování svých potřeb.
Jsou loajální k zaměstnavateli, zejména nezneužívají firemní prostředky, znalosti související s firmou ani své odborné dovednosti ku prospěchu svému nebo třetích osob. Vyvarují se jednání, které by jakkoliv ohrozilo plnění smluvního vztahu se zákazníkem nebo ohrozilo pověst firmy v očích veřejnosti.

4. Vztahy mezi bezpečnostními službami

4.1. Vztahy mezi členskými firmami jsou motivovány příslušností k profesnímu sdružení a z něho vyplývajícími společnými zájmy. V obchodní konkurenci a soutěži platí, že:

V hospodářské soutěži, ve vyhlášených výběrových řízeních a vlastních nabídkových řízeních respektují zákonná pravidla v duchu dobrých mravů soutěže, bez možnosti přivodit újmu jinému soutěžiteli nebo zákazníkovi.

4.2. Vztahy členských firem k veřejnoprávním bezpečnostním službám se řídí těmito zásadami:

Ve všech ohledech je respektována úloha a postavení těchto služeb. Členové Asociace napomáhají pracovníkům těchto složek v jejich záslužné činnosti.

Členové Asociace se cítí být součástí celospolečenského systému prevence kriminality a přispívají k prevenci kriminality ve střežených objektech a jejich okolí.

Účinnou spolupráci s veřejnoprávními bezpečnostními službami na úseku prevence kriminality aj. závadové činnosti považují za svojí občanskou povinnost a otázku profesní cti.

V Praze dne 11. května 2006

JUDr. Jiří Kameník
president

VYHLÁŠKA

Příloha č. 3

ze dne 8. ledna 2009

o obsahu a rozsahu kvalifikace pro výkon fyzické ostrahy a služby soukromého detektiva

Ministerstvo vnitra stanoví podle § 73a odst. 2 zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění zákona č. 274/2008 Sb., (dále jen „zákon“):

§1

Předmět úpravy

Tato vyhláška upravuje

a) podmínky pro získávání odborné způsobilosti

1. k provozování koncesované živnosti ostraha majetku a osob a koncesované živnosti služby soukromých detektivů,

2. zaměstnance podnikatele provozujícího koncesovanou živnost ostraha majetku a osob nebo koncesovanou živnost služby soukromých detektivů,

fyzických osob, po nichž zákon vyžaduje osvědčení o odborné kvalifikaci pro příslušnou pracovní činnost,

b) způsob provádění zkoušky odborné způsobilosti k získání odborné kvalifikace osoby vykonávající činnost ostraha majetku a osob nebo osoby vykonávající činnost služby soukromých detektivů (dále jen „zkouška“)a

c) obsahovou náplň zkoušky.

§2

Podmínky pro získávání odborné způsobilosti

Podmínkou pro získání odborné způsobilosti k

a) provozování koncesované živnosti ostraha majetku a osob nebo koncesované živnosti služby soukromých detektivů, nebo

b) výkonu činnosti ostraha majetku a osob nebo k výkonu činnosti služby soukromých detektivů,

pro osobu uvedenou v § 1 písm. a) je složení zkoušky.

§3

Provádění zkoušky

(1) Zkoušku provádí autorizovaná osoba splňující podmínky podle jiného právního předpisu upravujícího uznávání výsledků dalšího vzdělávání[1]), která je zároveň akreditovaná Ministerstvem školství, mládežeatělovýchovy podle zákona o zaměstnanosti[2]) (dále jen „autorizovaná osoba“).

(2) Na provádění zkoušky se použijí obdobně ustanovení jiného právního předpisu upravujícího uznávání výsledků dalšího vzdělávání[1]), není-li dále stanoveno jinak.

(3) Zkouška se skládá v českém jazyce před tříčlennou zkušební komisí.

(4) Členem zkušební komise nemůže být osoba, která je zaměstnancem, statutárním orgánem nebo členem statutárního orgánu stejného podnikatele jako žadatel, ani podnikatel, který je zaměstnavatelem žadatele nebo pro kterého žadatel vykonává činnost ostraha majetku a osob nebo činnost služby soukromých detektivů.

§4

Přihláška ke zkoušce

(1) Přihláška ke zkoušce obsahuje tyto údaje žadatele: a) jméno, popřípadě jména, a příjmení, b) datum narození, c) adresu místa pobytu,

d) činnost, pro jejíž provozování nebo výkon se vykonání zkoušky žádá.

(2) Přihlášku ke zkoušce podává u autorizované osoby žadatel.

(3) S písemným souhlasem žadatele můžepřihlášku ke zkoušce podat i podnikatel provozující koncesovanou živnost ostraha majetku a osob nebo koncesovanou živnost služby soukromých detektivů.

[1]) Zákon č. 179/2006 Sb., o ověřování a uznávání výsledků dalšího vzdělávání a o změně některých zákonů (zákon o uznávání výsledků dalšího vzdělávání), ve znění pozdějších předpisů.

[2]) § 108 zákona č. 435/2004 Sb., o zaměstnanosti, ve znění zákona č. 382/2005 Sb.

§5

Obsahová náplň zkoušky

Obsahová náplň zkoušky je stanovena v kvalifikačních a hodnotících standardech zpracovaných podle jiného právního předpisu[1]) uveřejněných v Národní soustavě kvalifikací

a) pro dílčí kvalifikaci strážný, jde-li o provozování živnosti nebo výkon činnosti ostraha majetku a osob, nebo

b) pro dílčí kvalifikaci detektiv koncipient, jde-li o provozování živnosti nebo výkon činnosti služby soukromých detektivů.

§6

Další náležitosti osvědčení o odborné kvalifikaci

(1) Žadateli, který u zkoušky prospěl, vydá autorizovaná osoba osvědčení o odborné kvalifikaci, které musí mimo údajů uvedených v jiném právním předpise[3]) dále obsahovat tyto údaje:

a) evidenční číslo osvědčení, b) název činnosti odpovídající předmětu podnikání, pro který je osvědčení o odborné kvalifikaci vydáváno.

(2) Osvědčením o odborné kvalifikaci se pro účely této vyhlášky rozumí osvědčení o získání dílčí kvalifikace, které není starší 5 let, bylo vydáno autorizovanou osobou a splňuje náležitosti podle odstavce 1.

§7

Účinnost

Tato vyhláška nabývá účinnosti dnem jejího vyhlášení.

Ministr:

MUDr. Mgr. **Langer** v. r.

[3]) § 19 zákona č. 179/2006 Sb.