Dohledové a poplachové přijímací centrum a jeho specifika v sektoru soukromé bezpečnosti

Bc. Ivan Hruška, DiS.

Diplomová práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Ivan Hruška, DiS.**
Osobní číslo:	**A12343**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Dohledové a poplachové přijímací centrum a jeho specifika v sektoru soukromé bezpečnosti**
Téma anglicky:	**Surveillance and Alarm Receiving Centers and Their Applications in Private Security**

Zásady pro vypracování:

1. **Vysvětlete technické řešení dohledového a poplachového přijímacího centra.**
2. **Vyjmenujte možnosti přenosu poplachového signálu od střeženého objektu.**
3. **Proveďte analýzu uplatnění dohledového a poplachového přijímacího centra na trhu komerční bezpečnosti.**
4. **Popište legislativní úpravu dohledového a poplachového přijímacího centra.**
5. **Analyzujte rozdílné podmínky v provozování dohledového a poplachového přijímacího centra v sektoru soukromé bezpečnosti.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KAMENÍK, Jiří, František BRABEC. Komerční bezpečnost. Praha: ASPI, a.s., 2007. ISBN 978-80-7357-309-6.**
2. **VALOUCH, Jan. Projektování bezpečnostních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. ISBN 978-80-7454-230-5.**
3. **VALOUCH, Jan. Projektování integrovaných systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 978-80-7454-296-1.**
4. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. Zlín: Radim Bačuvčík – VeRBuM, 2011. ISBN 978-80-87500-05-7.**
5. **IVANKA, Ján. Systemizace bezpečnostního průmyslu I. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-80-7318-850-4.**
6. **Zákon č. 89/2012 Sb., občanský zákoník.**
7. **Zákon č. 553/1991 Sb., o obecní policii.**
8. **ČSN EN 50131. Poplachové systémy- Poplachové zabezpečovací a tísňové systémy.**

Vedoucí diplomové práce: **JUDr. Jiří Kameník**

Datum zadání diplomové práce: **7. února 2014**

Termín odevzdání diplomové práce: **27. května 2014**

Ve Zlíně dne 7. února 2014

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce pojednává o dohledovém a poplachovém centru (dále jen DPPC) a jeho specifik v sektoru soukromé bezpečnosti. V úvodní teoretické části se zabývá technickým řešením DPPC a přenosem poplachového signálu od střeženého objektu. V další části popisuje možnosti uplatnění DPPC na trhu komerční bezpečnosti a popisuje současnou legislativní úpravu.

Cílem diplomové práce je popsat a vysvětlit jednotlivá specifika DPPC v sektoru soukromé bezpečnosti a to zejména se zaměřením na rozdílné podmínky v provozování DPPC.

Klíčová slova: dohledové a poplachové přijímací centrum, poplachový signál

ABSTRACT

This thesis discusses surveillance and alarm receiving centers (hereinafter referred to as SARC) and the specifics related to the private security sector. The introduction looks into the technical usage of a SARC and the transmission of the alarm signal from the guarded property. The next section talks about the application of a SARC in the commercial security market. As well as current legislation, as it applies to mobile squads responding to a SARC signal.

The aim of this thesis is to describe and explain the specifics of a SARC in the field of private security, specifically focusing on different conditions in the operation of a SARC.

Keywords: surveillance and alarm receiving centers, alarm signal

Děkuji **JUDr. Jiřímu Kameníkovi** za podporu a vedení při tvorbě této diplomové práce.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Tato diplomová práce pojednává o systému dohledového a poplachového přijímacího centra a jeho specifik při použití v sektoru soukromé a komerční bezpečnosti. Ochrana objektů nabývá na významu zejména z důvodů zvýšené kriminality, kdy klasické způsoby ochrany již nepostačují, a zároveň bývá instalace některého z bezpečnostních systémů také požadavkem pojišťovacích společností při uzavírání pojistky na daný objekt. Proto je důležité znát možnosti, jaké se v sektoru soukromé bezpečnosti nabízejí, a jaká je podstata fungování poplachových center.

V teoretické části se zabývám technickým řešením poplachových center a přenosem poplachového signálu od střeženého objektu. Popisuji současnou legislativní úpravu, zejména pro zásahy mobilních posádek prověřujících signál DPPC. Za zdroje informací mi poslouží dostupná odborná literatura, včetně technických norem vymezujících instalaci a zabezpečení dohledových center, informace od společností zabývajících se touto oblastí a publikující své nabídky na internetu, a diplomové práce studentů věnujicich se taktéž dohledovým a požárním poplachovým centrům. V této části zejména vysvětlím technickou podstatu fungování těchto center, způsob přenosu informací od objektu do centra a možnosti, jaké centrum v případě zjištění poplachu nabízí. V neposlední řadě uvedu také základní normy vztahující se k této problematice.

V praktické části se zaměřuji na možnosti uplatnění DPPC na trhu komerční bezpečnosti. Tato část vyjadřuje cíl mé práce – jakým způsobem lze poplachová centra využít v konkrétních situacích nejen pro soukromé vlastníky objektů, ale též pro komerční centra. Mnoho firem si není jisto, jaký typ zabezpečení je pro jejich firmu vhodný, proto se pokusím na příkladech ukázat, jaké typy poplachových center mohou být v takovém případě vhodné. Podobným způsobem budu postupovat také v případě soukromých vlastníků objektů.

V závěrečné části pak zhodnotím přínos připojení zabezpečovaných objektů k dohledovému a poplachovému příjimacímu centru a shrnu závěry své práce.

I. TEORETICKÁ ČÁST

1. TECHNICKÁ ZABEZPEČENÍ DOHLEDOVÉHO A POPLACHOVÉHO PŘIJÍMACÍHO CENTRA

Dohledové a poplachové přijímací centrum (DPPC) představuje jednu z možností, jak zabezpečit fyzický majetek před krádeží či poškozením. Jeho podstatou je vytoření místa s trvalou obsluhou, kam jsou přenášeny informace týkající se stavu jednoho nebo více poplachových zabezpečovacích a tísňových systémů, které jsou nainstalovány ve střežených objektech.

Jelikož požadavky na bezpečnější a rychlejší přenos signálu se stále zvyšují, signály v přenosové síti jsou přímo úměrné zvyšujícímu se objemu a důležitosti přenesených zpráv. Normy přesně stanoví počty kontrol u jednotlivých stupňů zabezpečení. Samozřejmě specifikují i mnoho dalších povinností směrem k odborně způsobilému provozovateli komunikačních přenosových tras, a to včetně případů, kdy je na základě vyššího stupně ohrožení předepsána povinnost náhradní předepsané trasy. [1]

V současnosti patří k nejvyužívanějším komunikačním přenosovým trasám následující způsoby:

- telefonní linka ISDN,
- rádiový přenos na vyhrazených frekvencích,
- přenos po síti GSM v hovorovém pásmu,
- přenos po síti GSM prostřednictvím GPRS,
- přenos po síti GSM prostřednictvím SMS,
- přenos pomocí internetové sítě a přenos pomocí vyhrazených přenosových cest.

U objektů, spadajících do kategorie nejvyššího stupně ohrožení (například banky, jiné finanční instituce, či strategicky významné objekty), je obvykle využívána kombinace dvou přenosových cest.

DPPC přenesený signál ze střeženého objektu přijme a pomocí speciálního monitorovacího programu umožní uživatelsky příjemné zobrazení podrobných přehledů o stavech

střežených objektů. Software zajišťuje přístup k veškerým informacím a režimovým opatřením nutným k rychlé a efektivní reakci na příchozí událost.

Součástí mnoha zabezpečovacích systémů je kromě střežení objektů pomocí poplachových zabezpečovacích a tísňových systémů také monitoring objektu kamerovým systémem. Obraz je přenášen na DPPC a pracovníci centra k takto získaným informacím přistupují prostřednictvím sítě Internet, ať už přes VPN sítě nebo šifrovaně. V případě přijetí poplachové zprávy ze zabezpečovacího systému na PCO se operátor vzdáleně připojí ke kamerovému systému v objektu a prostřednictvím kamer ověří poplachovou zprávu. Operátor může ve spolupráci s PCO výrazně redukovat falešné poplachy. Při výjezdu zásahové jednotky spolupracuje s touto skupinou při zadržení narušitelů [2] tím, že umožňuje podat výjezdové skupině, případně Policii přesnější informace o pohybu nežádoucích osob ve střeženém objektu, jejich popis nebo SPZ auta.

Na dohledové centra je také možno přenášet informace například o překročení teploty, úniku vody či plynu, nefunkčnosti výtahu atp., čímž umožňuje operačnímu centru adekvátně na tyto události reagovat kontaktováním odpovědné osoby.

1.1 Legislativní zakotvení DPPC

Podobně jako jiné oblasti bezpečnosti, také technologie DPPC musí respektovat platné normy. Do roku 2011 byly všeobecné požadavky pro poplachové zabezpečovací a tísňové systémy upraveny normou ČSN EN 50131-1. Vlastní přenos signálů a základní zásady provozu PCO pak byly řešeny normami řady ČSN EN 50136, zejména technickými normami ČSN EN 50136-2-2 a ČSN EN 50136-1-4. [1]

Na poplachové zabezpečovací systémy se dále vztahují některé další technické normy z hlediska požadavků na elektromagnetickou kompatibilitu, elektrickou bezpečnost a telekomunikační a rádiové zařízení.

V současné době, jsou bezpečnostní zařízení DPPC řešena normami ČSN EN 50518-1, ČSN EN 50518-2 a ČSN EN 50518-3.

1.1.1 Norma ČSN EN 50518 - 1

Norma ČSN EN 50518-1 se vztahuje na veškerá dohledová a poplachová přijímací centra. Stanovuje minimální požadavky na návrh, konstrukci a funkční zařízení pro budovy, v nichž se uskutečňuje monitorování, příjem a zpracování (poplachových) signálů generovaných poplachovými systémy jako integrální část celkového procesu zajištění bezpečí a zabezpečení. [3] Dohledové centrum proto musí splňovat stanovenou sílu zdí, okna se zabudovanou balistickou a požární odolností, detekční zařízení plynu, dostatečné množství zabezpečených datových úložišť, komunikačních tras a hardwaru, jakož i automatizovanou zálohu napájecích okruhů pro případ velkoplošného výpadku elektrického proudu. Požadavky normy se vztahují jak na případy dálkové konfigurace, v nichž více systémů přenáší informace do jednoho nebo více poplachových přijímacích center (ARC), tak na případy jediného centra určeného pro monitorování a zpracování poplachů generovaných jedním nebo více poplachovými systémy, nalézajícími se v tomtéž perimetru příslušného místa. Dále jsou v ní uvedeny stavební požadavky na dohledová centra z hlediska odolnosti proti napadení, proti požáru a na ohodnocení rizik. [1]

Podle normy musí být DPPC situován v místě s nízkým rizikem požáru, výbuchu, zaplavení, vandalismu a nebezpečí hrozícího z jiných míst. V případě, že DPPC není jediným uživatelem objektu, v němž je umístěno, musí být od zbytku budovy odděleno fyzickou barierou, sestávající ze stěn, podlah, stropů a nezbytných otvorů. [1]

Při volbě místa pro umístění DPPC je nutné posoudit možná rizika. Norma proto obsahuje návrh stavebních řešení DPPC [3]:

- konstrukce DPPC – konstrukční požadavky ohledně fyzického útoku, útoku střelnou zbraní, ochranu proti požáru, proti blesku
- příslušenství – umístění toalet, umývárny
- otvory – povoleny jsou pouze vstup z haly, nouzový východ, zasklené plochy, vstupní otvory pro kabeláže a potrubí, manipulační okénko, ventilace (požadavky jsou definovány zvlášť v dalších kapitolách této normy)
- vstupní předsíň – dvoje dveře bezpečnostní třídy 4, nesmí být otevírány současně s výjimkou řízených událostí a musí být vzájemně provázány a ovládány pouze z DPPC

Norma dále definuje požadavky na elektronickou detekci, vztahující se na všechny základní části DPPC, vztahující se na možná vznik následujících událostí: útok zvenčí, požár, vchod a východ, plyn, komunikace, tíseň, monitorování bezpečnosti personálu, signalizaci elektronických ochranných systémů, CCTV. Veškeré systémy uvedené v kapitole poplachových systémů DPPC musí být dodržovány podle požadavků příslušných norem. V případech, kdy normy neexistují, se musí údržba provádět podle směrnic výrobce tak, aby byla zaručena trvalá spolehlivost. [3]

1.1.2 Norma ČSN EN 50518 - 2

Norma ČSN EN 50518-2 se vztahuje na „veškerá dohledová a poplachová přijímací centra (DPPC), která monitorují, přijímají anebo zpracovávají signály, jež vyžadují okamžitou reakci. Norma stanovuje technické požadavky týkající se DPPC. Dále zahrnuje funkční kritéria a ověřování výkonnosti. [1]

Také se v ní upravují požadavky na výkonnost DPPC. Nejdůležitějším kontrolovaným faktorem je čas uplynulý mezi časem přijetí výstupního signálu z komunikátoru přijímacího centra do indikačního zařízení a časem počátku události, který musí splňovat následující výkonnostní kritéria [5] :

- v případě tísňových poplachů nesmí být tato doba delší než 30s u 80% přijatých signálů a 60s u 98,5% přijatých signálů

- v případě všech ostatních poplachů pak musí být 90s u 80% přijatých signálů a 180s u 98,5% přijatých signálů

Soulad s výše uvedenými kriterií musí být dosaženo v průběhu dvanácti po sobě jdoucích měsíců.

Další oblasti, které jsou v rámci této normy sledovány, pokrývají požadavky na komunikaci, příjem signálu a zásah dispečera, testování funkčnosti všech zařízení a postupy při závadách a podávání zpráv. Též je zde zahrnut údaj o evropské směrnici vztahující se k ochraně osobních údajů, což v ČR definuje zákon č. 101/2000Sb.

Ochrana osobních údajů je brána velmi vážně, proto je dodržování této směrnice povinné zejména při zpracování:

- údajů o zákazníkovi,

- údajů o vnější komunikaci DPPC,

- záznamů o zákrocích dispečera.

Výše uvedené údaje jsou archivovány po přesně stanovené období - údaje o klientovi a o zákrocích dispečera po dobu dvou let, informace o komunikaci DPPC po dobu tří měsíců. [5]

Návrh zákona o SBS

§ 39

Omezení při výkonu bezpečnostní činnosti technická služba

Při výkonu bezpečnostní činnosti technická služba je provozovatel povinen zajistit, aby informace ze zabezpečovacího systému nebo dohledového, poplachového a přijímacího centra byly přístupné pouze jeho vlastníkovi, provozovateli bezpečnostního systému nebo jím určené osobě.

Dále je stanoven požadavek na vypracování nouzového plánu pro případ vyřazení DPPC z činnosti, jež definuje postup odstranění následků – kontaktních údajů dodavatelů a poskytovatelů služeb, kteří provedou obnovení při zachování poskytování služeb.

1.1.3 Norma ČSN EN 50518 - 3

Norma ČSN EN 50518-3 obsahuje požadavky na personál, pracovní postupy a provoz dohledových poplachových center (pultů centralizované ochrany). Dále specifikuje požadavky na výcvik, bezpečnostní prověření a lustraci personálu, v neposlední řadě pak požadavky na testování center, správu databází a likvidaci údajů, řízení nouzových stavů, evakuačních postupů a audit poplachových dohledových center. [1]

Poslední část normy stanovuje minimální postupy a požadavky na provoz DPPC. Jsou stanoveny podmínky personálního obsazení, bezpečnostních prověrek a lustrace a také výcviku. DPPC musí být trvale obsazena nejméně dvěma dispečery. Pokud je DPPC provozováno současně s jiným DPPC a provozní postupy zajišťují stejný efekt jako u DPPC obsazeného dvěma dispečery, je tento požadavek splněn. [6]

Také je nutné zabezpečit, aby se v každém centru nacházela provozní dokumentace dostupná všem pracovníkům. Tato dokumentace musí obsahovat především předpisy pro provozní postupy, definovat postup pro testování, vstup a odchod z DPPC, správu databází, provozní kontinuitu a nouzové stavy, evakuační postupy či zpracování signálů.

Shoda je ověřována auditem, který je prováděn každoročně orgánem akreditovaným podle EN 45011 nebo EN - ISO/IEC 17020. Za případné neshody je odpovědný vedoucí DPPC, který také dohlíží na odstranění a opravení ve stanovených lhůtách.

Poslední kapitola ukládá požadavky na zdokumentování postupů definující ukládání, ochranu, oprávněné přemísťování, dobu platnosti a nakládání s údaji. Musí být vypracován postup pro zacházení, údržbu, ukládání, likvidaci a vedení zákaznických údajů. [6]

1.2 Základní požadavky na provoz DPPC

Základním účelem, který musí každé DPPC splňovat, je posílání vyhodnocených zpráv z bezpečnostních a jiných zařízení, která střeží objekty, na přijímací centrum bezpečnostní agentury. Po přijetí zprávy postupují bezpečnostní pracovníci DPPC dle stanovených pravidel pro jednotlivé typy událostí tak, aby co nejrychleji a nejefektivněji vyřešili vzniklý problém. Způsob řešení je dán nejen vnitřními směrnicemi, ale též způsobem a podmínkami smlouvy mezi DPPC a klientem.

Způsob ochrany pomocí dálkově ovládaného poplachového přijímacího centra je v současné době jedním z nejlepších a nejspolehlivějších způsobů, jak ochránit majetek. Úroveň kvality služeb, poskytovaných bezpečnostní agenturou, lze měřit zejména na základě doby, kterou potřebuje k adekvátní reakci na přijaté informace. Dalším kritériem může být také míra profesionality bezpečnostních pracovníků a úroveň modernizace techniky přenosu informací.

Kvalitně provedený zásah se pozná podle snahy co nejvíce minimalizovat škody na chráněném objektu, a to jak ze strany pachatele, tak i ze strany zasahujících zaměstnanců. Důraz musí být kladen především na ochranu života a zdraví každého účastníka zásahu.

Rychlost, s kterou dojde k zásahu, je ovlivněna dojezdovým časem, tedy dobou, kterou potřebuje bezpečnostní automobil zásahové skupiny k přejezdu z místa sídla zásahové centrály do místa napadeného objektu. Dobu dojezdu po zjištění útoku na objekt ovlivňuje

několik faktorů. Většinu z nich není možné ovlivnit (dopravní zácpy na cestách, kvalita přístupové komunikace, počasí a podobně). [7]

Velký vliv má také vzdálenost ohroženého objektu od nejbližšího centra zásahové jednotky. Každá společnost se pokouší rozmístit svá centra tak, aby mohly být zásahové jednotky zákazníkům vždy co nejblíže. Kvalita služeb se také odvíjí od míry organizovanosti jejích pracovníků, a též na správném zadávání a provádění rozkazů. Všichni zúčastnění mají za cíl zkrátit celkový čas od vzniku poplachu do výjezdu zásahové skupiny k objektu na minimum. Proto je nutné mít předem zpracované podrobné pokyny, které musí každý bezpečnostní zaměstnanec dokonale znát a dodržovat. Má - li být zásah co nejrychlejší a nejúčinnější, pracovníci si nemohou dovolit váhání a improvizování.

V současnosti jsou nedílnou součástí tréninku zaměstnanců také obecné a specifické modelové situace, které se neustále zdokonalují a propracovávají, a v nichž se pracovníci učí zvládat stresové situace. Právě profesionální přístup zaměstnanců je dalším článkem, který je pro dokonalou ochranu majetku zcela nezbytný. Každý uchazeč o práci v zásahových jednotkách musí splňovat všechna následující kritéria [7]:

- věk 21 let,
- trestní bezúhonnost,
- držitel zbrojního průkazu,
- držitel řidičského oprávnění minimálně kategorie B,
- minimálně dvouletá praxe atp.

Kromě výše zmíněných kvalit se také zkoumají fyzické a psychické předpoklady uchazečů k výkonu práce v poplachovém centru. Stávající zaměstnanci jsou pravidelně proškolování ze svých znalostí a schopností a v případě změny či zdokonalení systémových směrnic absolvují tito zaměstnanci semináře pro rozšíření dovedností potřebných k udržení vysoké úrovně profesionality.

Zásah profesionální jednotky by však nemohl být úspěšný, pokud by nebyl správně zvolen způsob přenosu informace z objektu na přijímací poplachové centrum. Při zvažování, jaký typ přenosu informací zvolit, by měly být zváženy následující požadavky:

- kontrola přenosu dat
- nejrychlejší přenos zprávy na DPPC,
- schopnost zařízení předávat informace o všech stavech v hlídaném objektu.

Operační středisko musí mít [8]:

- homologované poplachové přijímací centrum včetně záložního zdroje,
- speciální linky pro přenos dat (signálů) z PZTS do DPPC,
- počítač s diskem pro archivaci dat DPPC s databází všech hlídaných objektů,
- zařízení pro komunikaci: mobilní telefony, vysílačky, CB rádio,
- archiv protokolů z každého výjezdu zásahové jednotky,
- aktuální archiv listů fyzické ochrany,
- dokumentaci: manuály, směrnice k objektům, metodické pokyny, atd.

Personál obsluhující systémy DPPC musí před započetí práce projít náročným odborným výcvikem. Pro správný výkon této funkce by zaměstnanci DPPC měli splňovat následující podmínky:

- schopnost řešit mimořádné situace,
- schopnost pracovat ve stresu a pod tlakem,
- znalost DPPC po technické a manuální stránce,
- schopnost komunikace.

Pracovníci zásahových jednotek také musí splňovat určitá kritéria [9] :

- disciplinovanost,
- fyzická zdatnost,
- dobrá znalost zásahových metod,
- znalost topografie střežených objektů,
- schopnost ovládat zbraně a zkušenost s používáním zbraní a dalších donucovacích prostředků.

1.2.1 Služby na DPPC

Služby nabízené různými soukromými provozovately mohou být různorodé. Obvykle jsou založeny na komerčních základech. Základní rozdíl, který mezi nabídkami je, spočívá v postupu dispečera při příjmu poplachové informace a v ceně. Při výběru takové firmy by se měl zákazník řídit zejména svými specifickými požadavky a schopností firmy vytvořit každému zákazníkovi individuální nabídku.

Následující seznam služeb poskytovaných bezpečnostními agenturami představuje základní nabídku. Služby se samozřejmě můžou kombinovat.

1.2.2 Monitoring

Monitoring představuje základní službu, kterou bezpečnostní agentury nabízejí, a která je základním prvkem ochrany. Obsahuje monitoringový systém, ať již elektronický, nebo kamerový. Náplní této služby je sběr, vyhodnocení a archivace dat z objektů. Ve chvíli přijetí poplachové zprávy předává operátor DPPC zákazníkovi informace o vzniklé události na předem domluvená telefonní čísla. Zákazník pak sám dál rozhoduje, zda vzniklou situaci na objektu prověří on sám, nebo zda mají zasáhnout zásahové skupiny DPPC. Při telefonickém kontaktu se zákazníkem lze po domluvě využívat i předem domluvená hesla pro identifikaci osob, které rozhodují o způsobu prověření poplachu. [8]

1.2.3 Zásah

Klíčovou složkou zásahu je výjezdová skupina, která musí být neustále připravena a po obdržení poplachové zprávy okamžitě vyráží na místo prověřit situaci, a v případě potřeby provést preventivní nebo represivní zásah v rámci zákona. Zásahovou skupinu vždy vede k cíli operátor poplachového centra, který pomocí monitorovací konzole neustále předává aktuální informace o stavu v objektu, na kterém vznikl poplach. Poskytovatelé bezpečnostních služeb mají obvykle v nabídce dvě varianty platby tohoto typu služeb:

- Zákazník platí měsíční paušál, který zahrnuje všechny výjezdy k objektu.
- Zákazník platí provozovateli DPPC za každý výjezd.

1.2.4 Patrol

Patrol je preventivní nástroj ochrany objektů, charakterizovaný jako namátková fyzická ostraha. Spravuje ho zásahová skupina DPPC. Je to způsob, jak lépe využít času pracovníků zásahové jednotky v době jejich pohotovosti a zároveň zlepšit ekonomické výsledky.

Podstatou služby je provedení akce výjezdové skupiny v době plnění služby a provádění preventivní prověrky objektů a jejich okolí dle harmonogramu. Celá služba Patrol je

preventivní a jejím účelem je působit na podvědomí okolí a dát najevo, žeobjekt není ponechán bez kontroly, a je zabezpečen profesionální bezpečnostní skupinou. V případě přijaté poplachové zprávy je Patrol systém přerušen a prioritu má výjezd k napadenému objektu. V činnosti Patrol systému potom hlídka pokračuje, pokud není vytížená kontrolou poplachů na hlídaných objektech.

1.2.5 Doplňkové služby

Tyto doplňkové služby jsou agenturami nabízeny zejména proto, aby jim získaly více zákazníků. Doprovodným následkem je pak zlepšení komfortu nabízených bezpečnostních služeb. Mezi tyto služby patří například [8] :

- Vyrozumění odpovědného personálu, pokud objekt nebyl v určitém čase zastřežen.
- Zasílání SMS o stavu objektů. Z DPPC konzoly je možné na dálku komunikovat s elektronickým zařízením (zastínění oken, spouštění klimatizace, zapnutí osvětlení, spouštění topení atd.).
- Informování zákazníka DPPC o výpadku dodávky elektrické energie, o poruchách telefonní linky apod.
- Měsíční nebo týdenní výpisy (záleží na nabídce) z historie objektu, posílané poštou nebo v elektronické podobě.
- Správa odkódování a zakódování objektů pomocí dálkového ovládání ústředen PZTS.
- Dálkový dohled zákazníků nad objektypomocí kamerového systému CCTV.

Poskytovatelská firma může nabízet i následujícíc doplňkové služby [10]:

- Úklid různorodého charakteru v závislosti na typu objektu a druhu jeho znečištění. Lze zajistit úklid nejen kancelářských, ale i výrobních prostor, či prostor, kde je předpoklad většího znečištění. Rozsah a četnost úklidu je prováděna v plném rozsahu objednaných prací.
- Dodávku spotřebního zboží, zejména toaletního papíru, papírových ručníků, tekutého mýdla či solviny
- Přeprava peněžních zásilek či cenností, která je prováděna vycvičenou posádkou ozbrojenou střelnou zbraní. Přeprava je zajištěna v dohodnutých termínech podle požadavků zákazníků, který si může určit čas i trasu. Na požádání je možné v

doprovodném vozidle vyhradit místo pro zákazníka. Samozřejmostí je předložení pojistné smlouvy.

1.2.6 Servis

V některých případech je provozovatel DPPC zároveň i dodavatelem bezpečnostních monitorovacích systémů. Tím se nabídka ještě rozšiřuje nabídka – firma může zákazníkovi nabídnout v rámci zvýšeného měsíčního paušálu také non - stop servis bezpečnostního zařízení. V praxi tato služba umožňje v případě hlášení o poruše na DPPC vyrozumět operátora, a následně též technika, který sám zákazníkovi nahlásí poruchu a domluví termín opravy. Zákazník se tedy nemusí zabývat starostí o kontrolu funkčnosti systému. Technici, střídající se v operačním středisku, mají pohotovost celých 24 hodin tak, aby bylo možno provést okamžité opravy i v mimopracovní dobu.

1.2.7 Ostraha

Ostraha se využívá v případě zvýšeného rizika napadení chráněného objektu. Zásahová skupina provede opatření a v době zaznamenání napadení chráněné oblasti ihned informuje majitele objektu, ve vážných případech také Policii ČR.

Ostraha je zajištěna spolehlivými pracovníky s praxí, kteří jsou důsledně proškoleni – seznámeni s předpisy, směrnicemi a s obsluhou požárních a bezpečnostních signalizačních zařízení. Ovládají pořizování zápisů a jiných administrativních úkonů, které vyplývají z povinností ostrahy objektů. [10]

Z důvodů velké konkurence na trhu provozuje většina agentur DPPC působících v oblasti komerčního zabezpečení kompletní služby od zajišťování fyzické ochrany, přes transport hotovosti a cenin, až po technickou oblast (montáže PZTS, CCTV, EPS). Důležitou součástí zákazníkovy volby tak není rozsah služeb, ale spíše doporučení a záruka spolehlivosti.

2. HARDWAROVÉ SLOŽENÍ DPPC

Dohledové a poplachové přijímací centrum je možné provozovat buď jako osobní počítač, nebo jako samostatné nezávislé zařízení. V současnosti však bývá nejčastější verzí provozu DPPC jejich vzájemná kombinace.

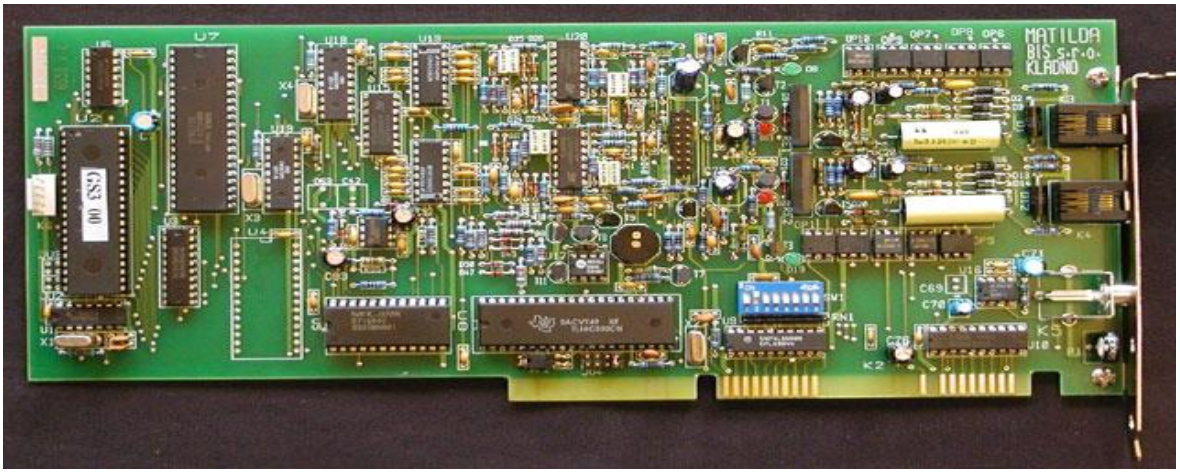
2.1 Osobní počítač

DPPC je v tomto případě tvořeno systémem založeným na osobním počítač, který může být přímo v základní desce osazen telefonní, radiovou, GSM či ISDN kartou. V některých případech jsou tyto karty zabudovány v externím boxu, který je připojen k počítači přes USB nebo sériové rozhraní.

Komunikační procesor telefonní karty se skládá ze dvou samostatně pracujících částí. Komunikační část je složena z obvodů, které se nazývají linková část a mají za úkol zpracování signálu z telefonních linek a digitálních dat. Druhou část tvoří počítačové rozhraní. Obě části spolu navzájem komunikují sériově. Účelem linkové části je impedanční přizpůsobení telefonní lince, příjem signálu z telefonní linky, kontrola napětí na telefonní lince a galvanické oddělení obvodů PC od telefonních obvodů. Na kartě je k dispozici generátor zvuků s výkonovým zesilovačem pro přivolání obsluhy. Je možné připojení externího reproduktoru. [10]

Nezbytnou součástí počítače fungujícího jako PPC je vyhodnocovací a řídící software.

Obrázek 1: Telefonní karta GS51 Matylda 1



Zdroj: [11]

Nevýhodou tohoto řešení DPPC je zejména zvýšená nutnost neustálé kontroly stability systému a hardwaru. Protože počítač musí zůstat v provozu nepřetržitě, pracovníci v případě výpadku proudu potřebují mít zajištěnou zálohu napájení.

2.2 Samostatné nezávislé zařízení

Tento typ zařízení se také nazývá Reky. Jejich podstatou jsou záložní zdroje, které jsou schopny samostatného provozu bez napájení až 12 hodin. Jeden rek většinou obsahuje sloty pro různé přenosové moduly – telefonní linková karta, ISDN karta, rádiová karta či karta pro tiskárnu. Jednotlivé karty mají svoji vnitřní paměť až na 2000 událostí, pro případ, že by došlo k výpadku proudu či by musel být Rek podroben servisní kontrole.

Velkou výhodou těchto typů zařízení je fakt, že nevyužívají žádný operační systém. Nejsou tudíž ohrožené nefunkčností takového systému, a jsou obecně velmi spolehlivé. Přední strana tohoto zařízení je většinou tvořena ovládací a programovací klávesnici společně s display klávesnici. Zprávy jsou zobrazovány na displeji a při vstupu dat zároveň tisknuty na tiskárně, protože displeje reků jsou maximálně dvouřádkové a zprávy by se postupem času mohly ztrácet. Na druhé straně je jejich nevýhodou právě fakt, že nejsou schopny zobrazovat zprávy v textovém formátu, nýbrž pouze v číselném, proto jsou méně adresné a rozklíčování číselného kódu trvá delší dobu než pouhé přečtení psané zprávy. Obsluha při příchodu zprávy tak musí nejprve dle pomocné dokumentace zjistit, o jaký objekt se jedná, jaký typ zprávy je signalizován a případně z které zóny je hlášen poplach.

Výše uvedený postup velmi omezuje provoz takového typu DPPC v bezpečnostních ústřednách. Pro zjednodušení musí být dodržen jednotný postup, kdy jsou jednotlivé kódy přiřazeny konkrétním zprávám – například kódy začínající číslem 3 jsou vyhrazeny pro poplach (u všech objektů). Situace je o mnoho složitější zejména u velkokapacitních ústředen, které mohou mít až 256 zón. Zde se musí vytvořit jednoduchý programovací systém, nejlépe tabulkový, pro přenosové zprávy.

Součástí zařízení je také napájecí karta, která zajišťuje napájení pro další karty v přijímači. Její součástí je automatická nabíječka a připojená záložní baterie. V případě výpadku proudu tato karta automaticky připojí zařízení na záložní baterii. Karta dohlíží na přítomnost a kapacitu záložní baterie a aktuální stav je předáván centrální procesorové jednotce a zobrazen na čelním panelu přijímače.

2.3 Kombinované provedení

Současná struktura moderních DPPC dává přednost kombinaci obou výše uvedených možností. Příchozí zpráva je tak nejprve přijata a zobrazena na LCD displeji přijímače v číselném formátu a poté je textově přeložena a zobrazena obsluze PPC v monitorovacím softwaru běžícím pod operačním systémem na počítači. Zvyšuje se tak uživatelský komfort a zrychluje reakce operátora. [12]

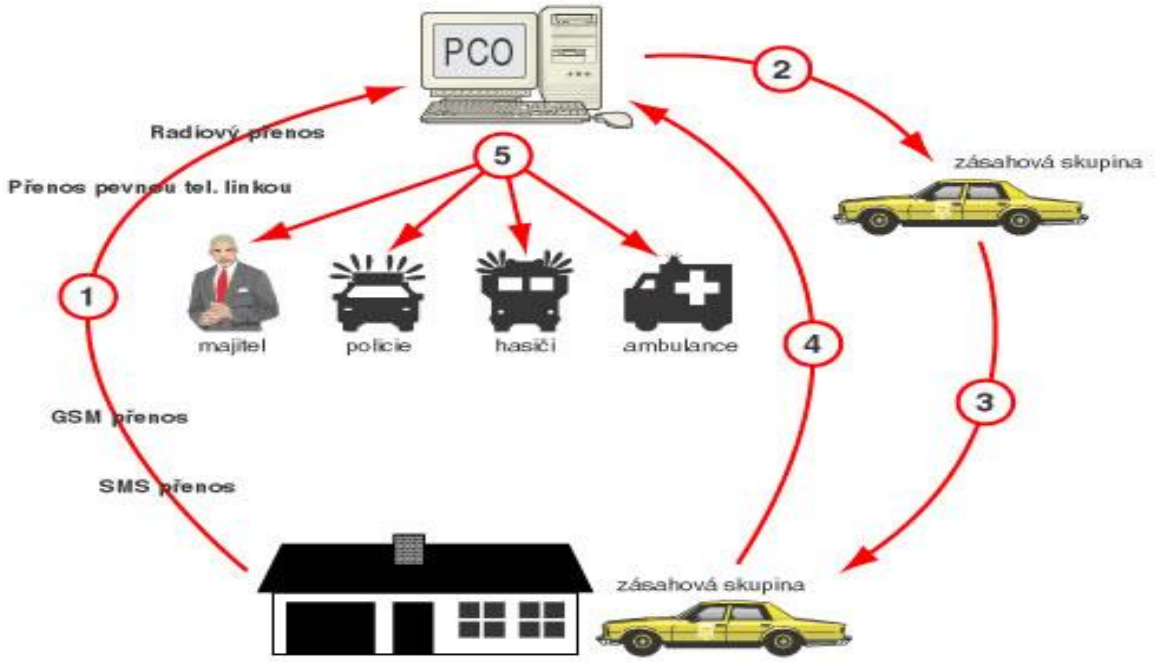
2.4 Přenos zpráv

Volba správného způsobu přenosu je důležitou součástí instalace poplachového zabezpečovacího a tísňového systému. Pokud by poplachová zpráva nemohla být přenesena ze střeženého objekt, poslána ke zpracování poplachovým přijímacím centrem, a nedokázala vyvolat adekvátní reakci na tuto zprávu, bylo by celé instalování bezpečnostní systému zbytečné.

2.4.1 Přenosové trasy

Přenosové trasy tvoří páteř každého zabezpečovacího systému. V současné době existuje několik způsobů, jak lze poplašný signál doručit od zdroje poplachu do poplachového centra. Následující obrázek ukazuje základní možnosti přenosu:

Obrázek 2: Schéma přenosu PS 1



Zdroj: [13]

Jednotná telefonní síť (JTS)

Přenos pomocí telefonní sítě představoval až do nedávné doby nejčastěji používanou přenosovou trasu. V současné době začíná být nahrazována sítí GSM. Způsob přenosu po telefonu se může odehrávat buď v hovorovém pásmu, které je využíváno nejčastěji, dále v nadhovorovém pásmu a ISDN.

Velkému rozšíření přenosu dat v hovorovém pásmu napomohlo široké pokrytí JTS ve střežených objektech a také integrace telefonního komunikátoru do desky ústředny. Toto zařízení funguje následovně: Linka se první připojí do ústředny EZS a následně se z ústředny EZS vytvoří připojení pro koncové zařízení. Takovéto připojení je vždy nutno dodržet, aby byla splněna podmínka priority vysílání informací ústřednou na PCO. Tam, kde je například pobočková telefonní ústředna, musí být telefonní signál veden do EZS a teprve poté do telefonní ústředny. Tímto řešením je PZTS je umožněno běžné používání telefonní linky pro hovory. V případě, že dojde na ústředně EZS k události, tato zajistí přerušení stávajícího hovoru uvolní si linku (pokud není volná) na dobu nezbytně nutnou předá informaci PCO a znovu linku uvolní pro další použití.

Aby nedošlo k zablokování linek, programují se zpravidla v ústředně PZTS hlavní a záložní telefonní linky. V případě, že je hlavní linka obsazena, začne ústředna vytáčet

záložní linku. Pokud je obsazena i záložní linka, postup se opakuje. Počet opakovaných vytáčení lze nastavit na ústředně. V případě, že se nemůže dovolat ani ústředna, je signalizována porucha komunikace.

Celý tento postup je časově náročný, a proto se na straně PPC využívá zapojení linek do série, které zajišťuje poskytovatel JTS. Ústředna vytočí hlavní linku a pokud je tato obsazena, je automaticky ve velmi krátké době přesměrována na další linku.

Další možností připojení pomocí telefonní sítě je ISDN. V ČR se tento typ přenosu příliš neujal, neboť jednodussím způsobem je přípojení pomocí mobilní sítě. ISDN (Integraded Services Digital Network) v sobě zahrnuje několik různých druhů informací (řeč, data, obrázky, video), různých funkcí (vytvoření, zpracování, uložení, přenos) a různých druhů koncových zařízení (samostatné přístroje nebo síť zařízení). Nabízí přenos pomocí analogově – digitálního převodu, který pošle informací k účastníkovi do jeho přístroje a tím aktivuje digitálně účastnickou přípojku umožňující připojit kromě digitálního telefonu další koncové zařízení s možností simultálního provozu.

Tento druh připojení v sobě obsahuje 2 typy přípojek [14]:

- 2B+D – účastnická – připojení až 8 koncových zařízení, 2 nezávislé B kanály (nosné) o rychlosti 64 kbit/s pro přenos hlasu, faxu, dat a jednoho D kanálu (řídící) o rychlosti 16 kbit/s pro přenos signalizace.

- 30B+D – přípojka pro pobočkové ústředny – 30 nezávislých B kanálů o rychlosti 64 kbit/s a jeden D kanál o rychlosti 16 kbit/s pro přenos signalizace.

Systém připojení telefonní sítě v nadhovorovém pásmu pracuje na bázi frekvence 20kHz, která byla vysílána po telefonní lince a na straně pultu centrální ochrany se mohly zobrazit pouze 2 informace (ANO, NE), signál buď byl, nebo nebyl. Tento typ připojení již ve větší části republiky historií, avšak v některých oblastech se stále mohou nalézt objekty střeženy touto technologií. Hlavní přednost přenosu v nadhovorovém pásmu je spočívá v nepřetržité kontrole spojení střeženého objektu s PCO.

GSM – sítě mobilních operátorů

Střežené objekty, které nedisponují přípojkou JTS a nelze u nich tedy využít radiového přenosu, je možné připojit pomocí sítě GSM (Global System for Mobile Comunications).

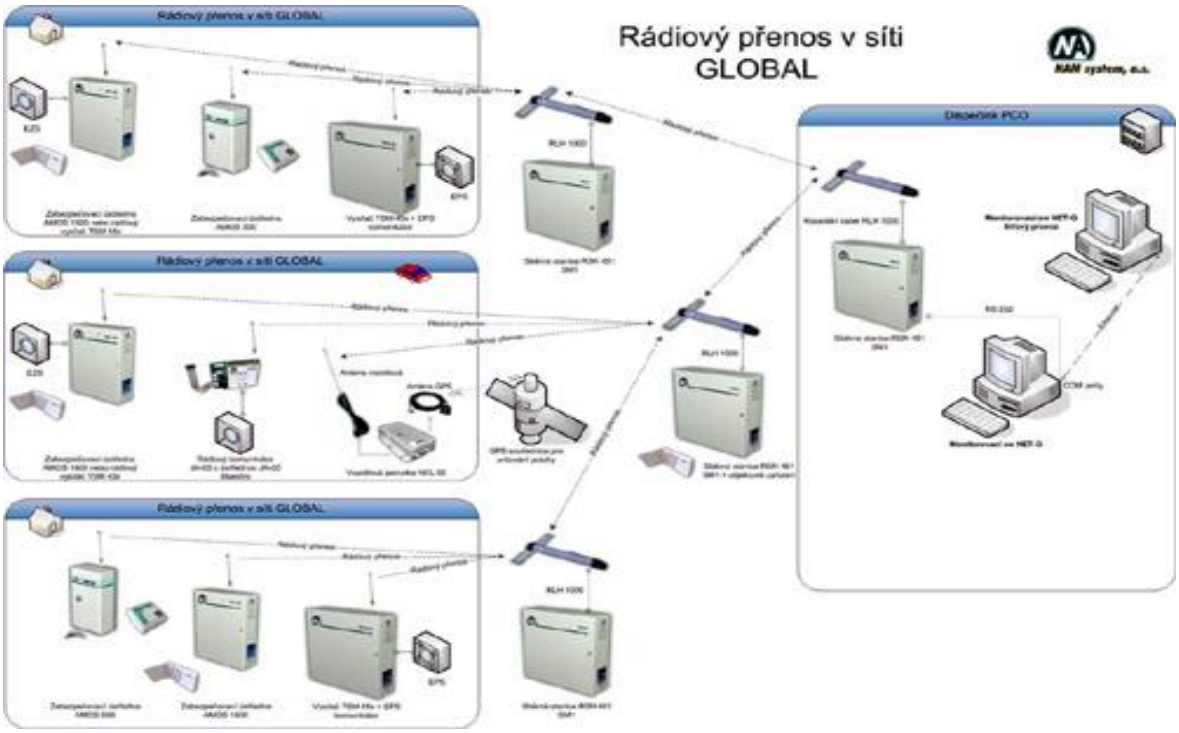
Ústředna PZTS je osazena GSM komunikátorem a dle použitého typu jsou zprávy přenášeny v hovorovém pásmu, v datovém pásmu pomocí služby GPRS a nebo pomocí SMS zprávy.

Hovorové pásmo představuje nejdražší variantu této formy přenosu. V takovém případě představuje výhodnější řešení připojení GSM brány na jednu z linkových karet přijímače PPC. Jako službu pro zákazníky jim PPC poskytne SIM kartu patřící do firemní sítě, v níž mobilní operátor obvykle poskytuje zvýhodněné tarify. V rámci takové „firemní sítě“ může být paušál snížen až na 100 Kč bez DPH a veškerá komunikace je zahrnuta v tomto paušálu. Nemusí být však omezován počet zpráv přenášených ze střeženého objektu na PPC.

GPRS – (General Packet Radio Service) je mobilní datová služba, která využívá přepojování paketů. Jejich podstatou je dynamické využívání neobsazených časových slotů, které může sdílet více uživatelů. Pro přenos informace se v tomto případě zpravidla využívá IP protokol pracující na síťové vrstvě.

Většina poskytovatelů uvádí, že uživatel jejich služeb platí pouze za dobu, po kterou je připojen, bez ohledu na objem dat, který během této doby přenese. Pro používané aplikace tento fakt garanci přenosové kapacity, kterou mají po celou dobu existence spojení k dispozici. Z pohledu operátora mobilní sítě takovéto přenosy znamenají především nutnost vyhradit pro uživatele příslušnou část kapacity sítě, a to po celou dobu připojení.

Obrázek 3: Přenosová trasa GPRS 1



Zdroj: [15]

Základní předností, kterou toto spojení nabízí, je obousměrná komunikace mezi PPC a komunikátorem instalovaným na střeženém objektu. Pokud se zákazník připojí v rámci tarifu „firemní sítě“, může se dostat na velmi nízký paušál za přenos. Na straně PPC lze nainstalovat takový přijímač, který dokáže využívat také přenos dat přes internet nebo je příjem zpráv zajištěn monitorovacím softwarem na úrovni služby.

SMS - (Short message service) představuje poslední variantu využití sítě GSM. Jeho podstatou je zasílání SMS v případě poplachu nebo stavu ohrožení objektu. Příjem na straně PPC je uskutečněn pomocí SMS komunikátoru a přijatá zpráv je obvykle zobrazena v monitorovacím softwaru. Takto nastavený komunikátor může být též využit pro odesílání zpráv z PPC vlastníkům střeženého objektu, kteří chtějí mít okamžitý přehled například o časech kódování nebo o poplachu. Lze také odesílat zprávy hlídkám či jiným určeným osobám.

Zásadní nevýhodou tohoto přenosu je závislost na datové sítí operátora - v případě jejího přetížení může dojít k doručení zprávy s velkým zpožděním.

GSM komunikátor umožňuje zejména následující služby [16]:

- reportovat až 8 uživatelům požadované události formou SMS a zavoláním (někdo může dostávat pouze poplachové informace, jiný také údaje o příchodu a odchodu uživatelů)
- ovládat systém dálkově mobilním telefonem (zavoláním a použitím klávesnice telefonu jako vzdálené klávesnice systému nebo pomocí SMS instrukcí).
- 2 různé funkce lze v domě dálkově ovládat dokonce pouhým prozvoněním (zdarma) z autorizovaných mobilních telefonů - např. otevírat garáž, zapínat světla apod.
- vzdálený přístup do systému internetem pomocí přístupového portálu www.GSMLink.cz. Díky tomu lze zjistit okamžitý stav střežení, zapínat a vypínat spotřebiče (např. topení). Servisní technik využívá webový portál pro vzdálený servis. Přístup přes internet je chráněn systémem hesel a šifrovaným protokolem.
- servisnímu technikovi umí GSM komunikátor předávat technické reporty (vybité baterie, poruchy napájení apod.). Umožňuje mu též dálkový přístup pro diagnostiku a změny nastavení (pomocí mobilu anebo pomocí počítače)
- přenos fotografií z kamerových detektorů (na mobilní telefony, na webový portál www.img.jablotron.cz, do e-mailu a nebo hlídacímu pultu)
- odposlech z objektu – připojením hlasové jednotky SP-02 může v případě potřeby uživatel poslouchat co se v domě děje (a může též promluvit)
- komunikaci na pult centrální ochrany – předávají se veškeré informace formou IP protokolu. Kontrola spojení s pultem je možná každou minutu, tzn. pachatel nemůže znemožnit zásah pultu přerušením komunikace (to se projeví jako poplach)
- v ČR je komunikátor dodáván se SIM kartou, kterou lze bezplatně aktivovat a použít pro všechny přenosy. Karta obsahuje zaváděcí střežení pultem centrální ochrany na půl roku zdarma (včetně výjezdů zásahové jednotky). Podrobnosti viz hlídání zdarma

ADSL přenos

V dnešní době se čím dál častěji používá také přenosů pomocí datového pásma linky. Velká výhoda tohoto typu přenosu spočívá ve schopnosti rychlé detekce přerušení datového spojení na DPPC. Další výhodou je, že během komunikace nedochází k přerušení hovorové linky a tato komunikace probíhá současně a nezávisle na hlasových službách.

ADSL přenos je dostupný na drtivé většině telefonních přípojek a je také velice dostupnou alternativou k připojení k DPPC z důvodu poměrně nízkých provozních nákladů. Tyto linky jsou zpravidla velice stabilní a v případě jejího selhání můžeme využít komunikaci s ústřednou pomocí mobilní sítě nebo jiné metody dostupné na ústředně. V drtivé většině poskytovatelů jsou poskytovány časově a datově neomezené tarify, které nám negenerují žádné další náklady nad sjednaný paušální poplatek. Vdnešní době již je většinou nějaká forma připojení do sítě internet využívána a tudíž je toto připojení využíváno i pro jiné účely než je připojení na DPPC. V případě, že na lince běží současně více druhů komunikace, je nutné uplatňovat pravidla QOS (Quality of service), tak, aby byla prioritní komunikace na DPPC. Tento proces může být realizován upřednostněním konkrétní IP adresy ve firewallu hraničního směrovače, sloužícího k připojení do sítě nebo také klasickou prioritizací paketů.

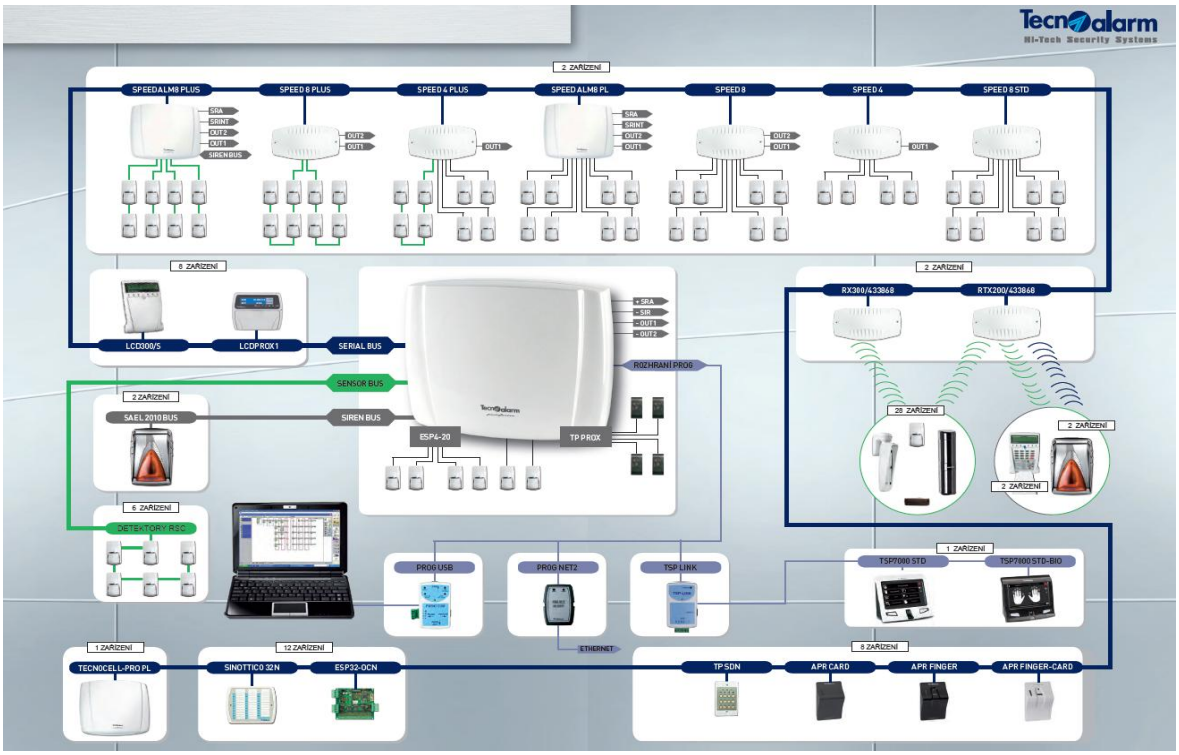
Internet

S rozvojem internetového připojení se tato forma přenosu stává hojně využívanou. Kromě přenosu poplachových a stavových informací je přenášen i obraz a zvuk. Je možný vzdálený dohled a ovládání PZTS. Pomocí přenosu obrazu z kamerových systémů odpadají některé výjezdy k planým poplachům. V případě střežení solárních elektráren to přináší i výraznou úsporu finančních prostředků.

Pro přenos informací využívají objektové komunikátory i přijímač DPPC dva protokoly transportní vrstvy UDP a TCP, případně oba dva. Pokud přijímač umí zpracovat oba, může automaticky přepínat zpracování příchozí zprávy, aniž by bylo třeba provádět změnu nastavení přijímače. V případě, že objektový komunikátor umí komunikovat oběma protokoly, provede se výběr manuálně. Pro přenos z ústředen PZTS se převážně používá protokol UDP.

Následující obrázek ukazuje možnost internetového přenosu informací z objektu zabezpečeného firmou SABS:

Obrázek 4: Internetové připojení SABS 1



Zdroj: [17]

TCP je spojově orientovaný protokol což znamená, že k navázání "end – to - end" komunikace potřebuje, aby proběhl mezi klientem a serverem tzv. "handshaking". Podstatu tohoto proces vysvětlím v následujícím odstavci. Poté, co bylo spojení navázáno, data mohou být posílána oběma směry. Charakteristické vlastnosti TCP protokolu jsou [18]:

- spolehlivost – TCP používá potvrzování o přijetí, opětovné posílání a překročení časového limitu. Pokud se jakákoliv data ztratí po cestě, server si je opětovně vyžádá. U TCP nejsou žádná ztracená data, jen pokud několikrát po sobě vyprší časový limit, tak je celé spojení ukončeno.
- zachování pořadí – Pokud pakety dorazí ve špatném pořadí, TCP vrstva příjemce se postará o to, aby se některá data pozdržela a finálně je předala správně seřazená.

• vyšší režie – TCP protokol potřebuje např. tři pakety pro otevření spojení, umožňuje to však zaručit spolehlivost celého spojení.

UDP je jednodušší protokol založený na odesílání nezávislých zpráv. Charakteristika protokolu je následující [18]:

• bez záruky – Protokol neumožňuje ověřit, jestli data došla zamýšlenému příjemci. Datagram se může po cestě ztratit. UDP nemá žádné potvrzování, přeposílání ani časové limity. V případě potřeby musí uvedené problémy řešit vyšší vrstva.

• nezachovává pořadí – Při odeslání dvou zpráv jednomu příjemci nelze předvídat, v jakém pořadí budou doručeny.

• jednoduchost – Nižší režie než u TCP (není zde řazení, žádné sledování spojení atd.).

LAN komunikátor – umožňuje [16]:

- stejné komunikace jako GSM komunikátor. Pro svou funkci nevyužívá GSM síť, ale kombinuje připojení internetu LAN (Ethernet pro datové přenosy) a telefonní linky (pro hlasové přenosy a SMS)
- tento komunikátor je vhodný tam kde je k dispozici spolehlivé připojení do Internetu a telefonní linka (např. ADSL)
- LAN připojení nevyžaduje žádné speciální nastavení lokální sítě ani pevnou IP adresu. Datový kabel komunikátoru se zapojuje do routeru stejně jako když si do internetu zapojujete laptop
- pro plnou funkčnost komunikátoru se požaduje na telefonní lince aktivovat funkci CLIP (přenos SMS a identifikace volajícího pevnou linkou)

Radiový přenos

Poslední z variant přenosu informací z ústředen PZTS je radiový přenos. Z výše uvedených forem je finančně nejnáročnější, neboť provozovatel PPC si musí pro zřízení vlastní radiové sítě a provozu na určené frekvenci zajistit povolení Českého telekomunikačního úřadu, a zákazník si potřebuje nainstalovat radiový vysílač, který je z používaných komunikátorů nejdražší.

Velkou nevýhodou je fakt, že spolehlivost přenosu je podmíněna dostatečnou silou signálu. Proto například v oblasti kopcovitého terénu musí být zřízena retranslační stanice, čímž

ještě více vzrostou náklady na provoz radiové sítě. V rádiovém přenosu jsou také vysoké požadavky na zajištění kvality sítě. V nekvalitní síti dochází ke ztrátám spojení, které je navíc nutno vždy prověřit, neboť může docházet k pouhému rušení, ale také může být objekt napaden. Naopak výhodou radiového přenosu je, zejména pro zákazníka, bezplatnost přenosu.

2.4.2 Přenosové formáty

Základem správného fungování DPPC je přenášení „kódované“ informace pomocí komunikátoru na PPC. V přenosovém centru musí být informace dekódována a zobrazena obsluze na pracovní stanici. Zpráva může být přenášena pomocí několika různých přenosových formátů. Volba takového formátu závisí zejména na parametrech ústředny, do níž je formát přenášen, a také na parametrech přijímače PPC.

Pulsní formát

Pulzními formáty jsou označovány takové formáty, které pro přenos jednotlivých zpráv využívají určitého počtu pulsů v určitém čase. V České republice je jedním z nejrozšířenějších formátů 4+2 (první čtyři čísla znamenají číslo objektu + další dvě čísla jsou kód zprávy). Jde o tzv. pulzní formát vysílaný po analogové lince. Mezi analogové formáty patří např. 4+2,4+3,4+1 Ademco expres, Radionics. Všechny tyto formáty využívají přenosové rychlosti 1200,2400, 4600 bit/s a záleží jen na typu DPPC, se kterým formátem a rychlostí dokáže pracovat.

Pro přenos zpráv využívají určitého počtu pulsů v určitém čase. Dva pulsy znamenají číslo 2, jedenáct pulsů znamená B. Kontrola přenosu spočívá v opakování přenášené zprávy. Nejběžněji používaným pulsním formátem je 4+2, kdy čtyři čísla udávají číslo objektu a dvě čísla značí kód události.

Přenosovou tabulku si vytváří správce daného PPC a může se tak mezi jednotlivými provozovateli PPC lišit. Technik, který provádí instalaci na objektu si musí tuto přenosovou tabulku vyžádat a ústřednu naprogramovat podle ní.

Maximální počet událostí, které je tento formát schopen přenést je 256, neboť se používá hexadecimální soustava. Z dvoumístného čísla události je proto možné získat pouze 256 kombinací. Z toho vyplývá, že tento formát přenosu je vhodný pouze pro malé instalace.

Při programování je třeba vzít v úvahu, že nula není definována, proto se programuje A a PPC automaticky překládá v čísle objektu A jako nulu, v případě události jako 10.

Tónový formát

Dalším druhem formátů jsou formáty tónové, mezi které patří například Contact ID, DTMF či Ademco CID. Každá číslice má svou přiřazenou dvojici tónů určité frekvence, přičemž celkem může být takových dvojic tónů maximálně 16. Díky takto vytvořetným kombinacím se podstatně zkrátila doba vytáčení a spojení s volanou stanicí.

Kontrola přenosu se provádí pomocí kontrolního součtu. Významně se tak zkracuje doba vytáčení a přenosu jedné informace na PPC. Při instalaci se na ústředně nastaví přenosový formát Contact ID a odpadá programování kódů k událostem. Obsah zprávy je následující [19]:

ACCT MT QXYZ GG CCC S

0123 18 1130 01 012 B

ACCT	identifikační číslo objektu (v tomto případě 123)
MT	typ zprávy (pro Contact ID 18 nebo 98)
Q	kvalifikátor typu zprávy (např. 1 = nová událost; 3 = obnova)
XYZ	kód události (např. 130 = poplach)
GG	označení podsystému (např. Grupa 1)
CCC	označení zóny nebo uživatele (v tomto případě poplach ze zóny 12)
S	kontrolní součet (součet všech čísel + kontrolní součet) MOD15 se musí rovnat nule. 0 je vysílána jako 10 a je takto započítána i do kontrolního součtu.

Modemový formát

SIA formát umožňuje plně duplexní přenos více informací najednou během časově krátkého přenosu. Formát využívá pro přenos zpráv z komunikátorů v objektu k PPC internetový protokol IP.

Výhody tohoto formátu jsou:

- sjednocení komunikace PZTS, EPS, videí a umožnění obousměrné komunikace
- synchronizace času v celé síti a možnost časových razítek u každé přenášené události
- zavádí kryptování zpráv s možností individuálních tabulek pro každý objekt – kódování metodou AES
- zavádí se vícenásobná identifikace zdrojů zpráv ID, MAC, IP adresa
- sjednocení výrobců, zvýšení konkurenceschopnosti a zjednodušení výběrových řízení
- umožňuje přímou kontrolu uživateli systému, dálkové ovládání systému s jistotou, že nelze komunikaci zneužít

Obsah zprávy [20]:

<LF><CRC><OLLL><“id“><seq><Rcvr><Lpref><#acct>[<pad>| data] [x.data]<timestamp><CR>

LF	ASCII znak 0 x A hex
CRC	započítávají se první platný znak ID až poslední znak před CR
OLLL	délka zprávy, započítávají se stejné znaky jako u CRC
„id“	toto pole obsahuje informaci (příznak) o použitém formátu datového pole ve zprávě , typu zprávy a informaci, zda je či není použito kryptování
Seq	vysílací zařízení přiřadí číslo každé generované zprávě. PPC vysílá toto číslo zpět v potvrzovací zprávě. Pokud zpráva není potvrzena, číslo se nezvyšuje. Rozsah čísel zpráv je 0001 - 9999
Rcvr	číslo přijímače slouží k dalšímu rozšíření identifikačního čísla, jako jeho prefix. Hodnoty jsou ASCII „R1 - R6“. Vysílání tohoto parametru je nepovinné
Lpref	Account prefix) rozšíření ID o další čísla ... L+1-6 hex čísel. Pokud toto nechceme využít vysíláme L0.Parametr je podobný jako linka přijímače
#acct	ID naprogramované v objektovém zařízení
pad	výplň datového pole na sudý násobek 16 pro kódování

data

x.data přidává k datům další rozšiřující informace např. MAC Adresu

timestamp (časové razítko) ... <_HH:MM:SS,MM – DD - YYYY> čas je GMT povolená diference pro platnost zprávy je +20/ - 40 sec.

CR ASCII znak 0 x D hex

Modemové formáty SIA představují třetí typ přenosových formátů. Hlavni výhodou SIA formátu je časově krátký přenos v íce informací najednou. Z ústředny PZTS je většinou potřeba přenést jen jednu, tu nejdůležitější zprávu. U SIA se používá tzv. full – duplex přenos, data se přenášejí oběma směry (tj. i z PPC do PZTS) , kounikace (až na přenosovou rychlost) velmi připomíná běžné modemy pro telefonní linky (28 800 bit/s). Data se přenášejí pomoci 1 a 0 (velmi připomíná starší způsob připojení na internet pomocí modemu). [21]

Dohledové centrum odpovídá na přenos informace dvěma signály, které se nazývají Handshake a Kissoff

- Handshake

Handshake generuje DPPC po zvednutí linky a potvrzuje ústředně připravenost přijmout data a průchodnost přenosové cesty. Handshake musí přesně časově a frekvenčně odpovídat následujícímu předpisu, jinak ústředna nezačne posílat data.

Tabulka č. 1: Princip Handshake

<table>
<tr><td>Signál</td><td rowspan="3">Vyzvánění</td><td rowspan="3">Pauza</td><td colspan="3">HANDSHAKE</td><td rowspan="3">Pauza</td><td rowspan="3">Data</td></tr>
<tr><td>Linka vyzvednuta</td><td></td><td></td><td></td></tr>
<tr><td>Linka položena</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td>1</td><td colspan="7">Vyzvánění na telefonní lince</td></tr>
<tr><td>2</td><td colspan="7">Prodleva před odesláním handshake minimálně 0,5 vteřiny až max 2 sec.
Tato prodleva slouží pro ustálení telefonní linky po zvednutí</td></tr>
<tr><td>3</td><td colspan="7">Signál 1400 Hz +/- 3% s trváním 100 msec+/- 5%</td></tr>
<tr><td>4</td><td colspan="7">Pauza 100 msec +/- 5%</td></tr>
<tr><td>5</td><td colspan="7">Signál 2300 Hz +/- 3% s trváním 100 msec +/- 5%</td></tr>
<tr><td>6</td><td colspan="7">Pauza před posláním dat 250 msec – max 300 msec po doznění handshake nebo kissoff</td></tr>
<tr><td>7</td><td colspan="7">Posílání dat</td></tr>
</table>

Zdroj: [22]

- Kissoff

Signál Kissoff oznamuje ústředně, že DPPC přijal zprávu bez chyb. Obckle je tento signál v Hz (např. 1400 Hz) v rozpětí +/- 3 % s dobou trvání minimálně 750 msec až 1 sec. Ústředna musí detekovat minimálně 400 msec signálu Kissoff, aby mohla signál vyhodnotit jako „platný“.

Ústředna akceptuje odchylku frekvence +/- 5% pro zpětnou kompatibilitu. Pokud ústředna nevyhodnotí signál jako platný, Kissoff musí zprávu opakovaně poslat minimálně 4x, než může telefonní linku položit a vytáčet znovu. Čítač posílání zpráv je pro každou zprávu samostatný a je resetován vždy po zachycení signálu Kissoff. Bezpečnostní ústředny využívají hexadecimálního (šestnáctkového) kódování [22]:

Zprávy, které jsou naprogramovány v ústředně PZTS, musí být následně přenášeny na PPC. Záleží také na požadavcích zákazníka, zdali chce, aby byly přenášeny pouze poplachové zprávy (většinou z důvodu úspory na telefonních poplatcích), nebo naopak umožní přenášení všech zpráv, což pak rozvíjí nabídku dalších doplňkových služeb (např. upozornění, že objekt není zakódován nebo kódování probíhá mimo určenou dobu atp.)

Přehled přenášených zpráv a jejich priorita:

1. Poplachové zprávy: zprávy s nejvyšší prioritou přenosu (narušení zóny, tísňové poplachy, požár, sabotáže)
2. Poruchové zprávy: informace o poruchách na PZTS (poruchy napájení, poruchy akumulátoru, porucha komunikace, poruchy expandérů atp.)
3. Testovací zprávy: automatické testy pro kontrolu komunikace
4. Systémové zprávy: nemusí být přenášeny (informace o změnách času, vstup do programu, ukončení programování, bypass zóny atp.)

Jednotlivé zprávy jsou v monitorovacím softwaru na pracovní stanici obsluhy PPC rozlišeny různými barvami (např. červené jsou alarmové zprávy, zelené jsou nezastřežené objekty, šedé naopak zastřežené.) pro lepší orientaci v příchozích zprávách. Poplachové a poruchové zprávy jsou zároveň označeny akusticky.

II. PRAKTICKÁ ČÁST

3. DPPC V KOMERČNÍ SFÉŘE

3.1 Stručná historie DPPC

Moderní historie DPPC začíná v roce 1853, kdy byl v New Yorku zbudován pult centralizované ochrany Edwinem Holmesem (první historicky doložený dokument týkající se PCO). Další pokrok byl zaznamenán v roce 1876, kdy Alexander Graham Bell převedl svoji myšlenku o dálkovém přenosu lidského hlasu s využitím drátů do praxe. Tyto dráty byly také určené a využívané k zabezpečovacímu pultu centralizované ochrany (tehdy ještě neoznačované pulty centralizované ochrany objektů).

Edwin Holmes, který byl zakladatelem Newyorské městské společnosti, dodnes nesoucí jeho jméno, se dále stal průkopníkem prvních telefonních ústředen a především elektrických poplašných zařízení. Dokázal vynalézt první telefonní kontakt, fungující na principu váhy sluchátka, která rozpojuje telefonní okruh. Tohoto principu je využíváno dodnes. Stal se průkopníkem a prosazovatelem komerčního používání poplašných a telefonních systémů v době, kdy neexistoval žádný výrobce zabývající se tématikou těchto zařízení. Další prvenství Edwin Holmes získal, když jako první muž vyrobil izolované elektrické vodiče a instaloval vlastní propojovací okruh mezi chráněnými objekty a vlastním centrálním úřadem.

Mezi seznam uživatelů Holmesovy centrály elektrické ochrany, založené v roce 1858 v Bostnu a v New Yorku, brzy patřilo mnoho prominentních zákazníků, mezi nimi mimo jiné Tiffany, Bowery Bank atd.

Roku 1872 vyvinul pro prodejny a výrobce šperků „elektrický sekretář“, kam se mohly klenoty ukládat. Tento sekretář byl připojen na centrální stanoviště se 24 hodinovou službou schopnou kdykoliv zakročit. Vroce 1873 předložil A.G.Bell prototyp telefonu, který již obsahoval elektrická vedení vytvořená podle Holmesových návrhů, spojující centrálu se zákazníky. V květnu 1877 pak byla v New Yorku dokončena první komerční telefonní ústředna.

V Československé republice byla první větší aplikace zabezpečovací techniky zaznamenána v roce 1933, kdy byly zřizovány automatické poplašné telefonní hlásiče. [23]

V období po druhé světové válce byla ochrana osob a majetku plně v kompetenci československého ministerstva vnitra, nejprve složek Sboru národní bezpečnosti (SNB), následně Veřejné bezpečnosti (VB) a Státní bezpečnosti (StB).

Za monopolního dodavatele komunikační techniky, elektrické zabezpečovací techniky (EZS) a požární techniky (EPS) byl určen „koncernový podnik" TESLA.

Největší rozmach elektrických zabezpečovacích systémů (dříve používané názvosloví „EZS" nahrazeno dále v textu jen „I&HAS") nastal v padesátých let minulého století, zejména zavedením těchto systémů v bankovních domech, využívajících elektrické spínací zámky trezorových dveří se světelnou a akustickou signalizací, systém kontaktních detektorů, trezorových vibračních detektorů a zařízení PETEX.

V letech 1950 - 1960 vyráběla I&HAS závodní pobočka Tesla Jihlava. Jednalo se zejména o jednoduché ústředny SU - 1, dálkové signalizace DS - 1, ale také o více smyčkové ústředny SU 5, SU 10, SU 15, které vzhledem ke své konstrukci, rozměrům jednoduchosti v obsluze používány na některých objektech ještě v současné době.

V roce 1958 bylo v podniku Obchodní zařízení a potřeby státního obchodu Praha započato s vývojem prvních zabezpečovacích elektrických prvků a systémů, na kterém se podílelo i Ministerstvo vnitra.

V 70. letech se k domácím výrobcům přidala i řada zahraničních firem, která tímto obohatila domácí trh o další systémy I&HAS.

V roce 1974 byla ve složkách tehdejší Veřejné bezpečnosti zřízena speciální pracoviště, která se zabývala využitím prostředků zabývajících se I&HAS. K velkému rozmachu došlo především s vývojem a uvedením na trh, nového systému I&HAS, jehož širšímu využití napomohlo Usnesení vlády ČSSR č. 73 z 18. března 1982 a navazující usnesení vlády ČSR č. 101 a Usnesení vlády SSR č. 115 ze dne 14. dubna 1982 centralizace zabezpečených objektů. Usnesení určovalo kategorie objektů a z toho vyplývající nároky na složitost I&HAS. Vznikla řada organizací, zabývajících se projekcí, montáží a servisem. [23]

V roce 1974 byl u Služby ochrany objektů VB v Příbrami zkušebně instalován první pult centralizované ochrany objektů (PCO/ARC). Nejprve byly napojeny čerpací stanice PHM, jeden peněžní ústav a sklady trhavin. Potom následovaly objekty obchodní sítě a objekty kulturního a památkového významu. Na základě vyhodnocení byl tento PCO/ARC rozšířen

do většiny krajských měst. Jednalo se o reléový linkový pult CENTR KM. Umožňoval napojení 120 objektů na teritoriu jedné telefonní ústředny.

V roce 1986 byla vydána ČSN 33 4590 I&HAS. Tím byl vnesen určitý řád do projekční a montážní činnosti zavedením homologačních podmínek a stanovením pravidel týkajících se PCO/ARC, konkrétně projektu a montáže. Během let přicházeli do policejní výzbroje další PCO/ARC – např. RONA, TCP 60, TRVZ a GENOVA.

V roce 1989 přestává být využití I&HAS a doménou pouze policie. V oboru ochrany majetku a osob, začínají podnikat nejrůznější výrobní, obchodní a montážní firmy a také bezpečností agentury. Rozvíjí se průmysl komerční bezpečnosti. [23]

3.2 Kritéria pro výběr

Výběr dodavatele se musí řídit specifickými kritérii. Montážní organizace musí mít zejména koncesní listinu na oblast poskytování technických služeb k ochraně majetku a osob. Podkladem pro specifikaci dodávaných bezpečnostních systémů má být bezpečnostní posouzení. Návrh a projektová dokumentace musí být zpracována podle technických norem. Při předání je třeba požadovat výchozí elektrickou revizi, zaškolení obsluhy a dokumentaci skutečného provedení. Při výběru dodavatele musí být zváženy možnosti dodavatele při nutnosti poskytnutí servisu, tedy doba reakce, dojezdová vzdálenost a cestovní náklady.

Také výběr bezpečnostní služby musí projít důkladnou přípravou. Při připojení na DPPC se doporučuje prověřit si, zdali má daná společnost koncesní listinu pro oblast ostrahy majetku a osob, ideálně plnící českou technickou normu pro provozování DPPC. Zákazník by měl požadovat smluvně garantovanou maximální dobu dojezdu, ve smlouvě musí být dohodnuta také reakce bezpečnostní služby na standardní poplach v případě tísně.

Podklady pro bezpečnostní posouzení vhodného typu instalace by měly zahrnovat zejména rozvahu v následujících oblastech:

a) Omezení přístupu. Je nutné vzít v úvahu, kdo všechno může mít přístup do prostor – zdali pouze personál, či také osoby z veřejnosti. Doporučuje se důsledné oddělení prostor s přístupem pro personál. Většinou postačí dveře se zámkem, případně kování koule-klika a klíč. V některých případech je vhodné použít také ucelený

systém kontroly vstupu s použitím např. systému bezkontaktních karet. Urychlí to pohyb osob a zajistí identifikaci. Dveře vedoucí do prostor, v nichž se ukládají cennosti, by měly být vybaveny čtečkou z obou stran.

b) Nabídka poplachových zabezpečovacích a tísňových systémů (alarmů). V případě nepřetržitého provozu se uplatní tísňová tlačítka, zejména ve větších či finančních institucích. Díky nim může obsluha při problémech rychle přivolat pomoc výjezdové hlídky nasmlouvané bezpečnostní služby. Tísňová tlačítka by měla být umístěna skrytě, avšak na dosah ruky obsluhy. Personál by měl obdržet režimovou směrnici s pokyny, kdy toto tlačítko použít a jakým způsobem. Ochrana života a zdraví osob má vždy přednost před ochranou majektu.

Každá společnost by měla nejprve provést analýzu a detailní plán prostor, do nichž bude bezpečnostní systém instalovat. Správný poskytovatel služeb by měl vytvořit takový program, který by odpovídal velikosti prostor, počtu pracovníků, účelu provozovny a dalším kritériím.

3.3 Analýza použití DPPC na trhu komerční instituce

V oblasti ochrany komerčních objektů je mnoho nových prostředků. Následující kapitoly ukazují, jakými směry se tato oblast ubírá, a jaké možnosti lze využít při ochraně bankovní instituce.

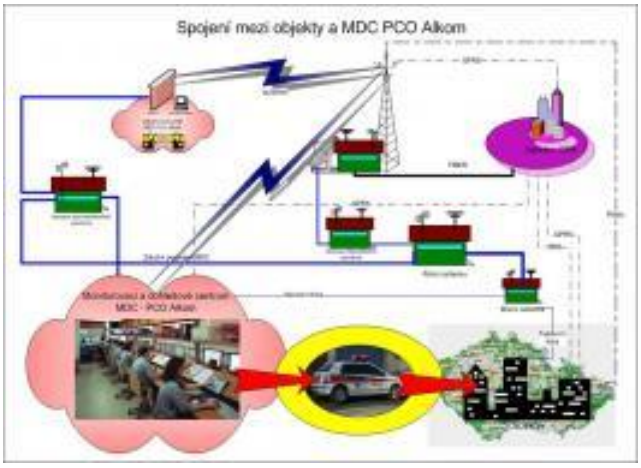
3.3.1 Dálková a vzdušná ochrana veřejných prostředků

Dálkový monitoring objektů umožňuje soustředit různé typy signálů a tím vytvořit systém, kde lze na jednom pracovišti monitorovat více míst objektu, popř. více objektů. Signály z jednotlivých objektových systémů (CCTV, EZS, EPS apod.), které tvoří základ zabezpečení, jsou prostřednictvím objektové stanice předávány centrální stanici, tedy pultu centralizované ochrany buď radiovou cestou, případně po telefonních nebo datových linkách. V případě poplachu, nebo jiné mimořádné události na kterémkoliv objektu operátor SCO zajistí její řešení. [24]

Jednou z možností vzdušné ochrany mohou být komplexní služby Multifunkčního dohledového centra (dále jen MDC), které bylo vybudováno na základě požadavků České

pošty. Činnost MDC vhodně doplňuje zajištění komplexních služeb v oblasti ochrany osob, majetku, efektivního monitoringu, dohledu, servisu, přenosu informací, ochrany dat a osobních údajů, řešení krizových situací, havárií vody, plynu, výpadků elektřiny. [25]

Obrázek 5: Fungování DPC 1



Zdroj: [25]

Tento systém reaguje na fakt, že standardní EZS zakončené sirénou nebo v lepším případě signalizací na mobilním telefonu zákazníka prostřednictvím zabudovaného komunikátoru se v praktickém životě stávají stále méně a méně praktické. Samotné sirény zloději často velmi snadno zneškodní, často i spuštěný alarm nevzbudí v okolí žádný zájem a přijatý signál o neoprávněném vniknutí do objektu nemusí zajistit plnohodnotnou ochranu zákazníkova majetku. [25] Proto se systém snaží nabídnout propracovaný systém, který by výše uvedené nedostatky eliminoval.

Sama společnost uvádí následující výhody jejich systému:

- jednotnost napojení – dohled nad všemi objekty zákazníka
- kvalita a odbornost personálu
- kvalita technického řešení připojení objektů
- komplexnost bezpečnostních, servisních a provozních služeb
- integrované servisní centrum
- zefektivnění servisních činností – pomocí dálkového dohledu ústředen EZS
- jednotné telefonní číslo v rámci celé České republiky – 12726

- jednotná odezva v případě krizové situace
- hot line technická pomoc 24 hod. Denně
- stanovení a kontrolování kvalitativních parametrů pro zásahové skupiny v celé ČR
- vedení a aktualizace pomocných evidencí včetně centrální evidence požadavků klienta
- kvalita zpracování a archivace informací a evidencí včetně jejich ochrany
- sledování technologických procesů
- standardizace bezpečnostních režimových opatření
- splnění podmínek certifikace zařízení v rámci EU za podmínek normy ČSN ISO/IEC 17799 "Postupy pro řízení informační bezpečnosti"
- zabezpečení datových uzlů, serverů a datových sítí
- snížení podílu lidského činitele v oblasti bezpečnostních technologií
- snížení nákladů na realizaci bezpečnostních opatření
- zvýšení znalostí a schopností při obsluze bezpečnostních systémů
- možnost integrace i dalších technologií jako např. EPS, ACS, WAN, LAN sítě, a další
- zlepšení komunikace, která bude probíhat dle předem připraveného scénáře
- spojení na oficiální linky pomoci
- spolupráce s bezpečnostními složkami státu (policie)
- kvalitní zabezpečení vlastního pracoviště
- fungování záložního pracoviště na jiném místě pro případ krizové události

Dalším způsobem, jak chránit objekty vzdušnou cestou, je nainstalování ACC (Aerial / Airborne Command and Control). Tento typ je vhodný pro zabezpečení rozlehlých areálů, provozoven, soukromých pozemků, ale i veřejných prostranství v průběhu společenských akcí. Jeho podstatou je bezpečnostní dohled pomocí bezpilotních létajících prostředků vybavených opticky velmi kvalitní videotechnologií s možností dálkového přenosu videosignálu. Díky těmto nejmodernějším prostředkům je možné nejen zvýšit efektivitu pozemního bezpečnostního personálu a zlepšit jeho reakční schopnosti, ale i nouzovou signalizací asistovat při evakuaci osob nebo napomoci při pátrání po pohřešovaných osobách a odcizených předmětech.

Součástí tohoto systému je zejména: [25]

- krátkodobý či trvalý dohled pomocí zajištěného létajícího prostředku s volitelnou videotechnologií (standardní Full HD kamera, noční vidění, termovize)
- krátkodobý dohled, monitoring, sledování pomocí UAV (drone)
- možnost monitoringu v nedostupných a technicky či geograficky náročných oblastech (výškové budovy, technická zařízení, produktovody, lesní a horské oblasti)
- opakované kontroly díky možnosti letů podle GPS souřadnic (monitoring průběhu investičních akcí)
- monitoring rizikových míst (vhodné pro zásahy v oblastech průmyslových havárií, živelných pohrom, nácviku krizových situací, atp.)

S využitím této moderní a vysoce sofistikované technologie ve spojení s profesionálním přístupem dokáže tento systém zajistit náročné požadavky klientů na zajištění bezpečnosti soukromých a podnikatelských aktivit. Navíc firma analyzuje již proběhlé zásahy, a na základě těchto analýz pak vylepšuje svůj systém. Každý typ je svým způsobem unikátní, neboť je programován speciálně dle požadavků klienta.

Následující obrázek ukazuje systém dohledového vzdušného centra:

Obrázek 6: Dohledové vzdušné centrum 1

Zdroj: [26]

Z hlediska rozsahu činností požadovaných klienty je tento systém na českém trhu ojedinělý a moderní. Činnost tohoto moderního MDC byla zahájena na podzim roku 2003 a neustále se rozvíjí. MDC zajišťuje bezpečnostní a servisní monitoring pro objekty na území celé České republiky.

Zároveň s tímto systém nabízí prohlídky proti odposlechu, které jsou považovány za nejúčinnější metodu, jak zabránit úniku citlivých informací. Toto opatření se jeví nezbytné pro ty, kteří si svých informací cení a chtějí je chránit. Prohlídky jsou prováděny rychle,

diskrétně a efektivně za pomoci nejmodernějšího dostupného technického vybavení, a mohou být prováděny v bytě, v kanceláři, v jednacích sálech či v osobních automobilech. Provádí je speciálně vyškolení pracovníci s dlouhodobou praxí v oboru, kteří mají přehled v moderních metodách odposlechu. bytů

Na základě požadavků lze instalovat technická zařízení znemožňující odposlech v pásmech GSM, UMTS a CDMA, rušičky sítí Wi-Fi. Technicky je tak minimalizováno riziko monitoringu pohybu zákazníka pomocí zařízení GPS.

Lze též zvýšit elektronickou bezpečnost tím, že firma zabezpečí výpočetní techniku a sítě klienta proti nežádoucímu úniku informací a jejich zneužití. V rámci této služby je instalován speciálně vyvinutý software umožňující skryté monitorování všech činností a komunikace na počítači. Výhodou tohoto produktu je jeho kompatibilita se všemi operačními systémy.

3.3.2 DPPC v ochraně bankovní instituce

Zaměstnanci finančních institucí, především pak pokladníci pracující s hotovostí, by měli nejen být profesionální, ale též pravidelně procházet školením, které by je alespoň teoreticky připravilo na možné loupežné přepadení pobočky. Nejčastější variantou je ozbrojené, často násilné napadení personálu a vyhrožování. Ve většině případů pachatel dává přednost menším pobočkám, kde je malý počet zaměstnanců a pečlivě volí dobu, kdy přepadení uskuteční.

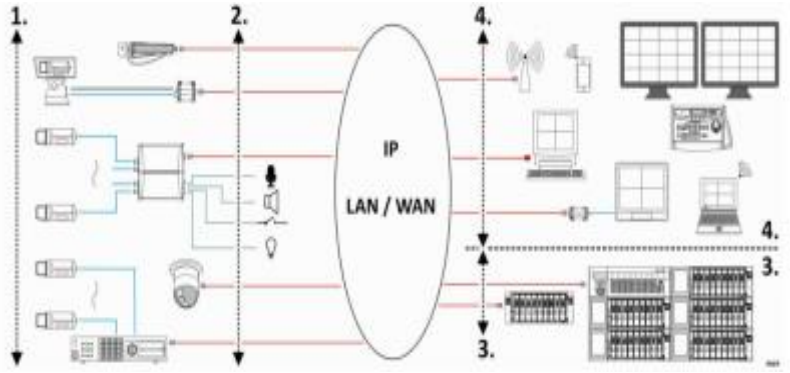
Pro tento případ bývají bankovní instituce zabezpečeny hned několika způsoby. Může se jednat například o využití detektorů pohybu, kamerového systému či detektorů tříštění skla. Tato zabezpečení však slouží ke střežení daného objektu především v době, kdy je již banka zavřená. V provozní době, kdy je banka otevřena k službám svých klientů, může vstoupit do banky i pachatel se skrytým úmyslem jejího přepadení. Pro tyto účely jsou zaměstnancům bank pořizovány tísňové hlásiče. [26]

Tísňové hlásiče ovládané zaměstnanci finančních ústavů slouží pro vyhlášení poplachu při napadení v průběhu pracovní doby. Tam, kde je to možné, bývají doplněny optickou signalizací poplachu viditelnou pouze zaměstnanci. Zaměstnanec má pak jistotu, že centrála DPPC na jeho akci zareagovala. Tísňové hlásiče jsou umístěny tak, aby ze strany zákazníka nebyly vidět. Jedná se tedy o různé druhy tlačítek, tísňové lišty, detektory

poslední bankovky a osobní bezdrátové tísňové hlásiče umožňující vyhlášení poplachu i mimo prostor objektu.

Následující schéma zobrazuje, jakým způsobem jsou v tomto případě rozmístěny jednotlivé prvky systému:

Obrázek 7: Schéma rozmístění zabezp. 1



Zdroj: [27]

Důležitá je v tomto případě instalace tísňových hlásičů. Ta by měla být realizovaná vhodnou kombinací veřejných, speciálních i osobních hlásičů. I když jsou nejčastějším místem útoku pachatele pokladní přepážky, je vhodná instalace i v ostatních místech, kde dochází k manipulaci s penězi. Jedná se například o přístupová místa k trezorům, bezpečnostním schránkám, k místům, kde jsou uloženy klíče.

Dále je nutné brát v úvahu, že zaměstnanec může při přepadení využít únikové cesty, nebo naopak může být uzamčen v místnosti. To jsou také místa, kde je vhodné umístit hlásiče. Zaměstnanci musí především o těchto hlásičích vědět. Jejich umístění musí být pro cizí osoby skryté. [26]

Tísňové hlásiče mohou být instalovány v následujících verzích:

- Speciální tísňové hlásiče lištové se instalují na zem pod stůl nebo na spodní stranu desky stolu, kde pracuje pokladní. Pro sešlápnutí lišty je vhodné její umístění v místě, kde pokladní může nepozorovaným natažením nohy a sešlápnutím lišty aktivovat hlásič.

V druhém případě se aktivují kolenem, při zdvihnutí nohy, popřípadě rukou. Obsluha při manipulaci sedí. Způsob aktivování tísňového hlásiče by mělo být daným zaměstnancem nacvičeno ihned po instalaci. Musí být přizpůsoben jeho pohybům, tak aby nebylo možné

jeho zpozorování. Pachatel sleduje především pohyby rukou, je tedy v tomto případě vhodnější použít nohu k aktivaci poplachu. Mnohdy je výhružka na vydání peněž předložena písemně pokladní a ostatní zaměstnanci o dané situaci nic netuší.

- **Speciální výklopná tlačítka** se instalují ze spodní desky stolu, tak aby nebyl spínač normálně vidět. Je potřeba zajistit aby indikační LED nebylo možné nijak zastínit. Je - li rameno rozevřeno mezi 20°a 45°, přepne se poplachový kontakt a rozsvítí se led indikace paměti poplachu. Po uvedení ramene do klidové polohy se poplachový kontakt vrátí do původní polohy, přičemž LED – kontrolka paměti zůstane svítit, dokud tato paměť nebude resetována rozpínacím tlačítkem.

Umístění výklopného hlásiče, by mělo být v místech, odkud jiní pracovníci banky vidí do prostoru pokladen a mohou se tak stát svědky přepadení. Dále v dalších prostorech, kde může dojít například k uzavření zaměstnance, v přístupových místnostech k trezorům, bezpečnostním schránkám a klíčům.

Vždy by měli být umístněny skrytě podle rozmístění nábytku a podle přirozeného pohybu rukou zaměstnance, tak, aby vzniklo co nejmenší riziko jeho zpozorování. Je vhodné umístit signalizaci do oddělených kanceláří, aby se ostatní pracovníci dozvěděli o vzniklém nebezpečí.

- **Automatické bankovkové detektory** se pomocí dvou šroubů připevňuje na dno peněžní zásuvky. V mechanicky odolném pouzdru je uložen mikrospínač, který po vyjmutí poslední bankovky způsobí vyvolání poplachu. Je vhodné je umístit ve všech pokladnách.

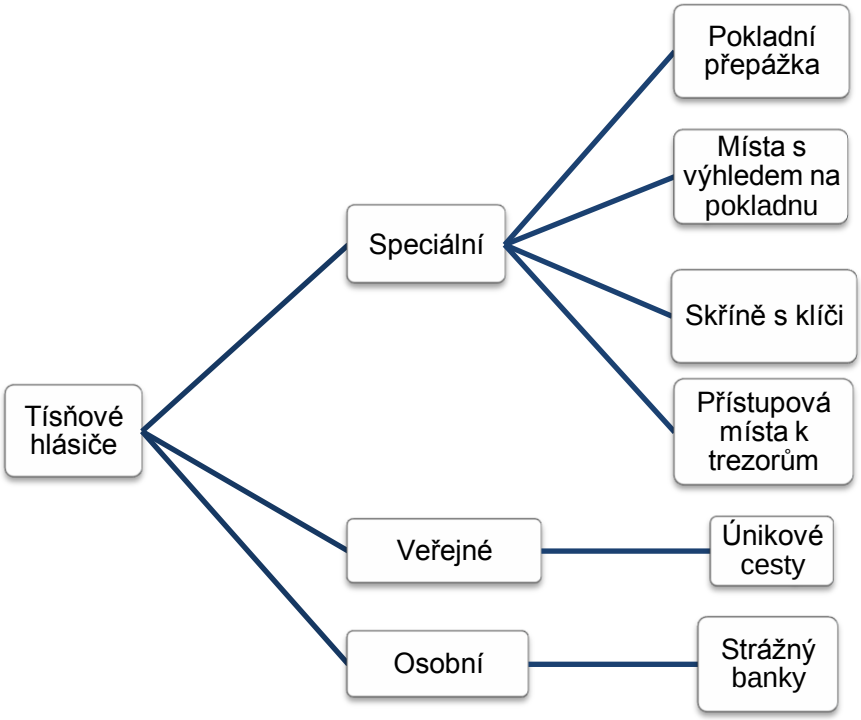
- **Osobní tísňové detektory** nosí ostraha banky a to skrytě v kapse nebo přivěšené např. na klíčích. Při obchůzce střeženého prostoru, kontroluje situaci a v případě zpozorování přepadení, může vyvolat skrytě poplach, případně zasáhnout. Osobními tísňovými hlásiči lze navíc ovládat osvětlení, ovládání dveří, což může také znesnadnit únik pachatele.

- **Veřejné tísňové hlásiče** by měly být umístěny v únikových chodbách. Jsou tak určeny pro zaměstnance, ale i zákazníky, kteří při úniku z přepadené banky mohou v tomto prostoru vyvolat poplach.

V případě vyvolání tísňového poplachu je vhodné, aby signalizace tísně byla ústřednou přeposlána do více míst. Jedná se tedy o přenos signalizace do DPPC soukromé bezpečnostní služby a policie. V rámci objektu by měl být informován strážný a také pracovníci v oddělených kancelářích, aby nevstupovali do míst loupežného přepadení.

Na následujícím schématu je zobrazeno, do jakých míst, zejména na pravé straně schématu, je nezbytné instalovat tísňové hlásiče.

Obrázek 8: Schéma umístění TH 1



Zdroj: Autor

Mohou být též použity různé typy kamer, dle požadovaného rozpočtu [28]:

- USB kamera: Typické webové kamery stojí něco mezi 500 a 2 000 Kč, připojují se k portu USB, některé mohou pořizovat obrázky v HD a mnohé mají automatické osvětlení pro fotografování za špatných světelných podmínek. Program SupervisionCam ve své bezplatné verzi ukládá obrázky pořízené kamerou. Ty jsou maximálně v rozlišení 640 x 528 bodů, což tyto kamery většinou zvládají. Větším problémem je extrémně veliká reklama, která se objeví na snímku a má tendenci zakrýt sledovaný objekt. Proto se vyplatí software za zhruba 40 eur zakoupit a zaregistrovat.
- Wifi kamera: Umožňuje volnost pohybu. Toto zařízení lze nejčastěji pořídit za cenu zhruba od 1 500 do 7 500 Kč. Ideální je sáhnout po IP kameře vybavené infračerveným nočním viděním a samostatně integrovaným detektorem pohybu. S těmito funkcemi může zákazník kameru využívat plnohodnotně i bez

dodatečného dohledového softwaru. Síťové kamery jsou totiž součástí sítě a mají vlastní IP adresu. Ve Windows 7 jsou detekovány automaticky a integrovány do systému.

- Venkovní kamera: Pro sledování vstupní brány nebo garáže bude nezbytné instalovat odolnou outdoorovou kameru do každého počasí (2 500 - 18 000 Kč). Ideální je sáhnout po bezdrátovém modelu, jinak musí být použita dvojice kabelů: jeden zdrojový a druhý pro přenos obrazového signálu. Kamera by měla být namontována na viditelné místo, avšak do výšky, kam na ni nelze snadno dosáhnout. Tak lze zabránit případnému odcizení, a zároveň bude mít zákazník přehled o svém majetku.
- Infračervená kamera: Obyčejné webové kamery nedisponují nočním viděním. Pro noční záznam proto musí být instalován model vybavený vestavěným infračerveným LED (1 300 -5 000 Kč). Zákazník si také může svépomocí upravit obyčejnou webovou kameru, pokud je dostatečně zručný. Poté by se cenová relace pohybovala okolo 800 Kč. Kupované modely mohou být připojované buď pomocí kabelů či ethernetu, případně je možné vybrat bezdrátovou variantu. Infračervené LED nejsou viditelné a v případě venkovních modelů mají dosah až 100 metrů, který se uvnitř snižuje na zhruba pět metrů.

Obrazy z těchto kamer lze zobrazit buď v prohlížeči počitače, ve smartphonu či tabletu, 24 hodin denně, v kterékoliv části domu.

Důležité je věnovat pozornost správnému nastavení HTTP Serveru. SupervisionCam disponuje integrovanou funkcí HTTP serveru. Ten lze aktivovat v nastaveních v kategorii »HTTP Server« zaškrtnutím políčka »Enable HTTP Server«. Jméno serveru bude identické s názvem počítače. K výstupům webových kamer je důležité zvolit správné heslo. Po celkovém potvrzení tlačítkem »Apply« nebo »OK« se ozve firewall systému Windows a zablokuje program. V okně je pak nutné povolit komunikaci pro privátní sítě. Rozlišení fotografií zákazník nastaví na maximální hodnotu (dle druhu webkamery).

Pro konfiguraci routeru je nezbytné znát IP adresu směrovače. Tu lze získat z bezplatné webové DNS služby typu No-IP.com. Zadá se URL, uživatelské jméno a heslo svého routeru. HTTP server aplikace SupervisionCam využívá port 80. Je však bezpečnější nastavit pro vzdálený přístup vyšší port, například 40 000 -, což se učiní pod volbou »Configuration / Settings / HTTP Server / Port«. Tento port pak musí být přesměrován

v nastavení routeru. Kupříkladu u novějších směrovačů D-Link (všechny využívají stejné webové rozhraní) se toto nachází pod záložkou Pokročilé nastavení »Advanced«, kde lze nastavit jak virtuální server, tak právě přesměrování portů. Vyplní se všechny potřebné údaje a ty se následně uloží.

Dále je nutné nastavit správně zobrazení záznamu v prohlížeči, čehož se docílí tím, že do prohlížeče bude zadáno DNS webovou adresu následovanou dvojtečkou a číslem portu, tedy něco jako http://myWebCam.no-ip.com:40000. Prohlížeč se zeptá na heslo SupervisionCam, po jeho zadání pak otevře přehledovou stránku (SupervisionCam protocol) s nejaktuálnějším obrazovým záznamem webové kamery. Historii posledních padesáti fotografií lze zobrazit pomocí odkazu /Doc$1/Destination.htm.

Pro větší prostory je možno nastavit přístup přes supervision view. Ten lze stáhnout ze stejnojmenného odkazu na přehledové stránce programu SupervisionCam. Po instalaci a spuštění je nutné najít webovou adresu DNS a heslo. Program se připojí k serveru SupervisionCam a zobrazí snímky z webové kamery. [28]

4. DPPC V SOUKROMÉ SFÉŘE

V současné době je možnost vybírat z celé řady softwarových řešení, která dokážou pomoci s ochranou soukromého objektu. Pozitivní je, že mnohá z nich jsou k dispozici zcela zdarma. Tyto programy by však vždy měly být spojeny s odborným naistalováním kamer a jejich pravidelnou údržbou.

Například open-source systému iSpy nabízí pestrou paletu funkcí. Výhodou jsou zejména následující skutečnosti: podporuje neomezený počet kamer a mikrofonů včetně detekce zvuku a pohybu, umožňuje plánovat nahrávání, samozřejmě k němu lze přistupovat také vzdáleně (jak v rámci sledování, tak kvůli zadávání příkazů, třeba přes smartphone), nechat jej automaticky nahrávat záznamy na YouTube, či nastavit, kam má posílat upozornění při detekci zvuku či pohybu. Pro našince je samozřejmě velmi pozitivní česká lokalizace. Zdarma bývá i software podporující jedinou značku kamer. Zde je v nabídce například poměrně kvalitní program Vivotek ST3402 s podporou pro šestnáct kamer (samozřejmě značky Vivotek) nebo třeba D-ViewCam určeného pro produkty D-Link. V případě, že zákazník potřebuje opravdu profesionální řešení nabízející podporu full HD záznamů či 64bitových systémů, nabízí se například Abus VMS.

Zajímavým doplňkem k zabudování dohledového centra může být elektronický hlídač EW01. Při detekci pohybu dokáže přístroj simulovat štěkot hlídacího psa (hlasitost až 105 dB). Hodí se k zajištění vchodových dveří či terasy. Cena se pohybuje okolo 1 800 Kč. Případně je možno zakoupit tazvanou FAKE TV. Tento produkt dokáže vzbudit dojem, že je zákazník ve své domácnosti a dívá se na televizi. Při pozorování zvenku je prakticky nemožné odhalit podvrh. Efekt simuluje 27“ televizor s podsvícením LED. Cena je přibližně 1 000 Kč, Pro náročné je možno zabudovat do vyznačených míst atrapu kamery. Ta by měla odradit potenciální narušitele simulováním video dohledu. Dodává se i s potřebnými kabely. [28]

Všechny výše zmíněné programy sice mohou ochránit soukromý majetek, avšak samy o sobě nepředstavují dostatečné zabezpečení. Proto je nutno věnovat pozornost správnému výběru poplašného a zabezpečujícího zařízení, který je provozován některou z ověřených společností.

4.1 Různé možnosti instalace zařízení PZTS

4.1.1 Systém ALEXOR

Tento bezdrátový zabezpečovací systém je vhodný pro zabezpečení domu nebo bytu. Jeho použití je velice jednoduché, dokáže rozpoznat různé nebezpečí a tak okamžitě ohlásit vloupání, požár, zatopení vodou, zdravotní obtíže i přivolat první pomoc.

Obrázek 9: Schéma systému ALEXOR 1

Zdroj: [29]

Součástí tohoto systému je perimetr, tedy venkovní detektor komerčního charakteru. Ten může pocházet od mnoha výrobců, může být určen pro různé kategorie objektů jak z hlediska parametrů, tak i z hlediska cenového. Poskytovatel se snaží sortiment nadále doplňovat, aby byl schopen vyhovět i specifickým požadavkům.

Úspěšné nasazení venkovních detektorů a zejména detekčních systémů se vzhledem k jejich specifikům i technické náročnosti neobejde bez příslušné prohlídky objektu. Odborný pracovník z poskytovatelské firmy obvykle přijde k zákazníkovi, a po zmapování objektu je schopen navrhnout systém venkovního či obvodového zabezpečení od návrhu systému až po jeho zprovoznění. [29]

Součástí tohoto systémy jsou následující komponenty.

- Kamerový systém (CCTV - Closed Circuit Television) se používá ke sledování zájmových prostor a k zobrazovní záběrů z kamer na monitorech. Skládá se z kamer, záznamového zařízení a software. Mohou obsahovat dodávky CCTV technologií pro ekonomické, středně náročné i vysoce náročné aplikace. Lze si vybrat také nejkomplexnější portfolio produktů pro systémy na bázi IP technologii, kde existuje jak ucelený a široký sortiment IP kamer a IP serverů, tak i komplexní softwarová a hw řešení. Součástí objednávky je také instalace.
- EKV - elektronická kontrola vstupu nebo docházkového systému. Produktové řady výrobků zahrnují identifikační zařízení (čtečky), převážně bezkontaktní a biometrické, dále přístupové řídicí jednotky a docházkové terminály, elektrické a elektromagnetické zámky, softwarové prostředky pro správu systémů a v neposlední řadě i podpůrné prvky a technologie, např. tiskárny pro potisk plastových karet.

  Sortiment výrobků se vždy snaží reflektovat aktuální trendy v přístupových systémech a reagovat na nabídku nových technologií renomovaných světových výrobců. Proto může firma svým obchodním partnerům nabídnout i nové technologie, například v podobě špičkového biometrického systému pro vyhodnocování charakteristik obličejů 3D VisionAccess. [29]
- DDS - Domovní dorozumívací systém, který lze obvykle rozdělit na AUDIO a VIDEO. Vstupní audiosystém je jednoduchý a levný systém pro zajištění kontrolovaného vstupu osob do objektu. Je tvořen dveřní jednotkou s mikrofonem a reproduktorem umístěnou u vstupu do objektu a telefony v jednotlivých pokojích. Vstupní videotelefony umožňují kontrolovaný vstup osob do budovy. Sestavu tvoří dveřní jednotka s barevnou kamerou a vnitřní zobrazovací jednotky s LCD displejem. Příchozí a uživatel obousměrně komunikují, uživatel pak stisknutím tlačítka pro ovládání dveří umožní příchozímu vstup. Protože jak samotný výběr nejvhodnější technologie, tak i vlastní projekce a instalace jsou komplexní záležitosti vyžadující v mnoha případech detailní znalosti jednotlivých technologií i režimových opatření, firma je připravena svým zákazníkům poskytnout všechny potřebné informace. [29]

4.1.2 Systém Domino

Systém DOMINO® je modulární obousměrná komunikační síť, koncepčně navazující na systém IVVS. Díky své modifikovatelnosti může být systém DOMINO® různě nakonfigurován jako obecní rozhlas, rozhlasový výstražný systém, zařízení pro sběr a přenos dat, a také jako systém pro ochranu soukromých nemovitostí.

Systém DOMINO® se běžně skládá z tzv. centrálního odbavovacího pracoviště a bezdrátové sítě. Bezdrátová síť je tvořená stanicemi systému DOMINO® , které slouží buď jako koncový prvek (stanice v režimu SLAVE), nebo jako signálový převaděč s jinými elektronickými sirénami. Centrální odbavovací pracoviště je tvořeno hlavní řídící stanicí (MASTER), která komunikuje s ostatními stanicemi v síti v pásmu 70 MHz či 160 Mhz.

Základní funkcí systému DOMINO® je vyhlašování informačních zpráv a vyhlašování výstražných a varovných zpráv, avšak vzhledem k jeho širokým možnostem použití lze na jeho DPPC připojit také jednotlivé domy a snímat nedovolený pohyb či vniknutí. Centrální odbavovací pracoviště tvoří řídící MASTER stanice DOMINO® spolu s obslužným počítačem, řídící a monitorovací software a externí záložní akumulátory MASTER stanice.

Možné doplňky centrálního odbavovacího pracoviště jsou digitální sirénový přijímač, telefonní komunikační modul GSM AM-PCO a záložní zdroj (UPS). [30]

Obrázek 10: Schéma systému DOMINO 1

Zdroj: [30]

Další variantou tohoto produktu je stanice SLAVE, která umožňuje některým aplikacím systému DOMINO® pracovat samostatně, bez nutnosti komunikace se centrálním odbavovacím pracovištěm a stanicí MASTER.

Komunikace mezi stanicemi probíhá digitálně v módu FSK. Akustické informace se přenášejí s FM modulací spolu s vloženými digitálními značkami, zajišťující jejich integritu. Komunikace mezi stanicemi systému může být i zašifrována.

Pro zálohování PC je využito záložního zdroje (UPS) a pro zálohování stanice MASTER je využito záložního akumulátoru, přičemž musí být zálohovány po dobu 72 hodin a zvládnout půl hodiny vysílání. [30]

K systému DOMINO® lze jako koncové prvky využít stanice DOMINO® Klasik. Základní koncový prvek systému DOMINO® a slouží k příjmu signálu ze stanice MASTER a k jeho zesílení a distribuci do přidružených reproduktorů.

Stanici DOMINO® klasik tvoří:

- VKV přijímač signálu v pásmu 70 MHz nebo 160 MHz
- nf audio zesilovač 2x 20W umožňující připojení až 4 reproduktorů s malou impedancí 8 a výkonem 15 W
- dobíjecí zdroj 14V / 1,5 A
- záložní akumulátor
- přijímací prutová anténa
- ochranná plastová skříň GEWI SS

Stanice DOMINO® Komfort tvoří modulární digitální stanice a oproti stanici DOMINO® Klasik umožňuje navíc celou řadu aplikací (například instalace obousměrného rádiového modulu) [30]

4.1.3 Systém OASIS

Oasis je moderní bezdrátový zabezpečovací systém určený k ochraně domů. Hodí se jak pro obytné prostory, tak i obchody, kanceláře, sklady dílny apod. Může hlásit vloupání, požár, zatopení vodou, nebezpečí mrazu, nebezpečí přehřátí, zdravotní obtíže, přepadení a

případně další rizika. Unikátní jsou v Oasisu bezdrátové detektory pohybu se zabudovanou kamerou. Posílají při poplachu fotografie (na mobilní telefon a počítač). Díky tomu je vidět co se v místě skutečně děje.

K Oasisu je v celé České republice nabízeno zaváděcí střežení pultem centrální ochrany na půl roku zdarma. Oasis umožňuje řídit přístup (otevírat elektrické zámky, garážová vrata, brány apod.). Otevření je možné zadáním číselného kódu, přiložením bezdotykového čipu nebo dálkovým ovládačem (např. z auta). Otevírání je přitom logicky propojeno s funkcí střežení.

Zabezpečovací systém nabízí i domovní automatizaci (ovládání spotřebičů na dálku, řízení topení, zapínání spotřebičů detektorem pohybu, detektorem otevření nebo dálkovým ovladačem).

Oasis je koncipován jako bezdrátový systém a díky tomu je jeho instalace snadná. Připojit lze také klasické prvky kabelem. Drátové a bezdrátové periferie lze libovolně kombinovat, takže je možná jak zcela bezdrátová, tak drátová anebo kombinovaná sestava.

Oasis nabízí mnoho prvků, z nichž lze systém složit dle přání zákazníka. Vychází koncepčně ze staršího systému Profi. Používá však modernější bezdrátový protokol (prvky mají delší komunikační dosah a nepotřebují viditelné antény), jeho baterie mají delší životnost a celkově má modernější design. Pro seznámení se s produktem je výhodné použít sadu Oasis, jejíž prvky jsou již z výroby nakonfigurovány.[16]

Velkou předností tohoto systému jsou následující vlastnosti [16]:

- 50 adres pro přiřazení prvků (prvkem se rozumí: detektor, klávesnice, dálkový ovládač, siréna nebo drátový vstup)
- 50 adres pro přiřazení oprávněných uživatelů (uživatel může systém ovládat číselným kódem, bezdotykovým čipem nebo kartou). Zabezpečovací systém zaznamenává veškeré ovládání do paměti a lze také nastavit, že pomocí SMS hlásí příchod a odchod uživatelů do objektu (např. pro sledování přítomnosti pracovníků, hlídání návratu dětí domů apod.)
- bezdrátové prvky komunikují kryptovaným protokolem v pásmu 868MHz na vzdálenost několika stovek metrů. Antény jednotlivých prvků jsou skryty uvnitř a

systém provádí nepřetržitou kontrolu připravenosti bezdrátových prvků (každých 9 minut)

- bezdrátové prvky jsou napájeny lithiovými bateriemi, které mají typickou dobu životnosti cca 3 roky. Vybití baterie systém hlásí (uživateli ale také servisnímu technikovi)
- všechny klávesnice systému obsahují čtečku bezdotykových identifikačních čipů a mají zabudovaný LCD displej, který poskytuje srozumitelné a přehledné informace o stavu systému
- speciální přístupové klávesnice jsou určeny pro otevírání dveří, vrat apod. Zapojují se kabelem do ústředny, mají vysoký stupeň krytí (lze je montovat venku) a lze určit, zda mají ovládat pouze přístup a nebo i střežení
- nejpohodlnější nastavení zabezpečovacího systému lze provést počítačem (připojuje se pomocí USB kabelu, nebo dálkově přes internet), nastavovací SW je dodáván zdarma. Nastavení je také možné pomocí instrukcí zadávaných z klávesnice
- možné je střežit buď celý dům, nebo jej lze střežit ve 2 stupních částečného střežení (A, AB, ABC), nastavit lze také nezávislé střežení 2 nezávislých sektorů v domě (např. byty dvou různých rodin)
- systém je certifikován podle ČSN EN 50131-1 do stupně 2 (nízká až střední rizika). Certifikace systému a certifikace montážní firmy je podmínkou pro uznání systému dle podmínek asociace pojišťoven. Podmiňuje výplatu pojistné náhrady v plné výši, případně se uplatňuje jako podmínka pro uznání slevy na pojistném (viz podmínky konkrétní pojišťovny)
- na prvky zabezpečovacího systému je při prokázané montáži certifikovaným technikem je na výrobek poskytována záruka 2 roky a prodloužení doby bezplatné opravy výrobku v servisu Jablotron na 5 let

4.2 Varianta instalace PZTS v soukromém objektu

Možností, jak instalovat bezpečnostní systém určený pro ochranu soukromých objektů, je mnoho. Zatímco komerční použití je projektováno pro prostory, do nichž běžně vstupuje mnoho lidí, soukromý pozemek je většinou určen pro použití pouze úzkému okruhu osob.

Proto zde může být použito více prvků, které mohou přenášet zprávy do DPPC a umožnist jejím pracovníkům adekvátní odpověď.

4.2.1 Bezdrátová varianta zabezpečení s automatickou regulací podmínek

Tato varianta pracuje se zabezpečením oken a dveří. Zabezpečení objektu je provedeno bezdrátově a jednotlivé zabezpečovací prvky komunikují s ústřednou na frekvenci 433 nebo 868MHz.

Pro zajištění maximálního komfortu uživatele je možné zastřežení/odstřežení objektu provádět bezdrátovou klíčenkou. Okna jsou chráněna bezpečnostními předokenními roletami, které zároveň plní funkci termoizolační. Také jsou opatřena magnetickými kontakty, které detekují jeho otevření. Pro detekci tříštění a rozbíjení skla mohou být použita skla Glasstrek DG457. Okna i vstupní dveře jsou opatřeny ochranou proti vysazení.

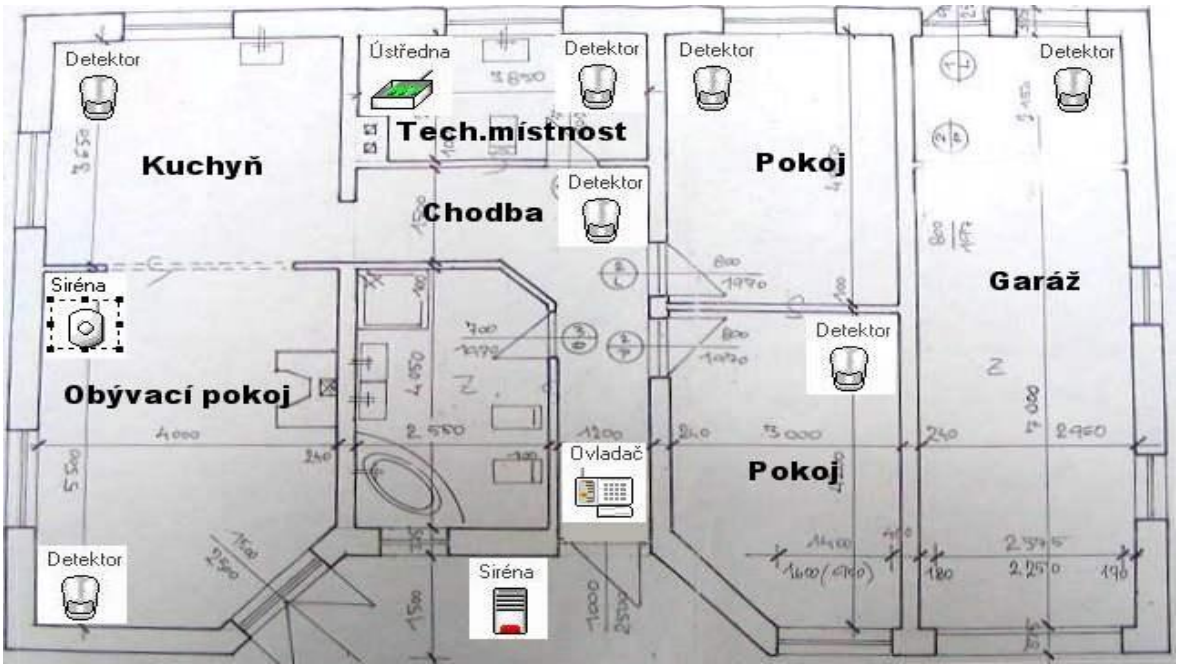
Snímání a regulace podmínek je prováděna zcela automaticky. Uživatel musí prvotně nastavit jednotlivá zařízení. Musí naprogramovat digitální termostatické hlavice HD - 20, určit mezní hodnoty snímaných podmínek na digitálním ukazateli klimatu CO - 100 a nastavit požadovanou relativní vlhkost, kterou mají udržovat zařízení Kruger HUMISAT a Master DH - 711.

Celkově je projekt řešený tak, že střežený objekt je rozdělen do 7 částí, které střeží celkem 7 zón. Na následujícím obrázku je zobrazena obytná plocha, do níž je instalováno PZS, bezpečnostní rolety a ústředna. Vzhledem k malé velikosti objektu není systém rozdělen na podsystémy. Zabezpečení objektu je provedeno bezdrátově. Jednotlivé zabezpečovací prvky komunikují s ústřednou bezdrátově na frekvenci 433 a 868MHz.

Při návrhu zabezpečení se vychází z toho, jaká jsou možná rizika napadení objektu. Základem každého systému je ústředna - mozek systému. V ústředně bývá obvykle zabudován GSM komunikátor, což je zařízení, které až 8 uživatelům při poplachu zašle sms zprávy s popisem události a rovněž je prozvoní. Zároveň je možno systém na dálku ovládat. Ústředna je ovládána klávesnicí. Ta je zcela oddělena od ústředny, takže při jejím zničení pachatelem nedojde k poškození systému, ale dojde k vyhlášení poplachu. Podle počtu místností a možných rizik napadení se instalují detektory pohybu, detektory otevření dveří. Jako doplňková ochrana se používají detektory tříštění skla. Pro ochranu objektu

proti požáru se používají detektory kouře a plynu. Při poplachu se aktivuje siréna. Do bytu se používají sirény vnitřní, do rodinných domů sirény vnitřní nebo venkovní popř. oba typy. Bezdrátový alarm lze kromě klávesnice ovládat klíčenkami jako např. autoalarm. Aby zabezpečovací systém vůbec fungoval, musí se skládat ze sestavy ústředna, klávesnice, detektor. Rozlišujeme ochranu prostorovou - detektory pohybu. Dále ochranu plášťovou - detektory otevření, rozbití skla. Obě ochrany je možné kombinovat. [31]

Obrázek 11: Schéma instalace PZ 1



Zdroj: [31]

V každé místnosti, kromě koupelny, je instalován detektor.

Při instalaci budou použity následující zařízení PZS a MZS:

- Cylindrická vložka Mul – T - Lock Integrator ®
- Bezpečnostní dveřní kování Richter SB5200 ZA
- Glassbreak Glasstrek DG457
- Bezpečnostní rolety

Další použitá zařízení [31]:

Ústředna Magellan MG5050PCB

- zabudovaný bezdrátový vysílač a přijímač
- možnost rozdělení na 2 podsystémy
- 32 zón
- 5 vstupů na desce pro drátové zóny
- 32 uživatelů a 32 dálkových ovladačů
- frekvenční pásma 433 nebo 868 MHz
- 4 drátová rozšiřitelná sběrnice

Bezdrátová klávesnice MG37

- ikonová bezdrátová klávesnice
- zobrazení poruch, přemostění a poplachů v historii
- nastavitelné podsvícení
- napájení: 2x AA alkalické baterie nebo 6V napájecí adaptér

Kryt a transformátor AWO105

- rozměry krytu ústředny 250 x 290 x 80mm
- instalovaný transformátor 18/30VA
- ochranný kontakt "TAMPER"
- prostor pro 7Ah akumulátor

Akumulátor TP12180

- akumulátor 12V 7Ah

Vnitřní bezdrátový PIR detektor MG - PMD75

- frekvenční pásmo 433 MHz nebo 868 MHz
- napájení: 3 x AA alkalické baterie
- imunní proti malým zvířatům do 40Kg
- zvýšená odolnost proti Vf rušení

Bezdrátový magnetický kontakt MG - DCT2

- miniaturní magnetický kontakt
- frekvenční pásmo 433 MHz nebo 868 MHz
- napájení: 1 x 3 V lithiová baterie (CR2450)
- životnost baterie: cca 1 rok
- dosah: 40 m

Bezdrátová venkovní siréna PS - 128

- vestavěný blikač se stroboskopem (1 Hz)
- frekvenční pásmo 433 MHz
- napájení: 3 x alkalická baterie „D“
- životnost baterie: 3 – 5 let (bez poplachu)
- dosah: 70 m

Dálkový bezdrátový ovladač MG - REM1

- 4tlačítkový ovladač s podsvícením kláves
- možnost naprogramování až 5 činností
- voděodolný kryt
- frekvenční pásmo 433 MHz nebo 868 MHz

- napájení: 1 x baterie CR2032
- dosah: 45 m

GSM/GPRS komunikátor PCS - 200

- Přenos zpráv prostřednictvím textových zpráv (až 16 telefonních čísel)
- uživatel může zastřežit nebo odstřežit systém zasláním textové SMS zprávy
- instalace pomocí 4vodičového sériové spojení
- napájení samostatné nebo z ústředny

Pojistka dveřních a okenních závěsů proti vysazení TAS - 112

- ochrana proti vysazení oken a dveří ze závěsů
- odolnost tlaku 1tuny
- dveře a okna lze otevřít maximálně o 90°

Rozšířená varianta zabezpečení počítá též s ochranou před výpadkem elektrické energie, a případně též před živelnými pohromami. V následující kapitole jsou vyčísleny také finanční náklady na jednotlivé typy zabezpečovacích prostředků.

Ochrana před výpadkem elektrické energie [32]

- Dočasný záložní zdroj el. Energie ZZ 200 s max. Zatížením 200 W - zdroj dodává el. energii pro oběhová čerpadla kotlů na dřevo, uhlí nebo krbová kamna, slouží také k napájení domácích elektrospotřebičů s napájením 230 V, příkonem 200 W. Zabezpečí krátkodobou dodávku el. energie pro EZS a elektrospotřebiče, doba dočasného provozu až 8 h při odebíraném příkonu 100 W, cena 4 000 Kč, 1 ks.
- APC Back UPS ES 550 pro zálohovaní el. Energie a přepěťovou ochranu EZS a elektrospotřebičů, cena 2100 Kč, 1 ks .
- Protipožární ochrana H 450EN detektor úniku oxidu uhelnatého CO - umístěn v technické místnosti u kotle centrálního vytápění, cena 1400 Kč, 1 ks.

- ARGUS BASIC požární hlásič, kouřový detektor požáru, lokální signalizace akustická a světelná, možnost napojení na EZS - umístěn ve všech místnostech na stropě, cena 540 Kč, 5 ks.

Vstupní prvky [32]

- Bezpečnostní jednokřídlé vchodové dveře MAGNUM včetně bezpečnostních zárubní splňující 3. bezpečnostní třídu, cena 26 000 Kč.
- RL - 037 domácí videotelefon s kamerou obsahující noční IR přísvit. Absence funkce pořizování a ukládání fotografií, cena 4 100 Kč, 1 ks.
- FG 200 okenní bezpečnostní klika s bezpečnostním kováním. Montáž do všech oken, cena 1 100 Kč, 9 ks.
- SCX bezpečnostní ochranná fólie na okenní skla splňující třídu odolnosti P1 A a P2 A normy ČSN EN 356 - instalovaná na balkónové dveře a okna umístěná v přízemí, cena 1m^2 = 1 137Kč, 11 m^2 .

Ochrana před zatopením a vyplavením

- LD 63HS autonomní záplavový detektor instalovaný v technické místnosti, kuchyni a koupelně. Lokální signalizace vestavěnou sirénou, cena 300 Kč, 4 ks.

EZS

- JA - 82K ústředna zabezpečovacího systému OASiS, 1 450 Kč, 1 ks
- JA - 82R radiový modul pro implementaci bezdrátových prvků , cena 2 650 Kč, 1 ks
- JA - 82Y GSM komunikátor pro komunikaci s mobilním telefonem a internetem, cena 6 590 Kč, 1 ks
- JA - 81F bezdrátová klávesnice pro ovládání a programování systému, cena 2 730 Kč, 1 ks
- PC - 01 bezdotyková RFID karta pro klávesnici JA - 81F, cena 50 Kč, 4 ks
- JA - 84P bezdrátový PIR detektor s vestavěnou kamerou a IR nočním přísvitem. Po detekci narušení pořizuje a odesílá snímek na internet a mobilní telefon uživatele, cena 3 050 Kč, 3 ks. [32]

4.3 Finanční analýza připojení na DPPC

Finanční náklady na střežení objektu se skládají ze dvou částí. Zpočátku je nutná jednorázová počáteční investice do instalace poplachového zabezpečovacího systému a poté většina firem vyžaduje měsíční paušál za ostrahu objektu připojením na DPPC. Frekvence plateb je samozřejmě na dohodě se zákazníkem, který si může zvolit z varianty čtvrtletní, pololetní i roční.

Náklady na střežení připojením k DPPC se liší rozsahem poskytovaných služeb a samozřejmě cenovou politikou jednotlivých provozovatelů DPPC.

Varianty nabízené většinou poskytovatelů jsou následující:

- vyšší paušál – v ceně za střežení jsou zahrnuty další služby – tj. výjezd k planému poplachu, fyzické střežení v případě, že na PZTS byla zjištěna závada, nebo opláštění objektu není dostatečně zajištěno (otevřená okna, neuzamčené dveře atp.) a také servisní paušál (tj. v ceně paušálu je zahrnuta i revize PZTS)
- nízký paušál – v ceně paušálu nejsou zahrnuty další služby – tj. zákazník platí výjezdy a náklady za další poskytnuté služby

Dalšími pravidelnými náklady mohou být poplatky za přenos zpráv na DPPC v závislosti na použitém komunikátoru. Kromě rádiového přenosu, který je bezplatný, jsou ceny závislé na poskytovateli služeb a dohodnutých podmínkách. V případě firem a jejich firemních sítí nemusí být přenos informací velká finanční zátěž.

Následující schéma znázorňuje, za jakou cenu by bylo možno instalovat a využívat zabezpečení bytu DPPC od konkrétní české firmy [31]:

Bezdrátový systém Jablotron řada JA-80 Oasis
Ústředna JA-82K 1290,- Kč
Radiový modul JA-82R 2520,- Kč
GSM komunikátor JA-82Y 5830,-Kč
Záložní akumulátor 12V 2,6 Ah pro ústřednu 350,- Kč
Klávesnice JA-81F s integrovanou čtečkou karet (přívěšků) 2420,- Kč
Detektor otevření dveří JA-83M 838,- Kč

Detektory pohybu JA-83P 3 ks (3x1318,-Kč) 3954,- Kč
Siréna bezdrátová JA-80L 1114,- Kč
Montáž, oživení, programování, zaškolení 2000,- Kč
Cena za dílo bez DPH 20316,- Kč
Cena za dílo včetně DPH 15 % je 23363,- Kč
Počet detektorů lze upravit. Záruka 5 let.

Další možná rozšíření lze zakoupit za následující ceny:

Bezdrátový systém Jablotron řada JA-80 Oasis [31]:
Přívěšky PC-02 - přikládají se ke klávesnici, nahrazují ovládání kódem 50,- Kč bez DPH.
Doplňková ochrana - bezdrátový detektor tříštění skla JA-80B 990,- Kč bez DPH.
Kombinovaný detektor pohybu a tříšť.skla v jednom puzdře JA-80PB 1800,- Kč bez DPH.
Protipožární ochrana - bezdrátový detektor kouře JA-80S 1156,- Kč bez DPH.
Ochrana proti úniku hořlavých plynů - bezdrátový detektor JA-60G 1390,- Kč bez DPH.
Možno zakoupit interkom SP-01 pro odposlech místnosti.
Možno zakoupit modul AC-82 s ovládáním spotřebičů na dálku pomocí sms nebo internetu za 990,- Kč bez DPH

Z výše uvedených informací je patrno, že investice do zabezpečovacího zařízení není malá. Pro efektivní ochranu je nezbytné využít kombinaci co největšího počtu ochranných prvků. Instalace systému OASIS je výhodná zejména díky jednoduché instalaci, malým nárokům na servis a údržbu, a zároveň poskytnutím vysokého procenta ochrany. Dle pracovníků firmy tento systém za poslední rok zaznamenal minimální počet planých poplachů, čímž předešel planým výjezdům pracovníků DPPC. Dle mého názoru všechny nabízené prvky systému mají své opodstatnění, a jejich cena je odpovídající.

ZÁVĚR

Účelem této diplomové práce bylo uvést možnosti použití dohledového a poplachového přijímacího centra a jeho specifik při použití v komerční i soukromé sféře. Byly uvedeny technické normy, které použití tohoto systému upravují, a přehledně popsány způsoby, jakými lze poplachové zařízení instalovat a na jakých principech funguje.

I přes stále se zvětšující počet soukromých objektů a firem nabízejících jejich zabezpečení nejsou zdaleka všechny objekty zabezpečeny. Případní narušitelé přitom neustále zdokonalují způsob, jakým lze vniknout do objektu. Také pojišťovny kladou velký důraz na správnou volbu zabezpečení objektu, a pokud majitel neučiní dostatečná zabezpečení, pojišťovna obvykle odmítne plnit v případě poškození obsah pojistky. Proto má práce obsahuje některé z variant poplachových zabezpečovacích systémů, které jsou v současné době na českém trhu k dispozici.

Rozdíl ve způsobu zabezpečení soukromých a komerčních objektů spočívá zejména ve velikosti objektu, který je zabezpečován, a tudíž ve způsobu volby systému a ve finančních nákladech. V zabezpečení uvedené bankovní instituce je důležité zejména určit klíčové body, na něž je nutné instalovat tísňové hlásiče, zatímco v soukromém objektu se spíše instalují detektory pohybu. Samozřejmostí pak jsou další prvky ochrany, které dohledové a poplachové přijímací centra doplňují.

Součástí této práce je též návrh, jak by mohlo vypadat zabezpečení konkrétního soukromého objektu. Při výběru jedné firmy je do objektu instalován určitý počet detektorů, které mají specifické vlastnosti. Nutné je zabezpečit neustálý dohled, a vyvarovat se planého spuštění poplachu. Přiložil jsem také stručnou finanční analýzu pořizovacích nákladů.

Při zpracování tématu jsem využíval svých dosavadních studijních znalostí a literatury, kterou jsem citoval. Potřebné informace jsem dále získával z internetu.

SEZNAM POUŽITÝCH ZDROJŮ

[1] POPARDOWSKI, Ivo. Poplachové zabezpečovací a tísňové systémy PCO, DPPC, PTS, PZTS – historie, legislativa, normativní zásady provozu. (online) 2013. [cit. 12/05/2014] Dostupné z: http://www.bezpecnostni-zpravodaj.cz/poplachove-zabezpecovaci-a-tisnove-systemy-pco-dppc-pts-pzts-historie-legislativa-normativni-zasady-provozu/

[2] Elektronická ostraha objektů. Loter.cz. (online) 2011. [cit. 12/05/2014] Dostupné z: http://www.loter.eu/clanek/elektronicka-ostraha-objektu/

[3] ČSN EN 50518 - 1. Dohledová a poplachová přijímací centra - Část 1: Umístění a konstrukční požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010.

[5] ČSN EN 50518 - 2. Dohledová a poplachová přijímací centra - Část 2: Technické požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011

[6] ČSN EN 50518 -3. Dohledová a poplachová přijímací centra - Část 3: Pracovní postupy a požadavky na provoz. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012.

[7] BOGDANSKI, Wojciech. Koncepce systému Kronos a porovnání s jinými systémy poplachových přijímacích center. Univerzita Tomáše Bati ve Zlíně, 2012. UTB Zlín. Diplomová práce

[8] LAUCKY, V. Technologie komerční bezpečnosti I.. Zlin: Univerzita Tomaše Bati ve Zlině, 2004. 64 s. ISBN 803181940

[9] ZAPLETAL, Pavel. Perspektiva PPC. Univerzita Tomáše Bati ve Zlíně, 2009. UTB Zlín. Diplomová práce.

[10] Bezpečnostní agentura Garance Písek. (online) 2014. [cit. 12/05/2014] Dostupné z: http://www.garance-pisek.cz

[11] Bezpečnostní agentura Random. (online) 2014. [cit. 12/05/2014] Dostupné z: http://www.radom.eu

[12] VALOUCH, Jan. Projektování bezpečnostních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. ISBN 978-80-7454-230-52.3

[13] Bezpečnostní agentura HP1. (online) 2014. [cit. 12/05/2014] Dostupné z: http://www.pcosecurityh1.cz

[14] JANSEN, Horst a Heinrich RÖTTER. Informační a telekomunikační technika. Vyd. 1. Praha: Europa - Sobotáles, 2004, 399 s. ISBN 8086706087.

[15] Bezpečnostní agentura HCM (online) 2014. [cit. 12/05/2014] Dostupné z: http://www.hcm.cz/centr-pult.php

[16] Bezpečnostní agentura BOMI System. (online) 2014. [cit. 12/05/2014] Dostupné z: http://www.kamerykvalitne.cz/fotky/fotov

[17] Bezpečnostní agentura SABS (online) 2014. [cit. 12/05/2014] Dostupné z: http://www.sabs.cz/wp-content/uploads/2014/01/web-syst%C3%A9my.png

[18] KINDL, Jiří. Projektování bezpečnostních systémů. 1. vyd. Zlín: Univerzita Tomáše Bati, 2004, 134 s. ISBN 8073181657

[19] AGA - ASOCIACE GREMIUM ALARM. Ademco Contact ID protokol SIA DC -05 -1999.09. Praha, 2007.

[20] SIA Digital Communication Standard – Internet Protocol Event Reporting. Alexandria, VA. (online) 2012. [cit. 12/05/2014] Dostupné z: http://www.siaonline.org

[21] NAM systém, a.s. Pult Centrálni Ochrany NAM GLOBAL: Výuková Skripta. Orlová.

[22] VYORÁLEK, Radim. Pulty centralizované ochrany. Univerzita Tomáše Bati ve Zlíně, 2005. UTB Zlín. Bakalářská práce.

[23] BUŘIČOVÁ, Kateřina. Pulty centralizované ochrany v podmínkách policejní praxe. Univerzita Tomáše Bati ve Zlíně, 2010. UTB Zlín. Diplomová práce.

[24] Dálkový monitoring objektů. Bezpečnostní agentura SBA expert. (online) 2014. [cit. 12/05/2014] Dostupné z: http://www.sbaexpert.cz/poskytovane-sluzby/bezpecnost/dalkovy-monitoring-objektu

[25] Dálkový monitoring (PCO – ARC). Bezpečnostní agentura Alcrom Security. (online) 2014. [cit. 12/05/2014] Dostupné z: http://www.alkom.cz/dalkovy-monitoring-pco-arc/

[26] Bezpečnostní agentura CS Solutions (online) 2014. [cit. 12/05/2014] Dostupné z: http://cssolutions.cz

[27] REJDÍK, Martin. IP kamerové systémy a jejich skladba. Internetový časopis Posterus. (online) 2013. [cit. 12/05/2014] Dostupné z: http://www.posterus.sk/?p=16195

[28] KHUDHUR, Patrik. Budujeme domácí zabezpečovací systém. Internetový časopis Chip. (online) 2014. [cit. 12/05/2014] Dostupné z: http://www.chip.cz/casopis-chip/earchiv/rubriky/technika/budujeme-dom-zab-system/

[29] Bezpečnostní agentura BFB Falco. (online) 2014. [cit. 12/05/2014] Dostupné z: http://www.bfb-falco.cz/sluzby.html#cenik%20ostraha

[30] Telekomunikační společnost SATTURN Holešov. (online) 2014. [cit. 12/05/2014] Dostupné z: www.satturn.cz

[31] Zabezpečovací systémy Jan Slivka. (online) 2014. [cit. 12/05/2014] Dostupné z: http://www.zabezpeceni.net/navrh-zabezpeceni.html

[32] JANSTA, J. Zabezpečení rodinného domu. Bakalářská práce 2013 Univerzita Pardubice: Fakulta ekonomicko – správní

KAMENÍK, Jiří, František BRABEC. Komerční bezpečnost. Praha: ASPI, a.s., 2007. ISBN 978-80-7357-309-6.

VALOUCH, Jan. Projektování integrovaných systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 978-80-7454-296-1.

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

IVANKA, Ján. Systemizace bezpečnostního průmyslu I. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-80-7318-850-4.

Zákon č. 89/2012 Sb., občanský zákoník, v platném znění

Zákon č. 553/1991 Sb., o obecní policii, v platném znění

ČSN EN 50131. Poplachové systémy- Poplachové zabezpečovací a tísňové systémy.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACC	Aerial / Airborne Command and Control
AES	Advanced Encryption Standard
CCTV	Closed Circuit Television
CDMA	Code Division Multiple Access
DPPC	Dohledové a poplachové přijímací centrum
EKV	Elektronická kontrola vstupu
EPS	Elektrická požární signalizace
EZS	Elektronické zabezpečovací zařízení
GPRS	General Packet Radio Service
GSM	Global System for Mobile Comunications
HW	Hardware IP Internet Protocol
ISDN	Integraded Services Digital Network
JTS	Jednotná telefonní síť
LAN	Local Autority Network
LCD	Liquit Crystal display
MAC	Media Access Control
MDC	Multifunkční dohledové centrum
PC	Personal Computer
PCO	Pult centralizované ochrany
PPC	Poplachové přijímací centrum
PS	Poplašný signál
PZS	Poplachový zabezpečovací systém
PZTS	Poplachový zabezpečovací a tísňový systém
QOS	Quality of Service

SCO	Systém centralizované ochrany
SIM	Subscriber Identity Module
SMS	Short message service
SPZ	Státní poznávací značka
SW	Software
VPN	Virtual Private Network
TCP	Transmission Control Protocol
TH	Tísňové hlásiče
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UMTS	Universl Mobile Telecommunication Servise
UPS	Uninterruptible Power Supply

SEZNAM OBRÁZKŮ

SEZNAM TABULEK