Varianty nejčastějších zásahů na varovný signál PZTS

Variants of the Most Common Intervention Reactions to Warning Signals of Intrusion and Emergency Alarm Systems

Bc. Pavel Prochorov

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. Pavel Prochorov**
Osobní číslo:	**A12372**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Varianty nejčatějších zásahů na varovný signál poplachového zabezpečovacího a tísňového systému**
Téma anglicky:	**Variants of the Most Common Intervention Reactions to Warning Signals of Intrusion and Emergency Alarm Systems**

Zásady pro vypracování:

1. **Vytvořte technický popis poplachového zabezpečovacího a tísňového systému (dále jen PZTS).**
2. **Jmenujte možnosti připojení PZTS.**
3. **Pojednejte o možnostech náhradního připojení PZTS.**
4. **Určete podmínky pro aplikaci PZTS.**
5. **Popište způsoby a taktiku zásahu na varovné signály.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **IVANKA, Ján. Systemizace bezpečnostního průmyslu I. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-80-7318-850-4.**
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. **KAMENÍK, Jiří, František BRABEC. Komerční bezpečnost. Praha: ASPI, a.s., 2007. ISBN 978-80-7357-309-6.**
5. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. Zlín: Radim Bačuvčík – VeRBuM, 2011. ISBN 978-80-87500-05-7.**
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**

ABSTRAKT

Diplomová práce je zaměřena na problematiku **zásahu na varovné signály PZTS** v oblasti průmyslu komerční bezpečnosti. Za hlavní cíl si klade vyhodnotit taktiku a způsoby zásahu na varovné signály a popsat její metodiku.

Úvodem popisuje technické stránky PZTS a uvádí jejich kladné a záporné stránky při integraci do bezpečnostního systému. V celé teoretické části přibližuje a podrobně rozebírá možnosti připojení PZTS na vyhodnocovací terminály z hlediska efektivnosti reakce na varovné signály a praktická část je vymezena na podrobný popis taktiky zásahů na varovné signály.

Klíčová slova: varovné signály PZTS, aplikační podmínky, přenosové trasy, náhradní připojení, taktika zásahu

ABSTRACT

The thesis is focused on the problems concerning warning signals I&HAS in the field of the commercial security industry. It´s main objective is to analyze tactics and procedures of response to warning signals I&HAS and to describe the methodology of it. The introduction describes the technical aspects of I&HAS and points out its positive and negative sides when it comes to an integration into a security system. The theoretical part brings near and analyzes options of I&HAS connectivity to processing terminals in terms of effectivity of response to warning signals. The practical part is specialized in elaborated descriptions of the methods used while intervening in emergency cases.

Keywords: high signs of I&HAS, installation requirements, transferal alignment, substitutive connection, intervention methods

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 **10**

I TEORETICKÁ ČÁST **11**

1 PRVKY ZABEZPEČOVACÍHO SYSTÉMU **12**

1.1 DEFINICE A ÚČEL PZTS 12

1.2 ROZDĚLENÍ PZTS 13

1.2.1 Prvky plášťové ochrany 13
1.2.2 Prvky prostorové ochrany 14
1.2.3 Prvky předmětové ochrany 15
1.2.4 Prvky obvodové ochrany 15

1.3 ÚSTŘEDNY PZTS 17

1.3.1 Drátové ústředny PZS 18
1.3.1.1 Ústředny analogové (smyčkové) 18
1.3.1.2 Ústředny sběrnicové 18
1.3.1.3 Ústředny smíšeného typu 19
1.3.2 Bezdrátové ústředny 20
1.3.3 Hybridní ústředny 20
1.3.4 Grafická schémata systému PZS 20

2 APLIKAČNÍ PODMÍNKY PZTS **22**

2.1 ČSN EN 50131-1 ED.2 23

2.1.1 Obsah normy 23
2.1.2 Funkce systému 24
2.1.3 Komponenty systému 24
2.1.4 Stupně zabezpečení 24
2.1.5 Třída prostředí 24
2.1.6 Funkční požadavky 25
2.1.7 Napájení 25
2.1.8 Provozní spolehlivost 26
2.1.9 Funkční spolehlivost 26
2.1.10 Požadavky na prostředí 27
2.1.11 Elektrická bezpečnost 27
2.1.12 Dokumentace 27
2.1.13 Značení 27

3 MOŽNOSTI PŘIPOJENÍ PZTS **29**

3.1 PŘENOSOVÉ TRASY 29

3.1.1 Nejvyužívanější komunikační přenosové trasy 29
3.1.1.1 Telefonní linka v hovorovém pásmu 30
3.1.1.2 Telefonní linka v nad-hovorovém pásmu 31
3.1.1.3 Telefonní linka ISDN 31
3.1.1.4 Rádiový přenos na vyhrazených frekvencích 31
3.1.2 GSM 33
3.1.2.1 Přenos po síti GSM v hovorovém pásmu 33
3.1.2.2 Přenos po síti GSM prostřednictvím GPRS 33

3.1.2.3 Přenos po síti GSM prostřednictvím SMS 34
3.1.2.4 Přenos pomocí internetové sítě 34
3.1.2.5 Vyhrazená přenosová cesta 34
3.2 NÁHRADNÍ PŘIPOJENÍ PZTS 35
3.2.1 Kombinace přenosových tras 35
3.2.1.1 Kombinace JTS a RADIO sítě 35
3.2.1.2 Kombinace JTS a GSM sítě 35
3.2.1.3 Kombinace GSM a RADIO sítě 36
3.2.1.4 Kombinace GSM či RADIO sítě a internetu 36
3.3 PŘENÁŠENÉ ZPRÁVY 37
4 DPPC 38
4.1 ROZDĚLENÍ DPPC 38
II PRAKTICKÁ ČÁST 40
5 ÚVOD DO PRAKTICKÉ ČÁSTI 41
6 PRACOVNÍCI DPPC 42
6.1 POVINNOSTI PRACOVNÍKŮ 44
6.1.1 Pracovník je povinen: 44
Zákazy pracovníkům 45
6.2 OCHRANNÉ PROSTŘEDKY PRACOVNÍKŮ 46
6.2.1 Mezi výbavu pracovníka řadíme: 46
7 ZÁSADY SPRÁVNÉHO POSTUPU PŘI ZÁSAHU 52
7.1 REAKCE NA VAROVNÉ SIGNÁLY 52
7.2 NORMY ZÁSAHOVÝCH ČASŮ 53
7.2.1 Předpoklady krátkého zásahového času 53
7.2.2 Norma ČSN EN 50134-7 Pokyny pro aplikace přivolání pomoci 53
7.2.2.1 Norma ČSN EN 50518-2 54
7.3 ZNALOST STŘEŽENÉHO OBJEKTU 54
7.4 JÍZDA NA MÍSTO ČINU 54
8 POSTUP ZÁSAHU 56
8.1 OBECNÉ POSTUPY 56
8.1.1 Dva možné postupy 57
8.1.1.1 DPPC řeší situaci samo 57
8.1.1.2 Součinnost s policií 57
8.1.1.3 Státní Policie ČR a městská policie 58
9 PŘÍKLADY ZÁSAHŮ 61
9.1 ZÁSAHY VE VEŘEJNĚ UŽÍVANÝCH SOUKROMÝCH PROSTORÁCH NA ZÁKLADĚ TÍSŇOVÉHO VOLÁNÍ 61
9.2 ZÁSAHY NA SIGNÁL POPLACHU A SABOTÁŽE 62
9.3 PLANÝ POPLACH 64
10 VAROVNÉ SIGNÁLY 66

10.1 ROZDĚLENÍ VAROVNÝCH SIGNÁLŮ 66
10.1.1 Poplach 66
10.1.2 Sabotáž 66
10.1.3 Tísňové volání 66
10.1.4 Zapnutí, vypnutí 66
10.1.5 Podpětí baterie 67
10.1.6 Vypnutí pod nátlakem 67
10.1.7 Požární poplach 67
10.1.8 Stisknutí klávesy A první pomoc 67
10.1.9 Stisknutí klávesy F hoří 67
10.1.10 Výpadek elektrické sítě 67
10.1.11 Ztráta komunikace 67
10.1.12 Rušení příjmu sběrné stanice 68
10.1.13 Ilegální vysílač 68
10.1.14 Neznámá zpráva 68
11 LEGISLATIVA 69
12 STATISTIKY 71
ZÁVĚR 73
ZÁVĚR V ANGLIČTINĚ 74
SEZNAM POUŽITÉ LITERATURY 75
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 78
SEZNAM PŘÍLOH 83

ÚVOD

V dnešní době se běžně setkáváme s případy, kdy byl vykraden byt, chata či celý dům. Majetková kriminalita neustále roste a čím dál více přibývá pachatelů, kteří se zaměřují na vniknutí do cizích objektů a odcizení majetku. Poplachové zabezpečovací a tísňové systémy (dále jen PZTS) v kombinaci s dohledovými a poplachovými přijímacími centry (dále jen DPPC) se snaží s tímto problémem bojovat. Dokáží detekovat narušení střeženého objektu a vyslat ihned varovný signál, ovšem nemohou zabránit odcizení majetku. Tomu mohou zabránit bezpečnostní agentury či orgány Policie ČR. Jakým způsobem reagují na tyto varovné zprávy a jak postupují během zásahu se dozvíte v této diplomové práci.

Jelikož jsou potenciální pachatelé v dnešní době sofistikovanější a vzhledem k současnému stavu ekonomiky na území České republiky i více motivováni, musíme bezpečnostní systémy velmi efektivně integrovat, aby měli příslušníci výjezdových služeb možnost, v co nejkratší době dorazit na místo činu a dopadnout pachatele. Výjezd na místo činu a provedení zásahu patří mezi velmi náročné a nebezpečné povolání, proto jsou na příslušníky těchto služeb kladeny vysoké nároky na připravenost, odolnost vůči stresu, znalost strategických postupů během zásahu a zejména na právní znalosti. Kvalitní bezpečnost našeho majetku má základy ve správné instalaci PZTS. Proto práce popisuje tyto systémy, uvádí jejich kladné a záporné technické vlastnosti a zaměřuje se zejména na současné možnosti připojení těchto systému k DPPC.

I. TEORETICKÁ ČÁST

1 PRVKY ZABEZPEČOVACÍHO SYSTÉMU

Při zabezpečovaní objektu se využívají nejen poplachové zabezpečovací a tísňové systémy, ale i další systémy, které zabezpečení zájmového objektu zefektivní. V praxi se při zabezpečování využívá takzvaný integrovaný bezpečnostní systém (zvaný jako IBS), který obsahuje tyto složky:

1. Mechanické zábranné systémy
2. Poplachové zabezpečovací a tísňové systémy
3. Režimová ochrana
4. Fyzická ochrana

Každá složka plní při zabezpečení svojí úlohu. Mechanická část plní úlohu odolnosti a zpomalení pachatele, poplachová část funkci informační a režimová se využívá při zabezpečování objektů, kde se nachází větší počet osob (většinou veřejné a komerční objekty) a plní úlohu organizační. Fyzická ochrana, nebo-li klasická ochrana, kde jsou příslušníci fyzické ostrahy pověření k ochraně a střežení objektu.

Pokud systém splňuje všechny výše uvedené složky, může se systém označovat za plně zabezpečený. Má práce je zaměřena pouze na složku PZTS, která má rozmanitou škálu prvků, které se do poplachového systému integrují. Níže budu tyto prvky uvádět, popisovat jejich technické parametry a rozebírat jejich kladné a záporné vlastnosti.

1.1 Definice a účel PZTS

Poplachový zabezpečovací a tísňový systém byl v terminologii České republiky dříve označován jako elektrický zabezpečovací systém. V současné době tento název nahradilo nové pojmenování „Poplachový zabezpečovací a tísňový systém“ (anglicky Intruder and Hold-up systém - I&HAS).

Poplachový zabezpečovací a tísňový systém je definován jako „kombinovaný systém, určený k detekování přítomnosti, vniknutí nebo pokusu o vniknutí vetřelce do střeženého objektu“[1]. Tento systém může plnit funkci pouze jako poplachový zabezpečovací systém nebo jako samostatný poplachový tísňový systém.

Jedná se o systém, jejíž cílovou funkcí je:

1. Ochrana života a zdraví osob

2. Ochrana majetku před krádeží vloupáním nebo poškozením

Zařízení PZTS představuje soubor: čidel, ústředen, přenosových zařízení, tísňových hlásičů, prostředků poplachové signalizace, záznamových a ovládacích zařízení, prostřednictvím kterých je signalizováno narušení střeženého objektu nebo prostoru.

1.2 Rozdělení PZTS

1. Poplachový tísňový systém (PTS) - Tísňové systémy jsou určeny k přenosu tísňových signálů. Jedná se o bezpečnostní prvek, který prostřednictvím fyzického kontaktu vysílá signál ohrožení a přivolání pomoci.

2. Poplachový zabezpečovací systém (PZS) – Systém, určený k detekci přítomnosti, vniknutí nebo pokusu o vniknutí vetřelce do střeženého objektu.

Tísňový systém je poměrně jednoduchý a tudíž ho v diplomové práci pouze zmiňuji. Podstatně rozmanitější systém zabezpečení tvoří PZS. PZS a její ochrana se obecně dělí do 4 skupin:

- Plášťová ochrana – okna, dveře, zdi
- Prostorová ochrana – jednotlivé prostory uvnitř objektu
- Předmětová ochrana – jednotlivé předměty, nacházející se v objektu
- Obvodová ochrana (perimetrická) – ploty, vrata, oplocení

Toto je nejzákladnější rozdělení jednotlivých chráněných částí objektu. Na dané části objektu se volí příslušné prvky PZS.

1.2.1 Prvky plášťové ochrany

Magnetické kontakty

Magnetické kontakty tvoří dvojí dílů – jazýčkový kontakt a permanentní magnet. Jazýčkový kontakt je tvořen zatavenou trubičkou naplněnou ochrannou atmosférou, v níž jsou dva feromagnetické kontakty. Permanentní magnet je nejčastěji zmagnetizovaný

váleček z feritu. [2] Tento prvek se využívá při detekci otevření dveří či okna, když je systém nastavený na střežení objektu.

Senzory na ochranu skleněných ploch

Tříštění skla vyvolává charakteristický zvuk, který se hmotou skla šíří jako vlnění v pevném tělese. Toto vlnění zachycuje čidlo pevně spojené s plochou skla. Při narušení skleněné plochy je vlnění vyhodnoceno elektronicky, a to čidly a čidla způsobí hlášení. [2]

Mechanické kontakty

Jedná se o mikrospínače, které jsou konstrukčně uzpůsobené pro zabudování do rámů proti západce zámku. [2]

Vibrační senzory

slouží ke hlídání průrazu stěn a stavebních konstrukcí. Základem je elektromechanický měnič doplněný vyhodnocovaní technikou. Tato čidla mají velkou šířku pásma vyhodnocovacích kmitočtů, nastavitelnou citlivost a optickou indikaci s pamětí. [2]

Existují i další prvky jako například: drátové senzory, rozpěrné tyče, poplachové fólie a tapety, které nebudu ve své práci rozepisovat do detailu. Výše uvedené a popsané jsou nejčastěji využívanými prvky plášťové ochrany.

1.2.2 Prvky prostorové ochrany

Základní rozdělení prvků prostorové ochrany:

1. Senzory pasivní – při detekci napadení registrují pouze fyzikální změny ve svém okolí
2. Senzory aktivní – při detekci napadení vytváří aktivní působení na okolí a detekují změnu vytvořeného fyzikálního prostředí.

Nejvyužívanějšími senzory jsou:

Pasivní infračervené senzory

Tyto senzory jsou označovány jako PIR senzory (passive infra red sensor). Jsou založeny na principu zachycení změn vyzařování v infračerveném pásmu kmitočtového spektra elektromagnetického vlnění. [2]

Při detekci narušení prostoru člověkem detekuje vlnovou délku elektromagnetického vlnění 9,4 nm, která je charakteristická pro lidskou teplotu těla**.**

Ultrazvukové senzory

Využívají část spektra mechanického vlnění nad pásmem kmitočtů slyšitelných lidským uchem. [2]

Jsou to senzory aktivní, které vysílají do prostoru vlnu a vyhodnocují změnu odražené vlny z prostoru. Pokud člověk vstoupí do místnosti, změní se i parametr vyzařované vlny, což se vyhodnotí jako vnik do prostoru.

1.2.3 Prvky předmětové ochrany

Jedná se o ochranu předmětů ve střeženém objektu či prostoru. K ochraně předmětů se nejčastěji využívají:

Závěsové senzory

Střežený předmět je zavěšen pomocí lanka na hák senzor. Senzor poté vyhodnotí síly, které působí na hák senzoru.

Polohové senzory

Jedná se o elektromagnetické nebo kontaktní senzory, která citlivě reagují na změnu polohy střeženého předmětu. [2]

1.2.4 Prvky obvodové ochrany

Jedná se o ochranu perimetru objektu. Je to první část, kterou pachatel musí překonat, aby se dostal do cílového objektu. Nevýhody použití prvků PZS při obvodové ochraně jsou časté planné poplachy způsobené okolními vlivy. Mezi nejčastěji využívanými prvky obvodové ochrany jsou:

Infračervené závory a bariéry

Pracují na principu přijímací a vysílací strany. Mezi těmito stranami probíhají infračervené paprsky, které když někdo naruší, tak vyhodnocovací strana detekuje narušení paprsků a vyvolá poplach.

Perimetrická pasivní infračervená čidla

Jedná se o čidla PIR, využívané ve venkovních prostorech. Je zde oproti klasickým prostorovým PIR senzorům využita jiná optika, která je odolnější vůči klimatickým a jiným venkovním okolním vlivům.

Na obrázku č. 1. můžete vidět jednotlivé prvky. Je zde ukázán i nejhlavnější prvek PZTS a tím je ústředna. V následující kapitole budou tyto ústředny uváděny, popisovány a rozebírány jejich kladné a záporné vlastnosti.

Obr. 1. Ukázka prvků PZTS [23]

1.3 Ústředny PZTS

Ústředny jsou v systému PZTS nejdůležitějším článkem. Je to mozek celého systému. Můžeme je definovat jako zařízení pro příjem, zpracování, ovládání a následný přenos informací.

Ústředna PZS plní tyto funkce:

- přijímá a vyhodnocuje výstupní signály detektorů PZS
- ovládá signalizační, přenosová, zapisovací a jiná zařízení, která indikují stavy PZS
- možnost ovládání PZS pomocí klávesnice a dalších ovládacích prvků (např. bezdrátové klíčenky)
- napájí detektory a další prvky PZS

- možnost diagnostiky systému PZS

Ústředny PZS lze dělit podle několika hledisek. Nejpoužívanější dělení je následující:

Podle způsobu připojování detektorů a dalších prvků PZTS k ústředně:

- ústředny drátové

-ústředny analogové (smyčkové)

-ústředny sběrnicové (možnost přímé adresace detektorů)

-ústředny smíšeného typu (jedná se o kombinaci analogového a sběrnicového typu)

- ústředny bezdrátové
- ústředny hybridní [4]

Podle stupně zabezpečení se ústředny PZS dělí na:

- ústředny s nízkým rizikem
- ústředny pro nízké až střední riziko
- ústředny pro střední až vysoké riziko
- ústředny s vyšším rizikem [4]

Podle počtu smyček se ústředny PZS dělí na:

- ústředny malé (1 - 8 smyček)
- ústředny střední (16 - 48 smyček)
- ústředny velké (nad 48 smyček) [4]

Podle struktury se ústředny PZS dělí na:

- kompaktní
- modulární [4]

1.3.1 Drátové ústředny PZS

1.3.1.1 Ústředny analogové (smyčkové)

Pro každou poplachovou smyčku mají analogové ústředny vstupní vyhodnocovací obvod. Ve smyčce může být umístěn jeden či více detektorů v závislosti na zapojení smyčky. K vyhlášení poplachového stavu systému PZS dochází, pokud dojde ke změně odporu smyčky. Aktivace poplachu je způsobená aktivací některého z detektorů na smyčce. Detektor svojí aktivaci signalizuje prostřednictvím rozpojení NC (normally closed) kontaktu nebo sepnutím NO (normally open) kontaktu. Smyčky jsou v praxi zapojeny nejčastěji sériovým zapojením. Nejčastějšími užívanými druhy zapojení smyček jsou:

- jednoduše vyvážená smyčka
- dvojitě vyvážená smyčka
- trojitě vyvážená smyčka
- smyčka s technologií zdvojení zón (ATZ - Advanced Technology Zones)

Každé zapojení má své výhody a nevýhody. Záleží na konkrétní aplikaci a požadavcích na PZS. V dnešní době jsou nejčastěji využívány ATZ smyčky, někdy i dvojitě vyvažované.

1.3.1.2 Ústředny sběrnicové

Komunikace u těchto ústředen je realizována prostřednictvím datového vedení. Komunikace probíhá primárně mezi ústřednou a detektory, ovšem v dnešní době začaly systémy využívat datová vedení i pro komunikaci mezi ostatními prvky systému. Ústředna opakovaně generuje adresy jednotlivých detektorů (nebo ostatních prvků PZS) a následně přijímá příslušné odezvy o stavech detektorů. Ústředna a jednotlivé detektory jsou propojeny nejčastěji pomocí čtyř vodičů, přičemž dva vodiče slouží k napájení a dva jsou určeny pro komunikaci.

Aby mohlo dojít ke komunikaci ústředny s detektorem, musí být každý detektor vybaven komunikačním modulem. Pokus o záměny detektorů pachatelem jsou řešen tím, že každý detektor vlastní svou jedinečnou adresu, která je velmi složitě zjistitelná. Díky této jedinečné adrese je možné přesně určit polohu narušení objektu. Oproti ústřednám analogovým mají sběrnicové vysokou odolnost proti překonání a tudíž se v komerčním

sektoru využívají zejména u rozsáhlých objektů, kde je obrovská výhoda možnosti připojení vysoký počtů prvků PZS.

1.3.1.3 Ústředny smíšeného typu

Jedná se o kombinaci analogové a sběrnicové ústředny, kde každá ústředna má určitý počet linek. Pomocí těchto linek jsou k vlastní ústředně připojeny koncentrátory. Koncentrátory slouží jako analogové ústředny, kdy jejich úkolem je soustřeďovat informace z detektorů připojených do proudových smyček. Komunikačním kanálem mezi ústřednou a koncentrátory je datová sběrnice. Na sběrnici lze mimo koncentrátorů připojit také klávesnici, komunikační moduly (např. pro připojení počítače) a další prvky. Nyní bych shrnul výhody a nevýhody všech drátových PZS oproti bezdrátovým.

Výhody:

- napájení všech součástí systému je uskutečňováno pomocí jednoho zdroje
- větší odolnost vůči rušení
- cenově méně náročnější komponenty
- snazší diagnostika komunikačních problémů mezi jednotlivými prvky a ústřednou

Nevýhody:

- nutnost začisťovacích prácí při montáži PZS v již hotových interiérech
- montáž drátových ústředen je mnohem náročnější oproti bezdrátovým

1.3.2 **Bezdrátové ústředny**

Tyto ústředny využívají bezdrátového propojení mezi prvky poplachového zabezpečovacího systému. Pracují převážně v pásmech 868 MHz a 433MHz. Hlavními přednostmi systému jsou:

- rychlá a nenáročná instalace
- snadné konfigurační změny

- minimální zásahy do interiéru
- snadné rozšíření systému o další prvky

Výhody a nevýhody oproti drátovým ústřednám jsou:

Výhody:

- snadnější a rychlejší montáž
- jednodušší přenášení celého systému na jiná místa

Nevýhody:

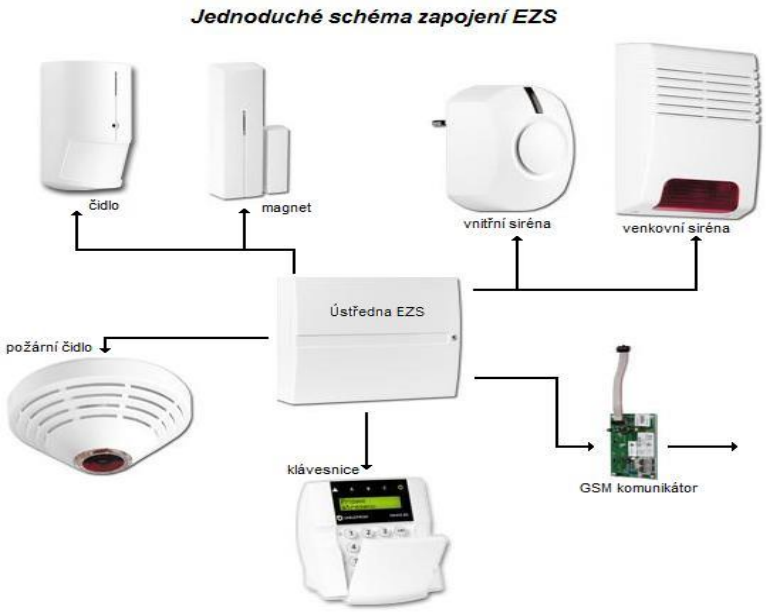
- napájení jednotlivých bezdrátových komponent systému jednotlivě
- nutná údržba (pravidelná výměna baterií u všech komponentů systému – přibližně jednou do roka) - ústředna PZS provádí automatickou kontrolu
- finančně náročnější komponenty

1.3.3 Hybridní ústředny

Ústředna umožňuje jak drátové připojení prvků PZS, tak bezdrátové. Výhody a nevýhody jsou totožné jako u obou předchozích systémů.

1.3.4 Grafická schémata systému PZS

Jednoduché grafické schéma můžete vidět na obrázku č. 2. Obrázek je starší, tudíž se zde objevuje zkratka EZS (elektronické zabezpečovací systémy), což byla bývalá zkratka PZTS



Obr. 2. Jednoduché schéma zapojení PZS[24]

2 APLIKAČNÍ PODMÍNKY PZTS

Při aplikaci PZTS je nutné vycházet z požadavků, které jsou kladeny na tyto systémy. Veškeré požadavky, týkající se systémů PZTS, vychází z normy ČSN EN 50131 Poplachové systémy - Poplachové zabezpečovací a tísňové systémy, [5] která není legislativně závazná, ale pouze plní funkci doporučených požadavků na systémy PZTS. Níže můžeme vidět tabulku s přehledem, co tato norma obsahuje.

pč.	Číslo normy	Název normy
1.	ČSN EN 50 131-1 ed.2	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky
2.	ČSN EN 50 131-2-2	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 2-2: Detektory narušení - Pasivní infračervené detektory
3.	ČSN EN 50 131-2-3	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 2-3: Požadavky na mikrovlnné detektory
4.	ČSN EN 50 131-2-4	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 2-4: Požadavky na kombinované pasivní infračervené a mikrovlnné detektory
5.	ČSN EN 50 131-2-5	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 2-5: Požadavky na kombinované pasivní infračervené a ultrazvukové detektory
6.	ČSN EN 50 131-2-6	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 2-6: Detektory otevření (magnetické kontakty)
7.	ČSN EN 50 131-2-7-1	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 2-7-1: Detektory narušení - Detektory rozbíjení skla (akustické)
8.	ČSN EN 50 131-2-7-2	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 2-7-2: Detektory narušení - Detektory rozbíjení skla (pasivní)
9.	ČSN EN 50 131-2-7-3	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 2-7-3: Detektory narušení - Detektory rozbíjení skla (aktivní)
10	ČSN EN 50 131-3	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 3: Ústředny
11.	ČSN EN 50 131-4	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 4: Výstražná zařízení
12	ČSN EN 50 131-5	Poplachové systémy - Elektrické zabezpečovací systémy - Část 5-3: Požadavky na zařízení využívající bezdrátové propojení
13	ČSN EN 50 131-6 ed. 2	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 6: Napájecí zdroje
14	ČSN EN 50 131-7	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 7: Pokyny pro aplikace
15.	ČSN EN 50 131-8	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 8: Zamlžovací bezpečnostní zařízení/systémy

Tab. 1. Přehled ČSN v oblasti poplachových zabezpečovacích a tísňových systémů [6]

V této normě je velmi mnoho jiných požadavků, ale já se zaměřím na normu ČSN EN 50131-1 ed.2, která udává požadavky při aplikaci PZTS.

2.1 ČSN EN 50131-1 ed.2

Uvedená norma byla zpracována technickou komisí CENELEC TC 79 Alarm systém a představuje specifikaci poplachových zabezpečovacích a tísňových systémů instalovaných v budovách.[6]

Účelem této normy je podpořit instalační firmy, investory, pojistitelé a uživatelé, v procesu zpracování a uvést přesné specifikace požadavků na technickou ochranu konkrétních objektů.

Důležitou skutečností je, že všechny uvedené požadavky jsou stanoveny jako minimální (hodnoty, rozsahy, počty atd.) a vždy je třeba při návrhu poplachového zabezpečovacího a tísňového systému brát v úvahu konkrétní podmínky v místě instalace, požadavky právních předpisů, pojistitelů a investora. [6]

2.1.1 Obsah normy

Norma upravuje zejména:

- funkce systému
- komponenty systému
- stupně zabezpečení
- třídy prostředí
- funkční požadavky
- napájení
- spolehlivost
- elektrickou bezpečnost
- dokumentaci a značení. [6]

2.1.2 Funkce systému

- PZTS musí obsahovat funkce specifikované normou ČSN EN 50131-1:[8]
- detekci vniknutí
- aktivace tísňových prostředků
- vyhlášení poplachu
- a zpracování informací

2.1.3 Komponenty systému

- Komponenty PZTS musí být klasifikovány v souladu s jejich odolností vůči prostředí
- musí být děleny do stupňů zabezpečení dle jejich určení,
- kompatibilnost systému
- je zde možnost integrovat i jiné aplikace, pokud ovšem nebudou negativně ovlivňovat další komponenty PZTS

2.1.4 Stupně zabezpečení

- PZTS musí být přiřazen stupeň zabezpečení, určující jeho provedení
- stupeň zabezpečení systému odpovídá prvku s nejnižším stupněm zabezpečení

2.1.5 Třída prostředí

- komponenty musí být použitelné v jedné z definovaných tříd prostředí I-IV
- komponenty musí být integrovány tam, kde mohou správně pracovat v předpokládaných okolních vlivech

Třída	Název prostředí	Teploty, příklad
I	vnitřní	+ 5 °C až +40°C obytné místnosti, obchodní objekty
II	vnitřní- všeobecné	- 10 °C až +40°C není stálá teplota, chodby, haly, schodiště
III	venkovní- chráněné (nebo extremní vnitřní podmínky)	- 25 °C až +50°C vně budovy, komponenty nejsou plně vystaveny povětrnostním vlivů, přístřešky, terasy.....
IV	venkovní- všeobecné	- 25 °C až +60°C vně budovy, komponenty jsou plně vystaveny povětrnostním vlivů

Tab. 2. Rozdělení tří prostředí [8]

2.1.6 Funkční požadavky

- Funkční požadavky v sobě nesou řadu požadavků, které musí systém splňovat, aby mohl efektivně a bez žádných závad, plnit svojí funkci.
- Mezi hlavní funkční požadavky patří detekce, provoz, zpracování signálu, indikace, hlášení, zabezpečení proti sabotáži, propojení systému, časové závislosti a paměť událostí.

2.1.7 Napájení

Základním prvkem pro napájení je napájecí zdroj.

- Je to část PZTS zajišťující energii pro jeho napájení. Nazývá se základní napájecí zdroj.
- Zdroj napájení PZTS je schopný napájet systém i v případě výpadku základního zdroje.
- Napájecí zdroje, které jsou součástí PZTS musí splňovat požadavky ČSN EN 50131-6. [7]

Existují tři typy napájecích zdrojů:

Typ A: Energie je dodávána z vnějšího zdroje (např. sítě) a v případě jeho výpadku je energie dodávána z dobíjecího náhradního zdroje (akumulátor), který je automaticky dobíjen z vnějšího zdroje energie.

Typ B: Energie je dodávána z vnějšího zdroje (například sítě), a v případě výpadku je energie dodávána z dobíjecího náhradního zdroje (např. lithiové baterie), který není automaticky dobíjen z vnějšího zdroje energie.

Typ C: Energie je dodávána pouze z náhradního zdroje, který je v tomto případě základním zdrojem energie (např. baterie). [8]

Zde můžeme vidět časové rozdělení napájení dle typů:

	Stupeň 1	**Stupeň 2**	**Stupeň 3**	**Stupeň 4**
Typ A	12	12	60	60
Typ B	24	24	120	120

Tab. 3. Minimální doba napájení [8]

	Stupeň 1	**Stupeň 2**	**Stupeň 3**	**Stupeň 4**
Maximální doba dobíjení na min. 80 % kapacity	72	72	24	24

Tab. 4. Požadovaná doba napájení [8]

2.1.8 Provozní spolehlivost

- Nutnost aplikace prostředků, které dokážou vyloučit chyby obsluhy,
- komponenty PZTS musí být jasně a srozumitelně označeny tak, aby minimalizovalo nesprávné činnosti.

2.1.9 Funkční spolehlivost

- Návrh PZTS musí zajistit funkčnost v souladu s požadavky norem,

- zabezpečení funkční spolehlivosti.

2.1.10 Požadavky na prostředí

- Činnost PZTS nesmí být negativně ovlivněna v případě vystavení negativním či extrémním vlivům (např. vysoká teplota či vlhkost),
- nesmí dojít k poškození komponent.

2.1.11 Elektrická bezpečnost

- Nutné zabezpečit ochranu proti úrazu elektrickým proudem,
- musí být vyznačená místa či předměty s možným elektrickým nábojem.

2.1.12 Dokumentace

Dokumentace ke komponentům musí obsahovat:

- název výrobce či dodavatele
- popis zařízení
- norma s níž je deklarována shoda
- název certifikačního orgánu
- stupeň zabezpečení
- třída prostředí

2.1.13 Značení

Veškeré komponenty PZTS musí být označeny následovně:

- název výrobce či dodavatele
- typ
- datum výroby
- stupeň zabezpečení
- třída prostředí

3 MOŽNOSTI PŘIPOJENÍ PZTS

Pokud je kvalitně integrován PZTS do střeženého objektu a jsou splněny veškeré aplikační podmínky pro efektivní provoz systému, je nutné tento systém připojit na místo, kde budou poplachové a tísňové signály přijímány, zpracovány a následně se bude na tyto signály adekvátně reagovat. K tomuto účelu slouží dohledová a přijímací poplachová centra (DPPC).

Systém PZTS neplní funkci zabránění neoprávněného vniknutí do objektu a ani nedokáže zabránit odcizení majetku ze střeženého objektu. Jeho funkci je pouze detekce a následné informování o narušení objektu. Proto se PZTS připojují na DPPC, kde jsou proškolení pracovníci, kteří dokáží vyhodnotit poplachový či tísňový signál a v co nejkratší době se pokusit dorazit na místo, kde byl poplach vyvolán. Popis jak tyto společnosti fungují, jsou uváděny v poslední kapitole této diplomové práce. Tato kapitola se zaměřuje na technicky nejdůležitější stránku celého systému a tím je připojení PZTS na DPPC.

3.1 Přenosové trasy

Jak je zřejmé, účinnost dálkového dohledu závisí na všech zmíněných částech řetězce. Nebude-li dobře fungovat vlastní zabezpečovací zařízení, poplachová informace vůbec nevznikne. Bude-li přenosová cesta přerušena nebo bude-li jinak nefunkční, nedojde poplachová zpráva do přijímacího střediska a výsledek bude prakticky stejný, jako kdyby bylo zabezpečovací zařízení nefunkční. Je tedy zřejmé, že je třeba přenosové cestě a její kvalitě věnovat dostatečnou pozornost. [17]

Komunikační přenosové trasy jsou tedy nejdůležitější částí DPPC. V moderní době se neustále vyžaduje zvyšování rychlosti přenosových tras, ovšem s každou novou technologií či systémem přichází i nové složitosti. Jsou zde kladeny vyšší nároky na znalosti a dovednosti projektantů, kteří zodpovídají za instalovaný systém. Nyní si popíšeme všechny nejvyužívanější komunikační přenosové trasy.

3.1.1 Nejvyužívanější komunikační přenosové trasy

- Telefonní linka v hovorovém pásmu (komutované spojení)
- Telefonní linka v nad-hovorovém pásmu

- 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
- Vyhrazená přenosová cesta [9]

3.1.1.1 Telefonní linka v hovorovém pásmu

Připojení prostřednictvím telefonní linky bylo dříve nejvyužívanější přenosovou trasou v oblasti zabezpečení. Jedná se o veřejnou telefonní síť s názvem JTS – jednotná telefonní síť, v angličtině značená jako PSTN - public switched telephone network. Tato možnost připojení byla praktikována z důvodu širokého pokrytí JTS. Tuto možnost připojení ovšem nahrazuje v dnešní době síť GSM, která bude popisována v dalších kapitolách.

Veškerý přenos při této metodě je uskutečňován pomocí hovorového pásma. Linka se nejprve připojí do ústředny PZTS a následně se z ústředny PZTS vytvoří připojení pro koncové zařízení. PZTS ústředna má vždy prioritu v procesu vysílání, tudíž pokud je nutné poslat informaci, jsou telefonní hovory přerušeny (pokud v té době právě probíhají), PZTS si zašle požadovanou zprávu a po odeslání opět linku uvolní.

Podstatnou částí veškerého programování je nastavení dvou linek. Jednu hlavní a pokud bude trasa obsazená, tak i linku záložní. Pokud je hlavní linka obsazená, bude ústředna vytáčet záložní linku. Může se stát, že i záložní linka bude obsazená, proto se v ústředně nastavuje počet opakování (průměrně se nastavuje na 6 opakování). V případě, že i po šesté se ústředna nedovolá, bude signalizována porucha spojení. Vzhledem k tomu, že je tento proces vytáčení časově velmi náročný, využívají DPPC sériové zapojení linek, které zajišťuje poskytovatel JTS. Rozdíl je ten, že pokud se ústředna nedovolá na hlavní linku, nedojde k zavěšení a vytáčení záložní linky, ale pouze se hovor přesměruje na záložní linku. To velmi sníží čas na dovolání se a zaslání informace.

3.1.1.2 Telefonní linka v nad-hovorovém pásmu

Tato varianta přenosu umožnila přenést stavovou informaci z ústředny PZTS na DPPC, aniž by znemožnila činnost telefonního přístroje. Systém pracuje na bázi frekvence 20 Khz, kde je signál přenášen po telefonní lince a DPPC byl doručován pouze stav ústředny (ano/ne). Stav vyjadřoval, zda signál je či není. Tento systém využívá komunikátor, který je schopen přenést až 256 informací.

Oproti přenosu v hovorovém pásmu, zde byla nepřetržitá kontrola spojení střeženého objektu s DPPC.

3.1.1.3 Telefonní linka ISDN

v ČR se tento typ přenosu příliš neujal z důvodu rozvoje mobilní sítě. ISDN (Integraded Services Digital Network) znamená integraci 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 analogově – digitálně převodenému signálu až k účastníkovi do jeho přístroje.

2 typy přípojek:

- 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.[10]

3.1.1.4 Rádiový přenos na vyhrazených frekvencích

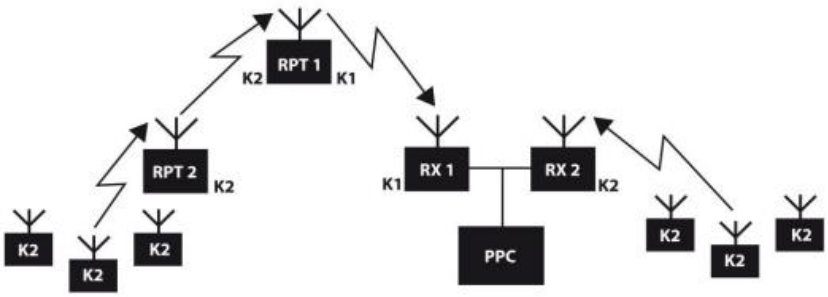
Tato varianta přenosu se považuje za nejbezpečnější a nejrychlejší. Je velmi složité ji napadnout a výpadky této sítě jsou velmi minimální.

Pokud bychom srovnali rychlost přenosu u telefonní linky JTS, doba od vzniku události střeženého objektu do doby přijetí na DPPC a následné vyhodnocení se pohybuje v rozmezích 10-20 vteřin. Může se stát, že v době vytáčení a odesílání zprávy pachatel zničí ústřednu, tudíž se zpráva na DPPC neodešle.

U rádiového přenosu závisí doba přenosu na umístění vysílače a hlavně topologii radiové sítě. Například pokud bychom vzali časovou prodlevu jednosměrné rádiové sítě bez retranslační stanice, tak se doba, kdy je zpráva vysílána, pohybuje kolem 330 ms. Tudíž pachatel nemá v podstatě žádnou šanci v této krátké době zničit ústřednu a zpráva bude tedy úspěšně doručena na DPPC.

Tato síť je velmi těžko napadnutelná a z hlediska spolehlivosti a rychlosti přenosu signálu je tato varianta nejlepší a v dnešní době velmi často využívaná. Nevýhodou oproti tomu je finančně náročnější pořizovací cena. Aby tato možnost mohla být uskutečněná, je nutné aby měl poskytovatel zřízenou vlastni rádiovou síť s provozní frekvencí, schvalovanou Českým telekomunikačním úřadem.

Další nevýhoda může nastat, pokud se objekt bude nacházet v kopcovitém terénu. V tomto případě se zřizuje retranslační stanice a tudíž zde rostou i náklady na provoz rádiové sítě. Níže je zobrazeno blokové schéma rádiové sítě s použitím retranslačních stanic.



Obr. 3. Blokové schémá radiové sítě [25]

Vysvětlivky k obrázku č. 4:

- **K2** objektový vysílač
- **RPT1, RPT2** retranslační stanice
- **RX1, RX2** přijímač PPC, kdy přijímač RX1 přijímá signál s retranslační stanice a RX2 přímo z objektových stanic
- **PPC** poplachové přijímací centrum. [11]

3.1.2 GSM

Existují objekty, kde není zřízená JTS přípojka a zároveň zde nelze využít rádiový přenos. (např. chatové oblasti a mobilní stavební buňky). V tomto případě je možnost připojení pomocí sítě GSM (Global System for Mobile Comunications). Na ústřednu PZTS se integruje GSM komunikátor a dle použitého typu jsou zprávy přenášeny v hovorovém pásmu, datovém pásmu prostřednictvím služby GPRS (General Packet Radio Service) a nebo pomocí SMS zprávy.

3.1.2.1 Přenos po síti GSM v hovorovém pásmu

Tato varianta formy přenosu je finančně nejdražší. Připojí se zde GSM brána na jednu z linkových karet přijímače DPPC. Majiteli střeženého objektu je poskytnuta SIM karta, patřící do firemní sítě, kde operátoři poskytují zvýhodněné paušální tarify a veškerá komunikace je v tomto paušálu zahrnuta. Není zde tudíž omezení počtu zpráv z ústředny PZTS na DPPC.

3.1.2.2 Přenos po síti GSM prostřednictvím GPRS

GPRS je mobilní datová služba, která využívá přepojování paketů, kdy se dynamicky využívají neobsazené časové sloty, které může sdílet více uživatelů. Pro přenos informace se v tomto případě zpravidla využívá IP protokol pracující na síťové vrstvě. Velkou výhodou je obousměrná komunikace mezi DPPC a komunikátorem instalovaným na střeženém objektu. Opět se v rámci „firemní sítě“ můžeme dostat na velmi nízký paušál za datový tarif. Na straně DPPC je instalován přijímač, který je využívaný i při přenosu přes internet (viz obr. 5) nebo je příjem zpráv zajištěn monitorovacím softwarem na úrovni služby. [11]

3.1.2.3 Přenos po síti GSM prostřednictvím SMS

Tento způsob je poměrně jednoduchý. DPPC přijímá SMS zprávy o poplachu nebo stavu objektu. Příjem je realizován pomocí SMS komunikátorů a všechny přijaté zprávy jsou zobrazeny v monitorovacím softwaru. Přijaté SMS zprávy lze filtrovat, ukládat na disk nebo vytisknout na papír.

Nevýhodami oproti tomu jsou velké finanční náklady na zakoupení a instalaci SMS brány ve střeženém objektu a zpožděné doručení SMS zprávy při přetížené síti.

3.1.2.4 Přenos pomocí internetové sítě

Tato varianta přenosu se stává čím dál více využívanější v oblasti zabezpečování objektů. Jsou zde totiž mnohem větší možnosti přenášení informací mezi PZTS a DPPC. Kromě přenosu poplachových a stavových informací lze přenášet i obraz a zvuk. Také je zde možnost vzdáleného dohledu a ovládání PZTS. Přenos obrazu z kamerových systémů eliminuje výjezdy k planým poplachům. K přenos informací využívají objektové komunikátory i přijímač DPPC dva protokoly transportní vrstvy UDP a TCP, případně oba dva.

3.1.2.4.1 Dva základní typy transportních protokolů:

- **TCP** – zpráva je doručena vždy. Doba trvání může být delší. Protokol zde čeká, až budou splněny podmínky k navázání TCP spojení. Pokud je spojení navázáno, může komunikace probíhat obousměrně.
- **UDP** – zpráva je doručena okamžitě bez navázání spojení, pokud je ovšem cesta k příjemci volná. V případě že není volná, zpráva zanikne. Nelze zde tudíž ověřit, zda byla zpráva příjemci doručena.

3.1.2.5 Vyhrazená přenosová cesta

Vyhrazená přenosová cesta je taková, která je neustále k dispozici pro spojení PZTS s DPPC, a která nevyžaduje spínání nebo nastavování před přenosem jednotlivých poplachových událostí.

3.2 Náhradní připojení PZTS

U klasických bytů či domů si majitelé zřizují propojení PZTS s DPPC jednou přenosovou trasou a to z ekonomických důvodů. U objektů s vyšším riziky (např. benzíny, banky, lékárny, továrny) se využívájí náhradní přenosové trasy. Cílem je zajistit zaslání poplachové či tísňové zprávy na DPPC i v případě, že dojde k poruše či napadení hlavní přenosové trasy.

3.2.1 Kombinace přenosových tras

Zpravidla se využívají kombinace variant přenosových tras uváděné v kapitole 3.1.

3.2.1.1 Kombinace JTS a RADIO sítě

Tato kombinace se využívala v minulosti, jelikož měla většina objektů zřízenou telefonní přípojku. V dnešní době se tato kombinace využívá velice zřídka. V této kombinaci je použita radiová síť jako primární přenosová trasa a JTS jako trasa náhradní při výpadku rádiové sítě. Může tomu být i naopak. Vše záleží, jak si to majitel objektu po odborné konzultaci s pracovníkem DPPC bude přát nainstalovat.

V případě, že DPPC nedostane kontrolní zprávu z objektu v předpokládaném intervalu (většinou do 5 minut) nebo, že ústředna PZTS v objektu nedostane potvrzení o příjmu vyslané zprávy, je využita náhradní přenosová trasa. Toto opatření eliminuje možnost, že pachatel vyřadí rádiovou přenosovou cestu a na DPPC nepřijde žádná zpráva.

Narušení obou přenosových cest v jediném okamžiku je prakticky neproveditelné. Pokud pachatel naruší rádiovou trasu, bude na DPPC vygenerovaná zpráva o nepřijetí kontrolního telegramu a zároveň může být paralelně předána zpráva o narušení střeženého objektu prostřednictvím náhradní trasy JTS. Pokud naopak pachatel přestřihne nebo zruší telefonické vedení, ústředna PZTS toto vyhodnotí a zašle poplachovou zprávu na DPPC.

3.2.1.2 Kombinace JTS a GSM sítě

Tato kombinace je totožná s kombinací uváděné v kapitole 3.2.1.1. Místo rádiové přenosové trasy je využita síť GSM. GSM síť je v dnešní době jednodušeji napadnutelná než-li síť rádiová. Nejčastějším napadením je využití principu rušení vysílaného signálu

pomocí takzvaných „rušiček“. Rádiovou síť lze také vyrušit, ale je to technicky náročnější oproti síti GSM.

3.2.1.3 Kombinace GSM a RADIO sítě

Touto kombinací je v dnešní době řešena převážná část zabezpečených objektů. Zda se využije GSM síť jako primární přenosová trasa a rádiová sít jako trasa náhradní či naopak, je závislé pouze na přání zákazníka a na jeho ekonomických možnostech.

3.2.1.4 Kombinace GSM či RADIO sítě a internetu

Tato kombinace je méně využitelná, ale v praxi ji určitě u některých objektů nalezneme. Většinou je internet použit jako náhradní přenosová trasa, pokud dojde k napadení sítě hlavní. Ovšem napadení internetové sítě je pro pachatele nejjednodušší možností všech výše zmiňovaných přenosových cest. Mezi nejznámější technikou napadení je přehlcení provozu sítě a tudíž zpráva nedorazí tam kam by měla. Proto se začaly využívat další bezpečnostní prvky k zajištění internetové přenosové cesty.

3.2.1.4.1 *VPN*

VPN (virtuální privátní síť) je v informatice prostředek k propojení několika počítačů prostřednictvím (veřejné) nedůvěryhodné počítačové sítě. Lze tak snadno dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní (a tedy důvěryhodné) sítě. Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů, dojde k autentizaci, veškerá komunikace je šifrována, a proto můžeme takové propojení považovat za bezpečné. [12]

Tento bezpečnostní prvek se přidává v případě internetového přenosu poplachových a tísňových zpráv za účelem šifrované komunikace. Nevýhodou zřízení VPN je, že DPPC musí být zřizovatelem této sítě a hlavně musí mít zřízenou i dešifrovací službu, která umožňuje šifrovanou komunikaci mezi PZTS a DPPC dešifrovat.

3.2.1.4.2 *Ipsec*

Ipsec (IP security) je bezpečnostní rozšíření IP protokolu založené na autentizaci a šifrování každého IP datagramu. [13]

Je to nadstandardní prvek při využití VPN u internetového přenosu, kdy je nejen šifrovaná komunikace, ale i navázání spojení je šifrované. Tento prvek je velmi složitě napadnutelný a pomocí něj v dnešní době vzrůstá počet objektů, které využívají internet jako náhradní přenosovou trasu.

Nevýhody internetové přenosové trasy spočívá v tom, že napadení internetové sítě není v dnešní době tak náročné a také je zde riziko výpadku internetu, tudíž poplachová zpráva může být pozdržena či vůbec nebude doručena a DPPC nebude uvědomeno o narušení střeženého objektu.

3.3 Přenášené zprávy

Jedná se o zprávy, které jsou naprogramovány v ústředně PZTS, aby byly přenášeny na DPPC. Při programování ústředny záleží především na požadavcích zákazníka, zda chce přenášet pouze poplachové zprávy, nebo naopak má zájem přenášet všechny zprávy. Jsou to například zprávy, které majitele objektu upozorní, že objekt není zakódován nebo kódování probíhá mimo určenou dobu.

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.) [11]

Veškeré zprávy jsou v monitorovacím softwaru na pracovní stanici obsluhy DPPC rozlišeny různými barvami pro lepší orientaci v příchozích zprávách. Poplachové a poruchové zprávy jsou navíc akusticky signalizovány.

4 DPPC

Dohledové a poplachové přijímací centrum, neboli DPPC je služba nabízená soukromými společnostmi. Tato společnost má vybudované své dispečerské stanoviště, které neustále střeží objekty zabezpečené pomocí poplachové zabezpečovací signalizace (PZS), nebo elektronické požární signalizace (EPS) které jsou na pult připojeny. Na tento pult mohou být přenášeny veškeré informace, které je daný systém elektronické signalizace schopen poskytnout. [14]

Současným trendem je kromě střežení objektů pomocí PZTS i monitoring objektu kamerovým systémem. Obraz je přenášen na DPPC a umožňuje případnou verifikaci poplachového signálu. Verifikací rozumíme doplňkové informace, které indikují pravděpodobnost, že došlo k ostrému poplachu. 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 např. o překročení teploty, únik vody či plynu, nefunkčnosti výtahu atp. a operační centra může na tyto události reagovat kontaktováním odpovědné osoby. [11]

4.1 Rozdělení DPPC

Jak již bylo zmíněno výše, DPPC je poskytováno v oblasti komerční bezpečnosti soukromými společnostmi. Ovšem vlastní DPPC může mít i policie. Jelikož se samotná policie rozděluje dle své územní působnosti a dle střežení svého majetku, tak i připojení na DPPC se rozděluje na:

- Státní Policii (ministerstva, ČNB)
- Městkou Policii (městský úřady)
- Obecní Policii (obecní úřady)
- Vojenskou Policii (majetek armády)

Každá z těchto složek vlastní DPPC, na které jsou napojeny všechny objekty, které jsou majetkem příslušného území. Například pokud je budova majetkem městské části, bude PZTS tohoto objektu připojeno na DPPC městské policie. Každý objekt v ČR je majetkem soukromým, městským, obecním či státním a podle toho se určuje, na které DPPC bude

daný objekt připojen. Další část bude soukromé DPPC detailně rozebírat a uvádět jejich praktické zásahy na varovné signály.

II. PRAKTICKÁ ČÁST

5 ÚVOD DO PRAKTICKÉ ČÁSTI

Veškeré technické popisy systému PZTS a možnosti jeho připojení na vyhodnocovací terminály jsou stejná, ať se jedná o zásah pracovníků DPPC, příslušníků Policie ČR či příslušníky armády České republiky. Jsou zde pouze jiné zákony, kterými se jednotlivé subjekty během zásahů řídí, ale principy a technologie PZTS a přenosových tras zůstávají pořád stejné. Praktická část diplomové práce je zaměřena převážně na popis DPPC v oblasti komerční bezpečnosti a na způsoby a taktiky během zásahů na varovné signály PZTS.

Veškeré informace, které jsem se během studia a práce v oblasti komerční bezpečnosti naučil, jsem si po konzultaci s různými společnostmi DPPC potvrdil, ujasnil si některé nejasnosti a dostudoval si legislativní změny, týkající se této tématiky. V této části všechny tyto informace budu uvádět a popisovat.

Ještě bych na začátek rád uvedl, že i když jsem konzultoval tuto problematiku s více společnostmi, tak veškeré taktiky a způsoby zásahů jsou u těchto společností podobná. Odlišnosti můžeme vidět pouze v interních pravidlech a směrnicích.

6 PRACOVNÍCI DPPC

Dohledová a poplachová přijímací centra mají své bezpečnostní pracovníky rozděleny dle jejich funkce. Níže si popíšeme, jak se tyto funkce rozdělují, jakou činnost jednotliví pracovníci plní a jaké mají odpovědnosti.

Velitel oddílu

- strážní činnost, včetně obsluhy nutných zařízení
- organizace služeb a obsazení střežených objektů
- kontrolní činnost nad pracovníky výjezdu a dispečinku
- kontrola výstroje a výbavy pracovníků
- kontroly údržby zásahových vozů
- evidence fyzické přípravy a ostatní evidenční činnosti
- vytvoření podkladových materiálů pro další zpracování
- údržba a úklid základen a vozidel
- komunikace se strážnými a vedením
- návrhy a postřehy pro zlepšení efektivity práce
- teoretická a, taktická a fyzická příprava - vedení tréninku
- výjezdová činnost

Pracovník výjezdu DPPC

- strážní činnost, včetně obsluhy nutných zařízení
- teoretická a taktická příprava
- údržba a úklid vozidel a základen
- evidenční činnost
- výjezdová činnost

Dispečer DPPC, práce na dispečinku

- kontakt se zákazníky, strážnými, vedením a eventuálně s Policií ČR
- obsluha PCO, telefonů a radiostanic
- evidenční činnost
- podklady pro techniky, hlášení závad technikům
- předání informací dispečerům a strážným
- kontrola komunikace s hlídkami i pracovníky fyzické ostrahy na stanovištích
- úklidová činnost na dispečinku
- výpisy DPPC, záznamy, video.

Pracovní náplň a odpovědnost dispečera je velice důležitá, ale především náročná. Musí mít slušné a vstřícné chování. Zpravidla je dispečer první osoba, která je informována o narušení objektu. Komunikuje s majiteli objektu, policií, hasiči a dalšími složkami a zároveň provádí kontrolu komunikace objektů i vozidel, strážnými stanovišti. Pokud se stanoviště nehlásí, nebo hlídka není na určeném místě, hlásí tento fakt veliteli oddílu nebo vedení firmy. Pokud se hlídka nehlásí DPPC, vyšle hlídku druhou, aby prověřila možné napadení. Provádí různé úkony dle specifikace pro jednotlivé druhy zabezpečení. Dbá na dodržování bezpečnostních kriterií. Těmi jsou například ověřování jmen, hesel a zpráv a zapisování zjištěných skutečností. Mimo jiné sleduje všechna dostupná bezpečnostní zařízení (PZTS, kamery, vysílače a jiné zařízení). Pokud dojde k narušení jednoho z bezpečnostních zařízení, povolá výjezd DPPC, aby narušení prověřili. Samozřejmě sleduje dění i v okolí dispečinku a před sídlem firmy.

Technik

- montáže a servisy
- evidenční činnost
- údržba DPPC
- opravy vozidel
- doplnění stavů pracovníků
- nákupy materiálu

- výjezdová činnost

6.1 Povinnosti pracovníků

Každý pracovník DPPC musí splňovat své povinnosti dle firemních směrnic a pracovního řádu. Níže je ukázka některých z povinností a zákazů pracovníkům DPPC.

6.1.1 Pracovník je povinen:

1. Znát pracovní směrnice, náplň práce, řády ostrahy a aktuální nařízení. Vždy jednat s platnými zákony a uposlechnout nařízení nadřízeného. Dbát na služební postupy. Nejvyšším nadřízeným je majitel firmy, dále jeho zástupci a velitelé. Mezi dvěma strážnými je to funkčně starší pracovník.

2. Dodržovat uniformní kázeň, chodit čistý a upravený. Uniforma musí mít všechny předepsané náležitosti, pokud je pracovník dostal. O typu ústroje rozhoduje majitel a dále dle služebního postupu. Vystupování pracovníka na veřejnosti musí být vždy slušné a budící respektu. Uniforma nebo její části jsou určené k nošení pouze ve službě.

3. Ve všech prostorách užívaných pracovníky udržovat pořádek, a užívat je tak, jak je specifikováno vedením. Nepovolené užívání vede k postihu. Cizím osobám je přístup povolen pouze kdy je v budově vedení, nebo osoby, které návštěvu pracovně očekávají. Tyto osoby mají zákaz vstupu na dispečerské pracoviště.

4. V každém místě ostrahy dodržovat stanovený řád, směrnice, postup a časový harmonogram stanovené práce.

5. Střežit předměty a objekty pozorně, důsledně kontrolovat všechna rizika a v případě zjištění trestné činnosti zasáhnout v rámci obecných směrnic pro zásah. K zásahu vždy využít veškeré dostupné prostředky ochrany zdraví. Při zásahu dbát svého zdraví a bezpečnosti.

6. Provádět stanovené evidenční záznamy, číselně a podrobně. Přebírat službu a výbavu odpovědně. Za převzaté věci odpovídá kdo je převzal.

7. Kdykoliv pomoci svým kolegům v nesnázích, pokud bude žádán, nebo sám tuto potřebu uzná za vhodnou. Nastoupit do služby, vyžaduje-li to nutnost situace.

8. Je-li třeba, komukoli poskytnout první pomoc v rozsahů svých schopností znalostí. Takovou pomoc poskytnout i pachateli, pokud tím není pracovník ohrožen.

9. Jakékoliv porušování řádů, směrnic a harmonogramů ihned hlásit nadřízenému, nebo majiteli firmy.

10. Prokazovat se služebním průkazem, nebo osobním číslem

11. Šetřit zdraví osob, proti kterým je zakročováno a dbát taktických postupů k vedení zákroku

Zákazy pracovníkům

1. Šířit informace o počtu zaměstnanců, o střežených objektech, adresách klientů, systémech ostrahy, řádech, harmonogramech, o metodách zvyšování kvalifikace výcviku. Tato povinnost platí i po ukončení pracovního poměru a je ošetřena zákoníkem práce. Porušení mlčenlivosti může být i trestným činem se všemi důsledky.

2. Vzdalovat se z místa ostrahy v době střežení. V nutném případě opuštění hlásit, vyčkat vystřídání a nahlásit takovou situaci veliteli oddílu.

3. Používat služební vozidlo k jiným než služebním jízdám. Jiné užití je povoleno pouze se souhlasem firmy.

4. Spát ve službě, pokud není spánek v režimu jeho služby zahrnut. Pokud je spánek do režimu zahrnut, musí reagovat na narušení a poplach rychle a s dodržováním norem stanovených časů. Pracovník, který není schopen takto reagovat a nestíhá stanovené normy, nesmí v pracovní době spát.

Ostatní pracovní záležitosti řeší Zákoník práce, nebo kolektivní smlouvy

6.2 Ochranné prostředky pracovníků

Každý člen zásahového týmu musí být vybaven základními prostředky a uniformou, především pro svoji ochranu a zadržení pachatele. Vybavenost jednotlivce se však liší podle dané situace a možných rizik zásahu.

6.2.1 Mezi výbavu pracovníka řadíme:

Uniforma

Slouží k identifikaci jednotlivce, k propagaci firmy, ale hlavně jako ochranný oděv při pohybu v objektech.

Obr. 5. Ukázka uniformy [27]

Přilba

Slouží jako ochranná pomůcka při tísňových a rizikových zákrocích v objektech. Dále i za předpokladu vysokého rizika.

Obr. 6. Ukázka přilby[28]

Neprůstřelná a taktická vesta

Pracovníci výjezdu jsou povinni vestu užívat při každém výjezdu.

Obr. 7. Ukázka neprůstřelné vesty [29]

Tomfa

Je základní obranný a pomocný donucovací prostředek k řešení závažných situací napadení strážného, nebo k vyvedení osob z objektu.

Obr. 8. Ukázka tomfy [30]

Slzný plyn (pepřový)

Ochranný prostředek a předejití fyzického kontaktu s útočníkem. Při závažnějších situacích používá zásahový tým slzné granáty.

Obr. 9. Ukázka slzného plynu [31]

Nůž

Ochranný prostředek, který lze použít jen k obraně života dle § 28 a § 29.

Obr. 10. Ukázka nože [32]

Střelné zbraně

Další z ochranných prostředků pro obranu života. Držitel musí mít platný zbrojní průkaz. Užití střelné zbraně je dle zákona na zodpovědnost držitele.

Obr. 11. Ukázka střelné zbraně [33]

Pouta

Prostředek, který zamezuje svobodu zadržených pachatelů do příjezdu Policie ČR

Obr. 12. Ukázka pout [34]

Svítilna

Každé výjezdové vozidlo musí být vybaveno dobíjecí svítilnou. Používá se při pohybu v neosvětlených prostorech, nebo v prostoru, kde by mohlo být světlo zhasnuto. Z bezpečnostních důvodu je nutno nosit svítilnu při svícení mimo lidskou osu, aby případný útok za tmy, hlavně střelbou nezasáhl člena zásahového týmu za svítilnou.

Obr. 13. Ukázka svítilny [35]

Obuv

Obuv by měla být černá, kožená a pevná na noze. Člen zásahového týmu musí být v obuvi schopen rychlého běhu, lezení a skákání přes překážky. Řidič zásahového vozidla musí být schopen v této obuvi bezpečně řídit vozidlo.

Obr. 14. Ukázka obuvi zásahového týmu [36]

Šroubováček

Prostředek nutný k vyřešení nevyřešitelných závad na PZS v objektu. Při výjezdu ho mají členové neustále při sobě.

Obr. 15. Ukázka šroubováčku [37]

Hasicí přístroj

Ve vozidle jsou dva typy. První je malý v podobě spreje, který je pro ochranu vozidla a hlídky, druhý je velký klasický a slouží pro ochranu střežených objektů.

Obr. 16. Ukázka hasícího přístroje [38]

Basebool pálka

Pomocný ochranný prostředek při tísňových voláních a přesile.

Obr. 17. Ukázka baseballové pálky [39]

7 ZÁSADY SPRÁVNÉHO POSTUPU PŘI ZÁSAHU

Veškeré podmínky mezi klientem a bezpečnostní agenturou jsou vedeny ve smlouvě. Jsou zde stanoveny zejména časy dojezdů na místo poplachu, odpovědný zástupce (pokud by majitel nebyl ka zastižení), kam se budou zasílat poplachové zprávy a další náležitosti, potřebné k řešení situací při vyhlášení poplachu. Ve smlouvě je primárně danné, že bezpečnostní agentura zastupuje majitele v potřebných úkonech a majitel věnuje agentuře kopii klíče k střeženému objektu, pokud by bylo zapotřebí vstoupit do objektu a majitel by nebyl poblíž.

Hlavními úkoly bezpečnostní agentury je vždy reagovat na poplachové signály, být na místě času stanoveném ve smlouvě a snažit se odvrátit hmotným škodám či újmám na zdraví. Zásadní věcí je zjištění k čemu při vyhlášení poplachu došlo a zaevidování veškerých informací pro předání majiteli.

Jsou lidé, kteří si poplachové zprávy z PZTS nechávají zasílat pouze na svůj mobil a služby bezpečnostních agentur nevyužívají z důvodu snížení nákladu na svojí bezpečnost. Já považuji toto řešení jako špatné. Za prvé pokud příjde poplachová zpráva na mobil, tak z většina případů není majitel schopen dorazit ke svému objektu dříve než jsou tomu schopni bezpečnostní agentury. A za druhé i kdyby majitel dorazil na místo včas, nemá takové proškolení a znalosti jako tyto agentury, tudíž podstupuje velké riziko a většinou není schopen tuto situaci řešit jinak než přivoláním policie. Jakým způsobem zasahují proškolené hlídky bezpečnostních agentur si popíšeme v dalších kapitolách

7.1 Reakce na varovné signály

Základem pro vyslání varovného signálu je systém PZTS ve střeženém objektu. Ten vyšle zprávu o narušení na DPPC, dojde k vyhodnocení přijaté zprávy a zobrazení nutných údajů pro výjezd.

Po vyhodnocení údajů vyšle dispečer bez zbytečného odkladu výjezdové vozidlo k objektu, kde došlo k narušení. Je li však z vyhodnocených výsledků patrné, že se jedná o nestandardní situaci, vysílá vozidla dvě. Výjezd vozidel musí být pohotový a splňovat Normy zásahových časů.

7.2 Normy zásahových časů

Obecně lze říci, že zásahový čas je čas, který členové výjezdu poskytují pachateli a je na jejich schopnostech a odpovědnosti jaký čas splní.

Předpokládaný čas k zásahu je stanoven dle uzavřených smluv a je ovlivněn sjízdností vozovky a situací v dopravě. Člen zásahového týmu musí byt neustále připraven k případnému výjezdu, neboť čas který stráví čímkoliv jiným, než jízdou objektu, je čas, který se nedá dohonit. Po vyhlášení výjezdu je nutné reagovat rychle a nezdržovat se například obouváním a oblékáním.

Služba výjezdového týmu se dělí na:

- *Aktivní doba služby*: je doba, která se stanovena na rizikovější část dne a být v tuto dobu připraven k okamžitému výjezdu
- *Pasivní doba služby*: je doba, kdy si každý musí stanovit svůj čas přípravy bot a oblečení tak, aby se během výjezdu nezdržoval.

7.2.1 Předpoklady krátkého zásahového času

- rychlost vyhodnocení přenesené poplachové zprávy dispečerem
- rychlost předání zprávy zásahové skupině, kterou dispečer pověřil
- rychlost pochopení přijaté zprávy pracovníkem výjezdu
- rychlost přípravy, oblečení, opuštění zázemí a nastartování vozidla
- rychlost orientace člena výjezdu o poloze objektu a výběr rychlé trasy
- rychlost na trase k objektu
- dostatek informací o objektu a znalost objektu pro zákrok na narušeném místě
- případná rychlost vyhodnocení rizik všemi složkami a přivolaní další pomoci

7.2.2 Norma ČSN EN 50134-7 Pokyny pro aplikace přivolání pomoci

Tato technická specifikace obsahuje doporučení poskytovatelům služeb (a jejich subdodavatelům) pro efektivní a účinnou řídicí politiku a postupy při instalaci, zkoušení,

obsluze a údržbě systémů přivolání pomoci včetně technického vybavení a organizování pomoci. [15]

Norem týkajících se DPPC A PZTS je mnoho, ale všechny spějí k minimální době přenosu poplachových zpráv. Reakční doba pomoci musí být minimální.

7.2.2.1 Norma ČSN EN 50518-2

Tato evropská norma se vztahuje na veškerá dohledová a poplachová přijímací centra, která monitorují a/nebo přijímají a/nebo zpracovávají signály, které vyžadují okamžitou reakci. Dále zahrnuje funkční kritéria a ověřování výkonnosti.[16]

7.3 Znalost střeženého objektu

Pro kvalitní a účinný zásah je povinností každého dispečera, pracovníka výjezdu, či člena oddílu ostrahy znát objekt, který je předmětem ostrahy a především informace o něm. Těmi jsou:

- adresa střeženého objektu
- umístění objektu v místě adresy a jeho rozsah
- přístupové a únikové cesty, vstupy, okna, rozložení místností, klíče.
- příjezdové trasy a orientace v mapě města
- popis rizik (zda má majitel psa, nepřehledné terény)

Dále je kladen důraz na znalost přesného místa narušení v objektu. Nutno je místo prověřit tak, aby případný pachatel nemohl uniknout. Pokud se v narušeném objektu nacházejí schody, výtah, dvůr nebo zahrada je zásah složitější.

7.4 Jízda na místo činu

Příjezd k objektu musí být rychlý a nenápadný. Vyslané vozidlo jede v posledních metrech bez majáků a sirén, aby nedošlo k upozornění pachatele na blížící se hlídku.

Je nutno vždy posoudit i prostředí před objektem a v jeho blízkosti. Pachatel se může zdržovat i ve vozidle před objektem nebo pachatelů může být více. Zvýšená pozornost

musí být věnována vozidlům, která stojí v okolí. Dispečerovi by měla být hlášena veškerá SPZ vozidel, která by mohla být podezřelá.

Během výjezdu na varovný signál využívají vozidla DPPC výstražné majáky oranžového světla. Tyto světla ovšem neznamenají, že se může vozidlo řídit zvláštními předpisy a porušovat zákony silničního provozu. V praxi se stává, že některé agentury nedbají předpisům, ignorují světelné signalizace, dopravní značení a rychlost jízdy a po eventuálním řešení dopravního přestupků se odkazují na to, že jednali v krajní nouzi a reagovali na varovný signál. Ve chvíli, kdy vozidlo jelo na místo poplachu, řidič přeci neví, zda se jedná či nejedná o krajní nouzi. Mohlo jít o planý poplach, vyvolaný poškozením některého z hlásičů PZTS a tudíž je jeho konání neoprávněné. V praxi se tato problematika neustále řeší a bylo by zapotřebí uvádět veškeré zákony, výjimky a případy, kdy se co smí či nesmí. Podstatné je vědět, že vozidla s oranžovými majáky nemají stejné pravomoce jako modré majáky Policie ČR.

Obr. 18. Zásahové vozidlo společnosti MAFAS [40]

8 POSTUP ZÁSAHU

O provedení zásahu rozhoduje výjezdová služba dle směrnic, zákonů, proškolení a poučení. Veškeré děje a skutečnosti na místě činu konzultuje s dispečerem, ovšem odpovědnost za své činy nese každý pracovník sám za sebe. Pracovník ostrahy a výjezdové služby se řídí vždy směrnicemi a poučením, které vlastnoručně podepsal a je si tedy vědom veškerých rizik, které podstupuje.

Pokud majitel střeženého objektu pozměnil organizační věci a předal tyto informace bezpečnostní agentuře, musí tato agentura ihned pozměnit směrnice a informovat bezpečnostní pracovníky. Pokud takto neučiní a pracovník ostrahy bude jednat dle neaktuálních směrnic, nese odpovědnost za škody agentura, nikoliv pracovník.

8.1 Obecné postupy

Prvotní postup můžeme rozdělit do tři kroků:

1. **Zjištění** závažnosti stavu v objektu - je to nejrizikovější část zásahu, neboť se nezná skutečný důvod poplachu. Nutné je reagovat tiše, nevystavovat se zbytečnému riziku, nevstupovat do neověřeného prostoru, hlídat únikové cesty, očekávat možný útok ozbrojeného pachatele a o všem informovat dispečera.

2. **Vyhodnocení** zjištěné situace a rozhodnutí o dalším postupu. Snažit se zajistit dostatek času pro případný příjezd pomoci.

3. **Provedení** zákroku vyžaduje odhadnout pachatele a možná rizika. V žádném případě jednotlivý člen týmu nebere situaci osobně, ale profesionálně. K dispozici má ochranné pomůcky a důvěru ve výcvik. Svým chováním nesmí dovést situaci k tomu, aby došlo ke zbytečnému zranění nebo usmrcení třetí osoby.

8.1.1 Dva možné postupy

Po příjezdu na místo poplachu je primární zajištění perimetru objektu (dveře okna, únikové cesty, balkóny, ploty) a poté postupovat jednou ze dvou možností:

1. Řešit situaci samostatně.
2. Hlídat perimetr objektu a vyčkat na příjezd policie.

8.1.1.1 DPPC řeší situaci samo

Pokud chce hlídka zasáhnout sama, vyzve pachatele k tomu, aby opustil objekt. Pokud takto neučiní vyzve hlídka pachatele podruhé s tím, že pokud neopustí soukromý objekt, budou moci použít služební zbraně nebo na něj bude poslán služební pes. Služební zbraň hlídka může použít v případě nutné obrany či krajní nouze, ovšem v rámci psychologického nátlaku je oznámení o použití střelné zbraně velice efektivní.

Většinu zásahů se snaží DPPC řešit sama a policii zapojují pouze v případech, kdy se jedná o ohrožení života, nebo pokud je zásah v místech veřejně přístupném (herny, hospody), kde jsou hrozby větší, jelikož zde mohou být i nevinné osoby.

Do objektu vstupuje zásahová hlídka pomocí klíčů. V případě narušení objektu, narušeným vstupem. V místě narušení je nutno nejprve prověřit, je-li pachatel stále v objektu. Nachází-li se v objektu výtah, je nutno jej zajistit. Výtah postačí zavolat. Zásahový tým by měl postupovat vždy po schodech, neboť výtah je pastí nebo únikovou cestou.

Pokud dojde k narušení objektu je nutné zajistit úniky a přivolat posilu. V případě tísňového volaní jsou vyslány na místo vždy dvě hlídky. Zasahují dle situace a maximální opatrností. Nutno předvídat přepadení ozbrojeného pachatele. Pří potvrzení této skutečnosti volá dispečer Policii ČR.

V případě, že zásahová hlídka nezadrží pachatele, kontaktuje majitele a policii. Místo narušení musí být hlídkou zajištěno do doby, než nedorazí na místo policie. V opačném případě by mohlo dojít k poškození případných stop a důkazů.

8.1.1.2 Součinnost s policií

Policie je na místo činu volána, kdy je zjevné, že se jedná o trestnou činnost nebo je nutné předat zadrženou osobu. Do příjezdu policie se snaží hlídka udržet pachatele, aby neunikl,

zajištěním únikových cest a perimetru objektu. Mnoho bezpečnostních agentur řeší situaci vždy přivoláním policie, přitom náplní jejich práce je zadržet pachatele při páchání trestné činnosti a následně využít policii k předání zadržené osoby. Role policie by měla být založena na:

1. Přebrání si zadrženého pachatele
2. Ztotožní zadržené osoby (na základě dokladu o totožnosti či otisků prstů)
3. Řízení o trestné činnosti

Prokázání a usvědčení o konání trestné činnosti je pro hlídku, která zadržela osobu, velice důležitá. Zbavují se tím veškerých obvinění za neoprávněné zadržení osoby dle § 76.

V praxi nastávají situace, kdy jsou na místo činu volány buď státní Policie České republiky nebo městská policie. Rozdíly mezi nimi si vysvětlíme v následující kapitole.

8.1.1.3 Státní Policie ČR a městská policie

Obecným rozdílem mezi těmito dvěma složkami spočívá v tom, že Policie ČR se snaží bojovat s kriminalitou zatímco městská a obecní policie se snaží zaměřovat na pořádkovou činnost a věci spojené s přestupky, poskytují tím státní policii možnost koncentrovat své síly na boj s kriminalitou. Obecní policie má samozřejmě více pravomocí, které jsou uváděny v zákoně č. 553/1991 Sb., o obecní policii, ovšem nás zajímá rozdíl mezi nimi, spojeným ve spoluprací s DPPC.

Existují případy, kdy hlídka vyjíždí na tísňový poplach do střežených provozoven, kde se může jednat nejen o trestný čin, ale i o přestupek. Proto příslušníci DPPC v lehkých případech, kdy se jedná zjevně pouze o přestupek, volají městskou policii, která pachateli ukládá pokutu v blokovém řízení. Pokud ovšem jde o trestnou činnost, tak se jednoznačně volá Policie ČR, jelikož městská policie má právo zadržet osobu páchající trestnou činnosti, stejně jako každý občan, ovšem musejí pachatele předat ze zákona Policii České republiky.

Žádná policie nemá právo ze zákona střežit a konat výjezdy na varovné signály u soukromých majetků. Policie je od toho, aby střežila státní, městský či obecní majetek. Ovšem v praktické životě se setkáváme s případy, kdy soukromé majetky politiků jsou chráněny státním sektorem. Takto by to mohlo být, pokud by politik žil ve státním bytě a

tudíž by stát střežil svůj majetek. Pokud ale politik žije v soukromém bytě či domě, tak proč by měl stát, tento dům chránit a posílat státní hlídky na varovné signály? Čím se liší politik, který po ukončení pracovní doby jde do svého soukromého bytu či domu, oproti běžnému občanovi, který taktéž vykonává pracovní činnost a po skončení pracovní doby jde spát do svého soukromého bydlení?

Vzhledem k rostoucí majetkové kriminalitě se každý občan začíná obávat o svůj majetek či zdraví a chce učinit jisté kroky k jejich zabezpečení. Dle svých občanských práv, konkrétně dle § 14 občanského zákoníku č. 89/2012 Sb., si může každý občan přiměřeným způsobem pomoci ke svému právu sám, je-li jeho právo ohroženo a je-li zřejmé, že by zásah veřejné moci přišel pozdě. [21] Proto vznikly bezpečnostní agentury, které chrání majetek a zdraví soukromých občanů. Integrace PZTS spojením s připojením na DPPC slouží jako prevence před nebezpečím. Pokud by občan spoléhal na veřejnou moc, tak by občan zjistil, že byl vykraden až tehdy, kdy je pachatel dávno pryč. Naproti tomu se může majitel a DPPC pomocí PZTS dozvědět o možném neoprávněném vniknutí do svého soukromého majetku a pokusit se chytit pachatele dříve, než uteče spolu s majitelovým majetkem. Níže můžeme vidět základní rozdělení policie.

8.1.1.3.1 *Státní Policie České republiky*

Policie České republiky je ozbrojený bezpečnostní sbor České republiky s celostátní působností a řídí se zákonem 273/2008 Sb., o Policii České republiky. Mezi nejhlavnější úkoly Policie ČR patří:

- Chrání bezpečnost osob a majetku
- Zajišťuje veřejný pořádek
- Odhaluje trestnou činnost, zjišťuje jejich pachatele a realizuje činnost k předcházení trestní činnosti

Úkolem státní policie dle zákona je zajišťovat veřejný pořádek, ovšem tyto přestupky se snaží řešit městská policie, aby se státní policie mohla soustředit na boj s kriminalitou.

8.1.1.3.2 *Městská policie*

Obecní Policie v České republice je orgánem obce, který zabezpečuje místní veřejný pořádek v rámci působnosti obce. Obecní policie se řídí zákonem č. 553/1991 Sb., o obecní

policii. V obci, která je městem se obecní policie nazývá městská policie. Mezi jejich nejhlavnější úkoly patří:

- Přispívat k ochraně a bezpečnosti osob a majetku
- Dohlížení na dodržování obecně závazných vyhlášek a nařízení obce.
- Podílení se na prevenci kriminality v obci.

Jsou zde i jiné úkoly, které plní, ale kdybychom měli jejich funkci shrnout, tak městská policie řeší problémy spojené s přestupky a veřejným pořádkem.

Dalo by se říci, že městský policajt a běžný občan se při páchání trestné činnosti řídí stejným paragrafem § 76 o zadržení osoby. Rozdílem je ovšem to, že městská policie dle § 12 zákona o obecní policii č. 553/1991 Sb., může požadovat po pachateli prokázání totožnosti, na což občan nemá žádné právo.

Tento paragraf odstavec 2. uvádí:

2) Strážník je oprávněn vyzvat osobu, aby prokázala svoji totožnost,

a) jde-li o osobu, vůči které provádí úkon k plnění úkolů obecní policie,

b) jde-li o osobu podezřelou ze spáchání trestného činu nebo přestupku či jiného správního deliktu, [22]

9 PŘÍKLADY ZÁSAHŮ

V této kapitole budou uvedeny příklady možných zásahů z běžného života. Jsou zde popsány postupy, taktiky a způsoby zásahu za účelem efektivního vyřešení rizikové situace.

9.1 Zásahy ve veřejně užívaných soukromých prostorách na základě tísňového volání

1. Po příjezdu na poplachové místo členové hlídky postupují dle obecných předpisů a směrnic pro tísňové volání

2. Hlídka po příjezdu a vniknutí do objektu musí zjistit příčinu tísňového volání. Je-li příčina patrná již po vstupu do objektu, reaguje na ni hlídka okamžitě bez dalšího zjišťování faktů za účelem zabránění vznikající hmotné škody, nebo újmy na zdraví. Po tomto prvotním zákroku následuje bližší obeznámení se situací vyslechnutím personálu a svědků, aby bylo možné posoudit, jde-li o trestný čin, přestupek či jiný prohřešek. První informaci hlídce předává zaměstnanec střeženého objektu a to nahlas, nebo má-li důvodnou obavu, že by jeho veřejné obvinění mělo pro něj rizikové následky, tak to hlídce prozradí potichu. Je povinností obsluhy věci sdělovat pravdivě, neboť hlídka k tomu přizpůsobí důraznost a provedení dalšího zákroku. Obsluha je pak povinna vyšetřujícím orgánům potvrdit skutečnosti řečené hlídce.

3. Zjistí-li hlídka, že se jedná o výtržnictví a pachatel či pachatelé jsou agresivní, budou se nejprve snažit agresivitě zamezit použitím mírnějších prostředků, aby nedošlo k újmě na zdraví či dalším hmotným škodám. Když se vše uklidní, kontaktuje se majitel a ten vyjádří jasně požadavek, má-li být výtržník zadržen či pouze vyveden z objektu. Pokud si majitel přeje zadržení pachatele, je nutné podat přivolané Policii trestní oznámení. Při vyvádění je pachatel požádán slušným způsobem, aby opustil soukromý majetek, dle přání majitele. Dále hlídka sleduje reakci a pokud je napadena, použijí prostředky k nutné obraně.

Je-li povaha nutného zákroku natolik závažná, že by hlídka byla nucena použít ke zvládnutí situace nejtvrdších prostředků (střelné zbraně, nože), přivolá Policii a zamezuje pouze odchodu výtržníků do příjezdu policie. Případ přivolání policie může nastat například i při početné přesile výtržníků k členům hlídky, pokud by nešlo o situaci nutné obrany a krajní nouze.

4. Jedná-li se o ozbrojené přepadení a je zjištěná nezvratná skutečnost, reaguje hlídka okamžitě. Nejprve kontaktuje dispečera a uvědomí ho situaci a dispečer ihned volá Policii ČR. Do příjezdu policie je snahou hlídky přesvědčit pachatele, aby od činu upustil, nebo aby nedošlo v prvé řadě ke zranění či zabití osob na místě činu i za cenu, že by nedošlo k zabránění vzniku hmotné škody. Pokud je nějaká možnost pachatele odzbrojit, jedná hlídka dle svého výcviku, tak aby při zásahu nedošlo k újmě na zdraví osob, nacházející se poblíž pachatele a poté čeká na policii, které pachatele předá. Ve chvíli odzbrojení jde o nutnou obranu, kde hrozí útok a tudíž je hlídka oprávněná použít veškeré přiměřené obranné způsoby, aby tomuto útoku zabránila.

Pokud dojde ke zranění některých z osob, musí někdo z hlídky poskytnout první pomoc a zároveň přivolat pomoc odbornou, nebo nejde-li jinak, odvézt postiženého sama, umožňuje-li to stav nemocného. Při poskytování první pomoci jedním z pracovníků hlídky, se nesmí opomíjet na možnost zranění dalších osob. Zbytek pracovníků hlídky postupují í nadále tak, aby odvrátili dalších zranění. Hlídka je povinna poskytnout první pomoc i zadržené osobě nebo osobě vyvedené, kde bylo nutno užít prostředků k vykonání zásahu a došlo při ní ke zranění pachatele. Musí tomu ovšem vyžadovat povaha zranění.

Je- li zjištěn v objektu požár, pak hlídka dle závažnosti přivolá odbornou pomoc a zatím se snaží zamezit dostupnými prostředky šíření ohně. Jsou-li přístupné elektrické rozvaděče a plynové uzávěry, musí je hlídka uzavřít a vypnout.

5. Dojde-li k zneužití hlídky nepravými informacemi, nese za tuto skutečnost odpovědnost objednavatel. Za provedení samotného zákroku nese odpovědnost hlídka.

6. Po příjezdu policie a zadržení pachatelů se celá akce zapisuje s příslušníky orgánu, hlídka a svědci podávají výpovědi, hlídka sepíše hlášení o zásahu a předá majiteli objektu a majiteli DPPC.

9.2 Zásahy na signál poplachu a sabotáže

1. Hlídka po příjezdu k objektu zjišťuje příčinu vyhlášení poplachu, současně dbá na možné únikové cesty, aby případný pachatel nemohl včas uniknout.

2. Hlídka kontroluje celý objekt, to znamená všechny přístupy, všechny prosklené plochy a dveře. Kontroluje jejich neporušenost a uzamčení. K přístupům využívá hlídka svěřené klíče k průchodu objektem. Dispečer sleduje, je-li v objektu signalizován další pohyb a

zjištěné údaje předává hlídce. Hlídka opouští objekt po 100% ujištění, že není narušen a že nedojde k promeškání trestného činu.

3. Hlídka může na místě zjistit, že objekt je zjevně neporušen, ovšem z jiných postřehů si není jistá. V takovém případě hlídka povolá majitele a provede kontrolu uvnitř objektu. Do příjezdu majitele vyčká alespoň jeden člen hlídky na místě.

4. Zjistí-li hlídka, že objekt je zjevně narušen a není zřejmé je-li pachatel uvnitř, vstupuje hlídka do objektu se snahou zadržet pachatele na místě. Je-li zřejmé, že pachatel uvnitř není, hlídka do objektu nevstupuje. Prověří všechny únikové cesty a úkryty v okolí narušeného objektu a povolá majitele a policii. Hlídka nevstupuje do objektu, aby nezničili důkazy. Do příjezdu majitele, nebo jím pověřeného zástupce setrvá hlídka u objektu. O celým výjezdu sepíše zprávu, která obsahuje čas poplachu, čas příjezdu na místo, jména členů hlídky, co bylo narušeno, popis narušení a znatelně odcizené předměty.

5.Pachatel je zadržován podle § 76 odst. 2, trestního řádu. Členové hlídky jsou oprávnění zadržet osoby přistižené při spáchání trestné činnosti ke zjištění totožnosti, zamezení útěku nebo k zajištění důkazů. Zadrženého ihned předá Policii. O zadržení je třeba sepsat zprávu.

6. Členové hlídky postupují při zákrocích, prohlídkách a jiném pohybu v narušeném objektu nebo jeho okolí tak, aby svojí přítomností nezničili důkazy vedoucí k objasňování trestného činu. Je-li v okolí pohyb cizích osob, zajišťují, aby tito lidé nevstupovali do objektu nebo jeho okolí, pokud by i tam hrozila újma důkazům o trestné činnosti.

7. Při sabotáži, nebo-li narušení systému poplachové zařízení, je úkolem hlídky informovat majitele, nebo pověřenou osobu a spolu s ní obejít celé poplachové zařízení, aby zjistili, zda není zjevně otevřena kterákoliv část zařízení (ústředna, čidlo), nebo není-li přestřižen kabel zařízení. Dále kontrolují přítomnost sirény. Je-li i bez zjevného zjištění porušení PZTS dále vysílán signál sabotáže, je nutné věc předat technikovi k ověření.

8. Při výpadku sítě, pokud nepřijde do dvou hodin obnova, věc nahlásíme majiteli a po dalších dvou hodinách je objekt zkontrolován.

9. Majitel má právo z důvodu osobního podezření požádat o zvýšenou kontrolu objektu. Pak je povinen udat množství těchto kontrol. Hlídka pak provede podrobnou kontrolu jako u objektu po poplachu.

10. Jsou případy, kdy se prověřuje zaměstnanec v objektu poplachu. Přijede-li hlídka do objektu po poplachu a nachází se tam osoba, která tvrdí, že je zaměstnancem, hlídka předá informace dispečerovi a ten kontaktuje majitele objektu. Na základě telefonického popisu majitele konáme obvyklé úkony k ověření totožnosti, zda se opravdu jedná o zaměstnance či ne. Také lze dotyčnou osobu ověřit porovnáním se seznamem zaměstnanců daného objektu. Ovšem k tomuto porovnání je třeba předložení dokladu totožnosti, což má právo požadovat po občanovi pouze policie. Tím, že osoba svobodně předloží doklad o totožnosti k porovnání, ještě nemusí znamenat, že není doklad falešný, proto způsob popisu osoby je z právního hlediska nenapadnutelný a kolikrát může být i přesnější. Nejlepší možností je, když se majitel může dostavit na místo v co nejkratší době a osobu rozpoznat.

V praxi může nastat situace, kdy dotyčná osoba chce odejít z místa činu a tudíž musí být zadržena. Podle popisu majitele se zjistí, že se jedná o neoprávněný vniknutí do soukromého majetku, ale majitel si bude přát, aby byla dotyčná osoba propuštěna bez dalšího řešení s Policií. V takovém případě nese osoba, jenž zadržela pachatele velké riziko, jelikož pachatel může podat žalobu na omezování osobní svobody dle trestního zákoníku č. 40/2009 sb. paragrafu §171 o omezování osobní svobody. Jedná se o to, že člen hlídky zadržel osobu dle §76, ovšem nepředal zadrženou osobu Policii a hlavně na osobu nebylo podáno trestné oznámení. Tudíž v tomto případě člen hlídky, pokud nechce riskovat podání žaloby na svojí osobu, musí předat dotyčného pachatel Policii ČR.

11. Další možností je hlášení o připravovaném poplachu. Toto hlášení je oprávněn podat pouze majitel objektu, nebo jím stanovený zástupce. Při tomto hlášení se uvádí datum, čas, své jméno, jméno objektu a důvod poplachu. Dispečer to zaeviduje a DPPC je obeznámena o budoucím poplachu v konkrétním čase a místě.

9.3 Planý poplach

1. Vozidla co nejrychleji dorazí k objektu a řeší situaci. O všech skutečnostech informují neprodleně dispečera, který je povinen vše řádně evidovat a operativně řeší nutné kroky. Dispečer je povinen informovat majitele objektu a Policii ČR. Pokud vyslané vozidlo nezjistí narušení objektu, zdržuje se skrytě v bezprostřední blízkosti objektu a objekt je zpravidla 30 minut sledován. Jediný možný důvod, kdy je sledovaný objekt opuštěn dříve než po uplynutí stanoveného času je jiná poplachová událost.

2. Příčiny planých poplachů jsou uvedeny v následující kapitole.

10 VAROVNÉ SIGNÁLY

Tato kapitola rozděluje varovné signály, uvádí příčiny vzniků a možnosti jejich řešení.

10.1 Rozdělení varovných signálů

10.1.1 Poplach

Zpráva o narušení pláště objektu (okna, dveře) nebo vnitřních prostor (sklad, místnost). Pomocí zabudovaných čidel je vyhodnocen druh poplachu.

10.1.2 Sabotáž

Ochrana vedení a instalovaných prvků v PZTS objektu. Jsou jimi kabely, čidla, sirény a ústředny PZTS. Ochrana je aktivní 24 hodin denně i pří vypnutém systému. Ve většině případů se jedná o pachatele, který odstraňuje prvky PZTS, cloní čidla, nebo poškodí sirénu. Vyslaná hlídka je povinná zkontrolovat kompletnost čidel a sirén. V případě neznalosti se spojí s technikem, kterému je předán sabotážní poplach k řešení.

10.1.3 Tísňové volání

Nejzávažnější typ poplachové zprávy. Jedná se o použití mechanických, nebo radiových tlačítek obsluhou v tísni. Dojde li k takové poplachové situaci, vyšle dispečer dvě zásahová vozidla. Ve většině případů se jedná o loupežné přepadení nebo ozbrojené pachatele.

10.1.4 Zapnutí, vypnutí

Zpráva o zapnutí, nebo vypnutí PZTS v objektu. Majitel objektu musí aktivovat příchod zpráv o zapnutí a vypnutí ve smyslu hlídání. Dispečer kontroluje zda-li večer došlo k zapnutí objektu. Pokud k zapnutí nedojde, ověří zda-li v objektu ještě někdo nezůstal. V případě nezjištění osoby v objektu volá dle pořadí na kontakty a oznamuje, že nedošlo k zapnutí. Buď majitel zapomene, nebo se zpráva na DPPC nedoručila z důvodu výpadku telefonu nebo přetížeností linek v určitém čase.

10.1.5 Podpětí baterie

Každý PZTS má svůj záložní akumulátor. Při výpadku proudu akumulátor napájí alarm. Tento typ zprávy informuje o tom, že záložní zdroj má závadu a je nutno tuto zprávu předat technikovi. V objektu hrozí, že dojde k celkové nefunkčnosti PZTS. Objekt je nutné zkontrolovat během noci.

10.1.6 Vypnutí pod nátlakem

Forma tísňového volání. Obsluha je donucena pachatelem vypnout PZTS. Zásahový tým kontroluje objekt nebo stav obsluhy. V případě zjištění podezřelé osoby volá zásahový tým Policii ČR, předstírá odjezd a skrytě sleduje objekt do příjezdu policie.

10.1.7 Požární poplach

Hlášení požárních detektorů o vzniklém kouři.

10.1.8 Stisknutí klávesy A první pomoc

Tísňové volání ze zdravotních důvodů.

10.1.9 Stisknutí klávesy F hoří

Požární tíseň vyhlášena obsluhou v objektu.

10.1.10Výpadek elektrické sítě

Zpráva, která dorazí po 30 minutách od výpadku. Dispečer sleduje výpadek zpravidla 3 hodiny. Nedojde li k obnově, kontaktuje dispečer objekt a jeho majitele. Důvodem potíží může být vadná pojistka v PZTS. V takovém případě je závada předána technikovi.

10.1.11Ztráta komunikace

Neboli objekt nekomunikuje. Příčina ztráty komunikace může být úmyslné porušení vysílače nebo antény. Nejprve je nutné prověřit funkčnost těchto bodů přenosu. Výjezd zásahového vozidla musí být stejně rychlý jako při výjezdu k poplachu, neboť se může jednat narušení frekvence pachatelem. Všechny výpadky musí být nahlášeny technikovi.

10.1.12Rušení příjmu sběrné stanice

Vzniká vysokou úrovní rušení v éteru. Častou příčinou je úmysl pachatele narušit frekvenci. V takovém případě se prověří okolí sběrné stanice. Údaje o sběrné stanici včetně jeho umístění jsou přísně tajné.

10.1.13Ilegální vysílač

Zpráva po resetu vysílače, nebo po jeho novém napojení na DPPC. Toto zprávu je nutné prověřit výjezdem, neboť se může jednat o snahu pachatele imitovat vysílání vysílače. Nutná spolupráce s technikem.

10.1.14Neznámá zpráva

Jedná se o zprávu, která byla doručena ústřednou na DPPC. Nemá definici, tudíž se jedná o zprávu neznámou. V takovém případě je objektu vyslaná hlídka, která prověří danou zprávu. Poté vše nahlásí technikovi.

11 LEGISLATIVA

Tato závěrečná kapitola diplomové práce shrnuje právní znalosti, které by měl každý pracovník DPPC znát, chápat a umět využít v praxi.

§ 29 nutná obrana

(1) Čin jinak trestný, kterým někdo odvrací přímo hrozící nebo trvající útok na zájem chráněný trestním zákonem, není trestným činem.

(2) Nejde o nutnou obranu, byla-li obrana zcela zjevně nepřiměřená způsobu útoku.[18]

§ 28 krajní nouze

(1) Čin jinak trestný, kterým někdo odvrací nebezpečí přímo hrozící zájmu chráněnému trestním zákonem, není trestným činem.

(2) Nejde o krajní nouzi, jestliže bylo možno toto nebezpečí za daných okolností odvrátit jinak anebo způsobený následek je zřejmě stejně závažný nebo ještě závažnější než ten, který hrozil, anebo byl ten, komu nebezpečí hrozilo, povinen je snášet. [19]

§ 76 Zadržení osoby podezřelé

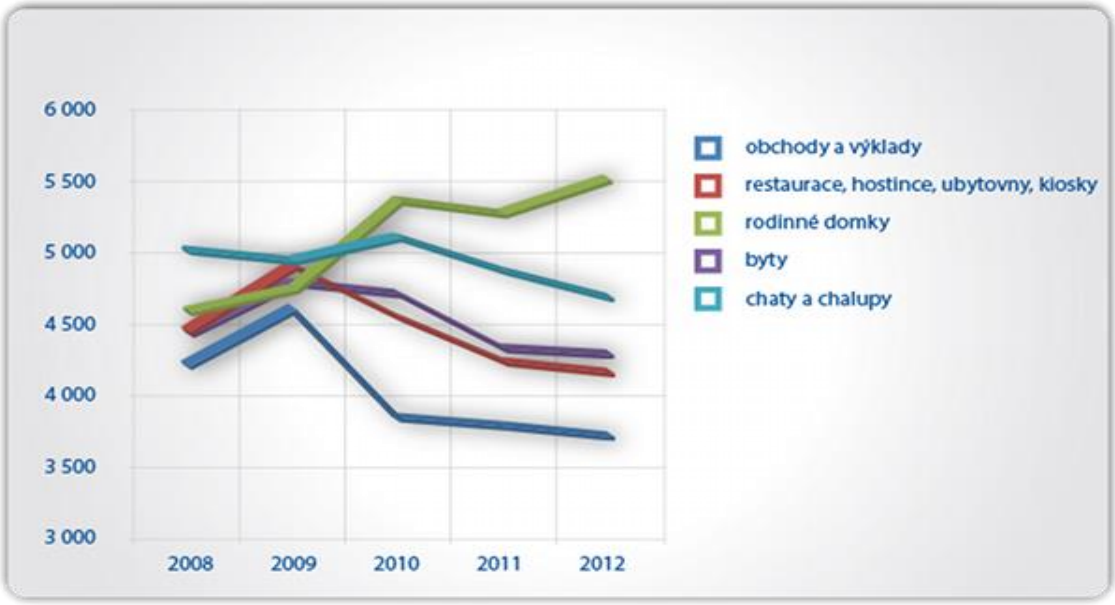
(2) Osobní svobodu osoby, která byla přistižena při trestném činu nebo bezprostředně poté, smí omezit kdokoli, pokud je to nutné ke zjištění její totožnosti, k zamezení útěku nebo k zajištění důkazů. Je však povinen tuto osobu předat ihned policejnímu orgánu; příslušníka ozbrojených sil může též předat nejbližšímu útvaru ozbrojených sil nebo správci posádky. Nelze-li takovou osobu ihned předat, je třeba některému z uvedených orgánů omezení osobní svobody bez odkladu oznámit.

(3) Policejní orgán, který provedl zadržení, zadrženou osobu vyslechne a o výslechu sepíše protokol, v němž označí místo, čas a bližší okolnosti zadržení a uvede osobní údaje zadržené osoby, jakož i podstatné důvody zadržení.

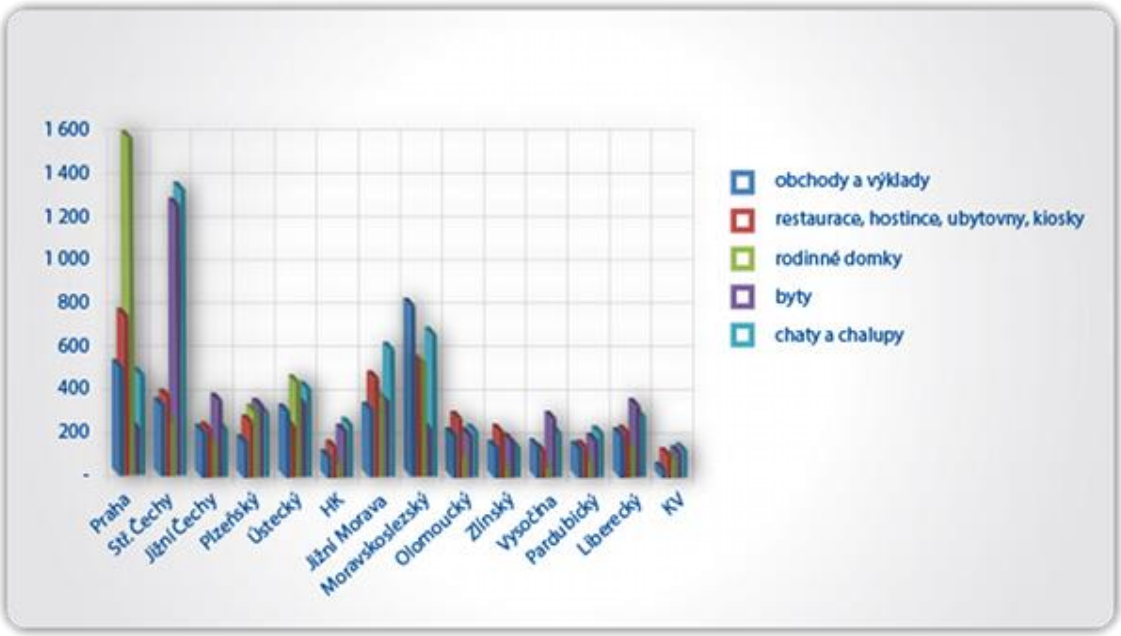
(4) Policejní orgán, který zadržení provedl nebo kterému byla podle odstavce 2 odevzdána osoba přistižená při trestném činu, ji propustí bezodkladně na svobodu v případě, že bude podezření rozptýleno nebo důvody zadržení z jiné příčiny odpadnou. Nepropustí-li zadrženou osobu na svobodu, předá státnímu zástupci protokol o jejím výslechu s vyhotovením usnesení o zahájení trestního stíhání a další důkazní materiál tak, aby státní zástupce popřípadě mohl podat návrh na vzetí do vazby. Návrh musí policejní orgán podat bez odkladu, aby osoba zadržená podle tohoto zákona mohla být odevzdána soudu nejpozději do 48 hodin od tohoto zadržení; jinak musí být propuštěna na svobodu. [20]

12 STATISTIKY

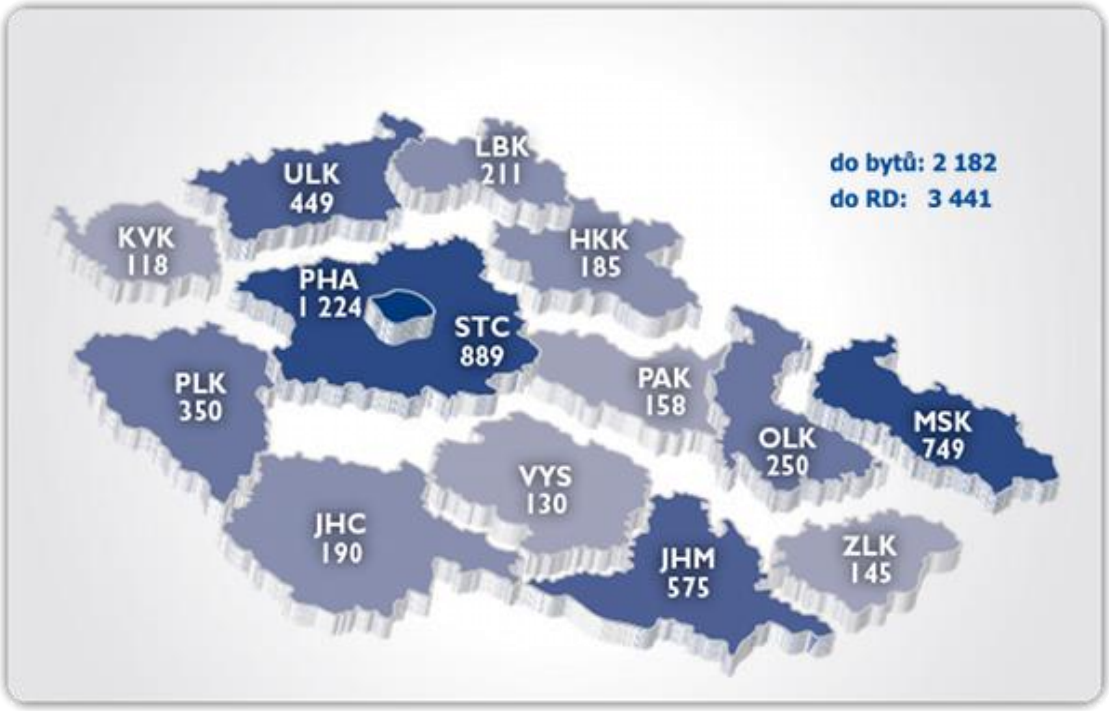
Níže na obrázcích je přehled statistik vykradených nemovitostí:



Obr. 19. Krádeže vloupáním v letech 2008 – 2012 [41]



Obr. 20. Krádeže vloupáním v roce 2012 dle krajů [41]



Obr. 21. Počet krádeží vloupáním do bytů a rod. Domků v 1. pololetí 2013 [41]

ZÁVĚR

Diplomová práce měla čtenáři popsat a rozebrat poplachové zabezpečovací a tísňové systémy, uvést jejich slabé a silné stránky a zejména uvést možnosti připojení systému na dohledová a poplachová přijímací centra. Aplikační podmínky a popis přenosových tras mělo všem čtenářům, kteří si plánují integrovat systém PZTS do svého majetku, přiblížit všechna technická kritéria k nejlepšímu možnému výběru připojení na DPPC.

Podstatnou částí diplomové práce bylo poukázat na náročnost práce pracovníků DPPC. Jakým způsobem a jaké taktiky během zásahů pracovníci DPPC využívají, jaká nesou rizika, jakými zákony se řídí a co vše musejí podstupovat během výkonu své práce, pojednává celá praktická část této práce. Jsou zde rozebrány krok po kroku příklady zásahů z praxe s ohledem na směrnice bezpečnostních agentur a zákonů České republiky.

Majetková kriminalita neustále roste a hodně lidí žijí v domnění, že jejich majetek je chráněn a že jim nic nehrozí. O zabezpečení svého majetku se začínají starat až poté, co byli nějakým způsobem poškozeni, což už bývá většinou pozdě. Vzhledem k tomu, že sám majitel střeženého objektu nebude nikdy schopen efektivně reagovat na varovné signály PZTS a policie nemá ze zákona právo střežit soukromý majetek, zbývá jediné možné řešení a to využít paragrafu § 14 občanského zákoníku č. 89/2012 Sb., kdy má občan právo si přiměřeným způsobem k svému právu pomoci sám. Tuto pomoc mohou občanovi za úplatu poskytnout soukromé bezpečnostní agentury, které se na ochranu majetku a zdraví specializují a mají profesionálně vyškolené pracovníky.

Služba DPPC není v dnešní době finančně náročná a dokáže odvrátit jak finanční ztráty, tak i předejít možným psychickým následkům napadené osoby, proto všem doporučuji zvážit tuto službu k ochraně sebe, své rodiny a svého majetku.

ZÁVĚR V ANGLIČTINĚ

My diploma thesis was to describe and analyze alarm, security, and emergency systems, mentioning their pros and cons, and to highlight ways of connecting the systems with supervisory stations guarding the devices. Instalation requirements and the description of transferal alignment should aid people, integrating I&HAS into their own property, to maintain the best possible connection with the supervisory stations mentioned above. An essential part of the diploma thesis was referring to hard work of employees of the supervisory stations. It unveils the methods and strategies used during the tasks, what risks do the employees have to take, what laws do they abide, while working, and everything they cope with. Numerous examples of the interventions were described, step by step, according to standards of security agencies and the laws of the Czech Republic. Property crime rate steadily grows, though many people feel safe and consider their properties as kept secure. They seldom care about it, until after they get robbed, which tends to be too late. In light of the fact that the owner of the guarded property alone is never going to be sufficient to effectively react to the emergency signals of the I&HAS, and the police are not, by law, allowed to watch private properties, the only way to protect one's own property is to act on his or her own in terms of the section § 14 of Civil Code of the Czech Republic no. 89/2012 Sb. This may also be provided, in exchange for financial means, by specialized security agencies, whose intentions are to protect and prevent their clients from theft. Nowadays, services of the supervisory and guarding stations are not financially demanding. Not only can they avert material damage, but also turn away eventual psychological harm of the victim, hence I hereby recommend to consider using this service to keep yourself, your family, and property, safe.

SEZNAM POUŽITÉ LITERATURY

[1] ČSN EN 50131-1 ed. 2. Poplachové systémy - Poplachové zabezpečovací a tísňové systémy- Část 1 Systémové požadavky. Praha Český normalizační institut, 2007. 40 s.

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

[3] Přispěvatelé Wikipedie, Pult centralizované ochrany [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 5. 11. 2012, 09:59 UTC, [citováno 18.11. 2013]<http://cs.wikipedia.org/w/index.php?title=Pult_centralizovan%C3%A9_ochrany&oldid=9257265>

[4] Ústředny poplachového zabezpečovacího a tísňového systému [online]. [cit. 2014-05-25]. Dostupné z:http://www.idbjournal.sk/rubriky/prehladove-clanky/ustredny-poplachoveho-zabezpecovaciho-atisnoveho-systemu.html?page_id=14869

[5] ČSN EN 50131-1 (334590) Poplachové systémy - Elektrické zabezpečovací systémy - Část 1: Všeobecné požadavky [online]. [cit.2014-05-25]. Dostupné z: http://www.technicke-normy-csn.cz/334590-csn-en-50131-1_4_53574.html

[6] VALOUCH, Jan. Projektování bezpečnostních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. ISBN 978-80-7454-230-5.

[7] ČSN EN 50131-6 (334590) Poplachové systémy - Elektrické zabezpečovací systémy - Část 6: Napájecí zdroje[online]. [cit. 2014-05-25]. Dostupné z: http://www.technicke-normy-csn.cz/334590-csn-en-50131-6_4_55120.html

[8] Přednáška projektování poplachových systémů Ing. Jana Valoucha Ph.D. Ze dne 16.3.2012

[9] LUČAN, Jiří. Tvorba edukačního materiálu s prvky e-learningu systému PCO GLOBAL. Zlín, 2007. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně

[10] JANSEN, Horst a Heinrich RÖTTER. Informační a telekomunikační technika.

Vyd. 1. Praha: Europa-Sobotáles, 2004, 399 s. ISBN 80-867-0608-7.

[11] KŘEMÉNKOVÁ, Jana. Technické řešení dohledového a poplachového přijímacího centra. Zlín, 20013. Diplomová práce. Univerzita Tomáše Bati ve Zlíně

[12] Wikipedie: Otevřená encyklopedie: Virtuální privátní síť [online]. c2014 [citováno 16. 05. 2014]. Dostupný z WWW: <http://cs.wikipedia.org/w/index.php?title=Virtu%C3%A1ln%C3%AD_priv%C3%A1tn%C3%AD_s%C3%AD%C5%A5&oldid=11342959>

[13] Wikipedie: Otevřená encyklopedie: IPsec [online]. c2013 [citováno 16. 05. 2014]. Dostupný z WWW: <http://cs.wikipedia.org/w/index.php?title=IPsec&oldid=9863983>

[14] Wikipedie: Otevřená encyklopedie: Pult centralizované ochrany [online]. c2014 [citováno 16. 05. 2014]. Dostupný z WWW: <http://cs.wikipedia.org/w/index.php?title=Pult_centralizovan%C3%A9_ochrany&oldid=9257265>

[15] ČSN CLC/TS 50134-7 (334594) Poplachové systémy - Systémy přivolání pomoci - Část 7: Pokyny pro aplikace[online]. [cit.2014-05-25]. Dostupné z: http://shop.normy.biz/detail/74853#nahled

[16] ČSN EN 50518-2 (334599) Dohledová a poplachová přijímací centra - Část 2: Technické požadavky [online]. [cit.2014-05-25]. Dostupné z: http://shop.normy.biz/detail/88622

[17] KAMENÍK, Jiří a František BRABEC. Komerční bezpečnost: soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. Vyd. 1. Praha: ASPI, 2007, 338 s. ISBN 978-807-3573-096

[18] § 28 [online]. [cit. 2014-05-25]. Dostupné z: http://zakony.centrum.cz/trestni-zakonik/cast-1-hlava-3-paragraf-28

[19] § 29 [online]. [cit. 2014-05-25]. Dostupné z: http://zakony.centrum.cz/trestni-zakonik/cast-1-hlava-3-paragraf-29

[20] § 76 [online]. [cit. 2014-05-25]. Dostupné z: http://zakony.centrum.cz/trestni-rad/cast-1-hlava-4-paragraf-76

[21] § 14 [online]. [cit. 2014-05-25]. Dostupné z: http://zakony.centrum.cz/obcansky-zakonik-novy/cast-1-hlava-1-dil-3-paragraf-14

[22] Předpis č. 553/1991 Sb. Zákon České národní rady o obecní policii [online]. [cit. 2014-05-25]. Dostupné z:http://www.zakonyprolidi.cz/cs/1991-553

[23] Ukázka prvků PZS: [online]. [cit. 2013-11-18]. Dostupné z: http://www.bsot.cz/index.php?what=15_25&lng=cz

[24] Jednoduché schéma zapojení PZS: [online]. [cit. 2013-11-18]. Dostupné z: http://www.elrev.cz/sluzby/bezpecnostni-systemy-ezs/

[25] https://dspace.k.utb.cz/bitstream/handle/10563/25276/k%C5%99em%C3%A9nkov%C3%A1_2013_dp.pdf?sequence=1

[26] Příklad přijímače IP [22] Paradox Security Systems. Paradox - Headquarters [online]. 2013 [cit.2013-05-13]. Dostupné z: http://www.paradox.com/Images/News/PressReleases/2008/PR_14/Paradox_IPR512.jpg

[27] Taktická vesta TYP - B [online]. [cit.2014-05-25]. Dostupné z: http://www.uniformycz.cz/index.php?show=prod&prod=228

[28] Speciální jednotky [online]. [cit.2014-05-25]. Dostupné z: http://specialnijednotky.blog.cz/

[29] Neprůstřelná vesta CS IIA/IIIA [online]. [cit.2014-05-25]. Dostupné z: http://www.banner-security.cz/cz/index.php?page=catalog&sort=collection§ion=6.&category=hlidaci-sluzby&product_id=270

[30] Tomfa [online]. [cit.2014-05-25]. Dostupné z: http://www.military-shop.cz/armyshop/product_info.php/products_id/1450

[31] Obranný slzný sprej [online]. [cit.2014-05-25]. Dostupné z: http://www.lucerny.cz/lucerny/eshop/39-1-ORIGINALNI-DARKY/0/5/187-OBRANNY-SLZNY-SPREJ

[32] Kapesní nůž [online]. [cit. 2014-05-25]. Dostupné z: http://firepoint.cz/kapesni-noze-c3/http-firepoint-cz-kapesni-noze-c3-kapesni-nuz-boker-i20-i20/

[33] Rvačka skončila třemi výstřely a rozsudkem [online]. [cit. 2014-05-25]. Dostupné z:http://ustecky.denik.cz/zlociny-a-soudy/20110627_ro_strileni.html

[34] Pouta se dvěma klíči chrom [online]. [cit. 2014-05-25]. Dostupné z: http://www.army-eshop.cz/store/goods-29303-51-pouta-se-dvema-klici-chrom.html

[35] Svítilna Mag-Lite Mini MagLite AA 3Wat LED černá [online]. [cit.2014-05-25]. Dostupné z:http://www.pazba.cz/zbozi/4178/Svitilna-Mag-Lite-Mini-MagLite-AA-3Wat-LED-cerna

[36] Obuv Security polobotka [online]. [cit.2014-05-25]. Dostupné z: http://www.uniformycz.cz/index.php?show=prod&prod=128

[37] Šroubovák mini - křížový [online]. [cit.2014-05-25]. Dostupné z: http://www.e-liquid.eu/product/nastroje/sroubovak-mini---krizovy/1828

[38] Hasící přístroje [online]. [cit.2014-05-25]. Dostupné z: http://www.certifikatprostrazne.cz/slovnicek-pojmu-a-pomucky

[39] Baseball pálka ALU 02 - hliníková [online]. [cit.2014-05-25]. Dostupné z:http://www.mirasport.sk/mirasport/eshop/2-1-SPORTOVE-POTREBY/116-2-BASEBALL/5/809-Baseball-palka-ALU-02-hlinikova

[40] Střežení objektů [online]. [cit.2014-05-25]. Dostupné z: http://www.mafascr.cz/sluzby/pult-centralizovane-ochrany/strezeni-objektu/

[41] STATISTIKA VYKRADENÝCH NEMOVITOSTÍ [online]. [cit.2014-05-25]. Dostupné z:http://www.sherlogmax.cz/cz/statistika-vykradenych-nemovitosti.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ATZ	Advanced Technology Zones
ATZ	Advanced Technology Zones
ČNB	Česká národní banka
DPPC	Dohledová a poplachová přijímací centra
EZS	Elektronické zabezpečovací systémy
GPRS	General Packet Radio Service
GSM	Global system for mobile
HAS	Hold-up system
I&HAS	Intruder and Hold-up system
IAS	Intruder system
IBS	Integrovaný bezpečnostní systém
IPsec	IP security
ISDN	Integraded Services Digital Network
JTS	Jednotná telefonní síť
NC	Normally closed
NO	Normally open
PIR	Pasivní infračervené senzory
PSTN	Public switched telephone network
PTS	Poplachový tísňový systém
PTS	Poplachový tísňový systém
PZS	Poplachový zabezpečovací systém
SMS	Short message service
VPN	Virtuální privátní síť

SEZNAM OBRÁZKŮ

OBR. 1. UKÁZKA PRVKŮ PZTS [23] 16
OBR. 2. JEDNODUCHÉ SCHÉMA ZAPOJENÍ PZS[24] 21
OBR. 3. BLOKOVÉ SCHÉMÁ RADIOVÉ SÍTĚ [25] 31
OBR. 4. PŘÍKLAD PŘJÍMAČE IP [26] 32
OBR. 5. UKÁZKA UNIFORMY [27] 45
OBR. 6. UKÁZKA PŘILBY[28] 45
OBR. 7. UKÁZKA NEPRŮSTŘELNÉ VESTY [29] 46
OBR. 8. UKÁZKA TOMFY [30] 46
OBR. 9. UKÁZKA SLZNÉHO PLYNU [31] 47
OBR. 10. UKÁZKA NOŽE [32] 47
OBR. 11. UKÁZKA STŘELNÉ ZBRANĚ [33] 48
OBR. 12. UKÁZKA POUT [34] 48
OBR. 13. UKÁZKA SVÍTILNY [35] 48
OBR. 14. UKÁZKA OBUVI ZÁSAHOVÉHO TÝMU [36] 49
OBR. 15. UKÁZKA ŠROUBOVÁČKU [37] 49
OBR. 16. UKÁZKA HASÍCÍHO PŘÍSTROJE [38] 50
OBR. 17. UKÁZKA BASEBALLOVÉ PÁLKY [39] 50
OBR. 18. ZÁSAHOVÉ VOZIDLO SPOLEČNOSTI MAFAS [40] 54
OBR. 19. KRÁDEŽE VLOUPÁNÍM V LETECH 2008 – 2012 [41] 69
OBR. 20. KRÁDEŽE VLOUPÁNÍM V ROCE 2012 DLE KRAJŮ [41] 69
OBR. 21. POČET KRÁDEŽÍ VLOUPÁNÍM DO BYTŮ A ROD. DOMKŮ V 1. POLOLETÍ 2013 [41] 70

SEZNAM TABULEK

TAB. 1. PŘEHLED ČSN V OBLASTI POPLACHOVÝCH ZABEZPEČOVACÍCH A TÍSŇOVÝCH SYSTÉMŮ [6] 22
TAB. 2. ROZDĚLENÍ TŘÍ PROSTŘEDÍ [8] 25
TAB. 3. MINIMÁLNÍ DOBA NAPÁJENÍ [8] 26
TAB. 4. POŽADOVANÁ DOBA NAPÁJENÍ [8] 26

SEZNAM PŘÍLOH

Příloha PI: Protokol o provedeném zásahu v narušeném objektu pod ostrahou DPPC

PŘÍLOHA P I: PROTOKOL O PROVEDENÉM ZÁSAHU V NARUŠENÉM OBJEKTU POD OSTRAHOU DPPC

Datum přijetí zprávy: Čas:

Číslo zprávy: Dojezdový čas:

Jméno vel. Výjezdu: RČ:

Jméno dispečera DPPC:

Objekt (Adresa):.....

Na místě zjištěno:

Postup reakce:

Kontaktování: Volána policie:

Čas :

Čas příjezdu kontaktní osoby: Čas dojezdu policie:

Jméno Kontaktní osoby:

Počasí:

Ostatní:

V Praze dne: ….....

podpis pracovníka